CommandCenter®
Secure Gateway

CC-SG

Handbuch für Administratoren

Version 3.1

CCA-0D-G

Januar 2007

255-80-5140-00

Diese Seite wurde absichtlich leer gelassen.

Urheberrechts- und Markenschutzinformationen

Einhaltung der FCC-Bestimmungen

In Tests wurde festgestellt, dass das Gerät die Grenzwerte für digitale Geräte der Klasse A gemäß Teil 15 der FCC-Bestimmungen einhält. Diese Grenzwerte sollen in kommerziell genutzten Umgebungen einen angemessenen Schutz vor Störungen bieten. Das in diesem Handbuch beschriebene Gerät erzeugt, verbraucht und gibt unter Umständen hochfrequente Strahlung ab und kann bei unsachgemäßer Installation und Verwendung zu Störungen des Rundfunk- und Fernsehempfangs führen. Der Betrieb dieses Geräts in Wohnumgebungen führt unter Umständen zu schädlichen Störungen.

Genehmigungen für Japan

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan ist nicht verantwortlich für Schäden an diesem Produkt, die durch einen Unfall, ein Missgeschick, durch Missbrauch, Fremdeingriffe am Produkt oder andere Ereignisse entstanden sind, die sich außerhalb der Kontrolle von Raritan befinden oder unter normalen Betriebsbedingungen nicht auftreten.

CE c UL us LISTED 1F61 I.T.E.

Unterstützung in Nord- oder Südamerika erhalten Sie vom technischen Kundendienst von Raritan unter der Telefonnummer +1-732-764-8886, der Faxnummer +1-732-764-8887 oder per E-Mail unter ***tech@raritan.com***

Der technische Kundendienst steht Ihnen von Montag bis Freitag zwischen 8.00 und 20.00 Uhr (US-Ostküstenzeit) zur Verfügung.

Außerhalb von Amerika erhalten Sie Unterstützung von den regionalen Raritan-Niederlassungen. Die entsprechenden Kontaktinformationen finden Sie auf der letzten Seite dieses Handbuchs.

Sicherheitsrichtlinien

So vermeiden Sie einen möglicherweise tödlichen Stromschlag und eventuelle Schäden an Raritan-Geräten:

- Verwenden Sie bei keiner Produktkonfiguration ein zweiadriges Stromkabel.
- Testen Sie die Netzsteckdosen an Computer und Monitor auf ordnungsgemäße Polung und Erdung.
- Verwenden Sie das Gerät nur mit geerdeten Ausgängen am Computer und Monitor. Trennen Sie Computer, Monitor und Appliance vom Netz, wenn Sie eine unterbrechungsfreie Stromversorgung verwenden.

Sicherheitsrichtlinien für die Gestellmontage

Bei Raritan-Produkten, die in ein Gestell eingebaut werden, sind folgende Vorsichtsmaßnahmen zu beachten:

- Die Betriebstemperatur in einer geschlossenen Gestellumgebung kann höher sein als die Raumtemperatur. Sorgen Sie dafür, dass die für die Appliances angegebene, maximale Umgebungstemperatur nicht überschritten wird (siehe Anhang A: Technische Daten).
- Sorgen Sie für eine ausreichende Luftzirkulation in der Gestellumgebung.
- Bauen Sie Geräte im Gestell sorgfältig ein, um eine ungleichmäßige mechanische Belastung zu vermeiden.
- Schließen Sie die Geräte mit Vorsicht an das Stromnetz an, um eine Überlastung der Stromkreise zu vermeiden.
- Erden Sie alle Geräte ordnungsgemäß, besonders die Anschlüsse an den Netzstromkreis (z. B. Mehrfachsteckdosen statt direkter Anschlüsse).

Inhalt

Abbildungen

Diese Seite wurde absichtlich leer gelassen.

Kapitel 1: Einleitung

Das CommandCenter Secure Gateway (CC-SG) ist eine bequeme und sichere Lösung von Raritan zur Verwaltung von UNIX-Servern, Firewalls, Routern, Load-Balancern, Geräten zur Stromzufuhrverwaltung und Windows-Servern.

CC-SG ermöglicht die zentrale Verwaltung mittels serieller Appliances und KVM-Appliances. CC-SG ist für den Betrieb in einer Vielzahl von Umgebungen konzipiert, von Rechenzentren mit hoher Dichte über Dienstanbieter-Umgebungen bis zu Unternehmensumgebungen, die über umfangreiche Remoteniederlassungen verfügen.

Bei Verwendung von CC-SG in Verbindung mit den Raritan Dominion- oder IP-Reach-Verwaltungsappliances auf Portebene optimiert und vereinfacht es die Administration der Zielgeräte (Knoten genannt) und Rechenzentrumsgeräte, indem es eine Verbindung mit dem IP-Netzwerk herstellt und die serielle Konsole und die KVM-Ports aller Knoten im verwalteten Netzwerk darstellt.

Vorbereitungen

Bevor Sie CC-SG nach den Anweisungen in diesem Dokument konfigurieren können, lesen Sie das Handbuch **Digitales Lösungskonzept von Raritan – Implementierungshandbuch**. Es enthält umfangreiche Anweisungen zur Implementierung von Raritan-Geräten, die von CC-SG verwaltet werden.

Zielgruppe

Dieses Dokument richtet sich an Administratoren, die über alle verfügbaren Berechtigungen verfügen. Weitere Informationen finden Sie in **Anhang C: Benutzergruppenberechtigungen**. Benutzer ohne Administratorstatus verfügen normalerweise über weniger Berechtigungen (beispielsweise nur die Knotenzugriffsberechtigungen). Diese Benutzer finden im **CommandCenter Secure Gateway-Benutzerhandbuch** weitere Informationen.

Terminologie/Abkürzungen

Im vorliegenden Handbuch werden folgende Begriffe und Abkürzungen verwendet:

- **Zugriffs-Client**: Ein auf HTML basierender Client zur Verwendung durch Benutzer mit normalen Zugriffsrechten, die auf einen von CC-SG verwalteten Knoten zugreifen müssen. Der Zugriffs-Client bietet keine Verwaltungsfunktionen.
- **Zuordnungen**: Beziehungen zwischen Kategorien und Kategorieelementen zu Ports und/oder Geräten. Wenn beispielsweise einem Gerät die Kategorie „Standort“ zugeordnet werden soll, sollten Sie zuerst die Zuordnungen erstellen, bevor Sie in CC-SG Geräte und Ports hinzufügen.
- **Kategorie**: Eine Variable, die bestimmte Werte oder Elemente enthält. „Standort“ ist beispielsweise eine Kategorie, die Elemente wie „New York City“, „Philadelphia“ oder „Data Center 1“ enthält. Wenn Sie in CC-SG Geräte und Ports hinzufügen, werden diese Informationen entsprechend zugeordnet. Es ist einfacher, zuerst die Zuordnungen richtig einzurichten und dann Geräte und Ports hinzuzufügen. Der Betriebssystemtyp ist eine weitere Kategorie, die Elemente wie „Windows®“, „Unix®“ oder „Linux®“ enthalten kann.
- **CIM** (Computer Interface Module): Die Hardware, die zur Verbindung eines Zielservers mit einem Raritan-Gerät verwendet wird. Für jedes Ziel ist ein CIM erforderlich. Eine Ausnahme bildet dabei das Dominion KX101-Gerät, das direkt mit einem Ziel verbunden wird und daher kein CIM erfordert. Vor dem Hinzufügen des Gerätes und der Konfigurationsports in CC-SG sollten die Zielserver eingeschaltet und mit den CIMs verbunden worden sein, die ihrerseits mit dem Raritan-Gerät verbunden sein sollten. Andernfalls wird der Portname in CC-SG durch den leeren CIM-Namen überschrieben. Nach der Verbindung mit einem CIM müssen die Server neu hochgefahren werden.
- **CommandCenter-NOC** (CC-NOC): Netzwerküberwachungsappliance zur Überwachung des Status von Servern, Geräten und Raritan-Geräten, die von CC-SG verwaltet werden.

- **Gerätegruppe**: Definierte Gruppe von Geräten, auf die ein Benutzer zugreifen kann. Gerätegruppen werden beim Erstellen von Richtlinien für die Zugriffssteuerung für Geräte in der Gruppe verwendet.
- **Geräte**: Raritan-Produkte, wie beispielsweise Dominion KX116, Dominion SX48, Dominion KSX440, IP-Reach, Paragon II Systemcontroller, Paragon II UMT832 mit USTIP usw., die von CC-SG verwaltet werden. Diese Geräte steuern die mit ihnen verbundenen Zielserver und -systeme.
- **Administrations-Client**: Ein auf Java basierender Client für CC-SG, der von Benutzern mit normalem Zugriff und Administratoren verwendet werden kann. Die Verwaltung ist nur mit diesem Client möglich.
- **Elemente**: Werte einer Kategorie. Das Element „New York City“ gehört beispielsweise zur Kategorie „Standort“ und das Element „Windows“ zur Kategorie „Betriebssystemtyp“.
- **Verwaiste Ports**: Ein verwaister Port kann bei der Verwaltung von Paragon-Geräten, bei Entfernung eines CIMs oder Zielservers aus dem System und bei der Abschaltung eines Zielservers (manuell oder unbeabsichtigt) entstehen. Weitere Informationen hierzu finden Sie im *Raritan-Benutzerhandbuch für Paragon II-Geräte*.
- **Hostname**: Ein Hostname kann verwendet werden, wenn die DNS-Serverunterstüztung aktiviert ist. Weitere Informationen finden Sie unter Netzwerkkonfiguration in **Kapitel 12: Erweiterte Administration**. Der Hostname und der vollständig qualifizierte Domänenname (Hostname + Suffix) dürfen nicht mehr als 257 Zeichen umfassen. Er kann aus einer beliebigen Anzahl von Komponenten bestehen, solange diese durch einen Punkt (.) voneinander getrennt sind. Die einzelnen Komponenten dürfen aus maximal 63 Zeichen bestehen, wobei das erste Zeichen ein Buchstabe sein muss. Die übrigen Zeichen können alphabetisch, numerisch oder Trenn- bzw. Minuszeichen („-“) sein. Trenn- bzw. Minuszeichen dürfen jedoch nicht an letzter Stelle einer Komponentenbezeichnung stehen. Obwohl das System bei der Eingabe der Zeichen die Groß-/Kleinschreibung beibehält, spielt die Groß-/Kleinschreibung bei der Verwendung des vollständig qualifizierten Domänennamens keine Rolle.
- **iLO/RILOE**: Integrated Lights Out/Remote Insight Lights Out Edition von Hewlett Packard für Server, die von CC-SG verwaltet werden können. Ziele eines iLO/RILOE-Geräts werden direkt ein- und ausgeschaltet bzw. aktiviert und deaktiviert. iLO/RILOE-Geräte werden nicht von CC-SG erkannt, sondern müssen manuell als Knoten hinzugefügt werden.
- **In-Band-Zugriff**: Korrekturen oder Problembehandlungen bei einem Ziel im Netzwerk erfolgen über das TCP/IP-Netzwerk. Über die folgenden In-Band-Anwendungen können Sie auf KVM- und serielle Geräte zugreifen: **RemoteDesktop Viewer**, **SSH Client**, **RSA Client**, **VNC Viewer**.
- **IPMI-Server** (Intelligent Platform Management Interface): Server, die von CC-SG gesteuert werden können. IPMI werden automatisch erkannt, können jedoch auch manuell hinzugefügt werden.
- **Out-of-Band-Zugriff**: Korrekturen oder Problembehebungen bei einem KVM- oder einem seriell verwalteten Knoten im Netzwerk erfolgen über Anwendungen wie Raritan Remote Console (RRC), RaritanConsole (RC) oder Multi-Platform Client (MPC).
- **Richtlinien**: Definieren Sie Berechtigungen, die Zugriffsart und auf welche Knoten und Geräte eine Benutzergruppe zugreifen darf. Richtlinien werden einer Benutzergruppe zugewiesen und enthalten verschiedene Parameter zur Festlegung der Steuerungsebene, wie beispielsweise Datum und Uhrzeit des Zugriffs.
- **Knoten**: Zielsysteme wie Server, Desktop PCs oder andere Netzwerkgeräte, auf die Benutzer von CC-SG zugreifen können.
- **Schnittstellen**: Schnittstellen bieten den Zugriff auf Knoten, entweder über eine Out-of-Band-Lösung wie eine Dominion KX101-Verbindung oder eine In-Band-Lösung wie einen VNC-Server.

- **Knotengruppe**: Definierte Gruppe von Knoten, auf die ein Benutzer zugreifen kann. Knotengruppen werden beim Erstellen von Richtlinien für die Zugriffssteuerung für Knoten in der Gruppe verwendet.
- **Ports**: Verbindungspunkte zwischen einem Raritan-Gerät und einem Knoten. Ports bestehen nur für Raritan-Geräte und kennzeichnen einen Pfad von dem Gerät zu einem Knoten.
- **SASL** (Simple Authentication and Security Layer): Eine Methode zum Hinzufügen von Authentifizierungsunterstützung für verbindungsgestützte Protokolle.
- **SSH**: Clients, wie beispielsweise Putty oder OpenSSH, stellen CC-SG eine Befehlszeilenschnittstelle zur Verfügung. Nur ein Teil der CC-SG-Befehle zur Verwaltung von Geräten und CC-SG wird über SSH ausgegeben. Weitere Informationen finden Sie in **Kapitel 12: Erweiterte Administration**.
- **Benutzergruppe**: Mehrere Benutzer mit der gleichen Zugriffsebene und den gleichen Berechtigungen. Die Standardbenutzergruppe **System Administrators** hat beispielsweise vollen Zugriff auf alle Konfigurationsaufgaben sowie Zielknoten.

Diese Seite wurde absichtlich leer gelassen.

Kapitel 2: Zugreifen auf CC-SG

Nachdem Sie CC-SG mit einer IP-Adresse konfiguriert haben, kann die CC-SG-Einheit am beabsichtigten Standort aufgestellt werden. Stellen Sie alle für den Betrieb der Einheit notwendigen Hardwareverbindungen her.
Wie Sie auf unterschiedliche Art und Weise auf CC-SG zugreifen können, ist in diesem Kapitel aufgeführt:

- **Browser**: CC-SG unterstützt verschiedene Webbrowser. (Eine vollständige Liste der unterstützten Browser und Plattformen finden Sie in der **Compatibility Matrix** (Kompatibilitätsmatrix) unter **http://www.raritan.com/support**. Klicken Sie auf der Seite **Support** auf **Firmwareaktualisierungen** und dann auf **CommandCenter Secure Gateway**.)
- **Thick-Client**: Sie können einen Java Web Start Thick-Client auf Ihrem Client-Computer installieren. Der Thick-Client funktioniert wie ein browserbasierter Client.
- **SSH**: Sie können auf Remotegeräte, die über den seriellen Port angeschlossen sind, über SSH zugreifen. Weitere Informationen finden Sie in **Kapitel 12: Erweiterte Administration**.
- **Diagnosekonsole**: Diese Konsole wird nur bei Problembehandlungen und für die Diagnose in Notfällen verwendet und stellt keinen Ersatz für die browserbasierte Benutzeroberfläche zum Konfigurieren und Betreiben der CC-SG-Einheit dar. Weitere Informationen finden Sie in **Kapitel 12: Erweiterte Administration**.

***Hinweis**: Die Benutzer können während des Zugriffs auf CC-SG mit dem Browser, Standalone-Client und SSH gleichzeitig verbunden sein.*

Browserbasierter Zugriff

1. Verwenden Sie einen unterstützten Internetbrowser, und folgenden URL eingeben: **http://<IP-Adresse>/admin** wobei <IP-Adresse> für die IP-Adresse von CC-SG steht. Beispiel: **https://10.20.3.30/admin**.
2. Wenn Sie eine nicht unterstützte Version der Java Runtime Environment auf Ihrem Computer verwenden, werden Sie durch eine Warnung darauf hingewiesen. Im angezeigten Fenster haben Sie die Möglichkeit, die korrekte JRE-Version vom CC-SG-Server (sofern verfügbar) oder von der Sun Microsystems-Website herunterzuladen. Sie können den Vorgang auch mit der falschen Version fortsetzen und auf **OK** klicken. Das Fenster **Anmeldung** wird geöffnet.

Abbildung 1 Fenster Anmeldung

3. Sind die vertraglichen Einschränkungen der Serviceleistungen aktiviert, lesen Sie den Text und markieren Sie das Kontrollkästchen **Ich stimme den Vertragsbedingungen zu**.
4. Geben Sie Ihren **Benutzernamen** und Ihr **Kennwort** ein, und klicken Sie auf **Anmelden**.

Thick-Client-Zugriff

Anstatt ein Applet über einen Webbrowser auszuführen, startet der CC-SG-Thick-Client eine Java Web Start-Anwendung, um eine Verbindung mit CC-SG herzustellen. Der Vorteil bei der Verwendung eines Thick-Clients anstelle eines Browsers liegt darin, dass der Client in Bezug auf Geschwindigkeit und Effizienz mehr Leistung als der Browser aufweist.

Thick-Client installieren

1. Laden Sie den Thick-Client von CC-SG herunter, indem Sie einen Webbrowser starten und folgenden URL eingeben: **http(s)://<IP-Adresse>/install** wobei <IP-Adresse> für die IP-Adresse von CC-SG steht.
2. Wenn eine Sicherheitswarnung angezeigt wird, klicken Sie auf **Start**, um das Herunterladen fortzusetzen.
3. Wird auf Ihrem Client-Computer Java Version 1.4 ausgeführt, wird ein Fenster **Desktop Integration (Desktop-Integration)** angezeigt. Wenn Java ein Desktop-Symbol für den Thick-Client anlegen soll, klicken Sie auf **Yes (Ja)**.
4. Nach dem Herunterladen wird ein neues Fenster angezeigt, in dem Sie die IP-Adresse von CC-SG angeben können.

Abbildung 2 Thick-Client IP-Eingabefenster

5. Geben Sie im Feld **Zu verbindende IP-Adresse** die IP-Adresse der CC-SG-Einheit ein, auf die Sie zugreifen möchten. Nachdem eine Verbindung aufgebaut wurde, steht diese Adresse in der Dropdown-Liste **Zu verbindende IP-Adresse** zur Verfügung. Die IP-Adressen werden in einer Eigenschaftendatei auf Ihrem Desktop gespeichert.
6. Ist CC-SG für sichere Browserverbindungen konfiguriert, müssen Sie das Kontrollkästchen **Secure Socket Layer (SSL)** markieren. Ist CC-SG nicht für sichere Browserverbindungen konfiguriert, müssen Sie das Kontrollkästchen **Secure Socket Layer (SSL)** deaktivieren. Diese Einstellung muss richtig sein, damit der Thick-Client eine Verbindung zu CC-SG herstellen kann.
   - **So prüfen Sie die Einstellungen in CC-SG**: Klicken Sie im Menü **Administration** auf **Sicherheit**. Sehen Sie sich auf der Registerkarte **Allgemein** das Feld **Browser-Verbindungsprotokoll** an. Wenn die Option **HTTPS/SSL** ausgewählt ist, müssen Sie das Kontrollkästchen **Secure Socket Layer SSL** im Fenster zur Eingabe der IP-Adresse des Thick-Clients aktivieren. Wenn die Option **HTTP** ausgewählt ist, müssen Sie das Kontrollkästchen **Secure Socket Layer SSL** im Fenster zur Eingabe der IP-Adresse des Thick-Clients deaktivieren.

7. Klicken Sie auf **Start**.
   - Wenn Sie eine nicht unterstützte Version der Java Runtime Environment auf Ihrem Computer verwenden, werden Sie durch eine Warnung darauf hingewiesen. Laden Sie entweder eine unterstützte Java-Version herunter, oder fahren Sie mit der installierten Version fort.
8. Der Anmeldebildschirm wird angezeigt, und der Thick-Client sieht aus und funktioniert wie ein browserbasierter Java-Client. Sind die vertraglichen Einschränkungen der Serviceleistungen aktiviert, lesen Sie den Text und markieren Sie das Kontrollkästchen **Ich stimme den Vertragsbedingungen zu**.
9. Geben Sie Ihren **Benutzernamen** und Ihr **Kennwort** in die entsprechenden Felder ein, und klicken Sie zum Fortfahren auf **Anmelden**.

Thick-Client verwenden

Nachdem der Thick-Client installiert wurde, haben Sie zwei Möglichkeiten, über Ihren Client-Computer darauf zuzugreifen. Diese Möglichkeiten werden von der Java-Version bestimmt, die Sie verwenden.

- **Java 1.4.x**

Verwendet Ihr Client-Computer **Java Version 1.4.x** und haben Sie bei der Installation des Thick-Clients im Fenster **Desktop Integration (Desktop-Integration)** auf **Yes (Ja)** geklickt, können Sie den Thick-Client über einen Doppelklick auf das Desktop-Symbol starten und auf CC-SG zugreifen. Wenn kein Desktop-Symbol vorhanden ist, können Sie dies jederzeit erstellen: Suchen Sie auf Ihrem Client-Computer nach **AMcc.jnlp**, und erstellen Sie eine Verknüpfung für diese Datei.

- **Java 1.5**

Wenn Ihr Client-Computer **Java Version 1.5** ausführt, können Sie:

a. In der Java-Systemsteuerung den Thick-Client über Java Application Cache Viewer starten.
b. In der Java-Systemsteuerung über Java Application Cache Viewer ein Desktop-Symbol für den Thick-Client installieren.

CC-SG-Fenster mit Komponenten

Bei einer gültigen Anmeldung wird das CC-SG-Anwendungsfenster angezeigt.

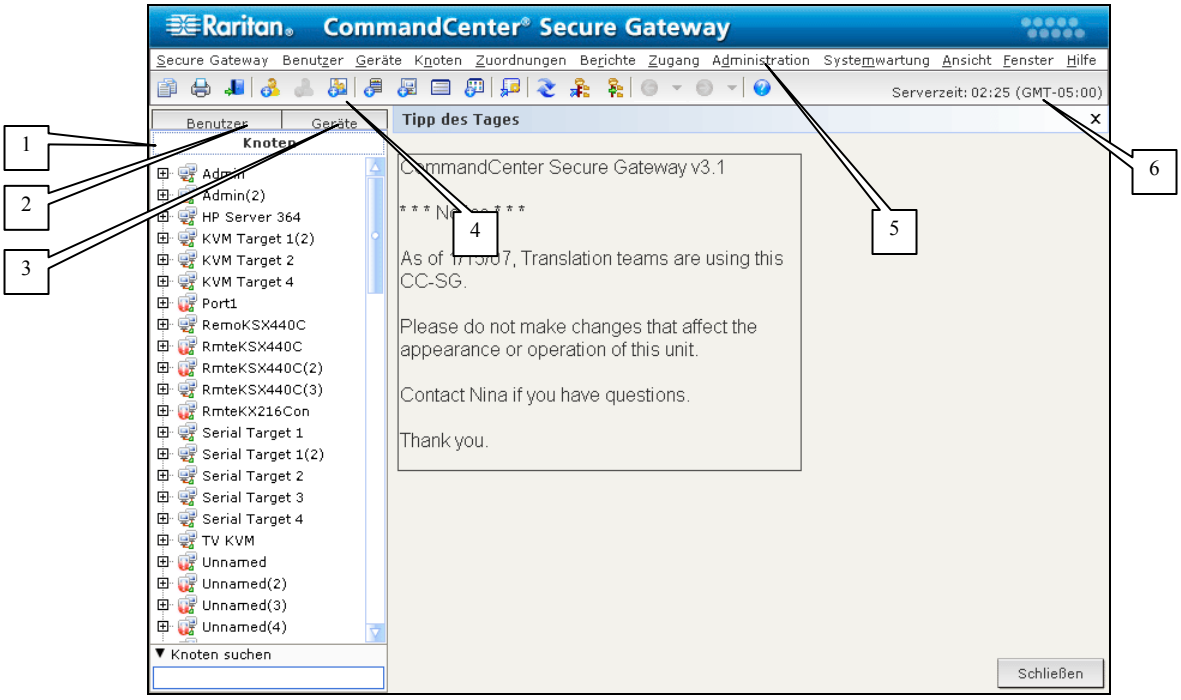


Abbildung 3 CC-SG-Fenster mit Komponenten

1. Registerkarte **Knoten**: Klicken Sie auf die Registerkarte **Knoten**, um alle bekannten Zielknoten in einer Strukturansicht anzuzeigen. Klicken Sie auf einen Knoten, um das Knotenprofil anzuzeigen. Schnittstellen sind unter den übergeordneten Knoten zusammengefasst. Klicken Sie auf das Plus- oder Minuszeichen (+ oder -), um die Struktur ein- oder auszublenden. Klicken Sie mit der rechten Maustaste auf eine Schnittstelle, und wählen Sie **Verbinden** aus, um eine Verbindung mit dieser Schnittstelle herzustellen. Sie können die Knoten nach Knotennamen (alphabetisch) oder Knotenstatus (Verfügbar, Beschäftigt, Nicht verfügbar) sortieren. Klicken Sie mit der rechten Maustaste auf die Strukturansicht, klicken Sie auf **Knotensortieroptionen** und dann auf **Nach Knotenname** oder **Nach Knotenstatus**.
2. Registerkarte **Benutzer**: Klicken Sie auf die Registerkarte **Benutzer**, um eine Strukturansicht aller registrierten Benutzer und Gruppen anzuzeigen. Klicken Sie auf das Plus- oder Minuszeichen (+ oder -), um die Struktur ein- oder auszublenden.
3. Registerkarte **Geräte**: Klicken Sie auf die Registerkarte **Geräte**, um eine Strukturansicht aller bekannten Raritan-Geräte anzuzeigen. Die einzelnen Gerätetypen sind durch unterschiedliche Symbole dargestellt. Ports sind unter den übergeordneten Geräten zusammengefasst. Klicken Sie auf das Plus- oder Minuszeichen (+ oder -), um die Struktur ein- oder auszublenden. Klicken Sie auf einen Port, um das Portprofil anzuzeigen. Klicken Sie mit der rechten Maustaste auf einen Port, und wählen Sie **Verbinden** aus, um eine Verbindung mit diesem Port herzustellen. Sie können die Ports nach Portnamen (alphabetisch) oder Portstatus (Verfügbar, Beschäftigt, Nicht verfügbar) sortieren. Klicken Sie mit der rechten Maustaste auf die Strukturansicht, klicken Sie auf **Portsortieroptionen** und dann auf **Nach Portname** oder **Nach Portstatus**.
4. **Symbolleiste mit Kurzbefehlen**: Diese Symbolleiste enthält Schaltflächen zum Ausführen der am häufigsten benötigten Befehle.

5. **Menüleiste für den Betrieb und zur Konfiguration**: Diese Menüs enthalten Befehle zum Bedienen und Konfigurieren von CC-SG. Sie können einige dieser Befehle auch ausführen, indem Sie mit der rechten Maustaste auf die Symbole auf den Registerkarten **Knoten**, **Benutzer** und **Geräte** klicken. Die angezeigten Menüs und Menüelemente hängen von Ihren Benutzerzugriffsberechtigungen ab.
6. **Serverzeit**: Aktuelle Uhrzeit und Zeitzone, die für CC-SG im Konfigurationsmanager konfiguriert wurde. Diese Uhrzeit wird zum Planen von Aufgaben im Aufgabenmanager verwendet. Weitere Informationen zur Aufgabenverwaltung finden Sie in **Kapitel 12: Erweiterte Administration**. Diese Uhrzeit unterscheidet sich eventuell von der auf dem Client verwendeten Uhrzeit.

IP-Adresse, Firmware-Version und Anwendungsversionen prüfen

Nach dem Anmelden sollten Sie die IP-Adresse bestätigen, die CC-SG-Serverzeit einrichten und die installierten Firmware- und Anwendungsversionen überprüfen. Sie müssen die Firmware und Anwendungen ggf. aktualisieren.

Bestätigen der IP-Adresse

1. Klicken Sie im Menü **Administration** auf **Konfiguration**, um das Fenster **Konfigurationsmanager** anzuzeigen.
2. Klicken Sie auf die Registerkarte **Netzwerksetup**.

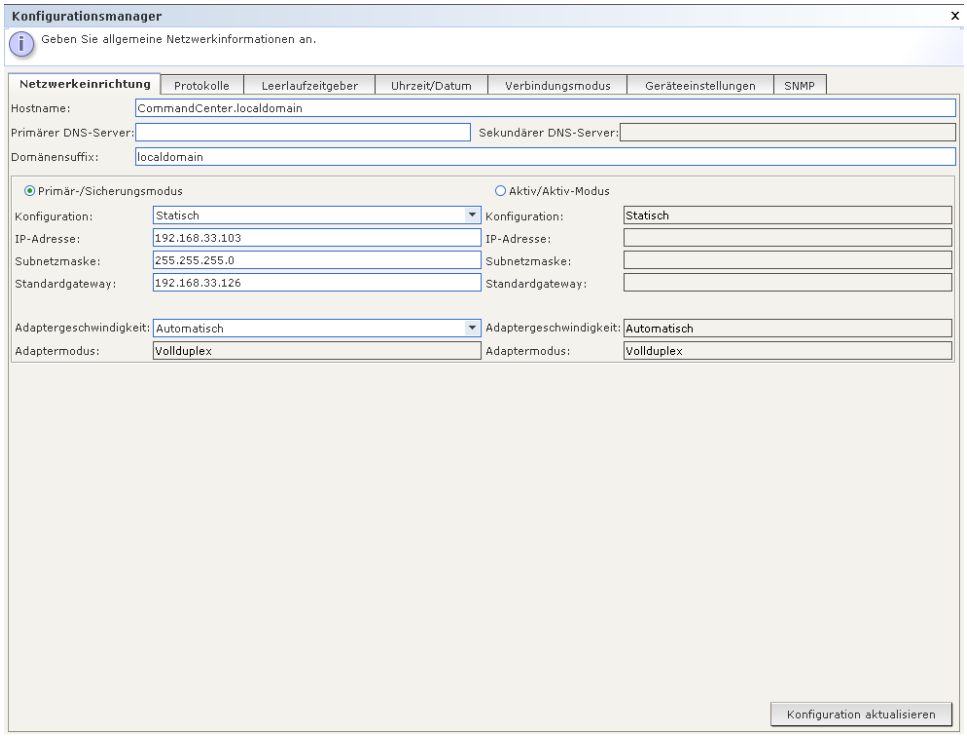


Abbildung 4 IP-Adresse bestätigen

3. Prüfen Sie, ob die Netzwerkeinstellungen richtig sind, und nehmen Sie ggf. Änderungen vor.
4. Klicken Sie auf **Konfiguration aktualisieren**, um die Änderungen zu übernehmen.
5. Klicken Sie im Bestätigungsfenster zum Übernehmen Ihrer Einstellungen auf **OK**, melden Sie sich ab und starten Sie CC-SG erneut.
6. Greifen Sie unter Verwendung der neuen IP-Adresse auf CC-SG zu.

CC-SG-Serverzeit festlegen

1. Melden Sie sich bei CC-SG an.
2. Klicken Sie im Menü **Administration** auf **Konfiguration**, um das Fenster **Konfigurationsmanager** anzuzeigen.
3. Klicken Sie auf die Registerkarte **Datum/Uhrzeit**.

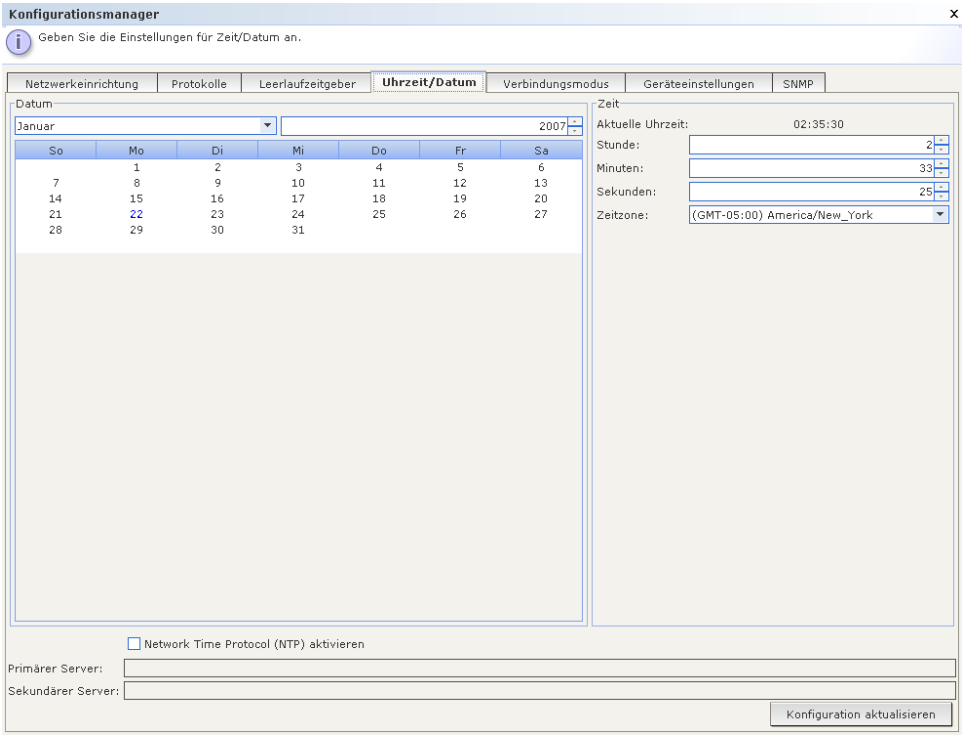


Abbildung 5 Konfiguration von Datum/Uhrzeit

4. Klicken Sie im Menü **Administration** auf **Konfiguration**, um das Fenster **Konfigurationsmanager** anzuzeigen.
5. Klicken Sie auf die Registerkarte **Datum/Uhrzeit**.
   c. **So stellen Sie das Datum und die Uhrzeit manuell ein**: **Datum**: Zum Einstellen des Datums klicken Sie auf die Dropdown-Liste und wählen darin den **Monat** aus. Wählen Sie das **Jahr** mit der Pfeil-nach-oben/unten-Schaltfläche aus, und klicken Sie im Kalenderbereich auf den **Tag**. **Uhrzeit**: Zum Einstellen der Uhrzeit klicken Sie auf die Pfeil-nach-oben/unten-Schaltfläche, um die **Stunde**, **Minuten** und **Sekunden** festzulegen. Klicken Sie anschließend auf die Dropdown-Liste **Zeitzone**, um die Zeitzone auszuwählen, in der CC-SG betrieben wird.
   d. **So stellen Sie das Datum und die Uhrzeit mittels NTP ein**: Markieren Sie das Kontrollkästchen **Network Time Protocol aktivieren** unten im Fenster, und geben Sie die IP-Adresse für den **Primären NTP-Server** und den **Sekundären NTP-Server** in die entsprechenden Felder ein.

***Hinweis**: Zum Synchronisieren des Datums und der Uhrzeit von angeschlossenen Computern mit dem Datum und der Uhrzeit eines zugewiesenen NTP-Servers wird das Network Time Protocol (NTP) verwendet. Wird CC-SG mit NTP konfiguriert, kann es zur konsistenten Verwendung der korrekten Uhrzeit seine Uhrzeit mit dem öffentlich verfügbaren NTP-Referenzserver synchronisieren.*

6. Klicken Sie auf **Konfiguration aktualisieren**, um die Uhrzeit- und Datumsänderungen auf CC-SG anzuwenden.
7. Klicken Sie auf **Aktualisieren**, um die neue Serverzeit im Feld **Aktuelle Uhrzeit** zu aktualisieren.
8. Klicken Sie im Menü **Wartung** auf **Neu starten**, um CC-SG neu zu starten.

CC-SG-Firmwareversion prüfen und aktualisieren

1. Melden Sie sich bei CC-SG an.
2. Wählen Sie **Info zu Raritan Secure Gateway** im Menü **Hilfe** aus. Die Firmwareversionsnummer wird in einem Popupfenster angezeigt. Klicken Sie auf **OK**.
3. Handelt es sich nicht um die aktuelle Version, müssen Sie Ihre Firmware aktualisieren. Sie können die Aktualisierungsdatei für die Firmware auf der Website von Raritan herunterladen oder von einer CD von Raritan kopieren. Speichern Sie die Datei mit der Firmwareaktualisierung auf Ihrem Client PC.

***Hinweis**: Bevor Sie CC-SG aktualisieren können, müssen Sie in den Wartungsmodus wechseln. Weitere Informationen finden Sie unter Wartungsmodus in **Kapitel 11: Systemwartung**.*

4. Klicken Sie im Menü **Systemwartung** auf **Wartungsmodus** und dann auf **Wartungsmodus starten**.
5. Geben Sie im Fenster **Wartungsmodus starten** in die entsprechenden Felder die Nachricht für Benutzer ein, die bei CC-SG abgemeldet werden, sowie die Dauer in Minuten, während der der Wartungsmodus ausgeführt werden soll. Klicken Sie dann auf **OK**.
6. Klicken Sie im Bestätigungsfeld auf **OK**.
7. Beim Starten des CC-SG-Wartungsmodus wird eine zweite Bestätigungsnachricht angezeigt. Klicken Sie auf **OK**.
8. Klicken Sie im Menü **Systemwartung** auf **Aktualisieren**.

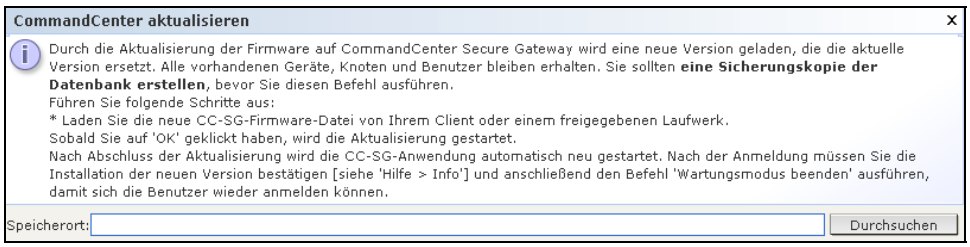


Abbildung 6 CommandCenter aktualisieren

9. Klicken Sie auf **Durchsuchen**, und wählen Sie die Datei zur Firmwareaktualisierung im angezeigten Dialogfeld zum Öffnen aus. Klicken Sie auf **Öffnen**.
10. Klicken Sie im Fenster **CommandCenter aktualisieren** auf **OK**.

***Hinweis**: Wenn Sie die Firmware als ZIP-Datei erhalten haben, entpacken Sie die Datei, und befolgen Sie die Anweisungen in der README-Datei.*

Anwendungsversionen prüfen und aktualisieren

Prüfen und aktualisieren Sie die CC-SG-Anwendungen, z. B. Raritan Console (RC) und Raritan Remote Client (RRC).

1. Klicken Sie im Menü **Administration** auf **Anwendungen**.

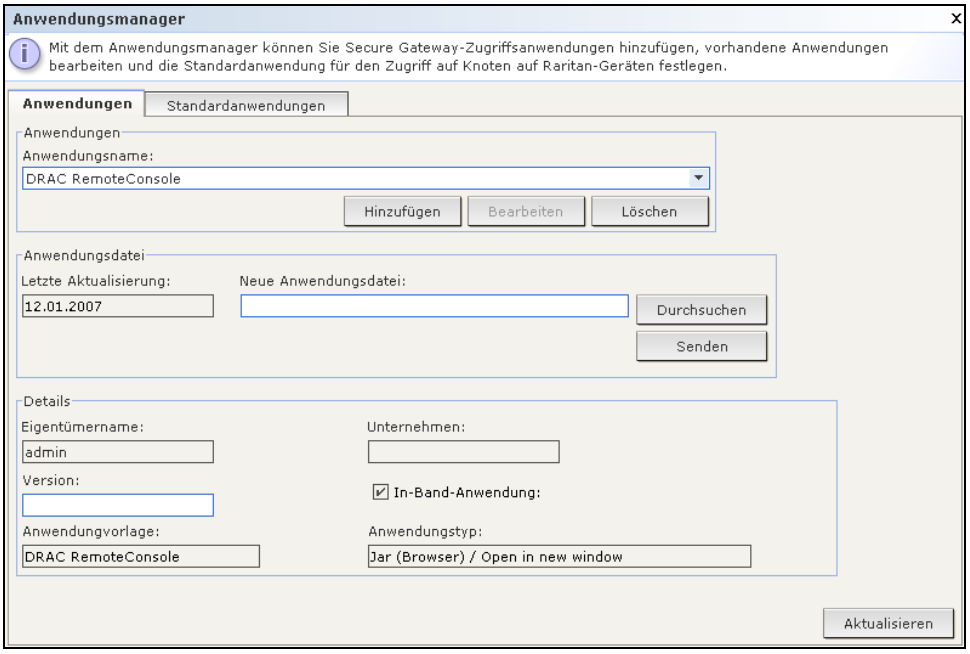


Abbildung 7 CC-SG-Anwendungsmanager

2. Klicken Sie auf die Dropdown-Liste **Anwendungsname**, und wählen Sie in der Liste eine Anwendung aus. Beachten Sie die Zahl im Feld **Version**.
3. Handelt es sich nicht um die aktuelle Anwendungsversion, müssen Sie die Anwendung aktualisieren. Sie können die Aktualisierungsdatei für die Anwendung auf der Website von Raritan herunterladen oder von einer CD von Raritan kopieren. Speichern Sie die Datei mit der Anwendungsaktualisierung auf Ihrem Client PC. (Eine vollständige Liste der unterstützen Browser und Plattformen finden Sie in der **Compatibility Matrix** (Kompatibilitätsmatrix) unter **http://www.raritan.com/support**. Klicken Sie auf der Seite **Support** auf **Firmwareaktualisierungen** und dann auf **CommandCenter Secure Gateway**.)
4. Klicken Sie auf die Dropdown-Liste **Anwendungsname**, und wählen Sie die zu aktualisierende Anwendung in der Liste aus.
5. Klicken Sie auf **Durchsuchen**, und wählen Sie die Datei zur Anwendungsaktualisierung im angezeigten Dialogfeld zum Öffnen aus. Klicken Sie auf **Öffnen**.
6. Der Anwendungsname wird im **Anwendungsmanager** im Feld **Neue Anwendungsdatei** angezeigt.
7. Klicken Sie auf **Upload**. Eine Statusanzeige informiert über den Ladevorgang der neuen Anwendung. Nach Abschluss des Uploads werden Sie in einem neuen Fenster darauf hingewiesen, dass die Anwendung der CC-SG-Datenbank hinzugefügt wurde. Die Anwendung kann nun konfiguriert und einem bestimmten Port zugewiesen werden.
8. Geben Sie bei Bedarf die neue Versionsnummer in das Feld **Version** ein. Das Feld **Version** wird bei einigen Anwendungen automatisch aktualisiert.
9. Klicken Sie auf **Aktualisieren**.
10. Klicken Sie zum Schließen des Fensters **Anwendungsmanager** auf **Schließen**.

CC-SG herunterfahren

Wird die Stromversorgung zu einer V1-Einheit, die CC-SG ausführt, unterbrochen, merkt sich die V1-Einheit den letzten Stromversorgungsstatus. Sobald die Stromzufuhr wiederhergestellt ist, fährt die V1-Einheit automatisch neu hoch. Wenn jedoch die Stromversorgung zu einer V1-Einheit unterbrochen wird, die ausgeschaltet ist, bleibt die V1-Einheit auch dann ausgeschaltet, wenn die Stromzufuhr wiederhergestellt wurde.

Wichtig: Drücken Sie nicht die POWER-Taste, um CC-SG zwangsweise herunterzufahren. Es wird empfohlen, CC-SG auf die nachstehend beschriebene Art und Weise herunterzufahren.

So wird CC-SG heruntergefahren:

1. Entfernen Sie die Blende, und drücken Sie die **POWER**-Taste. Bei G1-Einheiten befindet sich die **POWER**-Taste auf der Rückseite des Geräts.
2. Warten Sie etwa eine Minute, während CC-SG ordnungsgemäß heruntergefahren wird.

***Hinweis**: Benutzer, die über die Diagnostic Console in CC-SG angemeldet sind, erhalten eine kurze Broadcastnachricht, wenn die CC-SG-Einheit ausgeschaltet wird. Benutzer, die über einen Webbrowser oder SSH in CC-SG angemeldet sind, erhalten keine Nachricht, wenn die CC-SG-Einheit ausgeschaltet wird.*

3. Warten Sie, bis der Vorgang des Herunterfahrens vollständig abgeschlossen ist, bevor Sie den Netzstecker ziehen. Nur so kann CC-SG vor der Unterbrechung der Stromzufuhr alle Transaktionen beenden, die Datenbanken schließen und die Festplattenlaufwerke in einen sicheren Zustand versetzen.

Kompatibilitätsmatrix

Die Kompatibilitätsmatrix führt die Firmwareversionen von Raritan-Geräten und Softwareversionen von Anwendungen auf, die mit der aktuellen Version von CC-SG kompatibel sind. CC-SG überprüft diese Daten, wenn Sie ein Gerät hinzufügen, Gerätefirmware aktualisieren oder eine Anwendung zur Verwendung auswählen. Wenn die Firmware- oder Softwareversion inkompatibel ist, zeigt CC-SG eine Warnung an. Jede Version von CC-SG unterstützt nur die zum Erscheinungszeitpunkt aktuelle Firmwareversion und die vorherigen Firmwareversionen für Raritan-Geräte.

- Klicken Sie im Menü **Administration** auf **Kompatibilitätsmatrix**.

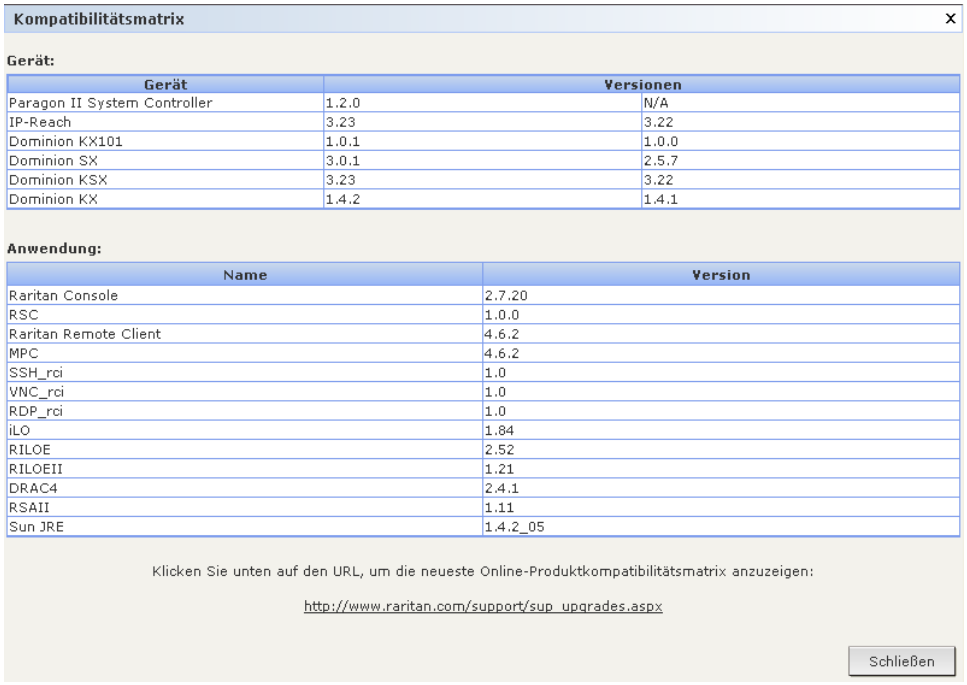


Abbildung 8 Kompatibilitätsmatrix

Diese Seite wurde absichtlich leer gelassen.

Kapitel 3: Konfigurieren von CC-SG mit dem Setup-Assistenten

Vorbereitung zum Konfigurieren von CC-SG mit dem Setup-Assistenten

Bevor Sie mit der CC-SG-Konfiguration fortfahren, müssen Sie die Systemkonfiguration abschließen.

- Konfigurieren und installieren Sie Dominion-Serie- und IP-Reach-Appliances (serielle und KVM-Geräte). Weisen Sie dabei eine IP-Adresse zu, und erstellen Sie ein CC-SG-Administratorkonto.

Überblick über den Setup-Assistenten

Der Setup-Assistent dient als einfache Möglichkeit, Erstkonfigurationsaufgaben für CC-SG auszuführen, nachdem die Systemkonfiguration abgeschlossen ist. Der Setup-Assistent führt Sie durch die Definition von Zuordnungen, das Erkennen und Hinzufügen von Geräten zu CC-SG, das Erstellen von Geräte- und Knotengruppen, das Erstellen von Benutzergruppen, das Zuweisen von Richtlinien und Rechten für Benutzergruppen und das Hinzufügen von Benutzern. Nachdem Sie den Setup-Assistenten abgeschlossen haben, können Sie Ihre Konfigurationseinstellungen einzeln ändern.

Setup-Assistenten starten:

Klicken Sie im Menü **Administration** auf **Setup-Assistent**. Der Setup-Assistent wird angezeigt. Im linken Fensterbereich wird der **Aufgabenassistent** in einer Strukturansicht dargestellt. Auf der rechten Seite werden die aktiven Aufgaben angezeigt.

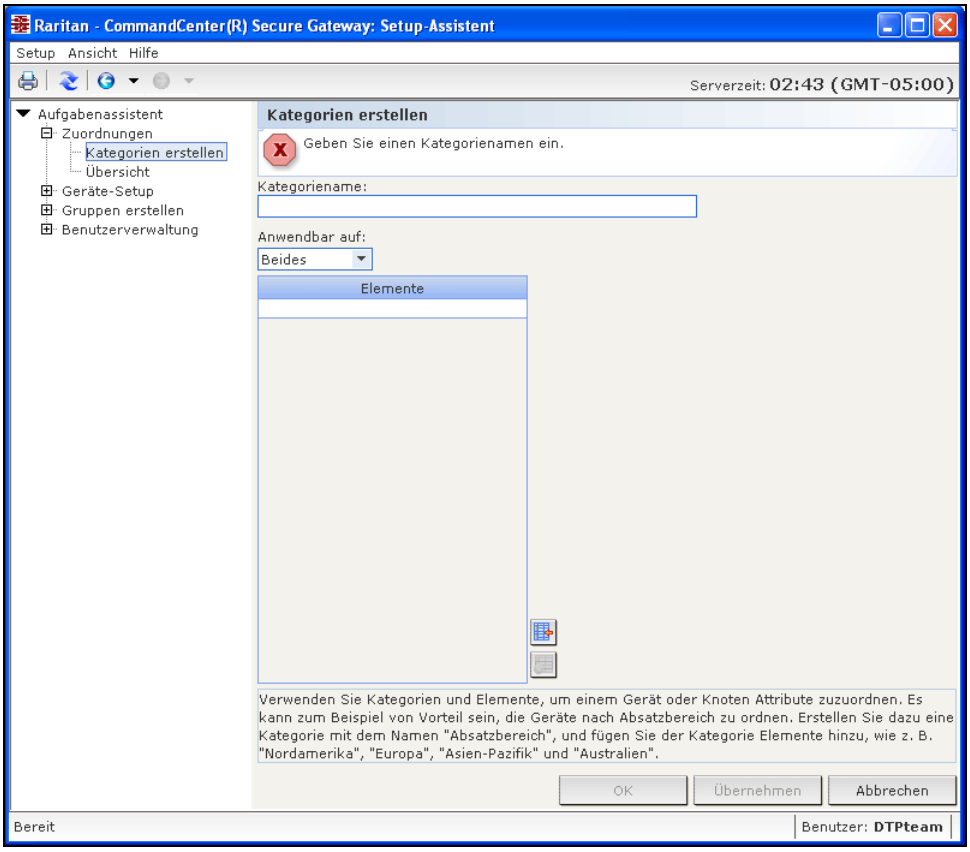


Abbildung 9 Fenster Setup-Assistent

Der Setup-Assistent ist in vier Aufgaben eingeteilt, die in den folgenden Abschnitten beschrieben werden:

- **Zuordnungen**: Definieren der Kategorien und Elemente, die Sie zum Verwalten Ihrer Geräte verwenden.
- **Geräte-Setup**: Erkennen von Geräten in Ihrem Netzwerk und Hinzufügen dieser Geräte zu CC-SG. Konfigurieren von Geräteports.
- **Gruppen erstellen**: Kategoriesieren der Geräte und Knoten, die CC-SG in Gruppen verwaltet, und Erstellen von Richtlinien mit unbeschränktem Zugriff für jede Gruppe.
- **Benutzerverwaltung**: Hinzufügen von Benutzern und Benutzergruppen zu CC-SG, und Auswählen der Richtlinien und Berechtigungen, die den Zugriff dieser Benutzer innerhalb von CC-SG und auf Geräte und Knoten bestimmen.

Zuordnungen

Sie können zur Organisation der von CC-SG verwalteten Geräte Zuordnungen einrichten. Jede Zuordnung enthält eine Kategorie (oberste Gruppe) und zugehörige Elemente (Kategorie-Untergruppen). Wenn Sie beispielsweise Geräte nach Standort sortieren möchten, können Sie eine Kategorie „Standort“ und Elemente mit Bezeichnungen der Serverstandorte wie „Philadelphia“, „New York“ und „New Orleans“ erstellen.

Kategorien und Elemente erstellen

1. Im Fenster **Setup-Assistent** wird als Standardfenster **Kategorien erstellen** angezeigt. Klicken Sie auf **Zuordnungen** und dann im linken Fensterbereich auf **Kategorien erstellen**, um das gleichnamige Fenster anzuzeigen.

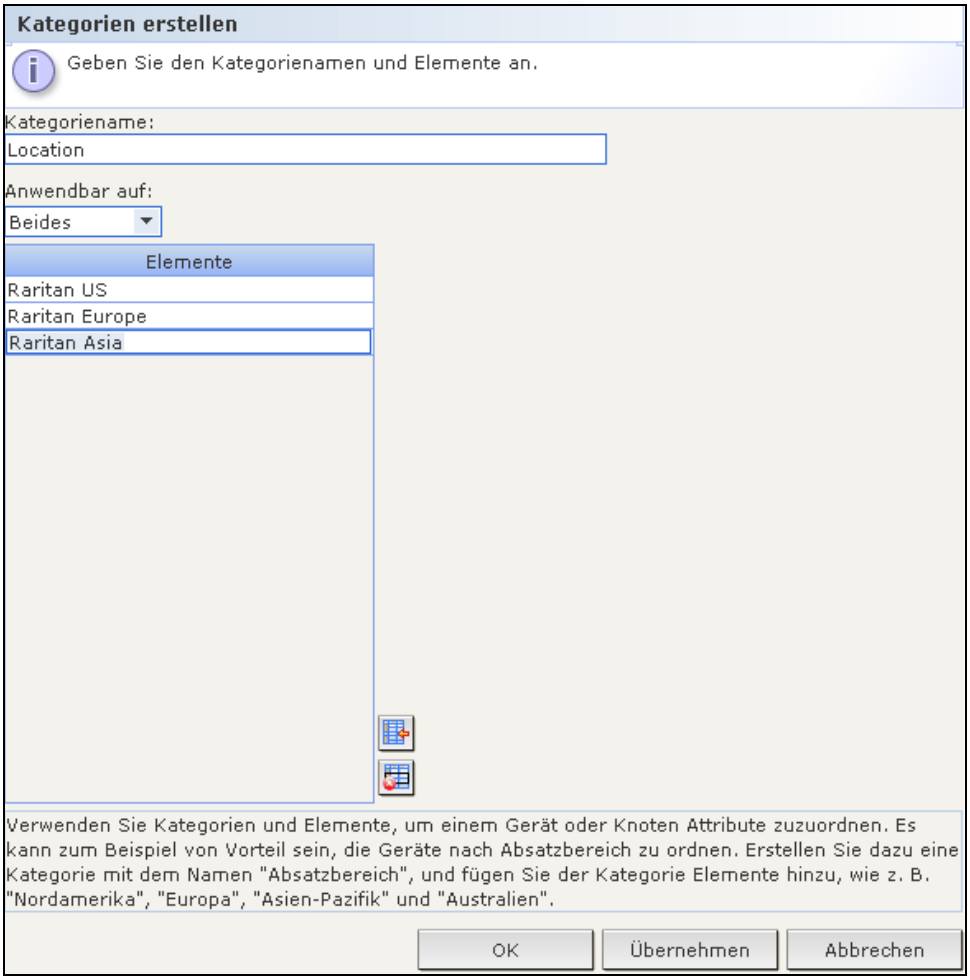


Abbildung 10 Setup-Assistent: Kategorien und Elemente erstellen

2. Geben Sie zum Verwalten der Geräte im Feld **Kategoriename** den entsprechenden Namen der Kategorie wie „Standort“ ein.
3. Im Feld **Anwendbar auf:** können Sie angeben, ob die Kategorie für Geräte, Knoten oder beides verfügbar sein soll. Klicken Sie auf das Dropdown-Menü **Anwendbar auf:**, und wählen Sie einen Wert aus der Liste aus.
4. Geben Sie in der Tabelle **Elemente** den Namen eines Elements in der Kategorie ein (beispielsweise „Raritan Deutschland“).
   - Klicken Sie auf das Symbol  , um bei Bedarf neue Zeilen in die Tabelle **Elemente** einzufügen.
   - Sie können Elemente löschen, indem Sie eine Zeile auswählen und auf das Symbol  klicken, um das ausgewählte Element in der Tabelle **Elemente** zu löschen.
5. Wiederholen Sie diese Schritte, bis Sie alle Elemente in der Kategorie zu der Tabelle **Elemente** hinzugefügt haben.
6. Wenn Sie eine andere Kategorie erstellen möchten, klicken Sie auf **Übernehmen**, um diese Kategorie zu speichern. Wiederholen Sie dann die Schritte in diesem Abschnitt, um weitere Kategorien hinzuzufügen.
7. Klicken Sie auf **OK**, wenn Sie alle Kategorien und Elemente erstellt haben. Der Fensterbereich **Zuordnungsübersicht** enthält eine Liste der Kategorien und Elemente, die Sie erstellt haben.
8. Klicken Sie zum Ausführen der nächsten Aufgabe **Geräte-Setup** auf **Weiter**. Befolgen Sie die Schritte im nächsten Abschnitt.

Geräte-Setup

Die zweite Aufgabe im Setup-Assistenten lautet **Geräte-Setup**. Über Geräte-Setup können Sie in Ihrem Netzwerk nach Geräten suchen, diese erkennen und sie zu CC-SG hinzufügen. Beim Hinzufügen von Geräten können Sie ein Element pro Kategorie auswählen, das dem Gerät zugeordnet werden soll.

Wichtig: Während der CC-SG-Konfiguration dürfen keine anderen Benutzer am Gerät angemeldet sein.

Geräte erkennen und hinzufügen

1. Der Fensterbereich **Geräte erkennen** wird angezeigt, wenn Sie nach der Zuordnungsaufgabe auf **Weiter** klicken. Sie können auch auf **Geräte-Setup** und dann im linken Fensterbereich in der Strukturansicht **Aufgabenassistent** auf **Geräte erkennen** klicken, um den gleichnamigen Fensterbereich zu öffnen.

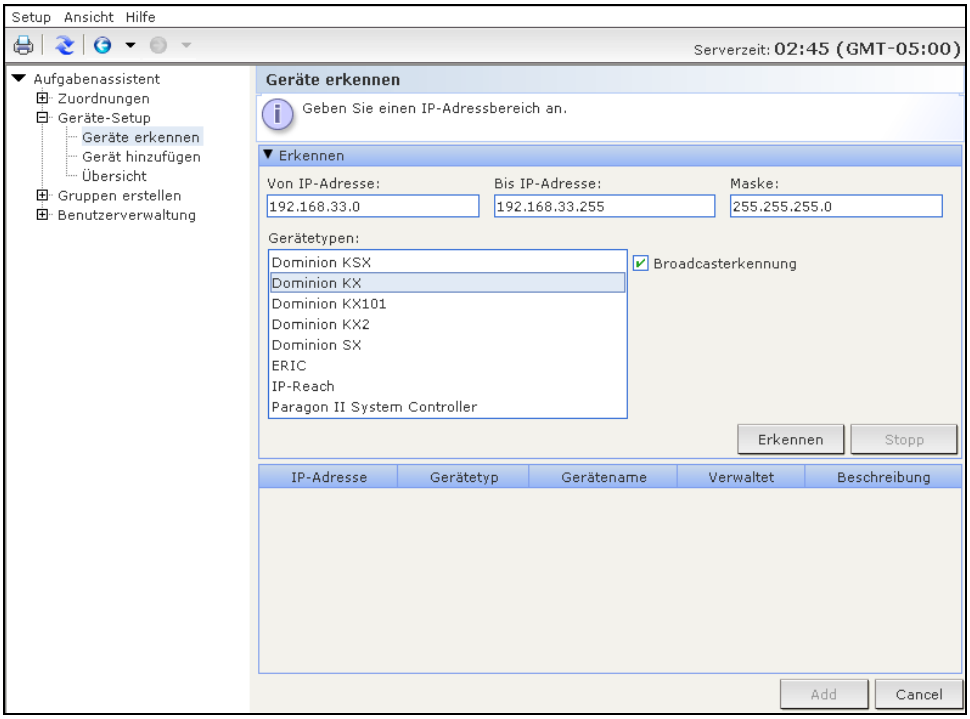


Abbildung 11 Setup-Assistent: Geräte erkennen

2. Geben Sie in die Felder **Von-Adresse** und **An-Adresse** den Bereich der IP-Adressen ein, den Sie nach den Geräten durchsuchen möchten.
3. Geben Sie in das Feld **Maske** die Subnetzmaske ein, die Sie nach Geräten durchsuchen möchten.
4. Wählen Sie in der Liste **Gerätetypen** die Gerätetypen aus, nach denen Sie in dem angegebenen Bereich suchen möchten. Sie können mehrere Gerätetypen auswählen, indem Sie die **STRG**-Taste bei der Auswahl gedrückt halten.
5. Klicken Sie auf **Broadcasterkennung**, wenn Sie nach Geräten im selben Subnetz suchen, in dem sich CC-SG befindet. Deaktivieren Sie **Broadcasterkennung**, wenn Geräte in allen Subnetzen erkannt werden sollen.
6. Klicken Sie auf **Erkennen**.
7. Nach Abschluss des Erkennungsvorgangs wird eine Bestätigungsnachricht angezeigt. Klicken Sie in der Bestätigungsmeldung auf **OK**.

8. Falls CC-SG Geräte des angegebenen Typs und im angegebenen Adressenbereich gefunden hat, werden die Geräte in der Tabelle unten im Fensterbereich **Geräte erkennen** angezeigt. Sie können oben im Fensterbereich auf den schwarzen Pfeil klicken, um den oberen Bereich auszublenden. Sie vergrößern dadurch die Suchergebnisse im unteren Fensterbereich.

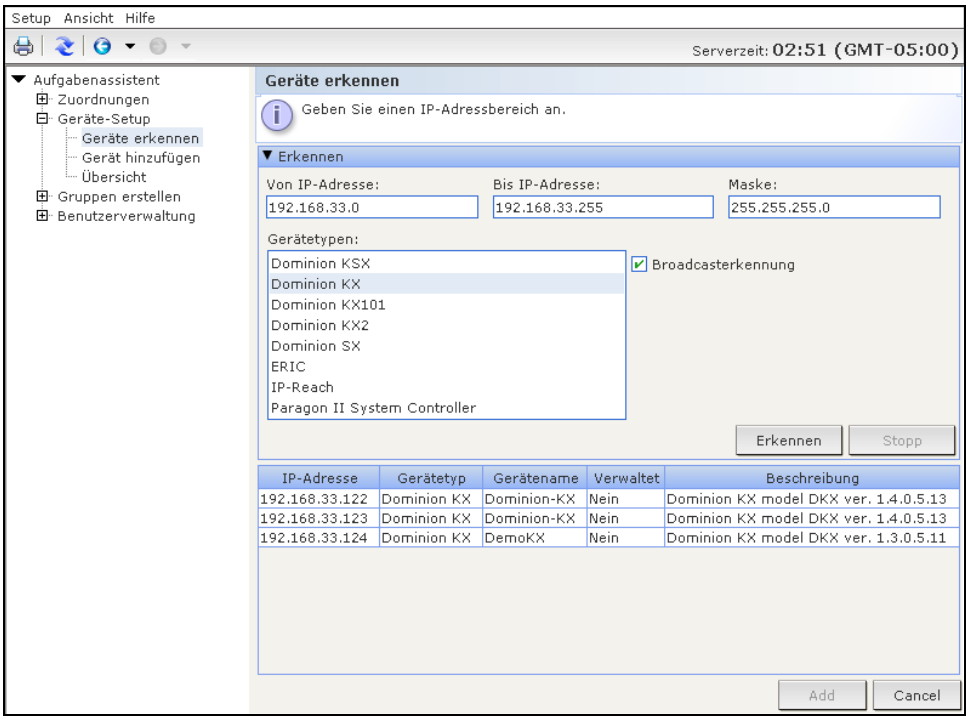


Abbildung 12 Setup-Assistent: Ergebnisse der Geräteerkennung

9. Wählen Sie in der Tabelle der erkannten Geräte das Gerät aus, das Sie CC-SG hinzufügen möchten, und klicken Sie auf **Hinzufügen**. Der Fensterbereich **Gerät hinzufügen** wird angezeigt. Dieser Fensterbereich hängt vom Gerätetyp ab, den Sie hinzufügen.

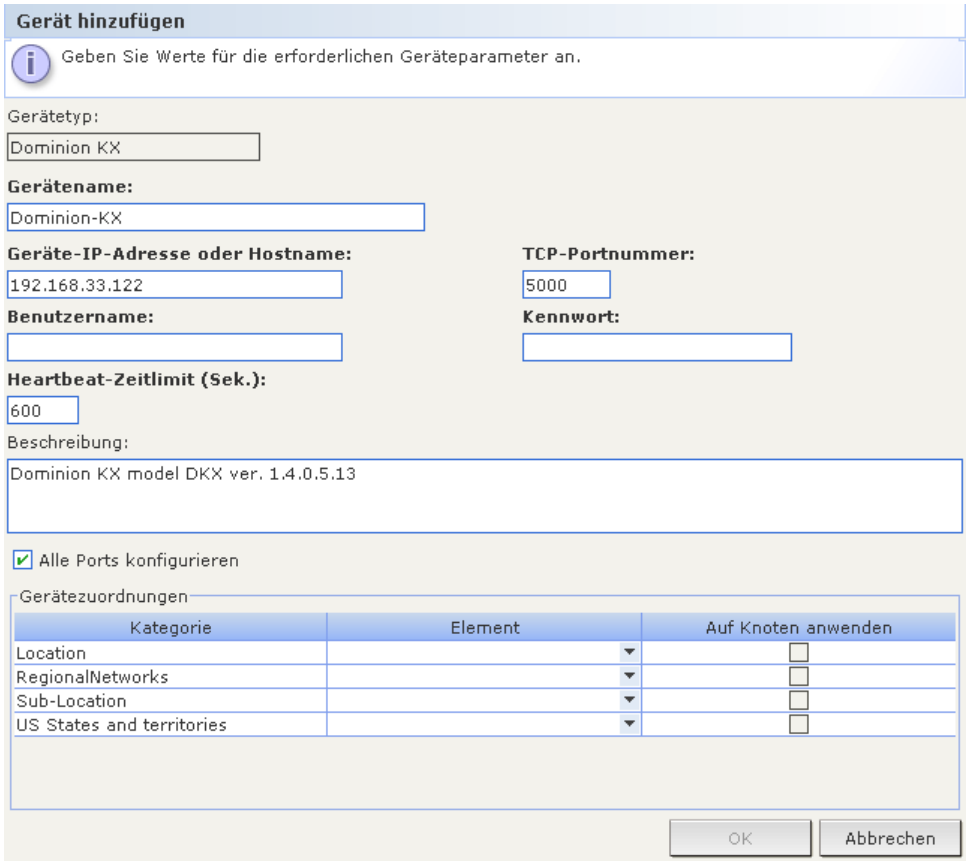


Abbildung 13 Setup-Assistent: Gerät hinzufügen

10. Sie können neuen Text in die entsprechenden Felder **Gerätename** und **Beschreibung** eingeben.
11. Vergewissern Sie sich, dass die IP-Adresse, die Sie beim Hinzufügen des Geräts zu CC-SG angegebenen haben, im Feld **Geräte-IP oder Hostname** angezeigt wird. Geben Sie andernfalls die richtige Adresse in das Feld ein.
12. Die Nummer des **TCP-Ports** wird abhängig vom Gerätetyp automatisch eingefügt.
13. Geben Sie in die entsprechenden Felder **Benutzername** und **Kennwort** ein, die Sie beim Hinzufügen des Geräts zu CC-SG erstellt haben.
14. Geben Sie im Feld **Heartbeat-Zeitlimit** die Dauer in Sekunden ein, die vor Überschreitung des Zeitlimits zwischen Gerät und CC-SG verstreichen sollte.
15. Wenn Sie ein Dominion SX-Gerät hinzufügen, markieren Sie das Kontrollkästchen **Lokaler Zugriff: Zulässig**, wenn ein lokaler Zugriff auf das Gerät zugelassen werden soll. Deaktivieren Sie das Kontrollkästchen **Lokaler Zugriff: Zulässig**, wenn kein lokaler Zugriff auf das Gerät zugelassen werden soll.
16. Wenn Sie manuell ein PowerStrip-Gerät hinzufügen, klicken Sie auf den Pfeil neben der Dropdown-Liste **Anzahl der Ports**, und wählen Sie die Anzahl der PowerStrip-Ausgänge aus.
17. Wenn Sie einen IPMI-Server hinzufügen, geben Sie in die entsprechenden Felder ein **Überprüfungsintervall** für die Verfügbarkeitsprüfung und eine Methode für die **Authentifizierung** ein, die der im IPMI-Server konfigurierten Methode entsprechen muss.
18. Wenn Sie alle verfügbaren Ports des Geräts konfigurieren möchten, markieren Sie das Kontrollkästchen **Alle Ports konfigurieren**. CC-SG fügt alle Ports des Geräts zu CC-SG hinzu und erstellt einen Knoten für jeden Port.
19. Klicken Sie unten im Fensterbereich unter **Gerätezuordnungen** auf den Pfeil der Dropdown-Spalte **Element**, die mit jeder Kategorie übereinstimmt, die Sie dem Gerät zuordnen möchten. Wählen Sie dann das gewünschte Element für die Zuordnung zum Gerät in der Liste aus.
20. Soll das Element auf das Gerät und die mit dem Gerät verbundenen Knoten angewendet werden, markieren Sie das Kontrollkästchen **Auf Knoten anwenden**.
21. Wenn Sie ein weiteres Gerät hinzufügen möchten, klicken Sie auf **Übernehmen**, um dieses Gerät zu speichern. Wiederholen Sie dann die Schritte in diesem Abschnitt, um weitere Geräte hinzuzufügen.
22. Klicken Sie auf **OK**, nachdem Sie alle gewünschten Geräte hinzugefügt haben. Im Fensterbereich **Geräteübersicht** wird eine Liste der Geräte angezeigt, die Sie hinzugefügt haben.
23. Klicken Sie zum Ausführen der nächsten Aufgabe **Gruppen erstellen** auf **Weiter**. Befolgen Sie die Schritte im nächsten Abschnitt.

Gruppen erstellen

Die dritte Aufgabe im Setup-Assistenten lautet **Gruppen erstellen**. Über **Gruppen erstellen** können Sie Geräte- und Knotengruppen definieren und den Satz von Geräten oder Knoten angeben, der in jeder Gruppe enthalten sein soll. Administratoren können Zeit sparen, indem Sie Gruppen ähnlicher Geräte und Knoten anstatt jedes Gerät oder jeden Knoten einzeln verwalten.

Gerätegruppen und Knotengruppen hinzufügen

1. Der Fensterbereich **Gerätegruppenmanager** wird angezeigt, wenn Sie nach Abschluss der Geräte-Setup-Aufgabe auf **Weiter** klicken. Sie können auch auf **Gruppen erstellen** und dann im linken Fensterbereich in der Strukturansicht **Aufgabenassistent** auf **Gerätegruppen hinzufügen** klicken, um den Fensterbereich **Gerätegruppenmanager** zu öffnen.
2. Geben Sie in das Feld **Gruppenname** einen Namen für die Gerätegruppe ein, die Sie erstellen möchten.

3. Sie haben zwei Möglichkeiten, Geräte einer Gruppe hinzuzufügen: **Geräte auswählen** und **Geräte beschreiben**. Auf der Registerkarte **Geräte auswählen** können Sie auswählen, welche Geräte zur Gruppe zugeordnet werden sollen. Wählen Sie die Geräte dazu einfach in der Liste der verfügbaren Geräte aus. Auf der Registerkarte **Geräte beschreiben** können Sie Regeln angeben, die Geräte beschreiben. Geräte, deren Parameter diesen Regeln entsprechen, werden der Gruppe hinzugefügt.

Geräte auswählen

a. Klicken Sie im Fensterbereich **Gerätegruppen hinzufügen** auf die Registerkarte **Geräte auswählen**.

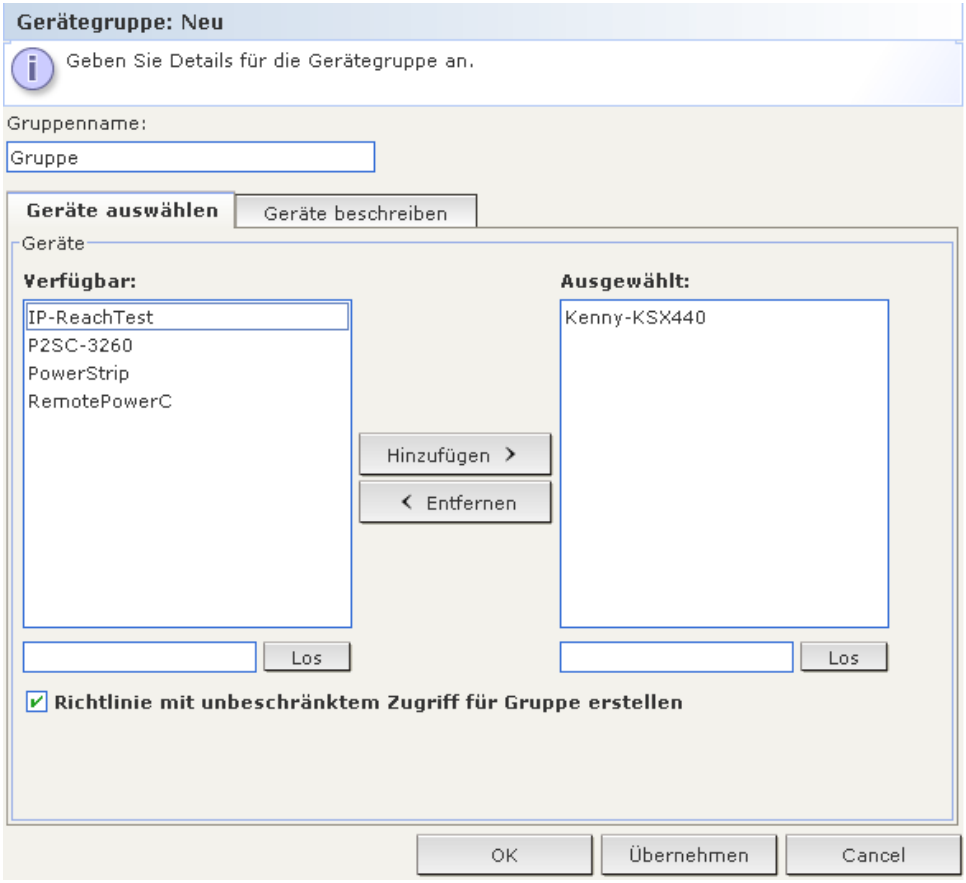


Abbildung 14 Setup-Assistent: Gerätegruppen hinzufügen, Geräte auswählen

b. Wählen Sie in der Liste **Verfügbar** das Gerät aus, das Sie der Gruppe hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**, um das Gerät in die Liste **Ausgewählt** zu verschieben. Geräte in der Liste **Ausgewählt** werden der Gruppe hinzugefügt.

- Wählen Sie zum Löschen eines Geräts in der Gruppe den Gerätenamen in der Liste **Ausgewählt** aus, und klicken Sie auf **Löschen**.
- Sie können das Gerät in der Liste **Verfügbar** oder **Ausgewählt** suchen. Geben Sie den Suchbegriff in das Feld unter der Liste ein, und klicken Sie auf **Los**.

Geräte beschreiben

a. Klicken Sie im Fensterbereich **Gerätegruppen hinzufügen** auf die Registerkarte **Geräte beschreiben**. Auf der Registerkarte **Geräte beschreiben** erstellen Sie eine Regeltabelle, in der die Geräte beschrieben werden, die Sie der Gruppe zuweisen möchten.

b. Klicken Sie auf das Symbol  , um eine neue Zeile in die Tabelle einzufügen.

c. Doppelklicken Sie auf die Zelle, die für jede Spalte erstellt wurde, um das Dropdown-Menü anzuzeigen. Wählen Sie in jeder Liste die gewünschten Regelkomponenten aus.

d. Markieren Sie das Kontrollkästchen **Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen**, wenn Sie eine Richtlinie für diese Gerätegruppe erstellen möchten, die jederzeit den Zugriff auf alle Knoten und Geräte in der Gruppe mit Steuerungsberechtigung zulässt.

e. Wenn Sie eine weitere Gerätegruppe hinzufügen möchten, klicken Sie auf **Übernehmen**, um diese Gruppe zu speichern. Wiederholen Sie dann die Schritte in diesem Abschnitt, um weitere Gerätegruppen hinzuzufügen.

f. Klicken Sie auf **OK**, nachdem Sie alle gewünschten Gerätegruppen hinzugefügt haben. Der Fensterbereich **Knotengruppenmanager** wird angezeigt. Sie können auch auf **Gruppen erstellen** und dann im linken Fensterbereich in der Strukturansicht **Aufgabenassistent** auf **Knotengruppen hinzufügen** klicken, um den Fensterbereich **Knotengruppenmanager** zu öffnen.

g. Geben Sie in das Feld **Gruppenname** einen Namen für die Knotengruppe ein, die Sie erstellen möchten.

h. Sie haben zwei Möglichkeiten, einer Gruppe Knoten hinzuzufügen: **Knoten auswählen** und **Knoten beschreiben**. Auf der Registerkarte **Knoten auswählen** können Sie auswählen, welche Knoten zur Gruppe zugeordnet werden sollen. Wählen Sie die Knoten dazu einfach in der Liste der verfügbaren Knoten aus. Auf der Registerkarte **Knoten beschreiben** können Sie Regeln angeben, die Knoten beschreiben. Knoten, deren Parameter diesen Regeln entsprechen, werden der Gruppe hinzugefügt.

Knoten auswählen

a. Klicken Sie im Fensterbereich **Knotengruppen hinzufügen** auf die Registerkarte **Knoten auswählen**.

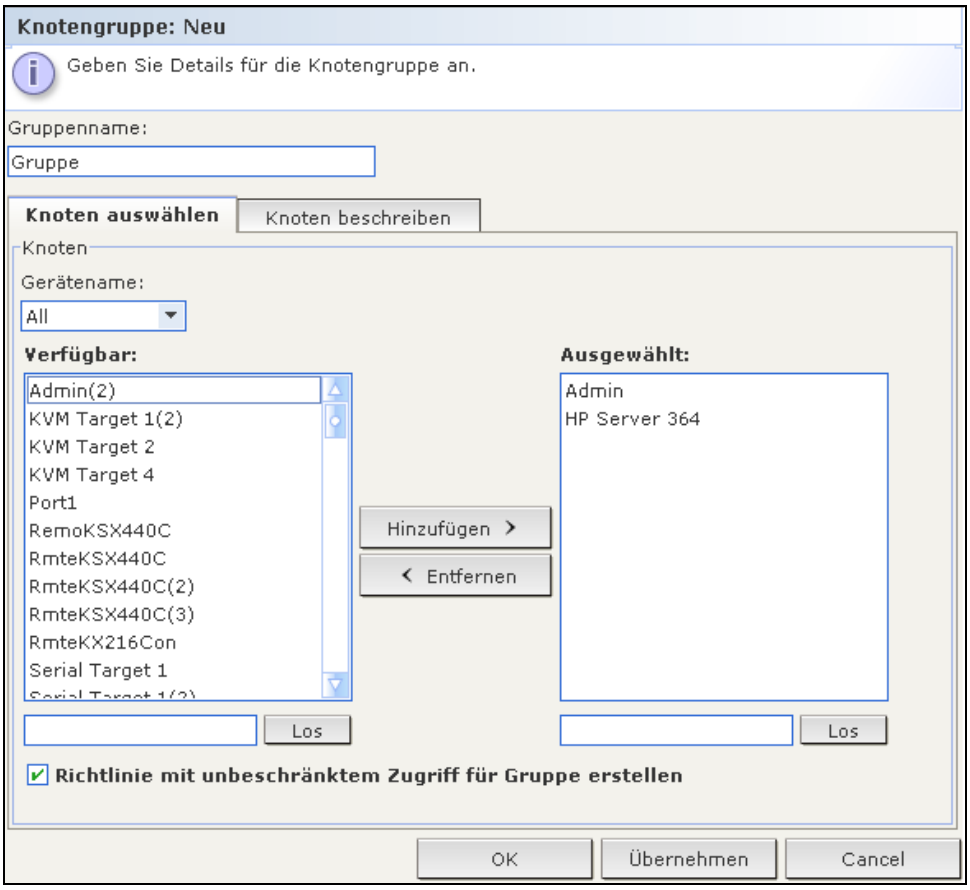


Abbildung 15 Setup-Assistent: Knotengruppen hinzufügen, Knoten auswählen

b. Wählen Sie in der Liste **Verfügbar** den Knoten aus, den Sie der Gruppe hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**, um den Knoten in die Liste **Ausgewählt** zu verschieben. Knoten in der Liste **Ausgewählt** werden der Gruppe hinzugefügt.

c. Wählen Sie zum Löschen eines Knotens aus der Gruppe den Knotennamen in der Liste **Ausgewählt** aus, und klicken Sie auf **Löschen**.

d. Sie können den Knoten in der Liste **Verfügbar** oder **Ausgewählt** suchen. Geben Sie den Suchbegriff in das Feld unter der Liste ein, und klicken Sie auf **Los**.

Knoten beschreiben

a. Klicken Sie im Fensterbereich **Knotengruppen hinzufügen** auf die Registerkarte **Knoten beschreiben**. Auf der Registerkarte **Knoten beschreiben** erstellen Sie eine Regeltabelle, in der die Knoten beschrieben werden, die Sie der Gruppe zuweisen möchten.

b. Klicken Sie auf das Symbol  , um eine neue Zeile in die Tabelle einzufügen.

c. Doppelklicken Sie auf die Zelle, die für jede Spalte erstellt wurde, um das Dropdown-Menü anzuzeigen. Wählen Sie in jeder Liste die gewünschten Regelkomponenten aus. Weitere Informationen finden Sie in **Kapitel 8: Richtlinien**.

d. Markieren Sie das Kontrollkästchen **Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen**, wenn Sie eine Richtlinie für diese Knotengruppe erstellen möchten, die jederzeit den Zugriff auf alle Knoten in der Gruppe mit Steuerungsberechtigung zulässt.

e. Wenn Sie eine weitere Knotengruppe hinzufügen möchten, klicken Sie auf **Übernehmen**, um diese Gruppe zu speichern. Wiederholen Sie dann die Schritte in diesem Abschnitt, um weitere Knotengruppen hinzuzufügen.

f. Klicken Sie auf **OK**, nachdem Sie alle gewünschten Knotengruppen hinzugefügt haben. Im Fensterbereich **Gruppenübersicht** wird eine Liste der Gruppen angezeigt, die Sie hinzugefügt haben.

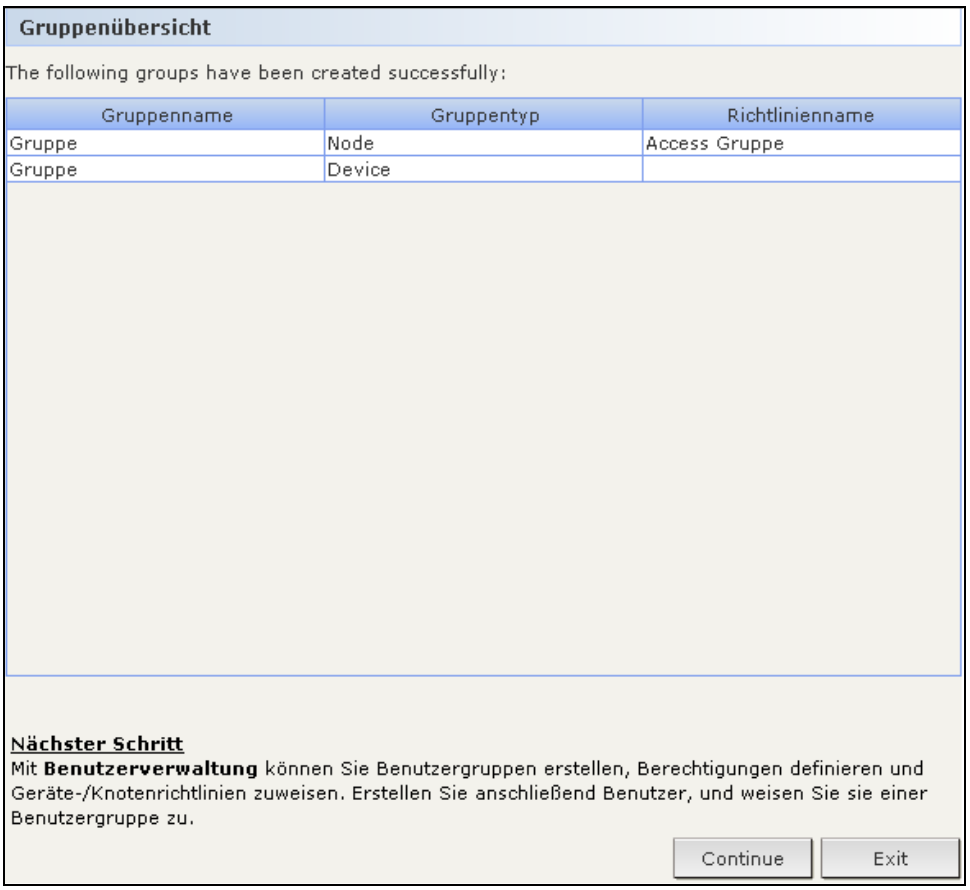


Abbildung 16 Setup-Assistent: Gruppenübersicht

g. Klicken Sie zum Ausführen der nächsten Aufgabe **Benutzerverwaltung** auf **Weiter**. Befolgen Sie die Schritte im nächsten Abschnitt.

Benutzerverwaltung

Die vierte Aufgabe im Setup-Assistenten lautet **Benutzerverwaltung**. Mit **Benutzerverwaltung** können Sie die **Berechtigungen** und **Richtlinien** auswählen, die den Zugriff und die Aktivitäten der Benutzergruppen bestimmen. Berechtigungen legen fest, welche Aktivitäten die Mitglieder der Benutzergruppe in CC-SG ausführen können. Richtlinien legen fest, welche Geräte und Knoten die Mitglieder der Gruppe anzeigen und bearbeiten können. Richtlinien basieren auf den Kategorien und Elementen. Nachdem Sie Benutzergruppen erstellt haben, können Sie einzelne Benutzer definieren und sie diesen Benutzergruppen hinzufügen.

Benutzergruppen und Benutzer hinzufügen

1. Der Fensterbereich **Benutzergruppe hinzufügen** wird angezeigt, wenn Sie nach der Aufgabe zum Erstellen von Gruppen auf **Weiter** klicken. Sie können auch auf **Benutzermanagement** und dann im linken Fensterbereich in der Strukturansicht **Aufgabenassistent** auf **Benutzergruppe hinzufügen** klicken, um den gleichnamigen Fensterbereich zu öffnen.
2. Geben Sie in das Feld **Benutzergruppenname** einen Namen für die Benutzergruppe ein, die Sie erstellen möchten.
3. Geben Sie in das Feld **Beschreibung** eine Beschreibung für die Benutzergruppe ein.

4. Klicken Sie auf die Registerkarte **Berechtigungen**, wählen Sie dann die Kontrollkästchen aus, die den Berechtigungen oder CC-SG-Aktivitäten entsprechen, die Sie der Benutzergruppe zuordnen möchten.
5. Im Bereich **Knotenzugriff** können Sie angeben, ob die Benutzergruppe über Zugriff auf **In Band-** und **Out-of-Band-**Knoten und auf Funktionen zur **Stromversorgungsverwaltung** verfügen soll. Markieren Sie die Kontrollkästchen, die den Zugriffsarten entsprechen, die Sie der Gruppe zuweisen möchten.

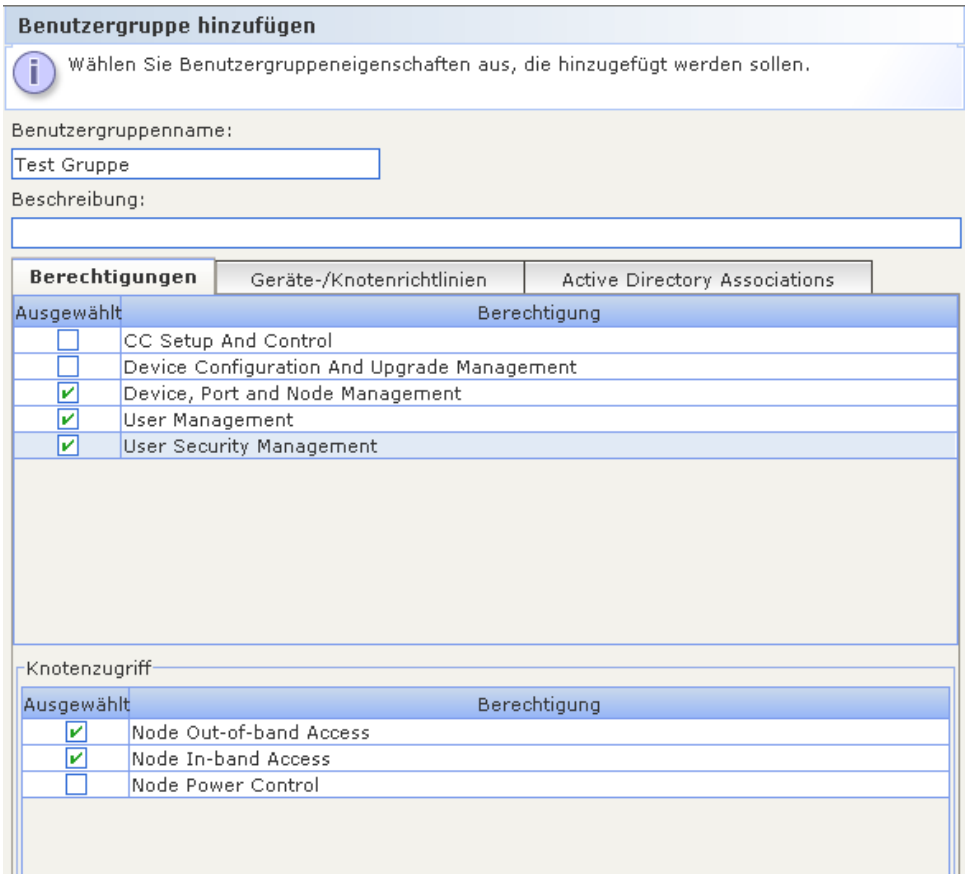


Abbildung 17 Benutzergruppe hinzufügen – Berechtigungen

6. Klicken Sie auf die Registerkarte **Richtlinien**.

7. Wählen Sie in der Liste **Alle Richtlinien** die Richtlinie aus, die Sie der Benutzergruppe zuweisen möchten, und klicken Sie auf **Hinzufügen**, um die Richtlinie in die Liste **Ausgewählte Richtlinien** zu verschieben. Richtlinien in der Liste **Ausgewählte Richtlinien** werden der Benutzergruppe zugewiesen. Wiederholen Sie diesen Schritt, um der Benutzergruppe weitere Richtlinien zuzuweisen.

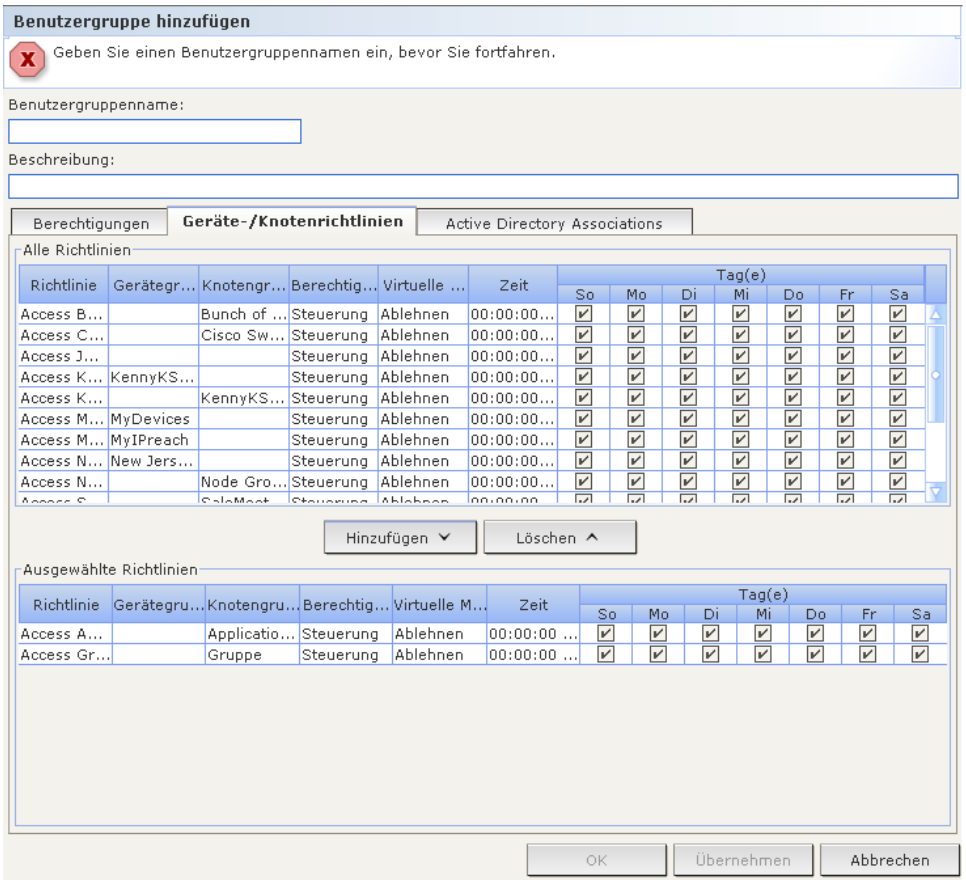


Abbildung 18 Benutzergruppe hinzufügen – Richtlinien

8. Wählen Sie zum Löschen einer Richtlinie in der Benutzergruppe den Namen der Richtlinie in der Liste **Ausgewählte Richtlinien** aus, und klicken Sie auf **Löschen**.
9. Wenn Sie Benutzer, für die Remoteauthentifizierung verwendet wird, mit Active Directory-Modulen verknüpfen möchten, klicken Sie auf die Registerkarte **Active Directory Associations** (Active Directory-Zuordnungen). Markieren Sie das Kontrollkästchen, das jedem Active Directory-Modul entspricht, das Sie mit dieser Benutzergruppe verknüpfen möchten.
10. Wenn Sie eine weitere Benutzergruppe hinzufügen möchten, klicken Sie auf **Übernehmen**, um diese Gruppe zu speichern. Wiederholen Sie dann die Schritte in diesem Abschnitt, um weitere Benutzergruppen hinzuzufügen.
11. Klicken Sie auf **OK**, nachdem Sie alle gewünschten Benutzergruppen hinzugefügt haben. Der Fensterbereich **Benutzer hinzufügen** wird angezeigt. Sie können auch auf **Benutzermanagement** und dann im linken Fensterbereich in der Strukturansicht **Aufgabenassistent** auf **Benutzer hinzufügen** klicken, um den gleichnamigen Fensterbereich zu öffnen.
12. Geben Sie im Feld **Benutzername** den Namen für den Benutzer zur Anmeldung bei CC-SG ein.
13. Markieren Sie das Kontrollkästchen **Anmeldung aktiviert**, wenn der Benutzer über die Anmeldeberechtigung für CC-SG verfügen soll.

14. Markieren Sie das Kontrollkästchen **Remoteauthentifizierung** nur, wenn der Benutzer mithilfe eines anderen Servers wie TACACS+, RADIUS, LDAP oder AD authentifiziert werden soll. Bei der Remoteauthentifizierung wird kein Kennwort benötigt. Die Felder **Neues Kennwort** und **Neues Kennwort erneut eingeben** sind deaktiviert wenn das Feld **Remoteauthentifizierung** markiert ist.
15. Geben Sie in die Felder **Neues Kennwort** und **Neues Kennwort erneut eingeben** das Kennwort ein, das der Benutzer zur Anmeldung in CC-SG verwenden soll.
16. Markieren Sie das Kontrollkästchen **Änderung des Kennworts bei der nächsten Anmeldung erzwingen**, wenn der Benutzer gezwungen werden soll, das zugewiesene Kennwort bei der nächsten Anmeldung zu ändern.
17. Markieren Sie das Kontrollkästchen **Änderung des Kennworts periodisch erzwingen** wenn Sie festlegen möchten, wie oft der Benutzer zur Kennwortänderung gezwungen werden soll.
18. Geben Sie in das Feld **Gültigkeitsdauer (in Tagen)** die Anzahl von Tagen ein, die der Benutzer dasselbe Kennwort verwenden kann, bevor eine Änderung erzwungen wird.
19. Geben Sie die E-Mail-Adresse des Benutzers in das Feld **E-Mail-Adresse** ein.
20. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Benutzergruppe**, und wählen Sie in der Liste die Benutzergruppe aus, der Sie den Benutzer zuweisen möchten.
21. Wenn Sie einen weiteren Knoten hinzufügen möchten, klicken Sie auf **Übernehmen**, um diesen Benutzer zu speichern. Wiederholen Sie dann die Schritte in diesem Abschnitt, um weitere Benutzer hinzuzufügen.
22. Klicken Sie auf **OK**, nachdem Sie alle gewünschten Benutzer hinzugefügt haben. Im Fensterbereich **Benutzerübersicht** wird eine Liste der Benutzergruppen und Benutzer angezeigt, die Sie hinzugefügt haben.

Diese Seite wurde absichtlich leer gelassen.

Kapitel 4: Erstellen von Zuordnungen

Zuordnungen

Sie können zur Organisation der von CC-SG verwalteten Geräte Zuordnungen einrichten. Jede Zuordnung enthält eine Kategorie (oberste Gruppe) und zugehörige Elemente (Kategorie-Untergruppen). Beispiel: Sie haben Raritan-Geräte, die Zielserver in einem Rechenzentrum in New York, Philadelphia und New Orleans verwalten. Sie können eine Zuordnung einrichten, die diese Geräte nach Standort organisiert. Sie können dann CC-SG so anpassen, dass Ihre Raritan-Geräte und Knoten nach der von Ihnen ausgewählten Kategorie (Standort) und den verknüpften Elementen (New York, Philadelphia und New Orleans) über die CC-SG-Schnittstelle angezeigt werden. Die Abbildung unten zeigt eine benutzerdefinierte Ansicht, die anhand dieses Beispiels erstellt wurde. Sie können die Organisation und Anzeige Ihrer Server in CC-SG beliebig nach Ihren Wünschen anpassen.

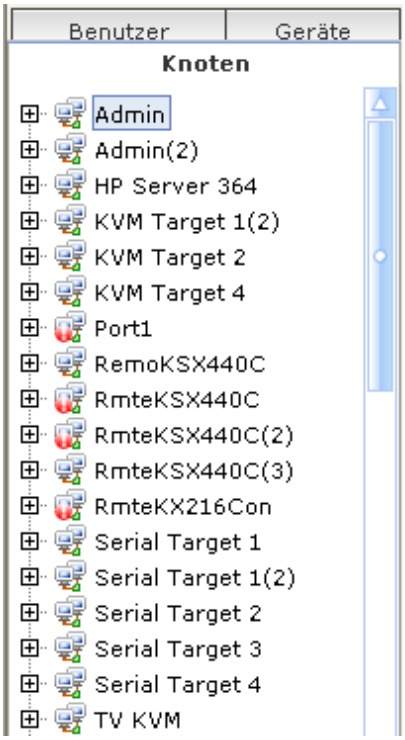


Abbildung 19 CC-SG-Zuordnungsbeispiel

Zuordnungsterminologie

Anhand der folgenden Definitionen können Sie Zuordnungen besser verstehen:

- **Zuordnungen**: Beziehungen zwischen Kategorien und Kategorieelementen zu Knoten und Geräten. So können Sie beispielsweise ein Gerät der Kategorie „Standort“ zuordnen. Sie sollten zuerst die Zuordnungen erstellen (oder sie später bearbeiten), bevor Sie in CC-SG Geräte und Ports hinzufügen.
- **Kategorie**: Eine Variable, die bestimmte Werte (genannt Elemente) enthält. „Standort“ ist beispielsweise eine Kategorie, die Elemente wie „New York City“ und „Philadelphia“ enthält. „Betriebssystemtyp“ ist eine weitere Kategorie, die Elemente wie „Windows“, „Unix“ oder „Linux“ enthalten kann. Wenn Sie in CC-SG Geräte hinzufügen, werden diese Informationen entsprechend zugeordnet.
- **Elemente**: Werte einer Kategorie. Das Element „New York City“ gehört beispielsweise zur Kategorie „Standort“.

- **Geräte**: Raritan-Produkte wie Dominion KX, Dominion SX, Dominion KSX, IP-Reach, Paragon II Systemcontroller, Paragon II UMT832 mit USTIP usw., die von CC-SG verwaltet werden. Diese Geräte steuern die mit ihnen verbundenen Zielsysteme oder Knoten.
- **Knoten**: Zielsysteme oder Server, auf die CC-SG zugreifen und die CC-SG verwalten kann. In CC-SG klicken Sie auf einen Knoten, um auf diesen über eine Schnittstelle zuzugreifen und diesen zu verwalten.

Zuordnungsbestimmende Kategorien und Elemente

Raritan-Geräte und Knoten werden nach Kategorien und Elementen organisiert. Jedes Paar Kategorie/Element wird einem Gerät und/oder einem Knoten zugeordnet. Daher müssen die Kategorien und Elemente vor dem Hinzufügen von Raritan-Geräten in CC-SG definiert werden.

Eine Kategorie ist eine Gruppe gleichartiger Elemente. Sie können beispielsweise Ihre Raritan-Geräte nach Standorten gruppieren. Dazu müssen Sie eine Kategorie und einen Standort definieren, der einen Satz an Elementen wie „New York“, „Philadelphia“ und „New Orleans“ enthält.

Kategorien und Elemente können auch von Richtlinien verwendet werden, um den Benutzerzugriff auf Server zu steuern. Mit dem Paar Kategorie/Element (Standort/New York) können Sie beispielsweise eine Richtlinie erstellen, um den Benutzerzugriff auf Server in New York zu steuern.

Nachfolgend einige Beispiele für typische Zuordnungskonfigurationen von Kategorien und Elementen:

KATEGORIE	ELEMENTE
Standort	New York City, Philadelphia, New Orleans
Betriebssystemtyp	Unix, Windows, Linux
Abteilung	Vertrieb, IT, Technik

Zuordnungskonfigurationen sollten möglichst einfach gehalten sein, um die organisatorischen Zielsetzungen in Bezug auf Server/Knoten und den Benutzerzugriff zu erfüllen. Ein Knoten kann nur einem Element einer Kategorie zugewiesen werden. So kann ein Zielserver beispielsweise nicht gleichzeitig dem Windows- und Unix-Element der Betriebssystemtyp-Kategorie zugeordnet werden.

Bei ähnlichen Servern, die wahlfrei organisiert werden müssen, stellt der folgende Vorschlag einen praktischen Ansatz für die Organisation Ihrer Systeme dar:

KATEGORIE	ELEMENT
Benutzergruppe1	usergroup1node
Benutzergruppe2	usergroup2node
Benutzergruppe3	usergroup3node

Geräte und Knoten werden beim Hinzufügen zu CC-SG mit den vordefinierten Kategorien und Elementen verknüpft. Wenn Sie Knoten- und Gerätegruppen erstellen und ihnen Richtlinien zuweisen, definieren Sie anhand der Kategorien und Elemente, welche Knoten und Geräte zu den einzelnen Gruppen gehören.

Zuordnungen erstellen

Sie haben zwei Möglichkeiten, Zuordnungen zu erstellen: Setup-Assistent und Zuordnungsmanager.

- **Setup-Assistent** vereint viele Konfigurationsaufgaben mithilfe einer automatisierten Schnittstelle. Der Setup-Assistent wird für die CC-SG-Erstkonfiguration empfohlen. Nachdem Sie den Setup-Assistenten abgeschlossen haben, können Sie Ihre Konfigurationseinstellungen einzeln ändern. Weitere Informationen finden Sie in Kapitel 3: Konfigurieren von CC-SG mit dem Setup-Assistenten.
- Mit dem **Zuordnungsmanager** können Sie nur mit Zuordnungen arbeiten. Konfigurationsaufgaben werden nicht automatisiert. Weitere Informationen finden Sie auf den folgenden Seiten im Abschnitt **Zuordnungsmanager**.

Zuordnungsmanager

Mit dem Zuordnungsmanager können Sie Kategorien und Elemente hinzufügen, ändern oder löschen.

Kategorie hinzufügen

1. Klicken Sie im Menü **Zuordnungen** auf **Zuordnung**. Das Fenster **Zuordnungsmanager** wird angezeigt.

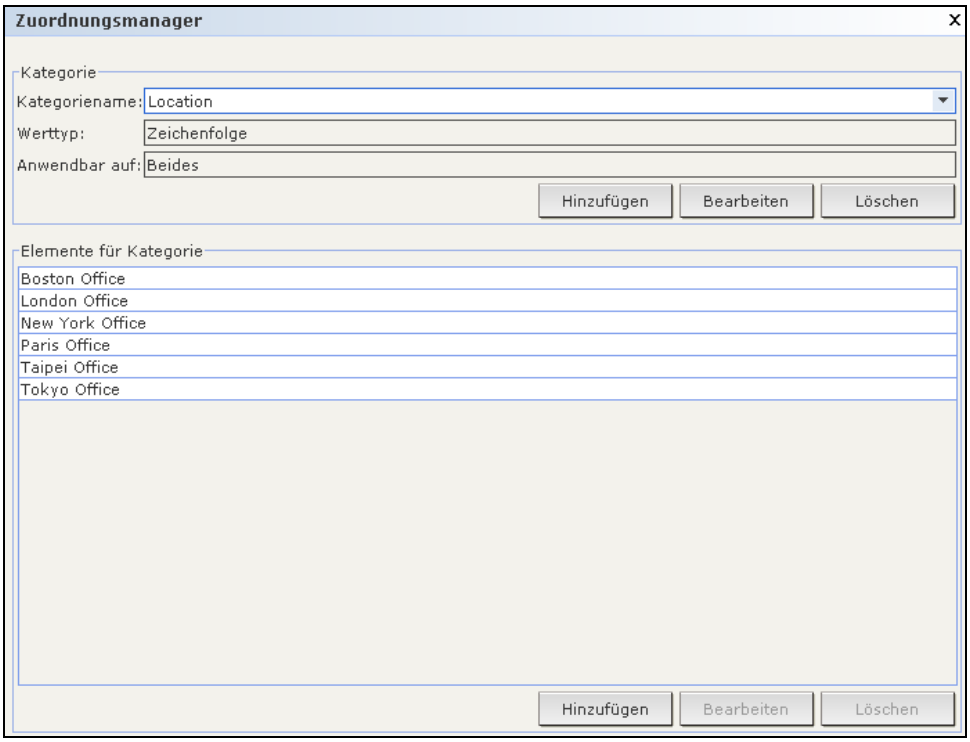


Abbildung 20 Fenster Zuordnungsmanager

2. Klicken Sie im Fensterbereich **Kategorie** auf **Hinzufügen**, um eine neue Kategorie hinzuzufügen. Das Fenster **Kategorie hinzufügen** wird angezeigt.

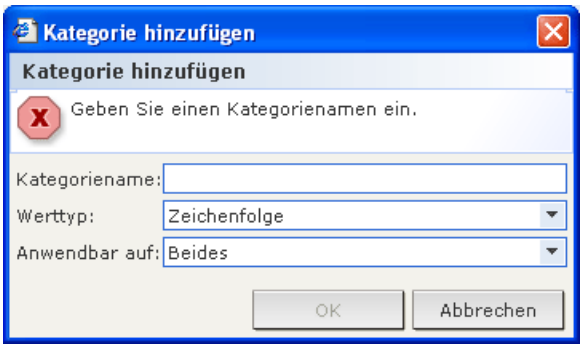


Abbildung 21 Fenster Kategorie hinzufügen

3. Geben Sie im Feld **Kategoriename** einen Kategorienamen ein. Der Name darf aus maximal 31 Zeichen bestehen.
4. Klicken Sie auf die Dropdown-Liste **Werttyp**, und wählen Sie den Werttyp **Zeichenfolge** oder **Ganze Zahl**.
5. Klicken Sie auf die Dropdown-Liste **Anwendbar auf**, und wählen Sie den Gerätetyp, auf den diese Kategorie angewendet werden soll: **Gerät**, **Knoten** oder **Beides**.
6. Klicken Sie zum Erstellen der neuen Kategorie auf **OK**, oder klicken Sie auf **Abbrechen**, um den Vorgang ohne Erstellen der Kategorie abzubrechen. Der neue Kategoriename wird im Feld **Kategoriename** angezeigt.

Kategorie bearbeiten

1. Klicken Sie im Menü **Zuordnungen** auf **Zuordnung**. Das Fenster **Zuordnungsmanager** wird angezeigt.
2. Klicken Sie auf die Dropdown-Liste **Kategoriename**, und wählen Sie die zu bearbeitende Kategorie aus.
3. Klicken Sie im Fensterbereich **Kategorie** auf **Bearbeiten**, um die Kategorie zu bearbeiten. Das Fenster **Kategorie bearbeiten** wird angezeigt.

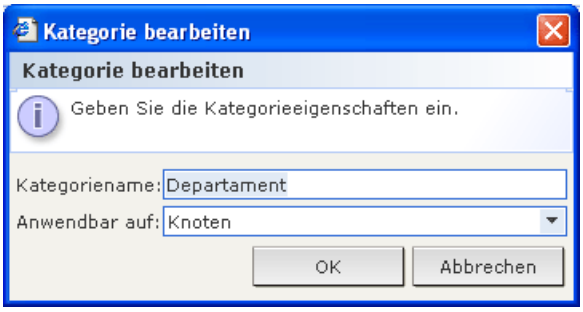


Abbildung 22 Fenster Kategorie bearbeiten

4. Geben Sie den neuen Kategorienamen im Feld **Kategoriename** ein.
5. Klicken Sie auf die Dropdown-Liste **Anwendbar auf**, um diese Kategorie auf **Geräte**, **Knoten** oder **Beides** anzuwenden. Ein Zeichenkettenwert kann nicht in einen Ganzzahlwert geändert werden, und umgekehrt. Wenn Sie diese Änderung vornehmen müssen, löschen Sie die Kategorie, und fügen Sie eine neue Kategorie hinzu.
6. Klicken Sie zum Speichern der Änderungen auf **OK**. Der aktualisierte Kategoriename wird im Feld **Kategoriename** angezeigt.

Kategorie löschen

Durch das Löschen einer Kategorie werden alle in dieser Kategorie erstellten Elemente gelöscht. Die gelöschte Kategorie wird in der Knoten- oder Gerätestrukturansicht nicht mehr angezeigt, sobald das Fenster aktualisiert wird oder der Benutzer sich in CC-SG ab- und wieder anmeldet.

1. Klicken Sie im Menü **Zuordnungen** auf **Zuordnung**. Das Fenster **Zuordnungsmanager** wird angezeigt.
2. Klicken Sie auf die Dropdown-Liste **Kategoriename**, und wählen Sie die zu löschende Kategorie aus.
3. Klicken Sie im Fensterbereich **Kategorie** auf **Löschen**, um die Kategorie zu löschen. Das Fenster **Kategorie löschen** wird angezeigt.

Abbildung 23 Fenster Kategorie löschen

4. Klicken Sie auf **Ja**, um die Kategorie zu löschen.

Element hinzufügen

1. Klicken Sie im Menü **Zuordnungen** auf **Zuordnung**. Das Fenster **Zuordnungsmanager** wird angezeigt.

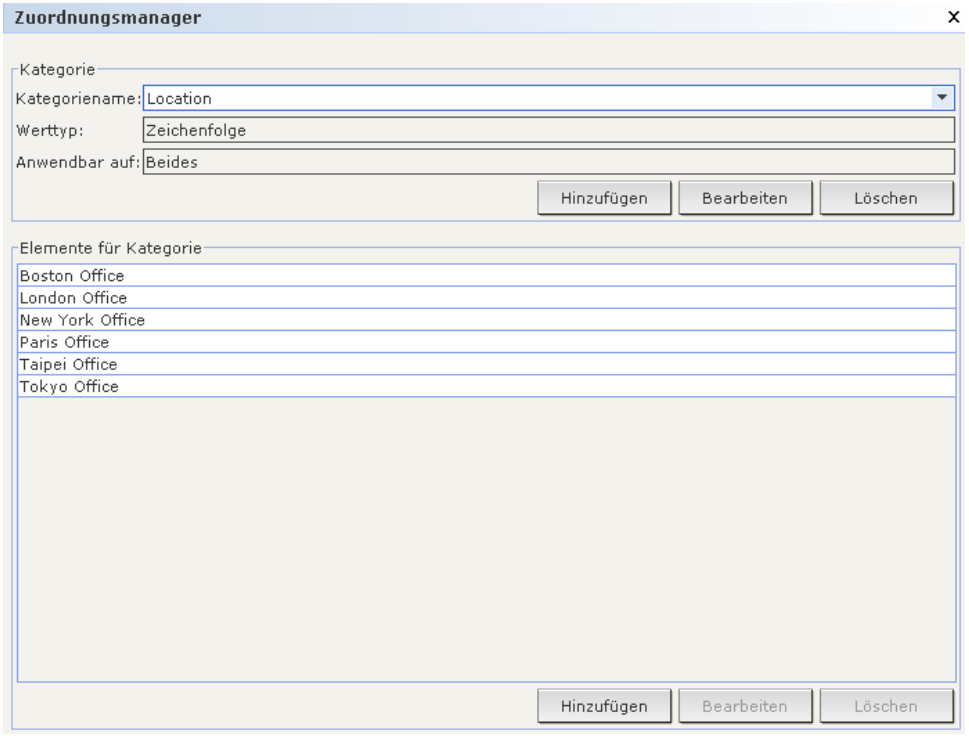


Abbildung 24 Fenster Zuordnungsmanager

2. Klicken Sie auf die Dropdown-Liste **Kategoriename**, und wählen Sie die Kategorie aus, der Sie ein neues Element hinzufügen möchten.

3. Klicken Sie im Fensterbereich **Elemente für Kategorie** auf **Hinzufügen**, um ein neues Element hinzuzufügen. Das Fenster **Element hinzufügen** wird angezeigt.

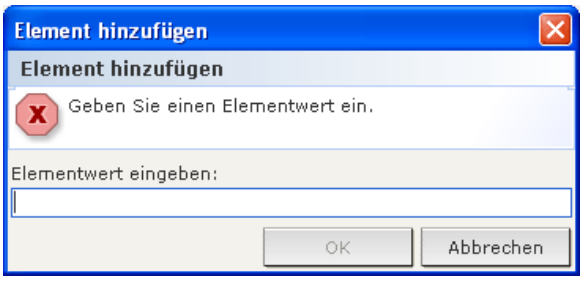


Abbildung 25 Fenster Element hinzufügen

4. Geben Sie den neuen Elementnamen im Feld **Elementwert eingeben** ein.
5. Klicken Sie zum Hinzufügen des Elements auf **OK**, oder klicken Sie auf **Abbrechen**, um das Fenster zu schließen. Das neue Element wird im Fensterbereich **Elemente für Kategorie** angezeigt.

Element bearbeiten

1. Klicken Sie im Menü **Zuordnungen** auf **Zuordnung**. Das Fenster **Zuordnungsmanager** wird angezeigt.
2. Klicken Sie auf die Dropdown-Liste **Kategoriename**, und wählen Sie die Kategorie zum Bearbeiten des Elements aus.
3. Wählen Sie in der Liste **Elemente für Kategorie** das zu bearbeitende Element aus, und klicken Sie im Fensterbereich **Elemente für Kategorie** auf **Bearbeiten**. Das Fenster **Element bearbeiten** wird angezeigt.

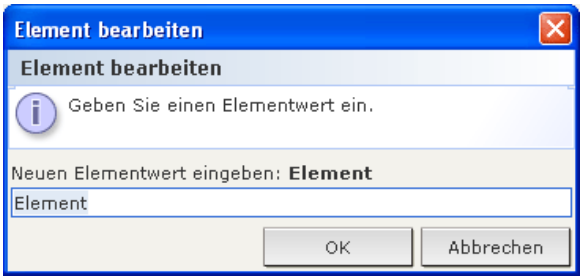


Abbildung 26 Fenster Element bearbeiten

4. Geben Sie den neuen Namen des Elements im Feld **Neuen Elementwert eingeben** ein.
5. Klicken Sie zum Aktualisieren des Elements auf **OK**, oder klicken Sie auf **Abbrechen**, um das Fenster zu schließen. Der neue Elementname wird in der Liste **Elemente für Kategorie** angezeigt.

Element löschen

Durch das Löschen eines Elements wird das Element aus allen Zuordnungen entfernt, und die Zuordnungsfelder sind leer.

1. Klicken Sie im Menü **Zuordnungen** auf **Zuordnung**. Das Fenster **Zuordnungsmanager** wird angezeigt.
2. Klicken Sie auf die Dropdown-Liste **Kategoriename**, und wählen Sie die Kategorie zum Löschen des Elements aus.

3. Wählen Sie in der Liste **Elemente für Kategorie** das zu löschende Element aus, und klicken Sie im Fensterbereich **Elemente für Kategorie** auf **Löschen**. Das Fenster **Element löschen** wird angezeigt.

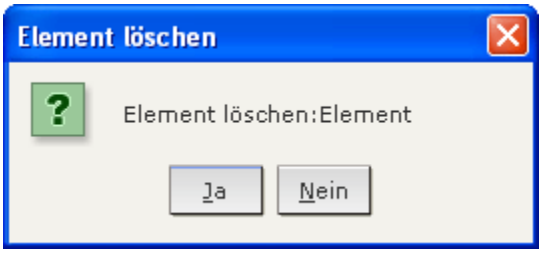


Abbildung 27 Fenster Element löschen

4. Klicken Sie zum Löschen des Elements auf **Ja**, oder klicken Sie auf **Nein**, um das Fenster zu schließen. Der Elementname wird aus der Liste **Elemente für Kategorie** entfernt.

***Hinweis**: Durch das Löschen eines Elements wird das Element aus allen Geräte- und Knotenkategoriezuordnungen entfernt, und alle vorher zugeordneten Elementfelder sind leer.*

Diese Seite wurde absichtlich leer gelassen.

Kapitel 5: Hinzufügen von Geräten und Gerätegruppen

Sie müssen Raritan-Geräte wie Dominion-Geräte und IP-Reach-Geräte zu CC-SG hinzufügen, bevor Sie CC-SG zur Konfiguration und Verwaltung verwenden können. Im Menü **Geräte** finden Sie alle Funktionen für Geräte und Ports. Sie können auch auf einige Funktionen zugreifen, indem Sie auf der Registerkarte **Geräte** mit der rechten Maustaste auf ein Gerät oder einen Port klicken, um das Kontextmenü mit Funktionen anzuzeigen.

***Hinweis**: Verwenden Sie zur Konfiguration von iLO/RILOE-Geräten, IPMI-Geräten, Dell DRAC-Geräten, IBM RSA-Geräten oder anderen „generischen“ Geräten das Menü **Knoten hinzufügen**, und fügen Sie diese Elemente als Verbindungsschnittstelle hinzu. Weitere Informationen finden Sie in **Kapitel 6: Konfigurieren von Knoten und Schnittstellen**.*

Die Registerkarte Geräte

Klicken Sie auf die Registerkarte **Geräte**, um die Strukturansicht **Geräte** anzuzeigen.

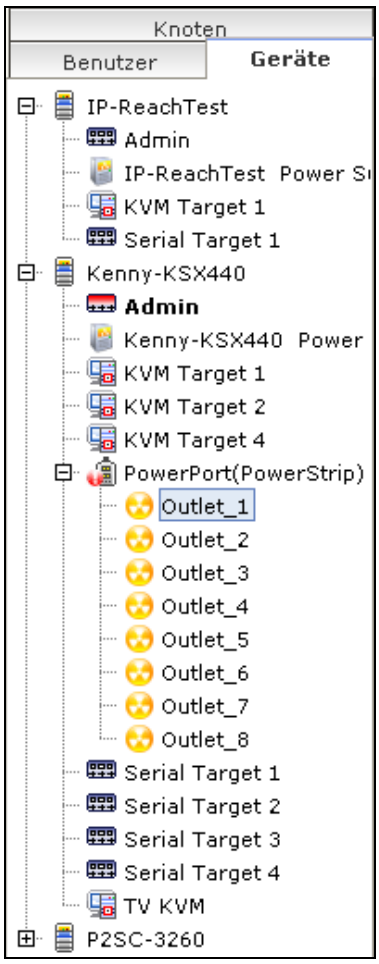


Abbildung 28 Gerätestruktur

Auf der Registerkarte **Geräte** werden Geräte und die entsprechenden konfigurierten Ports angezeigt. Ports werden unter den Geräten aufgeführt, denen sie zugewiesen sind. Geräte mit konfigurierten Ports werden in der Liste mit einem Pluszeichen (+) angezeigt. Klicken Sie auf das Pluszeichen (+), um die Portliste ein- oder auszublenden.

Geräte- und Portsymbole

Die KVM-, Stromversorgungs- und seriellen Geräte und Ports werden zur einfacheren Unterscheidung in der Gerätestrukturansicht durch unterschiedliche Symbole gekennzeichnet. Bewegen Sie den Mauszeiger auf ein Symbol in der Gerätestruktur, um einen Tooltip mit Informationen zum Gerät oder Port anzuzeigen.

SYMBOL	BEDEUTUNG
	Gerät verfügbar
	KVM-Port verfügbar oder verbunden
	KVM-Port inaktiv
	Serieller Port verfügbar
	Serieller Port nicht verfügbar
	Gerät wurde angehalten
	Gerät nicht verfügbar
	Powerstrip
	Ausgangsport

Wenn Sie auf der Registerkarte **Geräte** auf ein Gerät klicken, wird das Fenster **Geräteprofil** mit Informationen zum ausgewählten Gerät angezeigt.

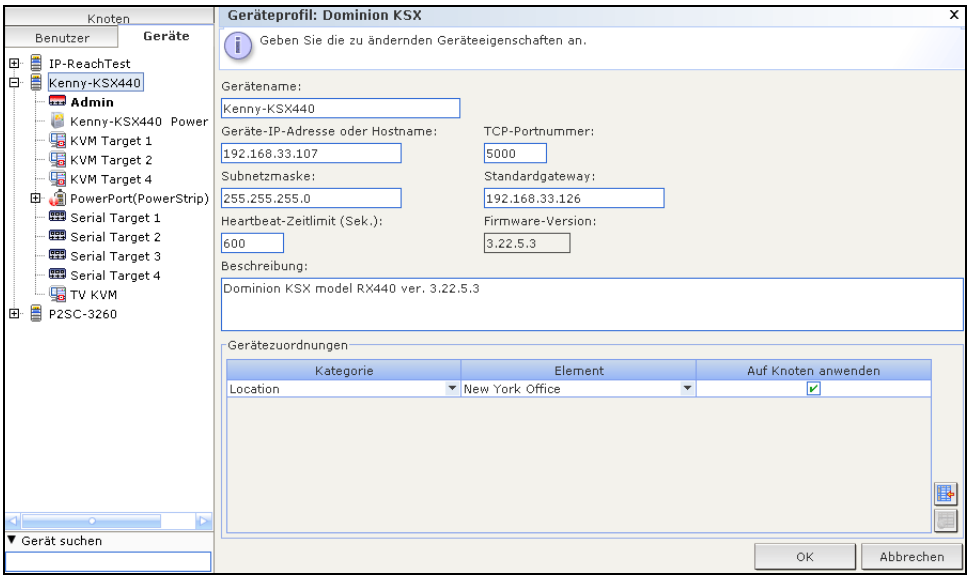


Abbildung 29 Registerkarte Geräte und Geräteprofil

Geräte suchen

Mithilfe der Registerkarte **Geräte** können Sie in der Struktur nach Geräten suchen. Die Suche zeigt Geräte nur als Ergebnisse ohne Portnamen an. Die Suche kann im Fenster **Mein Profil** konfiguriert werden. Weitere Informationen finden Sie in **Kapitel 7: Hinzufügen und Verwalten von Benutzern und Benutzergruppen**.

Geben Sie zur Suche nach einem Gerät unten in der Gerätestruktur in das Feld **Gerät suchen** einen Suchbegriff ein, und drücken Sie die **Eingabetaste**. Die Suchfunktion unterstützt Platzhalter:

PLATZHALTER	BESCHREIBUNG
?	Beliebiges Zeichen
[-]	Zeichen in einem Bereich
*	Kein oder mehrere Zeichen

Beispiel:

BEISPIEL	BESCHREIBUNG
KX?	Sucht nach **KX1** und **KXZ**, aber nicht nach **KX1Z**.
KX*	Sucht nach **KX1**, **KX**, **KXZ** und **KX1Z**.
KX[0-9][0-9]T	Sucht nach **KX95T**, **KX66T**, aber nicht nach **KXZ** und **KX5PT**.

Wichtig! Viele der Befehle in der Menüleiste können aufgerufen werden, indem Sie in der Gerätestruktur mit der rechten Maustaste auf ein Gerät oder einen Port klicken und aus dem angezeigten Kontextmenü einen Befehl auswählen.

Geräte hinzufügen

Sie müssen CC-SG Geräte hinzufügen, bevor Sie Ports konfigurieren oder Knoten über diese Ports Out-of-Band-Schnittstellen hinzufügen können. **Gerät hinzufügen** wird verwendet, um ein Gerät hinzuzufügen, dessen Eigenschaften Sie kennen und für CC-SG bereitstellen können.

So fügen Sie CC-SG ein Gerät hinzu:

1. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Gerät hinzufügen**. Das Fenster **Gerät hinzufügen** wird angezeigt.

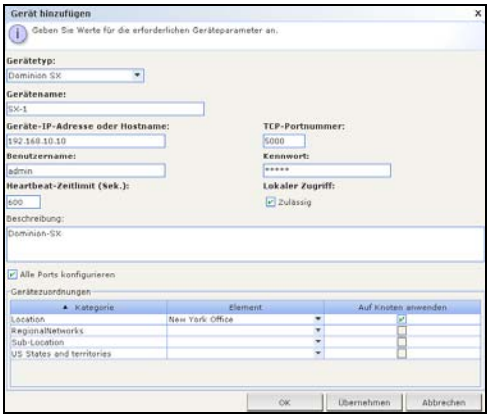


Abbildung 30 Fenster Gerät hinzufügen

2. Klicken Sie auf die Dropdown-Liste **Gerätetyp**, und wählen Sie einen Gerätetyp zum Hinzufügen in der Liste aus. Wenn Sie **PowerStrip** auswählen, wird der Bildschirm **Gerät hinzufügen** anders dargestellt.

KVM- oder serielle Geräte hinzufügen

3. Geben Sie den Namen des neuen Geräts im Feld **Gerätename** ein.
4. Geben Sie die IP-Adresse oder den Hostnamen des Geräts im Feld **Geräte-IP oder Hostname** ein. Die Regeln zur Vergabe von Hostnamen sind unter **Terminologie/Abkürzungen** in **Kapitel 1: Einleitung** beschrieben.
5. Geben Sie in das Feld **TCP-Portnummer** den TCP-Kommunikationsport ein, der zur Kommunikation mit dem Gerät verwendet wird. Die Standardportnummer der meisten Raritan-Geräte lautet 5000.
6. Geben Sie den für die Anmeldung verwendeten Benutzernamen im Feld **Benutzername** ein. Wenn Sie die Anweisungen im Handbuch **Digitales Lösungskonzept von Raritan – Implementierungshandbuch** befolgt haben, um Ihr Gerät zum Hinzufügen zu CC-SG vorzubereiten, geben Sie den Benutzernamen für den CC-SG-Administratorbenutzer ein, den Sie für das Gerät konfiguriert haben.
7. Geben Sie das für den Zugriff auf dieses Gerät erforderliche Kennwort im Feld **Kennwort** ein. Wenn Sie die Anweisungen im Handbuch **Digitales Lösungskonzept von Raritan – Implementierungshandbuch** befolgt haben, um Ihr Gerät zum Hinzufügen zu CC-SG vorzubereiten, geben Sie das Kennwort für den CC-SG-Administratorbenutzer ein, das Sie für das Gerät konfiguriert haben.
8. Geben Sie im Feld **Heartbeat-Timeout (Sek.)** die Zeit (in Sekunden) ein, die verstreichen soll, bevor zwischen dem neuen Gerät und CC-SG ein Zeitüberschreitungsfehler auftritt.
9. Markieren Sie bei Bedarf **Zulässig** unter **Lokaler Zugriff**, wenn Benutzer direkten Zugriff auf dieses Gerät haben sollen, während es von CC-SG verwaltet wird.
10. Sie können auch eine kurze Beschreibung für das Gerät in das Feld **Beschreibung** eingeben.
11. Markieren Sie das Kontrollkästchen **Alle Ports konfigurieren**, wenn alle Ports dieses Geräts automatisch der Registerkarte **Geräte** hinzugefügt werden sollen und ein Knoten für jeden Port dieses Geräts auf der Registerkarte **Knoten** erstellt werden soll. Entsprechende Knoten und Ports werden mit übereinstimmenden Namen konfiguriert. Ist das Kontrollkästchen beim Hinzufügen des Geräts aktiviert, wird ein neuer Knoten für jeden Port und eine Out-of-Band-Schnittstelle für diesen Knoten erstellt.

12. Sie können eine Liste der **Kategorien** und **Elemente** konfigurieren, um dieses Gerät und die damit verbundenen Knoten besser beschreiben und verwalten zu können. Weitere Informationen finden Sie in **Kapitel 4: Erstellen von Zuordnungen**.
    So konfigurieren Sie **Kategorien** und **Elemente**:
    a. Klicken Sie für jede aufgeführte **Kategorie** auf das Dropdown-Menü **Element**. Wählen Sie dann das Element zum Anwenden auf das Gerät in der Liste aus. Wählen Sie das leere Element im Feld **Element** für jede Kategorie aus, die Sie nicht verwenden möchten.
    b. Wenn Sie das Element verknüpften Knoten und Geräten zuweisen möchten, markieren Sie das Kontrollkästchen **Auf Knoten anwenden**.

    Wenn die Werte für **Kategorie** oder **Element**, die Sie verwenden möchten, nicht angezeigt werden, können Sie über das Menü **Zuordnungen** weitere hinzufügen. Weitere Informationen finden Sie in **Kapitel 4: Erstellen von Zuordnungen**.
13. Wenn Sie dieses Gerät konfiguriert haben, klicken Sie auf **Übernehmen**, um dieses Gerät hinzuzufügen und ein neues leeres Fenster **Gerät hinzufügen** anzuzeigen, in dem Sie weitere Geräte hinzufügen können. Oder klicken Sie auf **OK**, um dieses Gerät hinzuzufügen und den Bildschirm **Gerät hinzufügen** nicht anzuzeigen.
14. Ist die Firmwareversion des Geräts nicht mit CC-SG kompatibel, werden Sie darauf hingewiesen und gefragt, ob Sie fortfahren möchten. Klicken Sie auf **Ja**, um das Gerät zu CC-SG hinzuzufügen. Sie können die Firmware des Geräts aktualisieren, nachdem Sie es zu CC-SG hinzugefügt haben. Weitere Informationen finden Sie unter **Geräte aktualisieren** in diesem Kapitel.

PowerStrip-Gerät hinzufügen

Beim Hinzufügen eines PowerStrip-Geräts können Sie CC-SG erlauben, die Ausgänge automatisch zu konfigurieren. Nachdem die Ausgänge konfiguriert wurden, können Sie jeden Ausgang mit dem Knoten verknüpfen, der darüber mit Strom versorgt wird. Fügen Sie dem Knoten dazu eine Stromversorgungs-Schnittstelle hinzu. Weitere Informationen finden Sie in **Kapitel 6: Konfigurieren von Knoten und Schnittstellen**. Sie können auch das automatische Konfigurieren von Ausgängen durch CC-SG untersagen und die Ausgänge später konfigurieren.

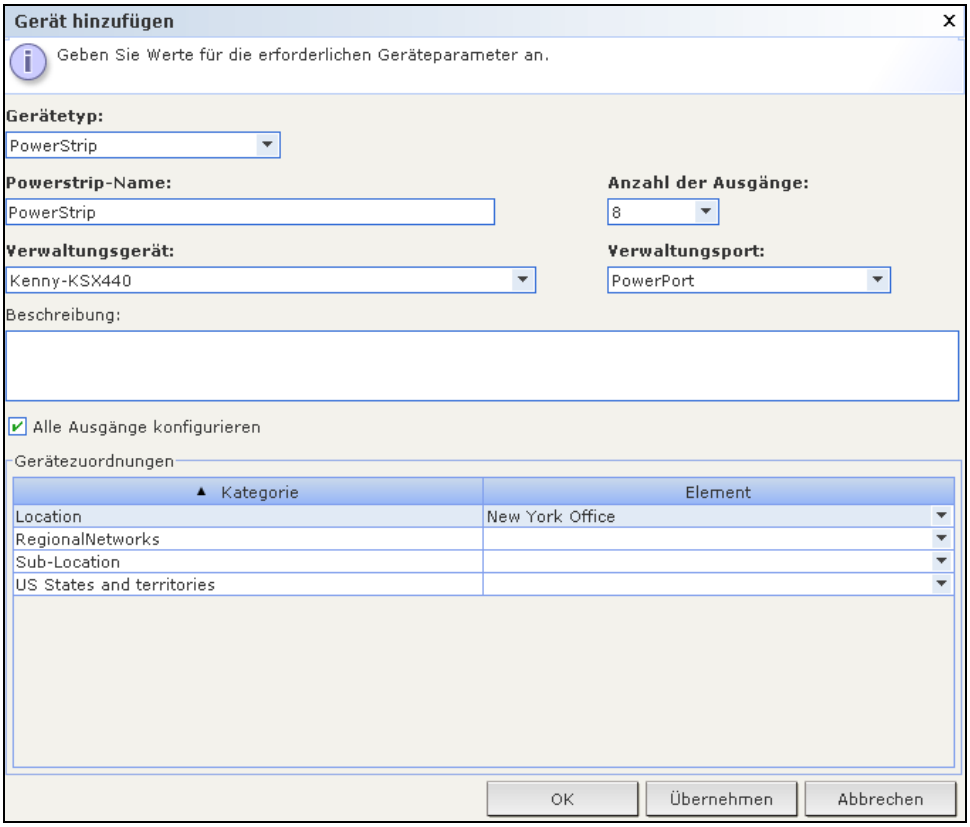


Abbildung 31 PowerStrip-Gerät hinzufügen

3. Geben Sie einen Namen in das Feld **Powerstrip-Name** ein.
4. Klicken Sie auf das Dropdown-Menü **Anzahl der Ausgänge**, und wählen Sie die Anzahl der Ausgänge für den Powerstrip aus.
5. Klicken Sie auf das Dropdown-Menü **Verwaltungsgerät**, und wählen Sie in der Liste das Gerät aus, das Sie zum Verwalten dieses Powerstrip verwenden möchten.
6. Klicken Sie auf das Dropdown-Menü **Verwaltungsport**, und wählen Sie den Port am Verwaltungsgerät aus, mit dem dieser Powerstrip verbunden ist.
7. Sie können auch eine kurze Beschreibung für den Powerstrip in das Feld **Beschreibung** eingeben.
8. Markieren Sie das Kontrollkästchen **Alle Ausgänge konfigurieren**, wenn jeder Ausgang dieses Geräts automatisch zur Registerkarte **Geräte** hinzugefügt werden soll.
9. Sie können eine Liste der **Kategorien** und **Elemente** konfigurieren, um diesen Powerstrip und die damit verbundenen Knoten besser beschreiben und verwalten zu können. Weitere Informationen finden Sie in **Kapitel 4: Erstellen von Zuordnungen**.
    - Klicken Sie für jede aufgeführte **Kategorie** auf das Dropdown-Menü **Element**. Wählen Sie dann das Element zum Anwenden auf das Gerät in der Liste aus. Wählen Sie das leere Element im Feld **Element** für jede Kategorie aus, die Sie nicht verwenden möchten.

    Wenn die Werte für **Kategorie** oder **Element**, die Sie verwenden möchten, nicht angezeigt werden, können Sie über das Menü **Zuordnungen** weitere hinzufügen. Weitere Informationen finden Sie in **Kapitel 4: Erstellen von Zuordnungen**.
10. Wenn Sie dieses Gerät konfiguriert haben, klicken Sie auf **Übernehmen**, um es hinzuzufügen und ein neues leeres Fenster **Gerät hinzufügen** anzuzeigen, in dem Sie weitere Geräte hinzufügen können. Sie können auch auf **OK** klicken, um diesen Powerstrip hinzuzufügen und den Bildschirm **Gerät hinzufügen** nicht anzuzeigen.

Geräte erkennen

Mit **Geräte erkennen** wird eine Suche nach allen Geräten in Ihrem Netzwerk gestartet. Die Suche erkennt automatisch alle neuen und bereits vorhandenen Raritan-Geräte in Ihrem Netzwerk, einschließlich Paragon II Systemcontroller, IP-Reach-, Dominion KX-, Dominion KX101-, Dominion KSX-, Dominion SX- und eRIC-Einheiten. Nach dem Erkennen der Geräte können Sie diese zu CC-SG hinzufügen, falls sie nicht bereits verwaltet werden.

1. Klicken Sie im Menü **Geräte** auf **Geräte erkennen**. Das Fenster **Geräte erkennen** wird angezeigt.

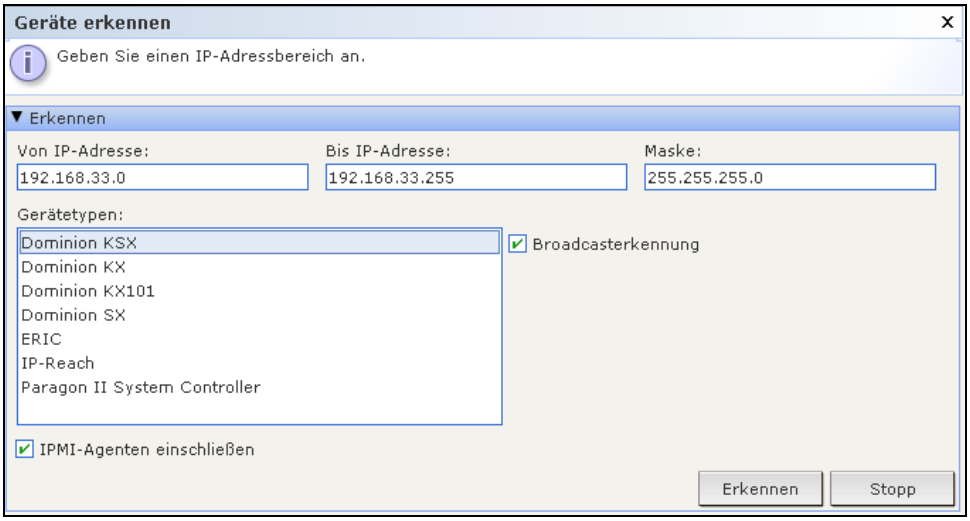


Abbildung 32 Fenster Geräte erkennen

2. Geben Sie in die Felder **Von IP-Adresse** und **Bis IP-Adresse** den Bereich der IP-Adressen ein, in dem sich die Geräte vermutlich befinden. Die Adresse im Feld **Bis IP-Adresse** sollte größer sein als die im Feld **Von IP-Adresse**. Legen Sie eine Maske für den Bereich fest. Wenn Sie keine Maske festlegen, wird die Broadcastadresse **255.255.255.255** gesendet, die an alle lokalen Netzwerke überträgt. Damit Geräte in Subnetzen erkannt werden, muss eine Maske festgelegt werden.

3. Klicken Sie auf **Broadcasterkennung**, wenn Sie nach Geräten im selben Subnetz suchen, in dem sich CC-SG befindet. Deaktivieren Sie **Broadcasterkennung**, wenn Geräte in verschiedenen Subnetzen erkannt werden sollen.
4. Wenn Sie nach einem bestimmten Gerätetyp suchen, können Sie ihn in der Liste **Gerätetypen** markieren. Standardmäßig sind alle Gerätetypen markiert. Klicken Sie bei gedrückter S**trg**-Taste auf einen oder mehrere Gerätetypen, um diese auszuwählen.
5. Markieren Sie das Kontrollkästchen **IPMI-Agenten einschließen**, wenn Sie Ziele suchen möchten, die eine IPMI-Stromversorgungssteuerung bieten.
6. Klicken Sie auf **Erkennen**, um die Suche zu starten. Sie können jederzeit während der Suche auf **Stopp** klicken, um den Suchvorgang abzubrechen. Die erkannten Geräte werden in einer Liste angezeigt.

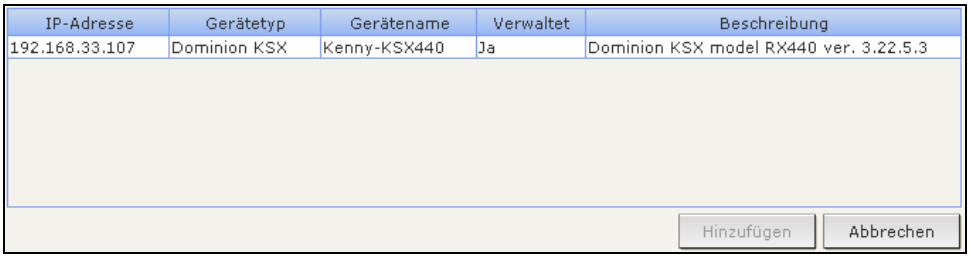


Abbildung 33 Fenster mit der Liste der erkannten Geräte

7. Sie können ein oder mehrere erkannte Geräte zu CC-SG hinzufügen. Wählen Sie dazu die Geräte in der Liste aus, und klicken Sie auf **Hinzufügen**. Der Bildschirm **Gerät hinzufügen** wird angezeigt, und einige Felder sind bereits ausgefüllt. Wenn Sie mehrere Geräte zum Hinzufügen ausgewählt haben, können Sie unten im Bildschirm auf **Zurück** und **Überspringen** klicken, um die Geräte zu suchen, die Sie hinzufügen möchten.

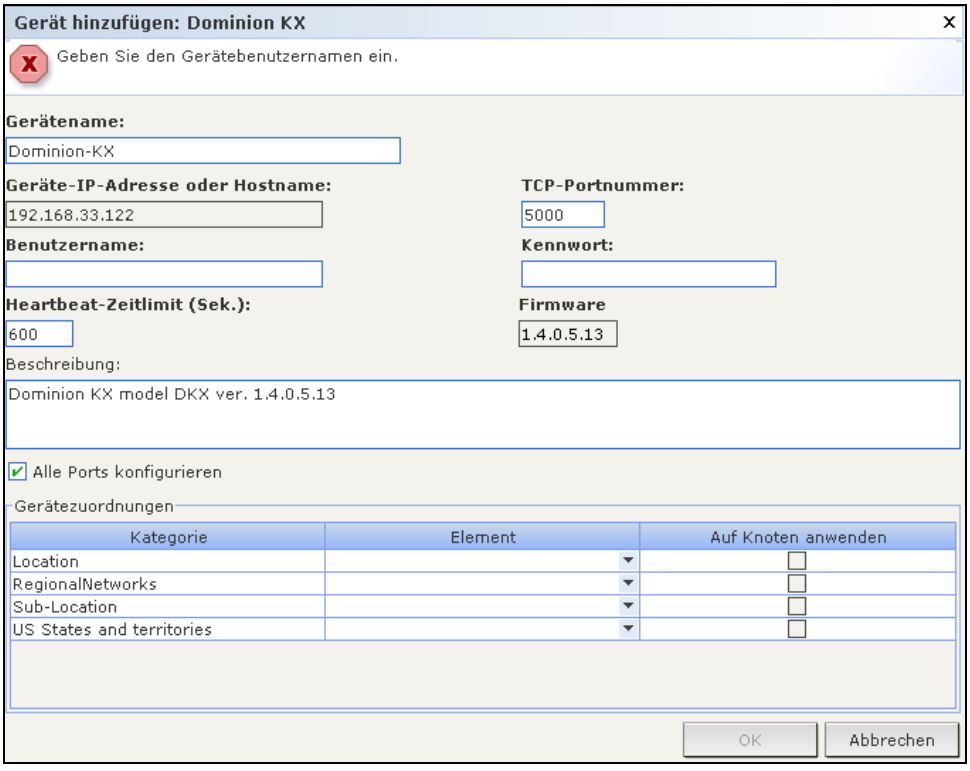


Abbildung 34 Erkannte Geräte hinzufügen

8. Geben Sie den Benutzernamen und das Kennwort (die speziell für CC-SG im Gerät erstellt wurden) in die Felder **Benutzername** und **Kennwort** ein, um eine Authentifizierung des Geräts durch CC-SG für die zukünftige Kommunikation zu ermöglichen. Wählen Sie die **Kategorien** und **Elemente** aus, die Sie auf das Gerät anwenden möchten. Wenn Kategorien und Elemente auch auf die Knoten angewendet werden sollen, die mit dem Gerät verknüpft sind, markieren Sie das entsprechende Kontrollkästchen **Auf Knoten anwenden**.
9. Sie können die folgenden Felder bei Bedarf anpassen: **Gerätename**, **Heartbeat-Timeout**, **Lokaler Zugriff** (falls für Gerätetyp verfügbar), **Beschreibung**, **Alle Ports konfigurieren** und **Gerätezuordnungen**.
10. Wenn Sie die Konfiguration dieses Geräts abgeschlossen haben, klicken Sie auf **Übernehmen**, um das Gerät hinzuzufügen und das Fenster **Gerät hinzufügen** für das nächste erkannte Gerät zu öffnen. Oder klicken Sie auf **OK**, um nur dieses Gerät hinzuzufügen und nicht mit den anderen erkannten Geräten fortzufahren.
11. Ist die Firmwareversion des Geräts nicht mit CC-SG kompatibel, werden Sie darauf hingewiesen und gefragt, ob Sie fortfahren möchten. Klicken Sie auf **Ja**, um CC-SG das Gerät hinzuzufügen, oder klicken Sie auf **Nein**, um den Vorgang abzubrechen. Sie können die Firmware des Geräts aktualisieren, nachdem Sie es zu CC-SG hinzugefügt haben. Weitere Informationen finden Sie unter **Geräte aktualisieren** in diesem Kapitel.

Gerät bearbeiten

Sie können ein Gerät bearbeiten, um es umzubenennen und seine Eigenschaften zu ändern.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät zum Bearbeiten aus. Der Bildschirm **Geräteprofil** wird angezeigt.

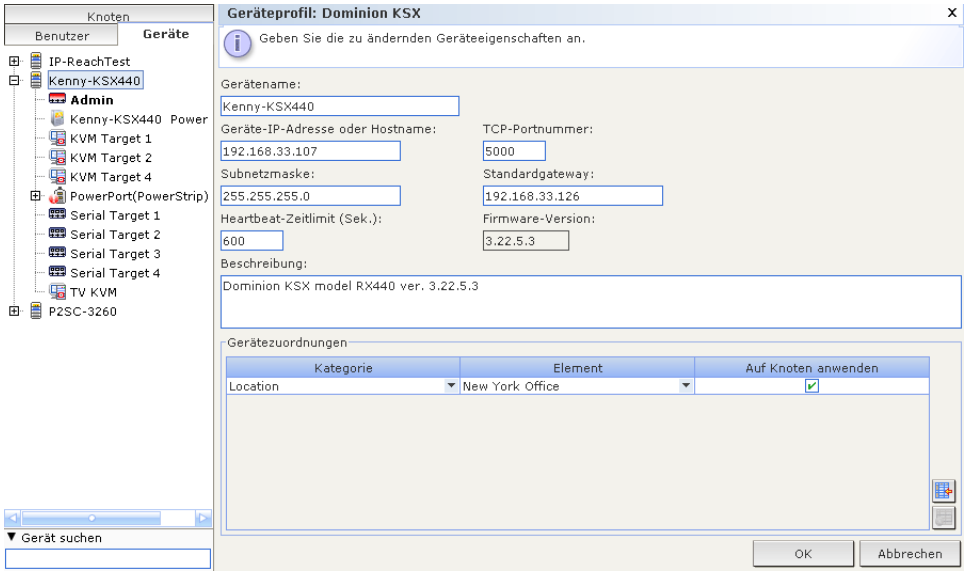


Abbildung 35 Bildschirm Geräteprofil

2. Geben Sie die neuen Geräteeigenschaften in die entsprechenden Felder ein. Bearbeiten Sie bei Bedarf die Kategorien und Elemente, die mit dem Gerät verknüpft sind.
3. Klicken Sie zum Speichern der Änderungen auf **OK**. Das Bearbeiten des Geräts wird durch die Meldung **Gerät wurde erfolgreich aktualisiert** bestätigt.

PowerStrip-Gerät bearbeiten

Sie können ein verwaltetes Powerstrip-Gerät bearbeiten, um es umzubenennen, die Eigenschaften zu ändern und den Status der Ausgangskonfiguration anzuzeigen.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Powerstrip-Gerät zum Bearbeiten aus. Der Bildschirm **Geräteprofil: PowerStrip** wird angezeigt.
2. Geben Sie die neuen Geräteeigenschaften in die entsprechenden Felder ein. Bearbeiten Sie bei Bedarf die Kategorien und Elemente, die mit dem Gerät verknüpft sind.
3. Klicken Sie auf die Registerkarte **Ausgang**, um alle Ausgänge des PowerStrip anzuzeigen.
   - Ist ein Ausgang mit einem Knoten verknüpft, können Sie auf den Hyperlink **Knoten** klicken, um das Knotenprofil anzuzeigen.
   - Ist ein Ausgang mit einem Knoten verknüpft, können Sie den Ausgang auswählen und dann auf **Stromversorgungssteuerung** klicken, um die Stromversorgungssteuerung für den verknüpften Knoten anzuzeigen.
4. Klicken Sie zum Speichern der Änderungen auf **OK**. Das Bearbeiten des Geräts wird durch die Meldung **Gerät wurde erfolgreich aktualisiert** bestätigt.

Gerät löschen

Sie können Geräte löschen, damit sie nicht mehr von CC-SG verwaltet werden.

Wichtig: Wenn Sie ein Gerät löschen, werden alle Ports entfernt, die für das Gerät konfiguriert sind. Alle Schnittstellen, die mit diesen Ports verknüpft sind, werden von den Knoten entfernt. Besteht keine weitere Schnittstelle für diese Knoten, werden die Knoten auch aus CC-SG entfernt.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät zum Löschen aus.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Gerät löschen**. Das Fenster **Gerät löschen** wird angezeigt.

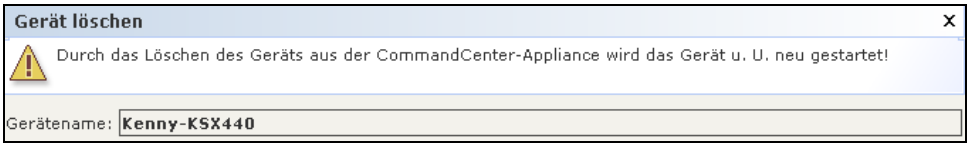


Abbildung 36 Fenster Gerät löschen

3. Klicken Sie zum Löschen des Geräts auf **OK**, oder klicken Sie auf **Abbrechen**, um den Vorgang ohne Löschen abzubrechen. Das Löschen des Geräts wird durch die Meldung **Gerät wurde erfolgreich gelöscht** bestätigt.

Hinweis: *Sie müssen KSX-Geräte zunächst unterbrechen, bevor sie erfolgreich aus CC-SG entfernt werden können. Klicken Sie zum Unterbrechen eines KSX-Geräts auf der Registerkarte* ***Geräte*** *mit der rechten Maustaste auf das Gerät, und klicken Sie dann auf* ***Verwaltung unterbrechen.*** *Klicken Sie in der Bestätigungsnachricht auf* ***Ja.*** *Das KSX-Gerät wird erneut gestartet. Nachdem Sie den Betrieb des Geräts unterbrochen haben, können Sie es in CC-SG löschen.*

Ports konfigurieren

Wenn Sie beim Hinzufügen des Geräts im Bildschirm **Gerät hinzufügen** das Kontrollkästchen **Alle Ports konfigurieren** nicht markiert haben und aus diesem Grund die Ports des Geräts nicht automatisch hinzugefügt werden, können Sie einzelne oder mehrere Ports des Geräts über den Bildschirm **Ports konfigurieren** zu CC-SG hinzufügen. Sie müssen die Ports konfigurieren bevor Out-of-Band-Schnittstellen, die diese Ports verwenden, zu Knoten hinzugefügt werden können.

Seriellen Port konfigurieren

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie ein serielles Gerät in der Gerätestrukturansicht aus.
2. Klicken Sie im Menü **Geräte** auf **Portmanager** und anschließend auf **Ports konfigurieren**. Das Fenster **Ports konfigurieren** wird angezeigt.

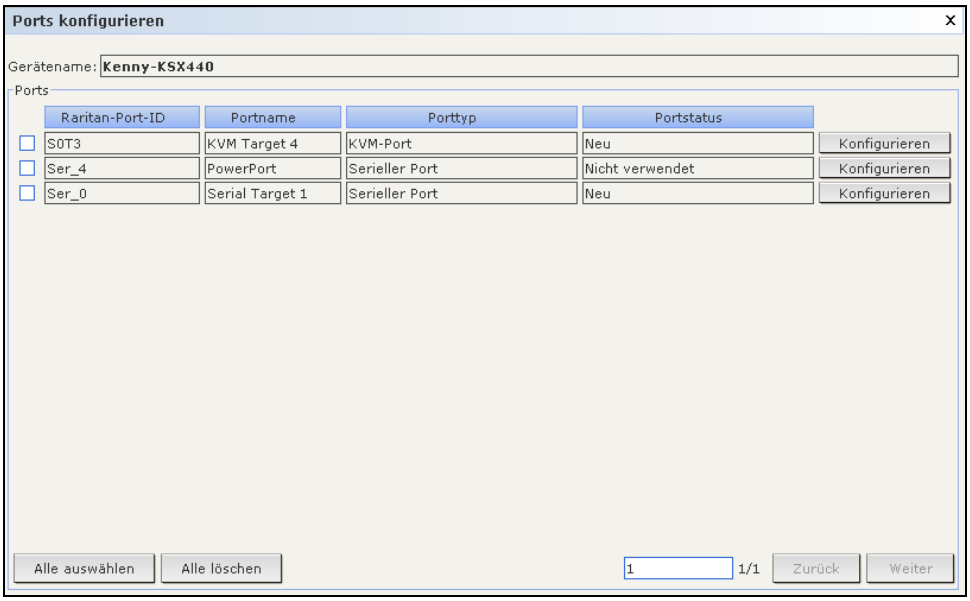


Abbildung 37 Fenster Ports konfigurieren

- Klicken Sie auf eine Spaltenüberschrift, um die Ports in aufsteigender Reihenfolge nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Spaltenüberschrift, um die Ports in absteigender Reihenfolge zu sortieren.

3. Klicken Sie neben dem zu konfigurierenden seriellen Port auf die entsprechende Schaltfläche **Konfigurieren**. Das Fenster **Seriellen Port konfigurieren** wird angezeigt.

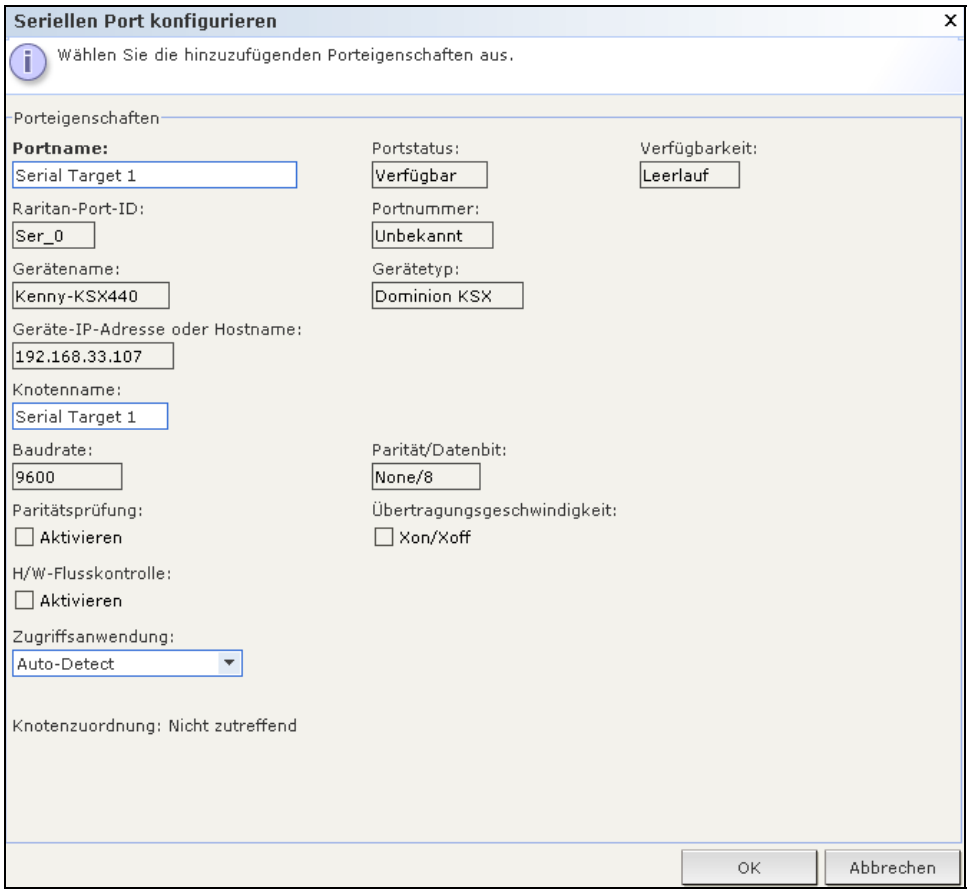


Abbildung 38 Fenster Seriellen Port konfigurieren

4. Geben Sie in das Feld **Portname** einen Portnamen ein. Der Einfachheit halber sollten Sie den Port nach dem mit dem Port verbundenen Ziel benennen.
5. Geben Sie einen Knotennamen in das Feld **Knotenname** ein, um einen neuen Knoten mit einer Out-of-Band-Schnittstelle über diesen Port zu erstellen. Der Einfachheit halber sollten Sie den Knoten nach dem mit dem Port verbundenen Ziel benennen. Sie geben also denselben Namen in die Felder **Portname** und **Knotenname** ein.
6. Klicken Sie auf das Dropdown-Menü **Zugriffsanwendung**, und wählen Sie die Anwendung aus, die Sie beim Verbinden mit dem Port über die Liste verwenden möchten. CC-SG wählt die entsprechende Anwendung basierend auf Ihrem Browser automatisch aus, wenn Sie **Automatisch erkennen** markieren.
7. Klicken Sie zum Hinzufügen des Ports auf **OK**.

KVM-Port konfigurieren

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie ein KVM-Gerät in der Gerätestrukturansicht aus.
2. Klicken Sie im Menü **Geräte** auf **Portmanager** und anschließend auf **Ports konfigurieren**. Das Fenster **Ports konfigurieren** wird angezeigt.

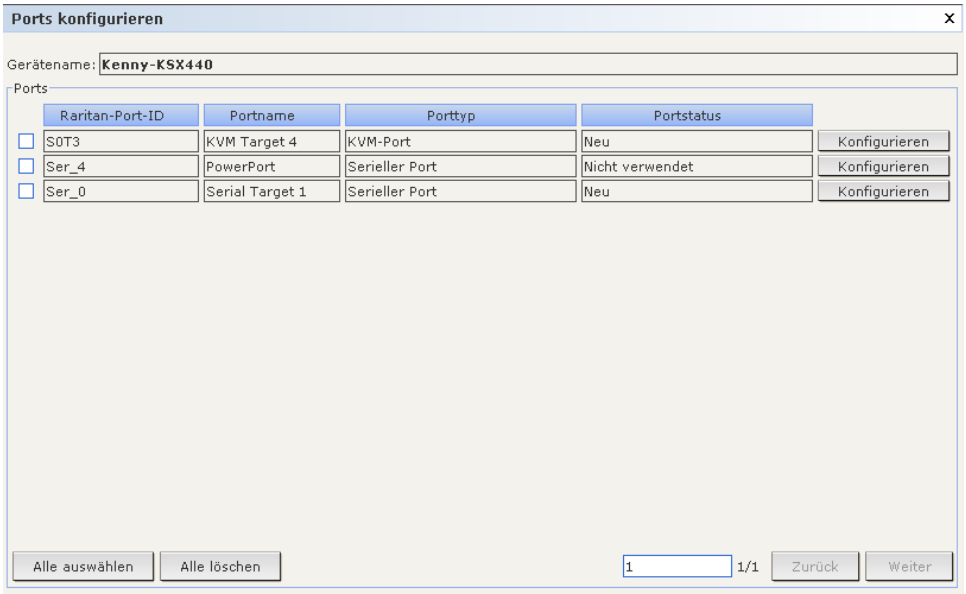


Abbildung 39 Fenster Ports konfigurieren

- Klicken Sie auf eine Spaltenüberschrift, um die Ports in aufsteigender Reihenfolge nach diesem Attribut zu sortieren. Klicken Sie erneut auf die Spaltenüberschrift, um die Ports in absteigender Reihenfolge zu sortieren.

3. Klicken Sie neben dem zu konfigurierenden KVM-Port auf die entsprechende Schaltfläche **Konfigurieren**. Das Fenster **KVM-Port konfigurieren** wird angezeigt.

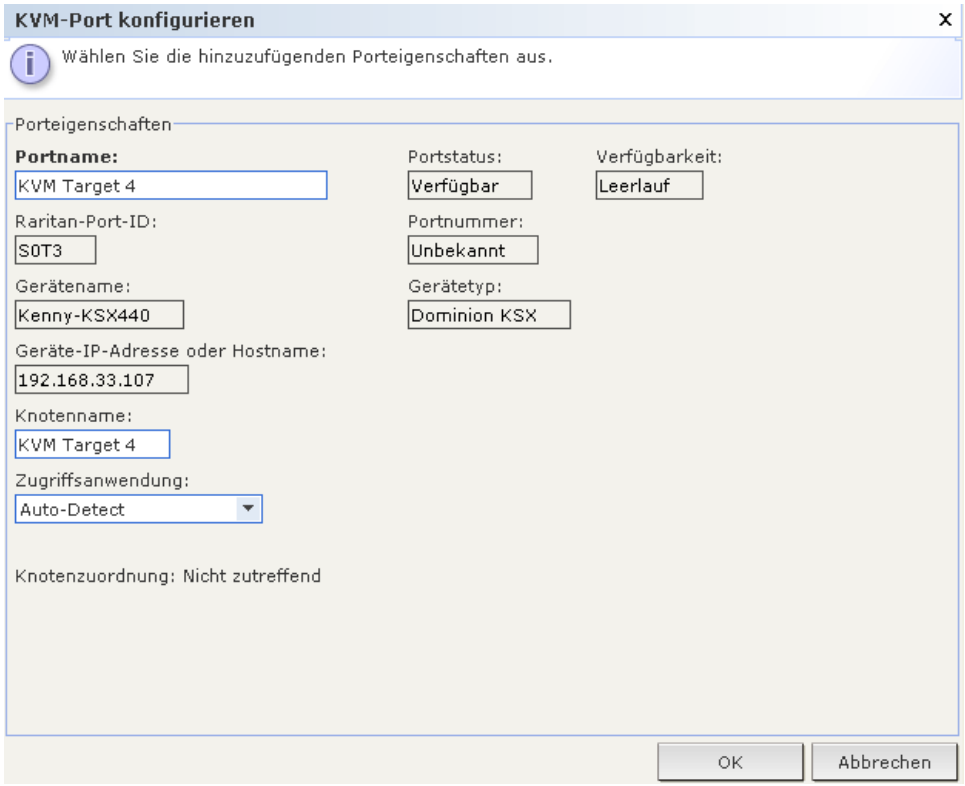


Abbildung 40 Fenster KVM-Port konfigurieren

4. Geben Sie in das Feld **Portname** einen Portnamen ein. Der Einfachheit halber sollten Sie den Port nach dem mit dem Port verbundenen Ziel benennen.
5. Geben Sie einen Knotennamen in das Feld **Knotenname** ein, um einen neuen Knoten mit einer Out-of-Band-Schnittstelle über diesen Port zu erstellen. Der Einfachheit halber sollten Sie den Knoten nach dem mit dem Port verbundenen Ziel benennen. Sie geben also denselben Namen in die Felder **Portname** und **Knotenname** ein.
6. Klicken Sie auf das Dropdown-Menü **Zugriffsanwendung**, und wählen Sie die Anwendung aus, die Sie beim Verbinden mit dem Port über die Liste verwenden möchten. CC-SG wählt die entsprechende Anwendung basierend auf Ihrem Browser automatisch aus, wenn Sie **Automatisch erkennen** markieren.
7. Klicken Sie zum Hinzufügen des Ports auf **OK**.

Ports bearbeiten

Sie können Ports bearbeiten, um den Namen oder die Zugriffsanwendung zu ändern, die mit vorhandenen, konfigurierten Ports verknüpft ist.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie den Port zum Bearbeiten aus. Der Bildschirm für Portprofile wird angezeigt.

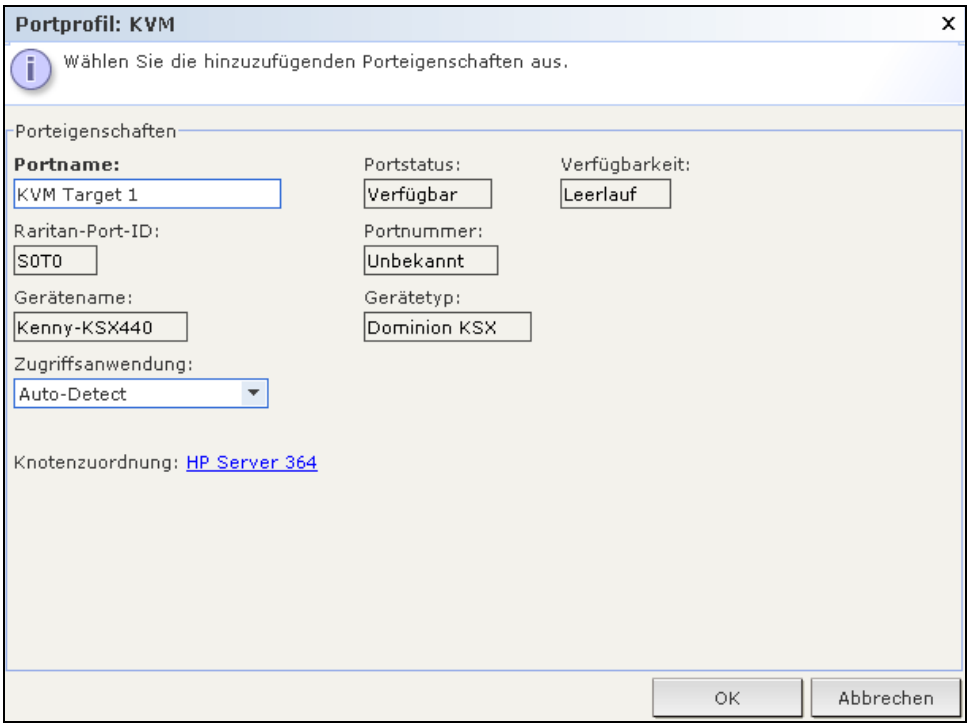


Abbildung 41 Portprofil

2. Geben Sie bei Bedarf einen neuen Portnamen in das Feld **Portname** ein.
3. Klicken Sie auf das Dropdown-Menü **Zugriffsanwendung**, und wählen Sie die Anwendung aus, die Sie beim Verbinden mit dem Port über die Liste verwenden möchten. CC-SG wählt die entsprechende Anwendung basierend auf Ihrem Browser automatisch aus, wenn Sie **Automatisch erkennen** markieren.
4. Klicken Sie auf **OK**, um die Änderungen am konfigurierten Port zu speichern.

Ports löschen

Löschen Sie Ports, um den Porteintrag aus einem Gerät zu löschen.

Wichtig: Wenn Sie einen Port löschen, der mit einem Knoten verbunden ist, wird die verknüpfte Out-of-Band-KVM- oder serielle Schnittstelle, die vom Port bereitgestellt wird, aus dem Knoten entfernt. Verfügt der Knoten über keine weiteren Schnittstellen, wird der Knoten auch aus CC-SG entfernt.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät aus, dessen Ports Sie löschen möchten.
2. Klicken Sie im Menü **Geräte** auf **Portmanager** und anschließend auf **Ports löschen**. Das Fenster **Ports löschen** wird angezeigt.

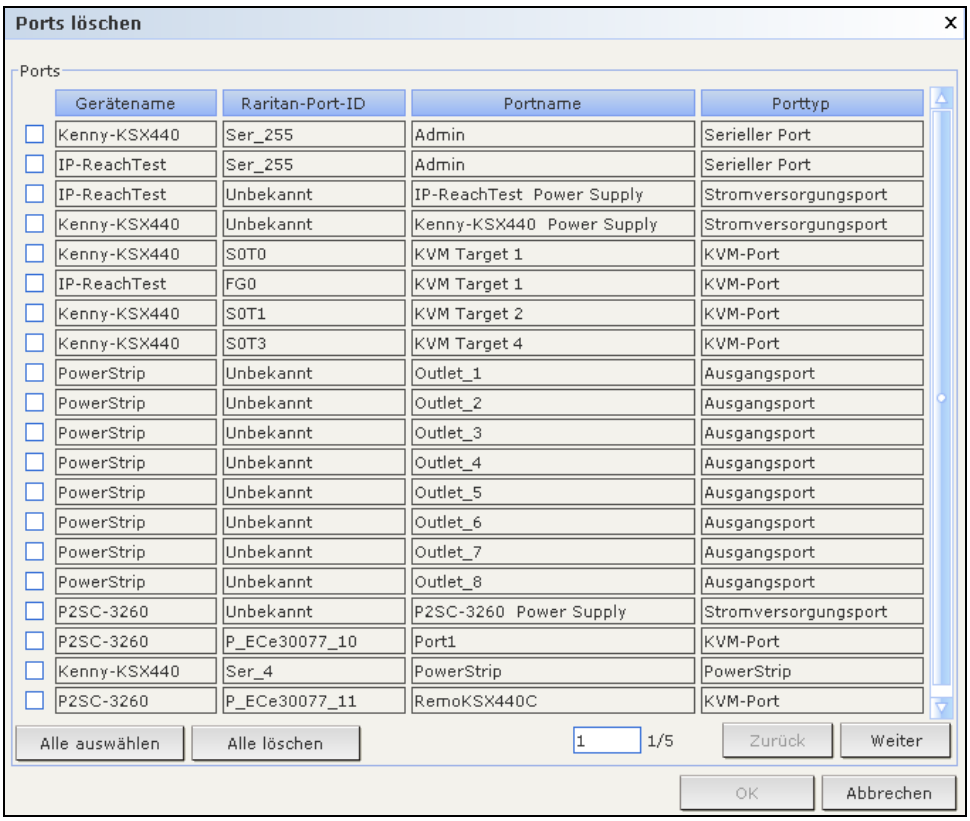


Abbildung 42 Fenster Ports löschen

3. Markieren Sie jeweils die Ports, die Sie aus dem Gerät löschen möchten.
4. Klicken Sie zum Löschen eines Ports auf **OK**. Das Löschen des Ports wird durch das Fenster **Port wurde erfolgreich gelöscht** bestätigt.

Geräteverwaltung

Nachdem ein Gerät zu CC-SG hinzugefügt wurde, können verschiedene Verwaltungsfunktionen neben der Konfiguration von Ports durchgeführt werden.

Massenkopieren für Gerätekategorien und -elemente

Mit dem Befehl **Massenkopieren** können Sie die einem Gerät zugeordneten Kategorien und Elemente auf mehrere andere Geräte mittels Kopieren übertragen. Die Kategorien und Elemente sind die einzigen bei diesem Vorgang kopierten Eigenschaften.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie in der Gerätestrukturansicht ein Gerät aus.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Massenkopieren**. Das Fenster **Massenkopieren** wird angezeigt.

3. Wählen Sie in der Liste **Alle Geräte** die Geräte aus, auf die Sie die Kategorien und Elemente des in das Feld **Gerätename** angezeigten Geräts kopieren möchten.
4. Klicken Sie auf > (Pfeil nach rechts), um der Liste **Ausgewählte Geräte** ein Gerät hinzuzufügen.
5. Wählen Sie zum Entfernen eines Geräts aus der Liste **Ausgewählte Geräte** das Gerät aus, und klicken Sie auf < (Pfeil nach links).
6. Klicken Sie zum Massenkopieren auf **OK**, oder klicken Sie auf **Abbrechen**, um den Vorgang ohne Kopieren abzubrechen. Das Kopieren der Gerätekategorien und Geräteelemente wird durch die Meldung **Gerät wurde erfolgreich kopiert** bestätigt.

Gerät aktualisieren

Über **Gerät aktualisieren** können Sie neue Versionen der Gerätefirmware herunterladen.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie in der Gerätestrukturansicht ein Gerät aus.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Gerät aktualisieren**. Das Fenster **Gerät aktualisieren** wird angezeigt.

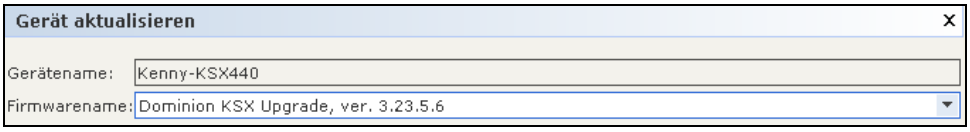


Abbildung 43 Fenster Gerät aktualisieren

3. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Firmwarename**, und wählen Sie die entsprechende Firmware in der Liste aus. Diese Informationen werden von Raritan oder Ihrem Händler bereitgestellt.
4. Klicken Sie zum Aktualisieren des Geräts auf **OK**. Das Aktualisieren von SX- und KX-Geräten dauert ca. 20 Minuten.

   Ist die Firmwareversion des Geräts nicht mit CC-SG kompatibel, werden Sie darauf hingewiesen und gefragt, ob Sie fortfahren möchten. Weitere Informationen finden Sie in **Kapitel 2: Zugreifen auf CC-SG**. Klicken Sie zum Aktualisieren des Geräts auf **Ja**.
5. Eine Meldung zum **Neustart** wird angezeigt. Klicken Sie zum Neustarten des Geräts auf **Ja**.
6. Das Aktualisieren des Geräts wird durch die Meldung **Gerät wurde erfolgreich aktualisiert** bestätigt.

Gerätekonfiguration sichern

Sie können alle Benutzerdateien zur Konfiguration und Systemkonfiguration für ein ausgewähltes Gerät sichern. Falls Probleme bei Ihrem Gerät auftreten, können Sie die vorherige Konfiguration von CC-SG mithilfe der erstellten Sicherungsdatei wieder herstellen.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät zum Sichern aus.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager**, **Konfiguration** und anschließend auf **Sicherungsknoten**. Das Fenster **Gerätekonfiguration sichern** wird angezeigt.

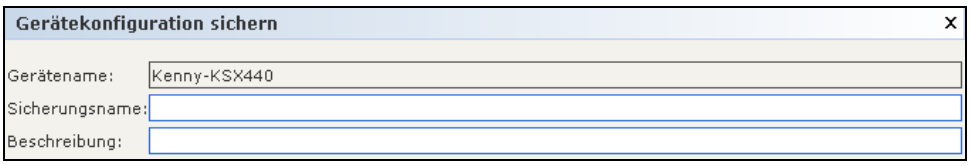


Abbildung 44 Fenster Gerätekonfiguration sichern

3. Geben Sie einen Namen für diese Sicherung in das Feld **Sicherungsname** ein.
4. Sie können auch eine kurze Beschreibung für die Sicherung in das Feld **Beschreibung** eingeben.
5. Klicken Sie auf **OK**, um die Gerätekonfiguration zu sichern. Das Sichern der Gerätekonfiguration wird durch die Meldung **Gerätekonfiguration wurde erfolgreich gesichert** bestätigt.

Gerätekonfiguration wiederherstellen

Sie können eine zuvor gesicherte Gerätekonfiguration auf einem Gerät wieder herstellen.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie die Geräte aus, die Sie für eine Sicherungskonfiguration wieder herstellen möchten.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager**, **Konfiguration** und anschließend auf **Wiederherstellen**. Das Fenster **Gerätekonfiguration wiederherstellen** wird angezeigt.

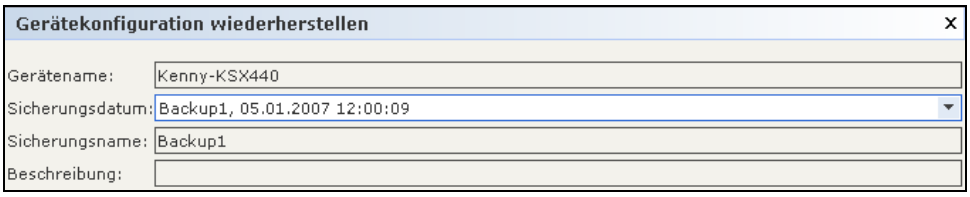


Abbildung 45 Fenster Gerätekonfiguration wiederherstellen

3. Klicken Sie auf die Dropdown-Liste **Sicherungsdatum**, und wählen Sie das Datum der letzten Sicherung des Geräts aus der Liste aus. Der Name und die Beschreibung der Sicherung werden in die entsprechenden Felder übernommen.
4. Klicken Sie zum Wiederherstellen der Sicherung auf **OK**.
5. Wenn die Meldung zum Neustart angezeigt wird, klicken Sie zum Neustarten des Geräts auf **Ja**. Die Wiederherstellung aller Benutzer- und Systemkonfigurationsdaten wird durch die Meldung **Gerätekonfiguration wurde erfolgreich wiederhergestellt** bestätigt.

Gerätekonfiguration kopieren

Mit diesem Befehl können Sie Konfigurationen von einem Gerät auf andere Geräte kopieren.

***Hinweis**: Eine Konfiguration kann nur zwischen Dominion SX-Einheiten mit derselben Portzahl kopiert werden.*

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie in der Gerätestrukturansicht das Gerät aus, dessen Konfiguration Sie auf andere Geräte kopieren möchten.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager**, **Konfiguration** und anschließend auf K**onfiguration kopieren**. Das Fenster **Gerätekonfiguration kopieren** wird angezeigt.
3. Wenn Sie auf diesem Gerät die Option **Gerät sichern** verwendet haben, können Sie stattdessen diese Konfiguration kopieren, indem Sie **Von gespeicherter Konfiguration** aktivieren und dann im Dropdown-Menü die gespeicherte Konfiguration auswählen.
4. Markieren Sie in der Spalte **Verfügbare Geräte** die Geräte, auf die Sie diese Konfiguration kopieren möchten, und klicken Sie auf > (Pfeil nach rechts), um die Geräte in die Spalte **Konfiguration kopieren in** zu verschieben. Mit < (Pfeil nach links) werden die ausgewählten Geräte aus der Spalte **Konfiguration kopieren in** entfernt bzw. verschoben.
5. Klicken Sie auf **OK**, um die Konfiguration auf die Geräte in der Spalte **Konfiguration kopieren in** zu kopieren.
6. Wenn die Meldung zum Neustart angezeigt wird, klicken Sie zum Neustarten des Geräts auf **Ja**. Das Kopieren der Gerätekonfiguration wird durch die Meldung **Gerätekonfiguration erfolgreich kopiert nach** bestätigt.

Gerät neu starten

Starten Sie ein Gerät mit dem Befehl **Gerät neu starten** neu.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät zum Neustart aus.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Gerät neu starten**. Das Fenster **Gerät neu starten** wird angezeigt.

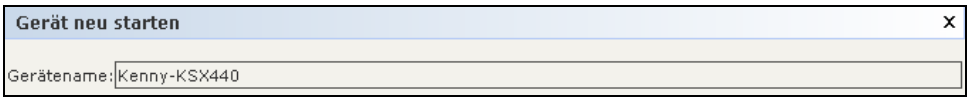


Abbildung 46 Fenster Gerät neu starten

3. Klicken Sie zum Neustarten des Geräts auf **OK**. Das Neustarten des Geräts wird durch die Meldung **Gerät wurde erfolgreich neu gestartet** bestätigt.

Gerät anpingen

Durch Anpingen eines Geräts können Sie feststellen, ob das Gerät in Ihrem Netzwerk verfügbar ist.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät zum Anpingen aus.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Gerät anpingen**. Das Fenster **Gerät anpingen** wird mit dem Ergebnis des Ping-Befehls angezeigt.

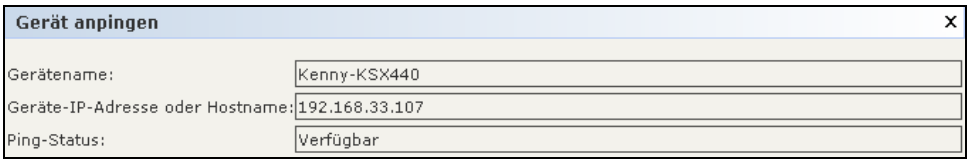


Abbildung 47 Fenster Gerät anpingen

Verwaltung unterbrechen

Sie können den Gerätebetrieb unterbrechen und damit vorübergehend die Steuerung durch CC-SG aussetzen, ohne die in CC-SG gespeicherten Konfigurationsdaten zu verlieren.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie die Geräte aus, deren CC-SG-Verwaltung unterbrochen werden soll.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Verwaltung unterbrechen**. Das Gerätesymbol in der Gerätestruktur zeigt an, dass das Gerät unterbrochen wurde.

Verwaltung fortsetzen

Sie können die CC-SG-Verwaltung für ein unterbrochenes Gerät fortsetzen, damit es wieder von CC-SG gesteuert werden kann.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie in der Gerätestrukturansicht das unterbrochene Gerät aus.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Verwaltung fortsetzen**. Das Gerätesymbol in der Gerätestruktur zeigt an, dass das Gerät aktiv ist.

Gerätestrommanager

Der Gerätestrommanager wird verwendet, um den Status eines Powerstrip-Geräts (einschließlich Spannung, Strom und Temperatur) anzuzeigen und alle Stromausgänge eines Powerstrip-Geräts zu verwalten. Anstatt Knoten einzeln ein- und auszuschalten, bietet der Gerätestrommanager eine auf Powerstrips zentrierte Ansicht der Ausgänge.

Bevor Sie den Gerätestrommanager verwenden können, muss eine physikalische Verbindung zwischen einer PowerStrip- und einer Dominion SX- oder Dominion KSX-Einheit hergestellt werden. Beim Hinzufügen des Powerstrip-Geräts müssen Sie definieren, welches Raritan-Gerät die Verbindung bereitstellt. Dadurch wird es mit dem seriellen Port des Dominion SX-Geräts oder mit dem Stromzufuhrport verknüpft, der dem Dominion KSX-Gerät zugeordnet ist und der die Verwaltung des Powerstrip bereitstellt.

1. Wählen Sie in der Gerätestrukturansicht ein Powerstrip-Gerät aus.
2. Klicken Sie im Menü **Geräte** auf **Gerätestrommanager**. Das Fenster **Gerätestrommanager** wird angezeigt.
3. Die Ausgänge werden im Fensterbereich **Status der Ausgänge** aufgeführt. Möglicherweise müssen Sie nach unten blättern, um alle Ausgänge anzuzeigen.
4. Verwenden Sie für jeden Ausgang die Optionsschaltflächen **Ein** oder **Aus**, um den Ausgang ein- oder auszuschalten.
5. Klicken Sie auf **Ein-/Ausschalten**, um das mit dem Ausgang verbundene Gerät neu zu starten.
6. Klicken Sie zum Schließen des Fensters **Gerätestrommanager** auf **Schließen**.

Administration starten

Falls verfügbar bietet der Befehl **Administration starten** Zugriff auf die Verwaltungsschnittstelle des ausgewählten Geräts.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät aus, dessen Verwaltungsschnittstelle Sie anzeigen möchten.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Administration starten**. Die Verwaltungsschnittstelle für das ausgewählte Gerät wird angezeigt.

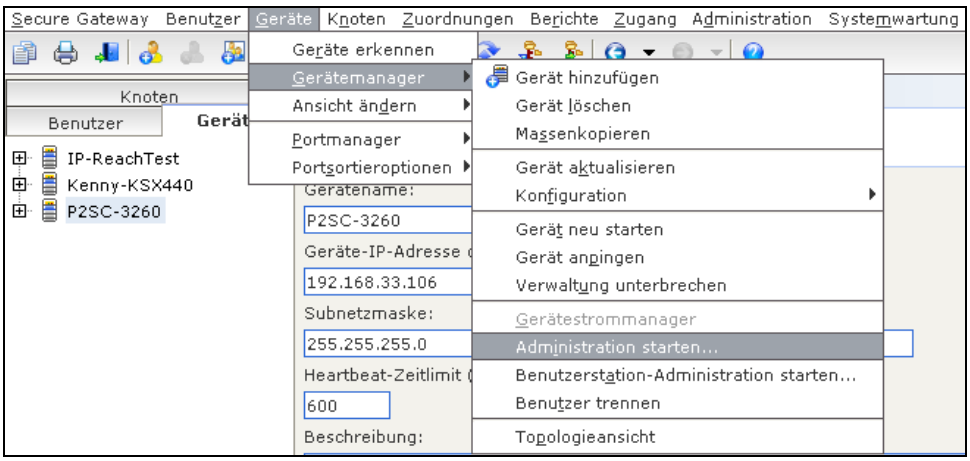


Abbildung 48 Administration starten für ein KX-Gerät

Topologieansicht

Die Topologieansicht zeigt das strukturelle Setup aller angeschlossenen Appliances in Ihrer Konfiguration an.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät aus, dessen Topologieansicht Sie anzeigen möchten.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Topologieansicht**. Die **Topologieansicht** für das ausgewählte Gerät wird angezeigt.

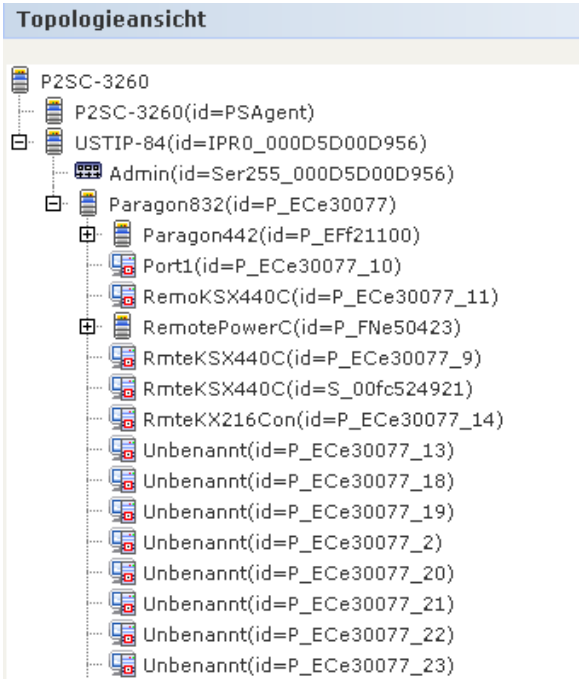


Abbildung 49 Topologieansicht

3. Sie können in der Topologieansicht wie in der Gerätestrukturansicht navigieren. Klicken Sie auf + oder –, um die Ansicht ein- oder auszublenden.
4. Klicken Sie zum Schließen des Fensters **Topologieansicht** auf **Schließen**.

***Hinweis**: Bis Sie die **Topologieansicht** schließen, ersetzt diese Ansicht den Bildschirm **Geräteprofil**, der normalerweise angezeigt wird, wenn ein Gerät ausgewählt wird.*

Benutzerverbindung trennen

Administratoren können die Gerätesitzung eines Benutzers beenden. Dazu zählen Benutzer, die beliebige Gerätevorgänge durchführen, wie beispielsweise Benutzer, die Verbindungen zu Ports herstellen, die Konfiguration eines Geräts sichern bzw. wiederherstellen oder die Firmware eines Geräts aktualisieren.

***Hinweis**: Firmwareaktualisierungen sowie Sicherungen und Wiederherstellungen von Gerätekonfigurationen können vor Beendigung der Gerätesitzung des Benutzers abgeschlossen werden. Alle anderen Vorgänge werden sofort beendet.*

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät aus, von dem Sie einen oder mehrere Benutzer trennen möchten.
2. Klicken Sie im Menü **Geräte** auf **Gerätemanager** und anschließend auf **Benutzer trennen**. Das Fenster **Benutzer trennen** wird angezeigt.

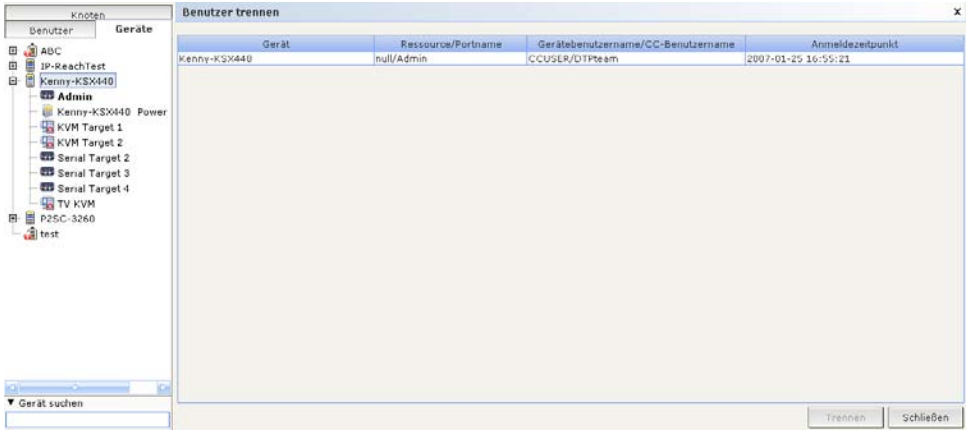


Abbildung 50 Benutzer trennen

3. Wählen Sie die Benutzer, deren Sitzung beendet werden soll, in der Tabelle **Benutzer trennen** aus.
4. Klicken Sie auf **Trennen**, um sie vom Gerät zu trennen.

***Hinweis**: Nur bei Dominion SX-Geräten können Sie neben den Benutzern, die mit dem Gerät über CC-SG verbunden sind, auch direkt am Gerät angemeldete Benutzer trennen.*

Geräte anzeigen

CC-SG bietet über die Registerkarte **Geräte** verschiedene Optionen zum Anzeigen von Geräten.

Strukturansicht

Wählen Sie die Strukturansicht aus, um Geräte in der Gerätestrukturansicht unter Verwendung der Standardansicht anzuzeigen. Wenn Sie **Strukturansicht** auswählen, wechseln Sie von einer benutzerdefinierten Ansicht zur Standardansicht. Weitere Informationen finden Sie unter **Benutzerdefinierte Ansicht** in diesem Kapitel.

1. Klicken Sie im Menü **Geräte** auf **Ansicht ändern**, und klicken Sie dann auf **Strukturansicht**. Die Standardansicht der Gerätestrukturansicht wird angezeigt.

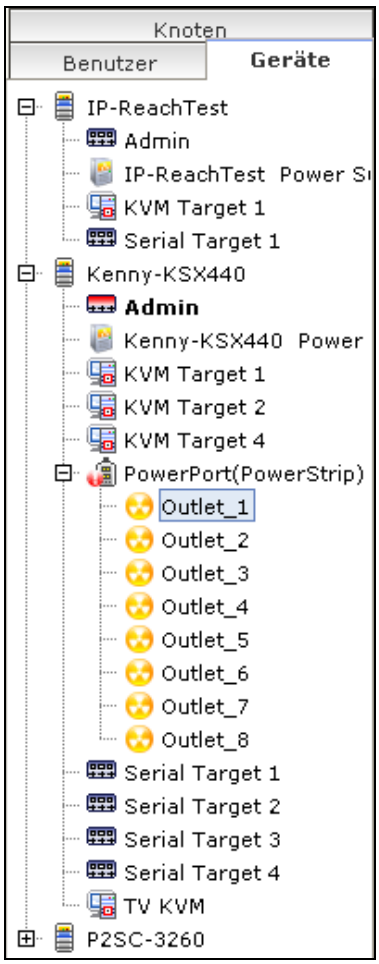


Abbildung 51 Standardansicht der Gerätestrukturansicht

Konfigurierte Ports werden verschachtelt unter ihren übergeordneten Geräten aufgelistet. Sie können die Reihenfolge ändern, in der Ports angezeigt werden, indem Sie auf das Menü **Geräte** und dann auf **Portsortieroptionen** klicken. Wählen Sie **Nach Portname** oder **Nach Portstatus** aus, um die Ports im Gerät alphabetisch nach Namen oder Verfügbarkeitsstatus zu sortieren. Nach Status aufgelistete Ports werden innerhalb ihrer Verbindungsstatusgruppe alphabetisch sortiert. Geräte werden ebenfalls entsprechend sortiert angezeigt.

Benutzerdefinierte Ansicht

Sie können die Gerätestrukturansicht anpassen, indem Sie die anzuzeigenden Geräte in einem bestimmten Format anordnen. Sie können Geräte nach Land, nach Zeitzone oder nach anderen Optionen anzeigen, die eine Unterscheidung der Geräte vereinfachen. Weitere Informationen zum Hinzufügen von Kategorien zu CC-SG finden Sie in **Kapitel 4: Erstellen von Zuordnungen**.

1. Klicken Sie auf die Registerkarte **Geräte**.

2. Klicken Sie im Menü **Geräte** auf **Ansicht ändern**, und klicken Sie dann auf **Benutzerdefinierte Ansicht erstellen**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.

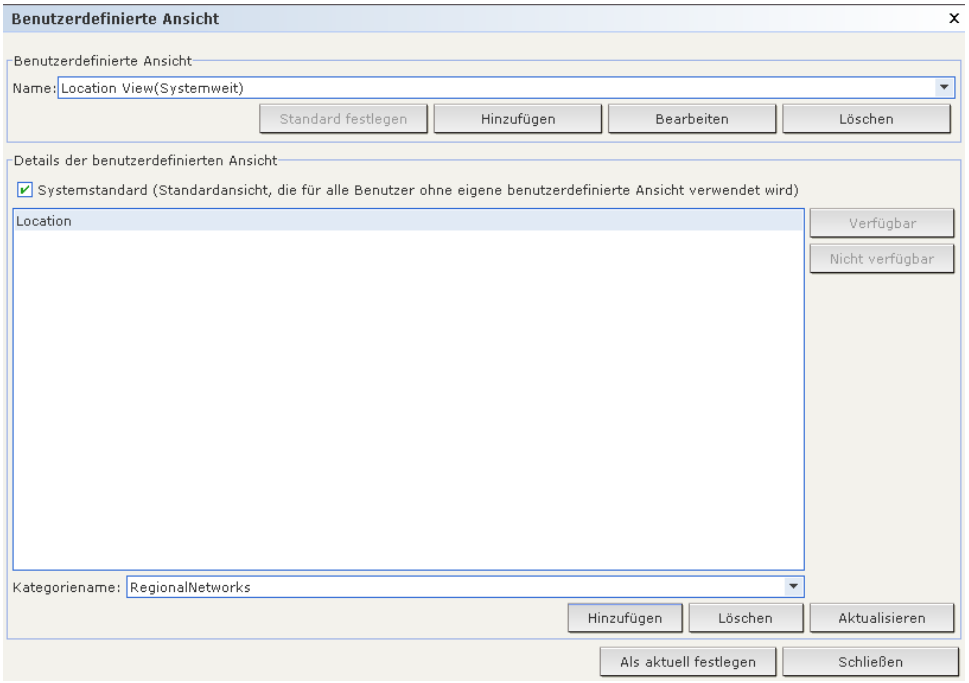


Abbildung 52 Fenster Benutzerdefinierte Ansicht

3. Klicken Sie zum Anpassen der Ansicht auf die Dropdown-Liste **Name**, und wählen Sie eine bereits in der Datenbank gespeicherte benutzerdefinierte Ansicht aus. Im Feld **Details der benutzerdefinierten Ansicht** werden Details über die Ansichtskategorien angezeigt.
4. Klicken Sie auf **Als aktuell festlegen**, damit die Gerätestrukturansicht anhand der ausgewählten benutzerdefinierten Ansicht angeordnet wird.
5. Klicken Sie auf **Standard festlegen**, wenn die ausgewählte benutzerdefinierte Ansicht beim Anmelden in CC-SG angezeigt werden soll.
6. Markieren Sie das Kontrollkästchen **Systemstandard**, um diese Ansicht als Standardansicht für alle Benutzer festzulegen, die nicht ihre eigene benutzerdefinierte Standardansicht verwenden.

Benutzerdefinierte Ansicht auswählen

So können Sie von der aktuellen Gerätestrukturansicht in eine bereits vorhandene benutzerdefinierte Ansicht wechseln:

1. Klicken Sie auf die Registerkarte **Geräte**.
2. Klicken Sie im Menü **Geräte** auf **Ansicht ändern**, und wählen Sie den Namen der benutzerdefinierten Ansicht unter **Benutzerdefinierte Ansicht erstellen** aus. Anstelle der Gerätestrukturansicht wird die ausgewählte benutzerdefinierte Ansicht angezeigt.

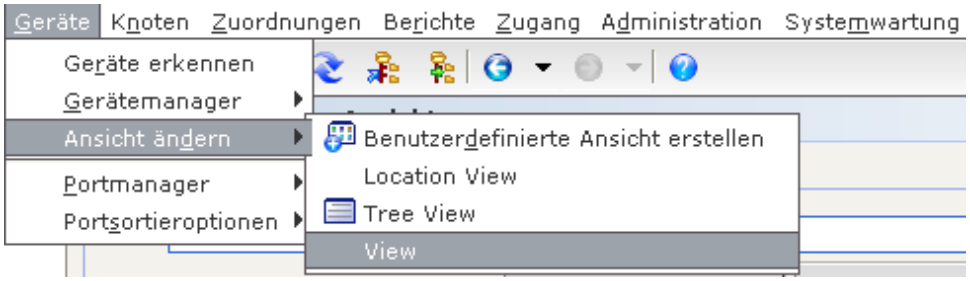


Abbildung 53 Benutzerdefinierte Ansicht auswählen

Benutzerdefinierte Ansicht hinzufügen

1. Klicken Sie auf die Registerkarte **Geräte**.
2. Klicken Sie im Menü **Geräte** auf **Ansicht ändern**, und klicken Sie dann auf **Benutzerdefinierte Ansicht erstellen**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.
3. Klicken Sie im Fensterbereich **Benutzerdefinierte Ansicht** auf **Hinzufügen**. Das Fenster **Benutzerdefinierte Ansicht hinzufügen** wird angezeigt.
4. Geben Sie einen neuen Namen für die benutzerdefinierte Ansicht ein, und klicken Sie auf **OK**, oder klicken Sie zum Schließen des Fensters auf **Abbrechen**. Der neue Ansichtsname wird im Feld **Name** angezeigt.
5. Klicken Sie unten im Fensterbereich **Details der benutzerdefinierten Ansicht** auf die Dropdown-Liste. Diese Liste enthält Kategorien zum Filtern von benutzerdefinierten Ansichten. Wählen Sie ein Detail in der Dropdown-Liste aus, und klicken Sie zum Hinzufügen des Details zum Fensterbereich **Details der benutzerdefinierten Ansicht** auf **Hinzufügen**. Wählen Sie die benötigten Details aus.
6. Wählen Sie zum Neusortieren der Details im Fensterbereich **Details der benutzerdefinierten Ansicht** ein Detail aus, und verwenden Sie die Schaltflächen **Nach oben** und **Nach unten**, um die Details in der Reihenfolge anzuordnen, in der Sie die Geräte sortieren möchten. Wenn Sie ein Detail aus der Liste entfernen möchten, wählen Sie das Detail aus, und klicken Sie im Fensterbereich **Details der benutzerdefinierten Ansicht** auf **Löschen**.
7. Klicken Sie zum Aktualisieren der benutzerdefinierten Ansicht auf **Aktualisieren**. Das Aktualisieren der benutzerdefinierten Ansicht wird durch die Meldung **Die benutzerdefinierte Ansicht wurde erfolgreich aktualisiert** bestätigt.
8. Klicken Sie auf **Als aktuell festlegen**, damit die Gerätestrukturansicht anhand der ausgewählten benutzerdefinierten Ansicht angeordnet wird.

Benutzerdefinierte Ansicht bearbeiten

1. Klicken Sie auf die Registerkarte **Geräte**.
2. Klicken Sie im Menü **Geräte** auf **Ansicht ändern** und anschließend auf **Benutzerdefinierte Ansicht**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.
3. Klicken Sie im Fensterbereich **Benutzerdefinierte Ansicht** auf die Dropdown-Liste **Name**, und wählen Sie die zu bearbeitende benutzerdefinierte Ansicht aus. Klicken Sie auf **Bearbeiten**. Das Fenster **Benutzerdefinierte Ansicht bearbeiten** wird angezeigt.
4. Geben Sie einen neuen Namen für die benutzerdefinierte Ansicht ein, und klicken Sie zum Bestätigen auf **OK**, oder klicken Sie zum Schließen des Fensters auf **Abbrechen**.
5. Klicken Sie unten im Fensterbereich **Details der benutzerdefinierten Ansicht** auf die Dropdown-Liste. Diese Liste enthält Kategorien zum Filtern von benutzerdefinierten Ansichten. Wählen Sie ein Detail in der Dropdown-Liste aus, und klicken Sie zum Hinzufügen des Details zum Fensterbereich **Details der benutzerdefinierten Ansicht** auf **Hinzufügen**. Wählen Sie die benötigten Details aus.
6. Wählen Sie zum Neusortieren der Details im Fensterbereich **Details der benutzerdefinierten Ansicht** ein Detail aus, und verwenden Sie die Schaltflächen **Nach oben** und **Nach unten**, um die Details in der Reihenfolge anzuordnen, in der Sie die Geräte sortieren möchten. Wenn Sie ein Detail aus der Liste entfernen möchten, wählen Sie das Detail aus, und klicken Sie im Fensterbereich **Details der benutzerdefinierten Ansicht** auf **Löschen**.
7. Klicken Sie zum Aktualisieren der benutzerdefinierten Ansicht auf **Aktualisieren**. Das Aktualisieren der benutzerdefinierten Ansicht wird durch die Meldung **Die benutzerdefinierte Ansicht wurde erfolgreich aktualisiert** bestätigt.
8. Klicken Sie auf **Als aktuell festlegen**, damit die Gerätestrukturansicht anhand der ausgewählten benutzerdefinierten Ansicht angeordnet wird.

Benutzerdefinierte Ansicht löschen

1. Klicken Sie auf die Registerkarte **Geräte**.
2. Klicken Sie im Menü **Geräte** auf **Ansicht ändern**, und klicken Sie dann auf **Benutzerdefinierte Ansicht erstellen**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.

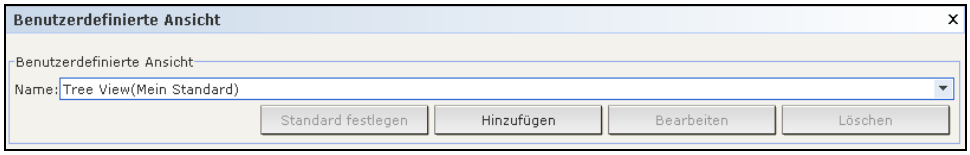


Abbildung 54 Fenster Benutzerdefinierte Ansicht

3. Klicken Sie im Fensterbereich **Benutzerdefinierte Ansicht** auf die Dropdown-Liste **Name**, und wählen Sie die zu löschende benutzerdefinierte Ansicht aus.
4. Klicken Sie im Fensterbereich **Benutzerdefinierte Ansicht** auf die Schaltfläche **Löschen**. Das Fenster **Benutzerdefinierte Ansicht löschen** wird angezeigt.
5. Klicken Sie auf **Ja**, um die benutzerdefinierte Ansicht zu löschen.

Sonderzugriff auf Paragon II-Systemgeräte

Paragon II System Controller (P2-SC)

Benutzer der Paragon II-Systemintegration können ihre P2-SC-Geräte zur CC-SG-Gerätestruktur hinzufügen und mit der P2-SC-Administrationsanwendung in CC-SG konfigurieren. Weitere Informationen zur Verwendung der P2-SC-Administration finden Sie im **P2-SC-Benutzerhandbuch** von Raritan.

Nach dem Hinzufügen des Paragon-Systemgeräts (das Paragon-System umfasst das P2-SC-Gerät, angeschlossene UMT- sowie IP-Reach-Einheiten) zu CC-SG, wird es in der Gerätestruktur angezeigt.

So greifen Sie auf den Paragon II-Systemcontroller zu:

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie den Paragon II-Systemcontroller aus.
2. Klicken Sie mit der rechten Maustaste auf den Paragon II-Systemcontroller, und klicken Sie dann auf **Administration starten**, um die Paragon II-Systemcontroller-Anwendung in einem neuen Browserfenster zu starten. Anschließend können Sie die PII UMT-Einheiten konfigurieren.

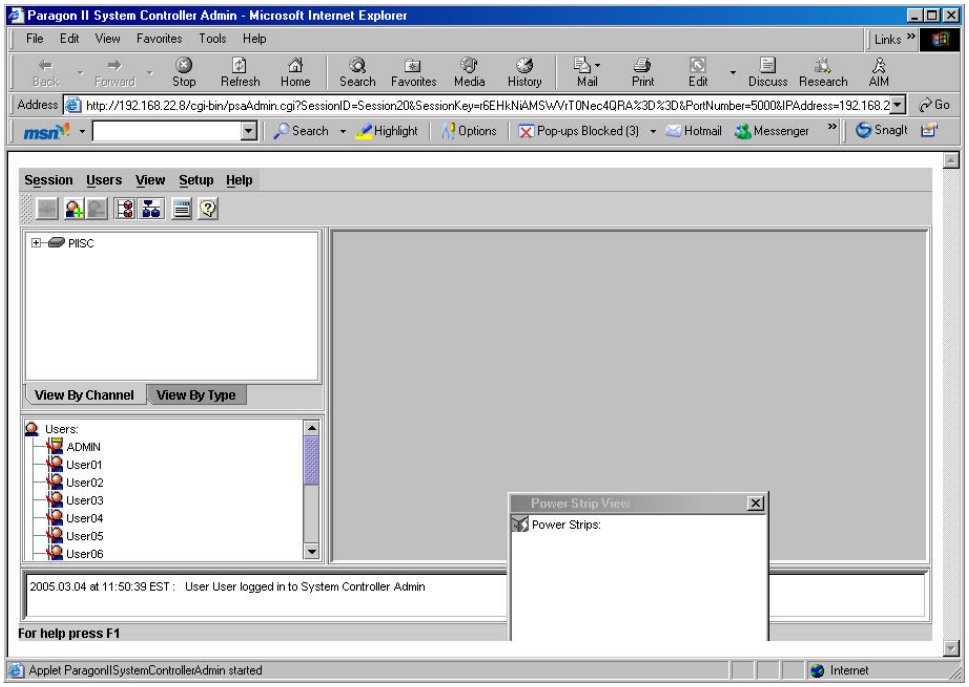


Abbildung 55 Paragon Manager-Anwendungsfenster

IP-Reach- und UST-IP-Verwaltung

Sie können direkt auf der CC-SG-Benutzeroberfläche administrative Diagnoseaufgaben an IP-Reach- und UST-IP-Geräten durchführen, die am Paragon-System angeschlossen sind.

Nach dem Hinzufügen eines Paragon-Systemgeräts zu CC-SG wird es in der Gerätestruktur angezeigt.

So greifen Sie auf die Remotebenutzerstation-Verwaltung zu:

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie **Paragon II-Systemcontroller** aus.
2. Klicken Sie mit der rechten Maustaste auf **Paragon II-Systemcontroller**, und klicken Sie dann auf **Remotebenutzerstation-Verwaltung**. Im angezeigten Fenster **Remotebenutzerstation-Verwaltung** werden alle verbundenen IP-Reach- und UST-IP-Einheiten angezeigt.
3. Klicken Sie in der Zeile des Geräts, mit dem Sie arbeiten möchten, auf die Schaltfläche **Verwaltung starten**, um Raritan Remote Console zu aktivieren und die blaue Gerätekonfigurationsanzeige in einem neuen Fenster zu öffnen.

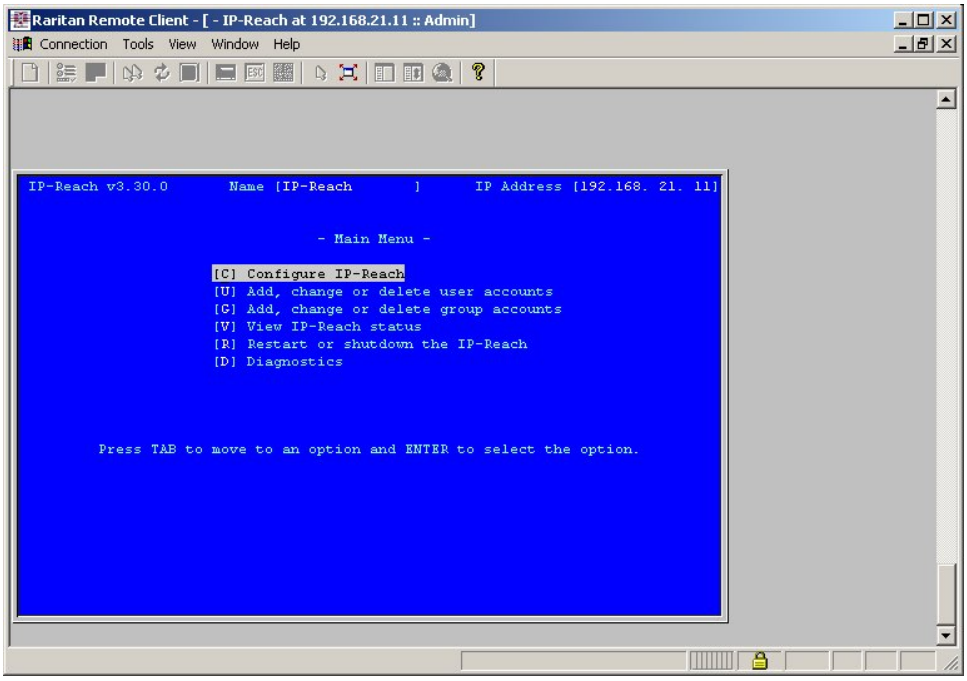


Abbildung 56 IP-Reach-Administrationsfenster

Gerätegruppenmanager

Über den Bildschirm des Gerätegruppenmanagers können Sie Gerätegruppen hinzufügen, bearbeiten und löschen. Wenn Sie eine neue Gerätegruppe hinzufügen, können Sie eine Richtlinie mit unbeschränktem Zugriff für die Gruppe erstellen. Weitere Informationen finden Sie in **Kapitel 8: Richtlinien**.

Gerätegruppe hinzufügen

1. Klicken Sie im Menü **Zuordnungen** auf **Gerätegruppen**. Das Fenster **Gerätegruppenmanager** wird angezeigt. Vorhandene Gerätegruppen werden im linken Fensterbereich angezeigt.

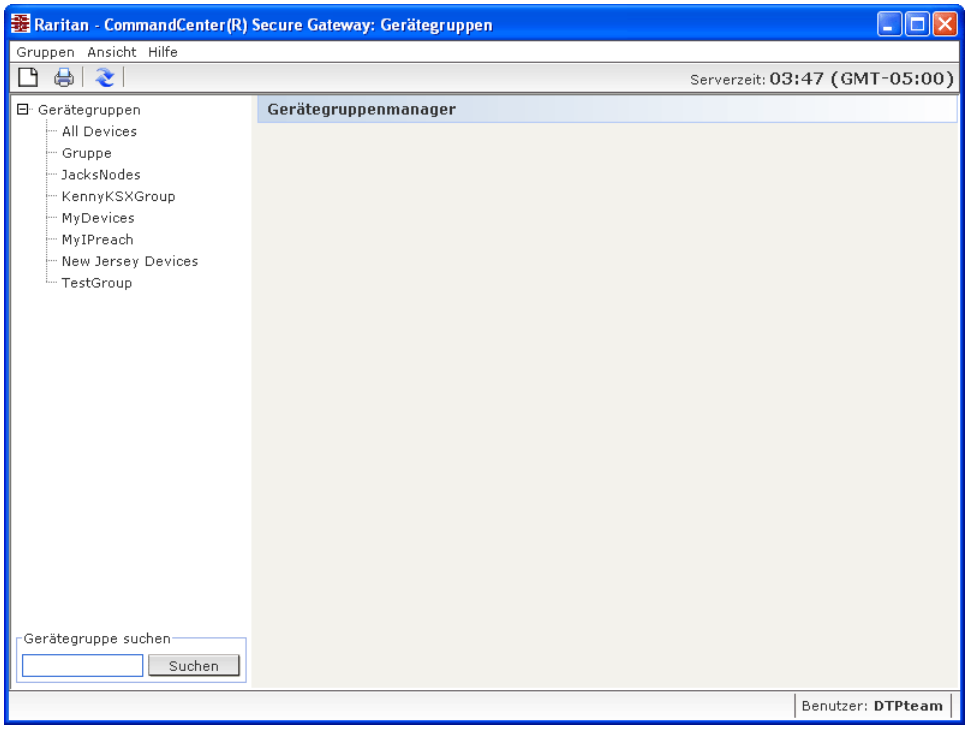


Abbildung 57 Gerätegruppenmanager

2. Klicken Sie auf der Symbolleiste auf das Symbol **Neue Gruppe** . Der Fensterbereich **Gerätegruppe: Neu** wird angezeigt.

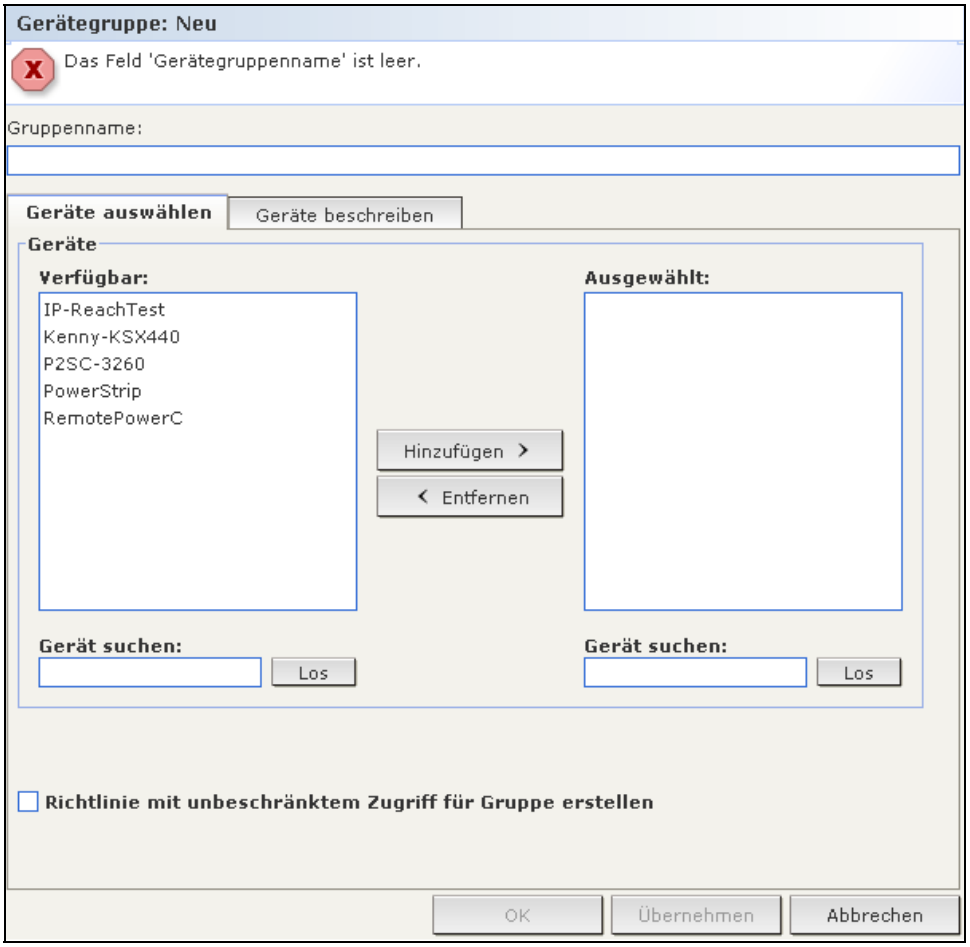


Abbildung 58 Gerätegruppe: Neuer Fensterbereich, Registerkarte Geräte auswählen

3. Geben Sie in das Feld **Gruppenname** einen Namen für die Gerätegruppe ein, die Sie erstellen möchten.
4. Sie haben zwei Möglichkeiten, Geräte einer Gruppe hinzuzufügen: **Geräte auswählen** und **Geräte beschreiben**. Auf der Registerkarte **Geräte auswählen** können Sie auswählen, welche Geräte zur Gruppe zugeordnet werden sollen. Wählen Sie die Geräte dazu einfach in der Liste der verfügbaren Geräte aus. Auf der Registerkarte **Geräte beschreiben** können Sie Regeln angeben, die Geräte beschreiben. Geräte, deren Parameter diesen Regeln entsprechen, werden der Gruppe hinzugefügt.

Geräte auswählen

a. Klicken Sie im Fensterbereich **Gerätegruppe: Neu** auf die Registerkarte **Geräte auswählen**.
b. Wählen Sie in der Liste **Verfügbar** das Gerät aus, das Sie der Gruppe hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**, um das Gerät in die Liste **Ausgewählt** zu verschieben. Geräte, die sich in der Liste **Ausgewählt** befinden, werden der Gruppe hinzugefügt.

- Wählen Sie zum Löschen eines Geräts aus der Gruppe den Gerätenamen in der Liste **Ausgewählt** aus, und klicken Sie auf **Löschen**.
- Sie können das Gerät in der Liste **Verfügbar** oder **Ausgewählt** suchen. Geben Sie den Suchbegriff in das Feld unter der Liste ein, und klicken Sie auf **Los**.

Geräte beschreiben

a. Klicken Sie im Fensterbereich **Gerätegruppe: Neu** auf die Registerkarte **Geräte beschreiben**. Auf der Registerkarte **Geräte beschreiben** erstellen Sie eine Regeltabelle, in der die Geräte beschrieben werden, die Sie der Gruppe zuweisen möchten.

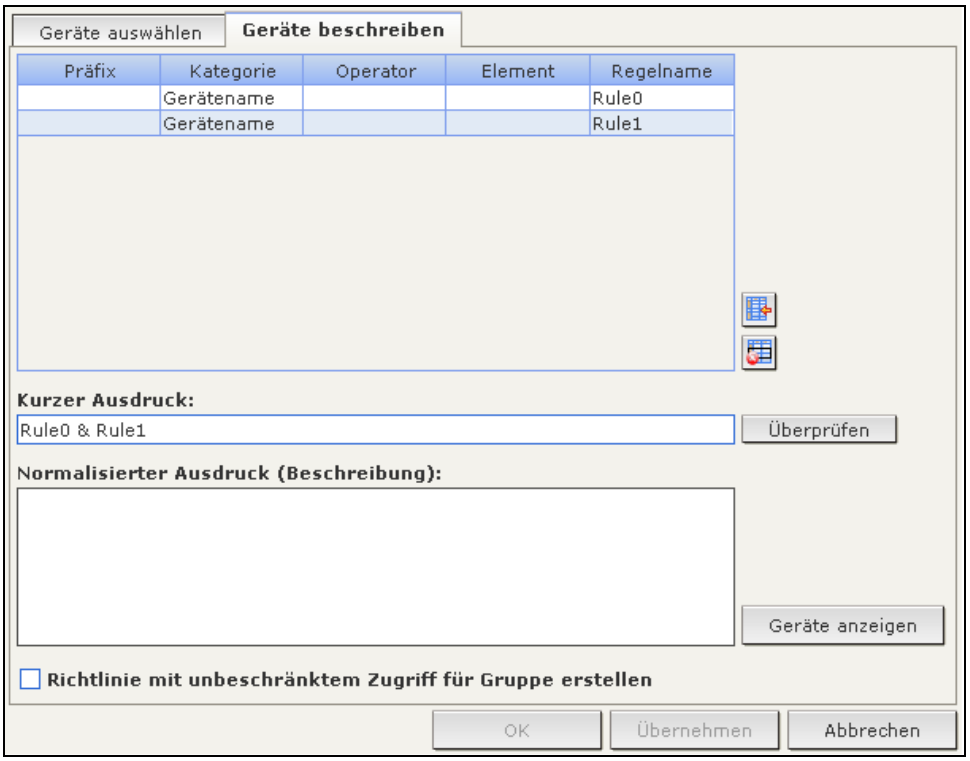


Abbildung 59 Registerkarte Geräte beschreiben

b. Klicken Sie auf das Symbol  , um eine neue Zeile in die Tabelle einzufügen.

c. Doppelklicken Sie auf die Zelle, die für jede Spalte erstellt wurde, um das Dropdown-Menü anzuzeigen. Wählen Sie in jeder Liste die gewünschten Regelkomponenten aus.

- **Präfix**: Feld leer lassen oder **NOT** auswählen. Wenn **NOT** ausgewählt ist, sucht diese Regel nach Werten, die dem Ausdruck nicht entsprechen.
- **Kategorie**: Wählen Sie ein Attribut aus, das in der Regel bewertet wird. Es sind alle Kategorien verfügbar, die Sie im **Zuordnungsmanager** erstellt haben.
- **Operator**: Wählen Sie einen Vergleichsvorgang, der zwischen Kategorien und Elementen durchgeführt werden soll. Es stehen drei Operatoren zur Verfügung: = (ist gleich), **LIKE** (zum Suchen des Elements in einem Namen) und <> (ist nicht gleich).
- **Element**: Wählen Sie einen Wert für das Kategorieattribut zum Vergleich aus. Hier werden nur Elemente dargestellt, die mit der ausgewählten Kategorie verknüpft sind. (Beispiel: wenn eine Kategorie „Abteilung“ bewertet wird, werden Elemente mit der Bezeichnung „Standort“ nicht angezeigt).
- **Regelname**: Der Name, der der Regel in dieser Zeile zugewiesen wurde. Dieser Name kann nicht bearbeitet werden. Er wird zur Beschreibung im Feld **Kurzer Ausdruck** verwendet.

Die Regel „Abteilung = Technik“ würde beispielsweise alle Geräte beschreiben, bei denen die **Kategorie** „Abteilung“ auf „Technik“ eingestellt ist. Dies geschieht genau dann, wenn Sie die Zuordnungen während des Vorgangs **Gerät hinzufügen** konfigurieren.

d. Wenn Sie eine weitere Regel hinzufügen möchten, klicken Sie auf das Symbol zum Einfügen einer neuen Zeile  , und nehmen Sie dann die entsprechenden Konfigurationen vor. Wenn Sie mehrere Regeln konfigurieren, können Sie genauere Beschreibungen anfertigen, indem Sie mehrere Kriterien zur Bewertung von Geräten bereitstellen.

e. Die Regeltabelle stellt nur Kriterien zur Bewertung von Knoten bereit. Definieren Sie eine Beschreibung für die Gerätegruppe, indem Sie die Regeln nach **Regelname** zum Feld **Kurzer Ausdruck** hinzufügen. Erfordert die Beschreibung nur eine Regel, geben Sie einfach den Namen der Regel in das Feld ein. Werden mehrere Regeln bewertet, geben Sie die Regeln in das Feld mithilfe logischer Operatoren ein, um die Regeln in ihrer Beziehung zueinander zu beschreiben:

- **&** - der UND Operator. Ein Knoten muss die Regeln auf beiden Seiten dieses Operators für die Beschreibung (oder den Abschnitt einer Beschreibung) erfüllen, um als wahr bewertet zu werden.
- | - der ODER Operator. Ein Gerät muss nur eine Regel auf einer Seite dieses Operators für die Beschreibung (oder den Abschnitt einer Beschreibung) erfüllen, um als wahr bewertet zu werden.
- **(** und **)** – Gruppierungsoperatoren. Die Beschreibung wird in einen Unterabschnitt aufgeteilt, der in Klammern steht. Der Abschnitt innerhalb der Klammern wird bewertet, bevor die restliche Beschreibung mit dem Knoten verglichen wird. Gruppen in Klammern können in einer anderen Gruppe in Klammern verschachtelt werden.

Beispiel: Wenn Sie Geräte beschreiben möchten, die zur Technikabteilung gehören, muss die Regel wie folgt aussehen: `Abteilung = Technik`. Dies wird als Regel0 bezeichnet. Geben Sie dann Regel0 in das Feld **Kurzer Ausdruck** ein.

Ein weiteres Beispiel: Wenn Sie eine Gerätegruppe beschreiben möchten, die zur Technikabteilung gehört oder den Standort „Philadelphia“ aufweist, und festlegen möchten, dass alle Geräte mindestens über 1 GB Speicher verfügen müssen, dann müssen Sie drei Regeln erstellen. `Abteilung = Technik` (Regel0) `Standort = Philadelphia` (Regel1) `Speicher = 1GB` (Regel2). Diese Regeln müssen in Relation zueinander gesetzt werden. Da das Gerät entweder der Technikabteilung angehören oder den Standort „Philadelphia“ aufweisen kann, verwenden Sie den ODER Operator **|**, um die beiden zu verbinden: `Regel0|Regel1`. Dieser Vergleich wird zuerst durchgeführt, indem er in Klammern eingeschlossen wird: `(Regel0|Regel1)`. Da die Geräte beide diesen Vergleich erfüllen UND 1 GB Speicher aufweisen müssen, wird der UND Operator **&** verwendet, um diesen Abschnitt mit Regel2 zu verbinden: `(Regel0|Regel1)&Regel2`. Geben Sie diesen Ausdruck in das Feld **Kurzer Ausdruck** ein.

- Wenn Sie eine Zeile in der Tabelle löschen möchten, wählen Sie die Zeile aus, und klicken Sie auf das Symbol zum Löschen der ausgewählten Zeile  .
- Wenn Sie eine Liste der Geräte anzeigen möchten, deren Parameter den von Ihnen definierten Regeln entsprechen, klicken Sie auf **Geräte anzeigen**.

f. Klicken Sie auf **Überprüfen**, wenn eine Beschreibung im Feld **Kurzer Ausdruck** enthalten ist. Wurde die Beschreibung fehlerhaft gebildet, wird ein Warnhinweis angezeigt. Wurde die Beschreibung richtig gebildet, wird eine normalisierte Form des Ausdrucks im Feld **Normalisierter Ausdruck** angezeigt.

g. Klicken Sie auf **Geräte anzeigen**, um anzuzeigen, welche Knoten diese Anforderungen erfüllen. Ein Ergebnisfenster **Geräte in der Gerätegruppe** wird mit den Geräten angezeigt, die durch den aktuellen Ausdruck zusammengefasst werden. Sie können dadurch prüfen, ob die Beschreibung richtig geschrieben wurde. Ist dies nicht der Fall, können Sie zur Regeltabelle oder dem Feld **Kurzer Ausdruck** wechseln, um Anpassungen vorzunehmen.

h. Markieren Sie das Kontrollkästchen **Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen**, wenn Sie eine Richtlinie für diese Gerätegruppe erstellen möchten, die jederzeit den Zugriff auf alle Geräte in der Gruppe mit Steuerberechtigung zulässt.

i. Wenn Sie eine weitere Gerätegruppe hinzufügen möchten, klicken Sie auf **Übernehmen**, um diese Gruppe zu speichern. Wiederholen Sie dann die Schritte in diesem Abschnitt, um weitere Gerätegruppen hinzuzufügen. Wenn Sie keine Gerätegruppen mehr hinzufügen möchten, klicken Sie auf **OK**, um diese Gruppe zu speichern und das Fenster **Gerätegruppe: Neu** zu schließen.

Gerätegruppe bearbeiten

1. Klicken Sie im Menü **Zuordnungen** auf **Gerätegruppen**. Das Fenster **Gerätegruppenmanager** wird angezeigt.

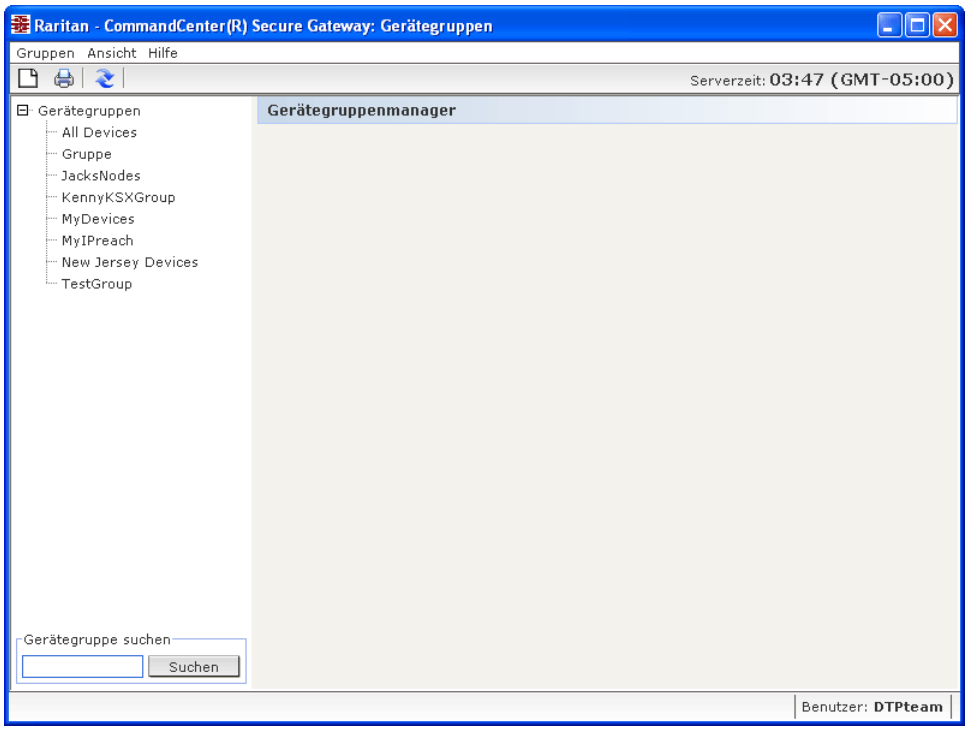


Abbildung 60 Fenster Gerätegruppenmanager

2. Vorhandene Gerätegruppen werden im linken Fensterbereich angezeigt. Wählen Sie die Gerätegruppe aus, deren Namen Sie ändern möchten. Der Fensterbereich für Gerätegruppendetails wird angezeigt.
3. Geben Sie zum Bearbeiten des Gerätegruppenamens einen neuen Namen in das Feld **Gruppenname** ein.
4. Bearbeiten Sie die Geräte, die in der Gerätegruppe enthalten sind, über die Registerkarten **Geräte auswählen** oder **Geräte beschreiben**. Weitere Informationen erhalten Sie im vorangehenden Abschnitt **Gerätegruppe hinzufügen**.
5. Klicken Sie zum Speichern der Änderungen auf **OK**.

Gerätegruppe löschen

1. Klicken Sie im Menü **Zuordnungen** auf **Gerätegruppen**. Das Fenster **Gerätegruppenmanager** wird angezeigt**.**

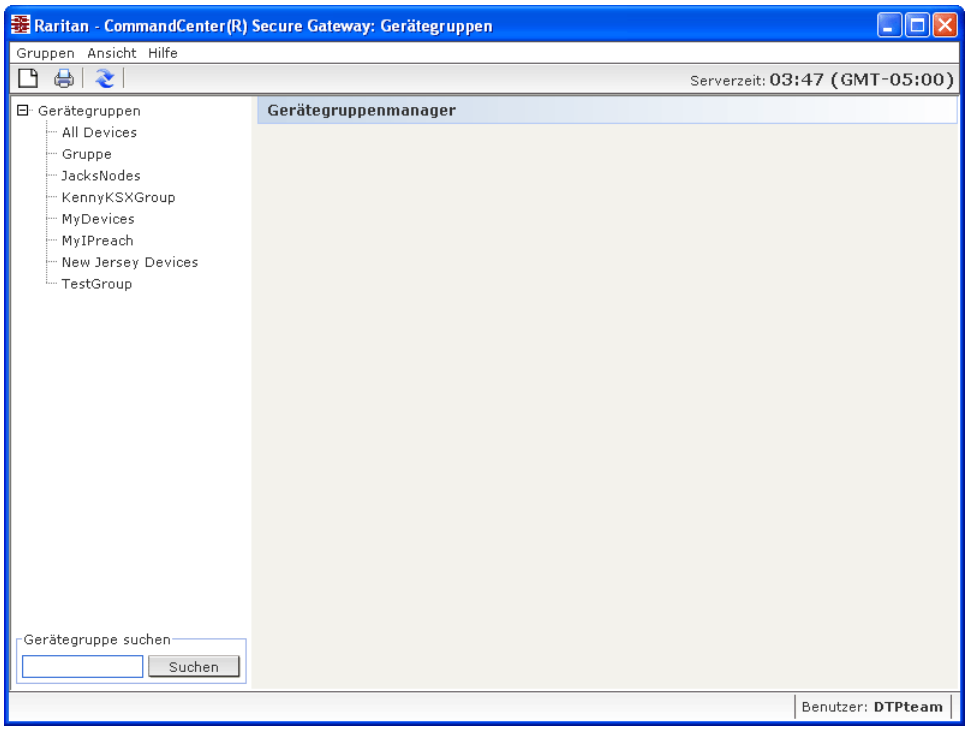


Abbildung 61 Fenster Gerätegruppenmanager

2. Vorhandene Gerätegruppen werden im linken Fensterbereich angezeigt. Wählen Sie die Gerätegruppe aus, die gelöscht werden soll. Der Fensterbereich für Gerätegruppendetails wird angezeigt.
3. Klicken Sie im Menü **Gruppen** auf **Löschen**.

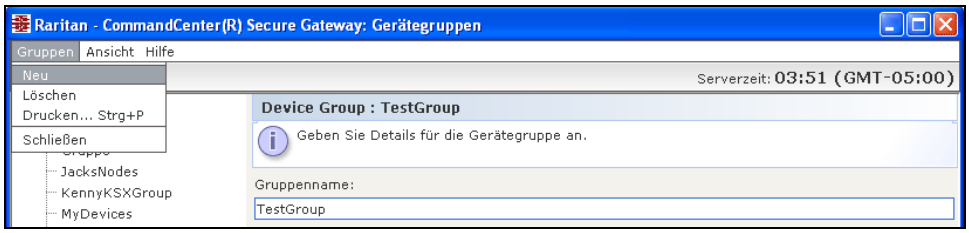


Abbildung 62 Fenster Gerätegruppe löschen

4. Der Fensterbereich zum Löschen von Gerätegruppen wird angezeigt. Klicken Sie auf **Löschen**.

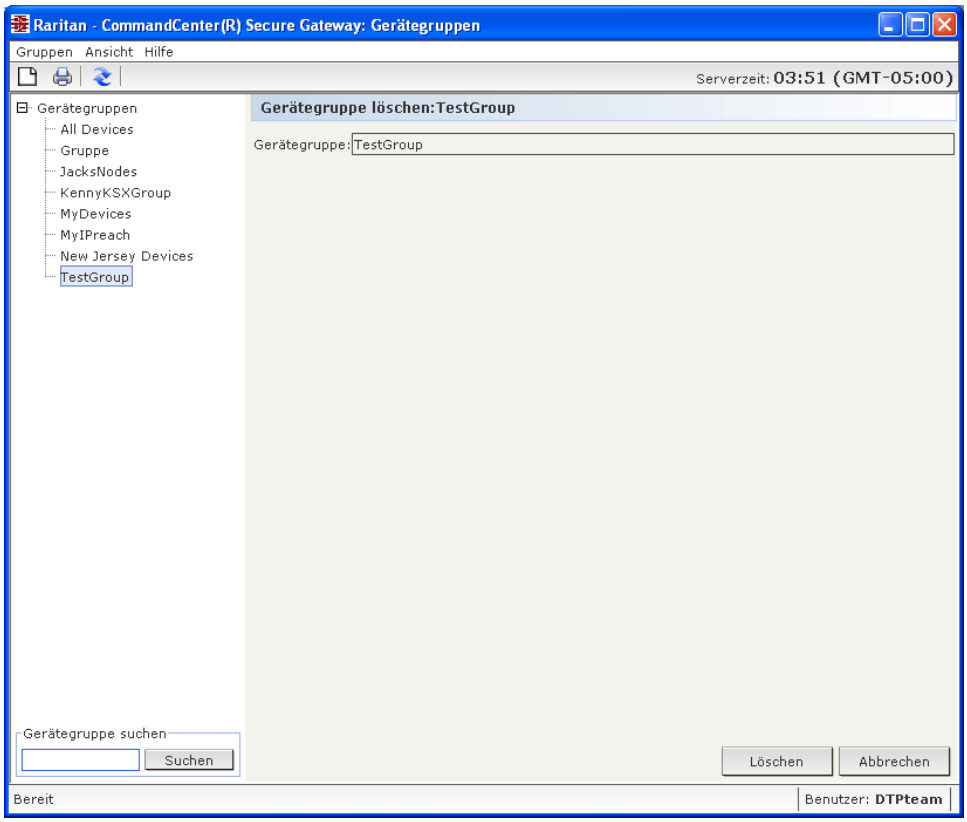


Abbildung 63 Fensterbereich Gerätegruppe löschen

5. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Kapitel 6: Konfigurieren von Knoten und Schnittstellen

In diesem Kapitel wird beschrieben, wie Knoten und die verknüpften Schnittstellen angezeigt, konfiguriert und bearbeitet werden. Weitere Informationen zum Verbindungsaufbau zu Knoten finden Sie im **CommandCenter Secure Gateway-Benutzerhandbuch** von Raritan.

Knoten anzeigen

In CC-SG können Sie alle Knoten in der Knotenstrukturansicht anzeigen und einen Knoten zur Ansicht des Knotenprofils auswählen.

Knotenstrukturansicht

Wenn Sie auf die Registerkarte **Knoten** klicken, werden die verfügbaren Knoten in der Knotenstrukturansicht angezeigt. Knoten werden alphabetisch nach Namen angezeigt oder entsprechend ihrem Verfügbarkeitsstatus aufgeführt. Nach Status aufgeführte Knoten werden innerhalb ihrer Verfügbarkeitsgruppe alphabetisch sortiert. Klicken Sie zum Wechseln der Sortiermethode mit der rechten Maustaste auf die Strukturansicht. Klicken Sie dann auf **Knotensortieroptionen**, und wählen Sie **Nach Knotennamen** oder **Nach Knotenstatus** aus.

Knotenprofil

Klicken Sie in der Knotenstrukturansicht auf einen Knoten, um den Bildschirm **Knotenprofil** zu öffnen. Dieser Bildschirm enthält Informationen zu dem Knoten, der Standardschnittstelle und den Kategorien und Elementen, die dem Knoten zugewiesen wurden.

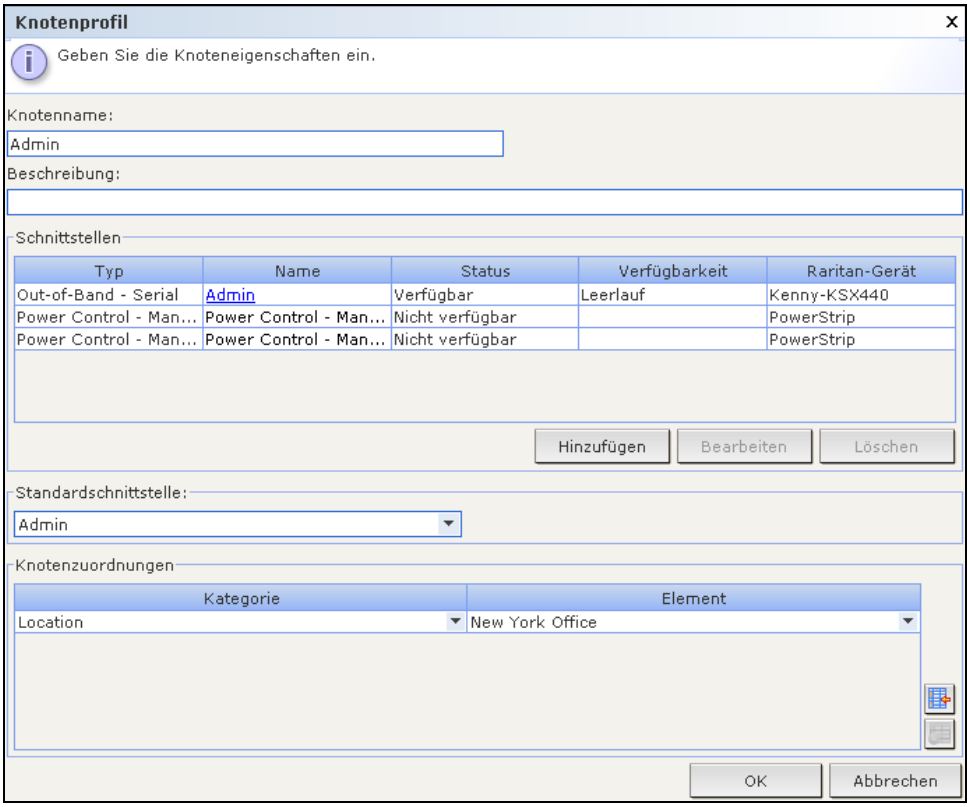


Abbildung 64 Registerkarte Knoten und Bildschirm Knotenprofil

Knoten- und Schnittstellensymbole

Knoten verfügen zur leichteren Unterscheidung über unterschiedliche Symbole in der Knotenstrukturansicht. Bewegen Sie den Mauszeiger auf ein Symbol in der Strukturansicht **Knoten**, um einen Tooltip mit Informationen zum Knoten anzuzeigen.

SYMBOL	BEDEUTUNG
	Knoten verfügbar: der Knoten verfügt über mindestens eine **verfügbare** Schnittstelle.
	Knoten nicht verfügbar: der Knoten hat bis jetzt noch keine **verfügbare** Schnittstelle.

Überblick über Knoten- und Schnittstellen

Knoten

Jeder Knoten stellt ein Ziel dar, das über CC-SG entweder über In-Band- (direkte IP) oder Out-of Band-Methoden (verbunden mit einem Raritan-Gerät) verfügbar ist. Ein Knoten kann beispielsweise ein Server in einem Gestell, der mit einem Raritan KVM-Gerät über ein IP-Gerät verbunden ist; ein Server mit einer HP iLO-Karte; ein PC in einem Netzwerk mit VNC oder eine Netzwerkinfrastuktureinheit mit einer seriellen Verbindung zur Remoteverwaltung sein.

Sie können CC-SG manuell Knoten hinzufügen, nachdem Sie die Geräte hinzugefügt haben, mit denen sie verbunden sind. Knoten können jedoch auch automatisch erstellt werden. Markieren Sie dazu beim Hinzufügen von Geräten im Bildschirm **Gerät hinzufügen** das Kontrollkästchen **Alle Ports konfigurieren**. Mithilfe dieser Option kann CC-SG automatisch alle Geräteports hinzufügen und einen Knoten und eine Out-of-Band KVM- oder serielle Schnittstelle für jeden Port hinzufügen. Sie können diese Knoten und Schnittstellen jederzeit wie in diesem Kapitel beschrieben bearbeiten. Weitere Informationen finden Sie in **Kapitel 3: Konfigurieren von CC-SG mit dem Setup-Assistenten** oder **Kapitel 5: Hinzufügen von Geräten und Gerätegruppen: Geräte hinzufügen**.

Knotennamen

Knotennamen müssen eindeutig sein. CC-SG stellt Vorschläge bereit, wenn Sie manuell einen Knoten mit einem bereits vorhandenen Knotennamen hinzufügen möchten. Wenn CC-SG automatisch Knoten hinzufügt, wird über ein Nummernsystem sichergestellt, dass Knotennamen eindeutig sind.

Schnittstellen

In CC-SG sind Knoten über Schnittstellen verfügbar. Sie müssen jedem neuen Knoten mindestens eine Schnittstelle hinzufügen. Sie können einem Knoten verschiedene Arten von Schnittstellen hinzufügen, um verschiedene Zugriffsarten bereitzustellen. Abhängig vom Knotentyp steht Folgendes zur Verfügung: Out-of-Band KVM, seriell oder Steuerung der Stromversorgung, oder In-Band SSH/RDP/VNC und DRAC/RSA/ILO.

Ein Knoten kann mehrere Schnittstellen, jedoch nur eine serielle Out-of-Band oder KVM-Schnittstelle aufweisen. Ein PC mit Windows Server 2003 kann beispielsweise eine Out-of-Band KVM-Schnittstelle über die Ports für Tastatur, Maus und Monitor und eine Stromversorgungs-Schnittstelle zum Verwalten des Ausgangs aufweisen, mit dem er verbunden ist.

Wichtig! Viele der in diesem Kapitel beschriebenen Befehle in der Menüleiste können aufgerufen werden, indem Sie mit der rechten Maustaste auf einen Knoten klicken und aus dem angezeigten Kontextmenü einen Befehl auswählen.

Knoten hinzufügen

So fügen Sie CC-SG einen neuen Knoten hinzu:

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Klicken Sie im Menü **Knoten** auf **Knoten hinzufügen**. Der Bildschirm **Knotenprofil** wird angezeigt.

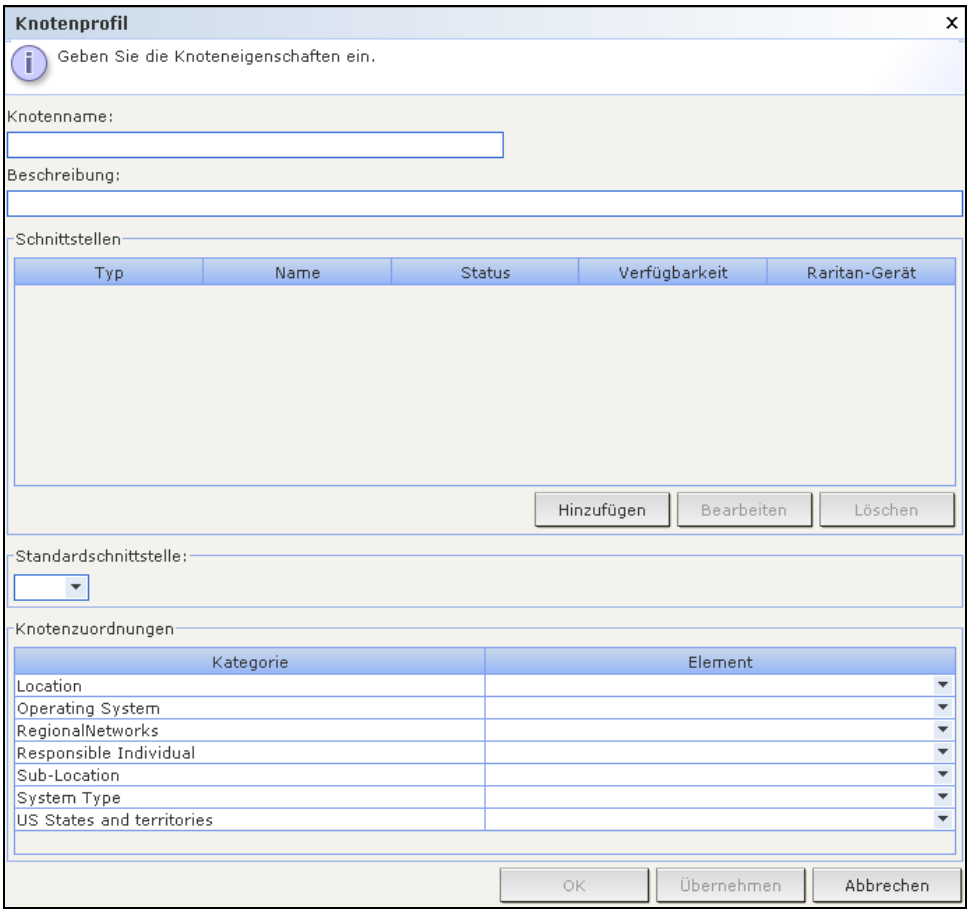


Abbildung 65 Fenster Knoten hinzufügen

3. Geben Sie den Namen des neuen Knotens im Feld **Knotenname** ein. Alle Knotennamen in CC-SG müssen eindeutig sein.
4. Sie können auch eine kurze Beschreibung für diesen Knoten in das Feld **Beschreibung** eingeben.
5. Sie müssen mindestens eine Schnittstelle konfigurieren. Klicken Sie im Bereich **Schnittstelle** des Bildschirms **Knoten hinzufügen** auf **Hinzufügen**, um eine Schnittstelle hinzuzufügen. Weitere Informationen finden Sie im folgenden Abschnitt **Schnittstellen hinzufügen**.
6. Sie können eine Liste mit **Kategorien** und **Elementen** konfigurieren, um diesen Knoten besser beschreiben und verwalten zu können. Weitere Informationen finden Sie in **Kapitel 4: Erstellen von Zuordnungen**.
   - Klicken Sie für jede aufgeführte **Kategorie** auf das Dropdown-Menü **Element**. Wählen Sie dann das Element zum Anwenden auf den Knoten in der Liste aus. Wählen Sie das leere Element im Feld **Element** für jede Kategorie aus, die Sie nicht verwenden möchten.
   - Wenn die Werte für **Kategorie** oder **Element**, die Sie verwenden möchten, nicht angezeigt werden, können Sie über das Menü **Zuordnungen** weitere hinzufügen. Weitere Informationen finden Sie in **Kapitel 4: Erstellen von Zuordnungen**.
7. Klicken Sie auf **OK**, um den Knoten zu speichern. Der Knoten wird der Knotenliste hinzugefügt.

Schnittstellen hinzufügen

1. Bei einem vorhandenen Knoten: Klicken Sie auf die Registerkarte **Knoten**, und wählen Sie den Knoten aus, dem Sie eine Schnittstelle hinzufügen möchten. Klicken Sie im Bereich **Schnittstellen** des Bildschirms **Knotenprofil** auf **Hinzufügen**.
   Beim Hinzufügen von neuen Knoten: Klicken Sie im Bereich **Schnittstellen** des Bildschirms **Knoten hinzufügen** auf **Hinzufügen**.
   Das Fenster **Schnittstelle hinzufügen** wird angezeigt.
2. Klicken Sie auf das Dropdown-Menü **Schnittstellentyp**, und wählen Sie die Verbindungsart für den Knoten aus:

   In-Band-Verbindungen
   - **DRAC KVM**: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem Dell DRAC-Server über eine DRAC-Schnittstelle herzustellen. Sie müssen anschließend eine DRAC-Stromversorgungs-Schnittstelle konfigurieren.
   - **RDP**: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem Knoten über ein Remote-Desktop-Protokoll (beispielsweise die Remote-Desktop-Verbindung auf einem Windows-Server) herzustellen.
   - **RSA KVM**: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem IBM RSA-Server über eine RSA-Schnittstelle herzustellen. Sie müssen danach eine RSA-Stromversorgungs-Schnittstelle konfigurieren.
   - **SSH**: Wählen Sie diese Option aus, um eine SSH-Verbindung zu einem Knoten herzustellen.
   - **VNC**: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem Knoten über eine VNC-Serversoftware herzustellen.
   - **iLO/RILOE KVM**: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem HP-Server über eine iLO- oder RILOE-Schnittstelle herzustellen.

   Out-of-Band-Verbindungen
   - **KVM**: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem Knoten über ein Raritan KVM-Gerät (KX, KX101, KSX, IP-Reach, Paragon II) herzustellen.
   - **Seriell**: Wählen Sie diese Option aus, um eine serielle Verbindung zu einem Knoten über ein serielles Raritan-Gerät (SX, KSX) herzustellen.

   Stromversorgungsverbindungen
   - **DRAC**: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem Dell DRAC-Server zu erstellen.
   - **IPMI**: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem Knoten über eine IPMI-Verbindung herzustellen.
   - **Verwalteter Powerstrip**: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem Knoten herzustellen, der über einen seriell verwalteten Raritan-Powerstrip versorgt wird.
   - **RSA**: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem RSA-Server zu erstellen.
   - **iLO/RILOE**: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem HP iLO/RILOE-Server zu erstellen.
3. Abhängig von den ausgewählten Optionen wird ein Standardname im Feld **Name** angezeigt. Sie können diesen Namen bei Bedarf ersetzen. Dieser Name wird neben der Schnittstelle in der Knotenliste angezeigt.

Für In-Band-Verbindungen und DRAC-, RSA- und iLO/RILOE-Stromversorgungsverbindungen:

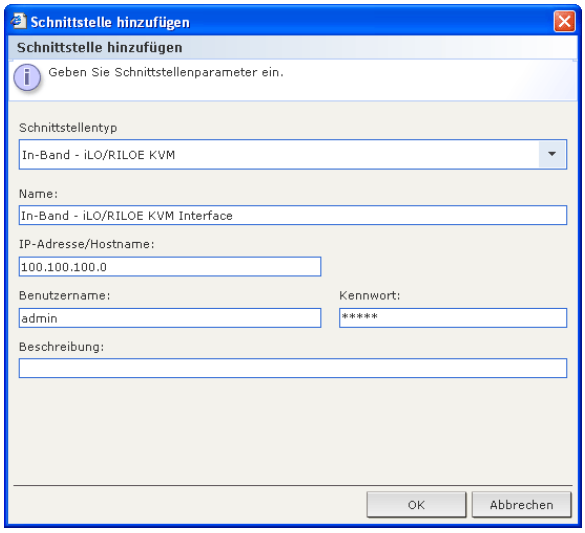


Abbildung 66 Schnittstelle hinzufügen – In-Band iLO/RILOE KVM

a. Geben Sie die IP-Adresse oder den Hostnamen dieser Schnittstelle in das Feld **IP-Adresse/ Hostname** ein.
b. Geben Sie bei Bedarf einen TCP-Port für diese Verbindung in das Feld **TCP-Port** ein.
c. Geben Sie einen Benutzernamen für diese Verbindung in das Feld **Benutzername** ein.
d. Geben Sie bei Bedarf ein Kennwort für diese Verbindung in das Feld **Kennwort** ein.
e. Klicken Sie auf **OK**, um dem Knoten die Schnittstelle hinzuzufügen. Der Bildschirm **Knoten hinzufügen** oder **Knotenprofil** wird angezeigt.

Für Out-of-Band KVM-, Out-of-Band serielle Verbindungen:

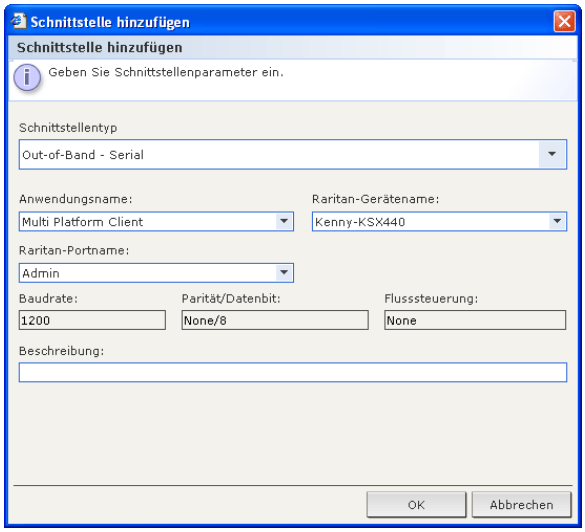


Abbildung 67 Out-of-Band KVM-Verbindung konfigurieren

a. Klicken Sie auf das Dropdown-Menü **Anwendungsname**, und wählen Sie die Anwendung aus, die Sie beim Verbinden mit dem Knoten über die Schnittstelle in der Liste verwenden möchten. CC-SG wählt die Anwendung basierend auf Ihrem Browser automatisch aus, wenn Sie **Automatisch erkennen** markieren.

b. Klicken Sie auf das Dropdown-Menü **Raritan-Gerätename**, und wählen Sie das Raritan-Gerät aus, das Zugriff auf diesen Knoten bereitstellt. Hinweis: Sie müssen zunächst ein Gerät zu CC-SG hinzufügen, bevor dies in der Liste angezeigt werden kann.

c. Klicken Sie auf das Dropdown-Menü **Raritan-Portname**, und wählen Sie den Port des Raritan-Geräts aus, das Zugriff auf diesen Knoten bereitstellt. Der Port muss in CC-SG konfiguriert werden, bevor er in der Liste angezeigt wird. Bei seriellen Verbindungen werden die Werte für **Baudrate**, **Parität** und **Flusssteuerung** anhand der Portkonfiguration ausgefüllt.

d. Klicken Sie auf **OK**, um dem Knoten die Schnittstelle hinzuzufügen. Der Bildschirm **Knoten hinzufügen** oder **Knotenprofil** wird angezeigt.

Bei verwalteten Powerstrip-Verbindungen:

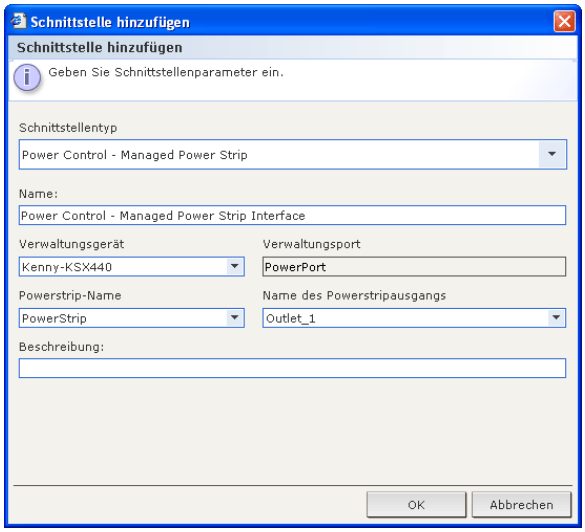


Abbildung 68 Stromversorgungs-Steuerungsschnittstelle für verwalteten Powerstrip konfigurieren

a. Klicken Sie auf das Dropdown-Menü **Verwaltungsgerät**, und wählen Sie das Raritan-Gerät aus, das den Powerstrip verwaltet, der den Knoten mit Strom versorgt. Das ausgewählte Gerät muss zu CC-SG hinzugefügt werden, bevor die entsprechenden Optionen verfügbar sind.

b. Klicken Sie auf das Dropdown-Menü **Powerstrip-Name**, und wählen Sie den Powerstrip aus, der den Knoten mit Strom versorgt. Der Powerstrip muss in CC-SG konfiguriert werden, bevor er in der Liste angezeigt wird.

c. Klicken Sie auf **Name des Powerstripausgangs**, und wählen Sie den Namen des Ausgangs aus, mit dem der Knoten verbunden ist.

d. Sie können auch eine Beschreibung für die Stromversorgungs-Schnittstelle in das Feld **Beschreibung** eingeben.

e. Klicken Sie auf **OK**, um dem Knoten die Schnittstelle hinzuzufügen. Der Bildschirm **Knoten hinzufügen** oder **Knotenprofil** wird angezeigt.

Bei IPMI-Stromversorgungsverbindungen:

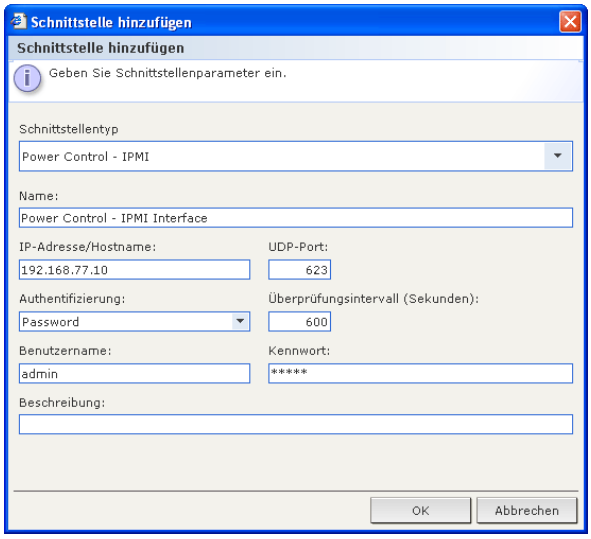


Abbildung 69 IPMI-Stromversorgungsverbindung konfigurieren

a. Geben Sie die IP-Adresse oder den Hostnamen dieser Schnittstelle in das Feld **IP-Adresse/ Hostname** ein.
b. Geben Sie einen UDP-Port für diese Schnittstelle in das Feld **UDP-Port** ein.
c. Klicken Sie auf das Dropdown-Menü **Authentifizierung**, und wählen Sie ein Authentifizierungsschema für die Verbindung mit dieser Schnittstelle aus.
d. Geben Sie für diese Schnittstelle ein Überprüfungsintervall im Feld **Überprüfungsintervall (Sekunden)** ein.
e. Geben Sie einen Benutzernamen für diese Schnittstelle im Feld **Benutzername** ein.
f. Geben Sie bei Bedarf ein Kennwort für diese Schnittstelle im Feld **Kennwort** ein.
g. Klicken Sie auf **OK**, um dem Knoten die Schnittstelle hinzuzufügen. Der Bildschirm **Knoten hinzufügen** oder **Knotenprofil** wird angezeigt.

Ergebnisse nach dem Hinzufügen von Schnittstellen

Nachdem Sie eine Schnittstelle hinzugefügt haben, wird diese auf dem Bildschirm **Knoten hinzufügen** oder **Knotenprofil** in der Tabelle **Schnittstellen** und dem Dropdown-Menü **Standardschnittstelle** angezeigt. Sie können auf das Dropdown-Menü klicken, um die Standardschnittstelle auszuwählen, die für Verbindungen zu Knoten verwendet werden soll.

Nachdem Sie die Änderungen im Bildschirm **Knoten hinzufügen** oder **Knotenprofil** gespeichert haben, werden die Namen der Schnittstellen auch in den Knotenlisten verschachtelt unter dem Knoten angezeigt, für den sie den Zugriff bereitstellen.

Verbindung zu einem Knoten herstellen

Nachdem ein Knoten mit einer Schnittstelle verknüpft ist, haben Sie verschiedene Möglichkeiten, eine Verbindung zu diesem Knoten über die Schnittstelle herzustellen. Weitere Informationen hierzu finden Sie im Raritan-Handbuch **CommandCenter Secure Gateway-Benutzerhandbuch**.

Abbildung 70 Verbindung zu einer konfigurierten Schnittstelle eines Knotens herstellen

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Wählen Sie den Knoten aus, zu dem Sie eine Verbindung herstellen möchten. Der Bildschirm **Knotenprofil** wird angezeigt.
3. Klicken Sie in der Tabelle **Schnittstellen** auf den Namen der Schnittstelle, über die Sie die Verbindung herstellen möchten.

Alternative:

1. Klicken Sie auf der Registerkarte **Knoten** auf das Symbol + neben dem Knoten, zu dem Sie eine Verbindung aufbauen möchten. Eine Liste der Schnittstellen wird darunter angezeigt.
2. Doppelklicken Sie auf den Namen der Schnittstelle, über die Sie eine Verbindung herstellen möchten.

Schnittstellen bearbeiten

So bearbeiten Sie eine Schnittstelle:

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Klicken Sie auf den Knoten mit der Schnittstelle, die Sie bearbeiten möchten. Der Bildschirm **Knotenprofil** wird angezeigt.
3. Wählen Sie in der Tabelle **Schnittstellen** die Schnittstellenzeile aus, die Sie bearbeiten möchten.
4. Klicken Sie auf **Bearbeiten**. Das Fenster **Schnittstelle bearbeiten** wird angezeigt.

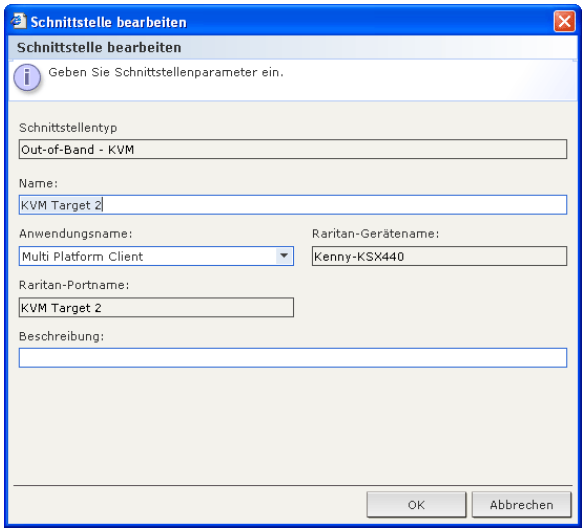


Abbildung 71 Schnittstellen bearbeiten

5. Sie können den Typ einer vorhandenen Schnittstelle nicht ändern. Sie können die Werte **Schnittstellenname**, **Beschreibung** sowie die Werte für andere Felder dieses Typs ändern. Weitere Informationen finden Sie im Abschnitt **Schnittstellen hinzufügen** oben.

Schnittstellen löschen

So löschen Sie eine Schnittstelle eines Knotens:

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Klicken Sie auf den Knoten mit der Schnittstelle, die Sie löschen möchten. Der Bildschirm **Knotenprofil** wird angezeigt.
3. Wählen Sie in der Tabelle **Schnittstellen** die Schnittstellenzeile aus, die Sie löschen möchten.
4. Klicken Sie auf **Löschen**. Sie werden aufgefordert, Ihre Auswahl zu bestätigen.
5. Klicken Sie auf **Ja**, um die Schnittstelle zu löschen.

Knoten anpingen

Sie können einen Knoten über CC-SG anpingen, um sicherzustellen, dass die Verbindung aktiv ist.

1. Klicken Sie auf die Registerkarte **Knoten**, und wählen Sie den Knoten zum Anpingen aus.
2. Klicken Sie im Menü **Knoten** auf **Knoten anpingen**. Die Ergebnisse des Pingvorgangs werden angezeigt.

Knoten bearbeiten

Vorhandene Knoten werden auf der Registerkarte **Knoten** angezeigt und können bearbeitet werden. So bearbeiten Sie Knoten:

1. Klicken Sie auf die Registerkarte **Knoten**, und wählen Sie den Knoten zum Bearbeiten aus. Der Bildschirm **Knotenprofil** wird angezeigt.

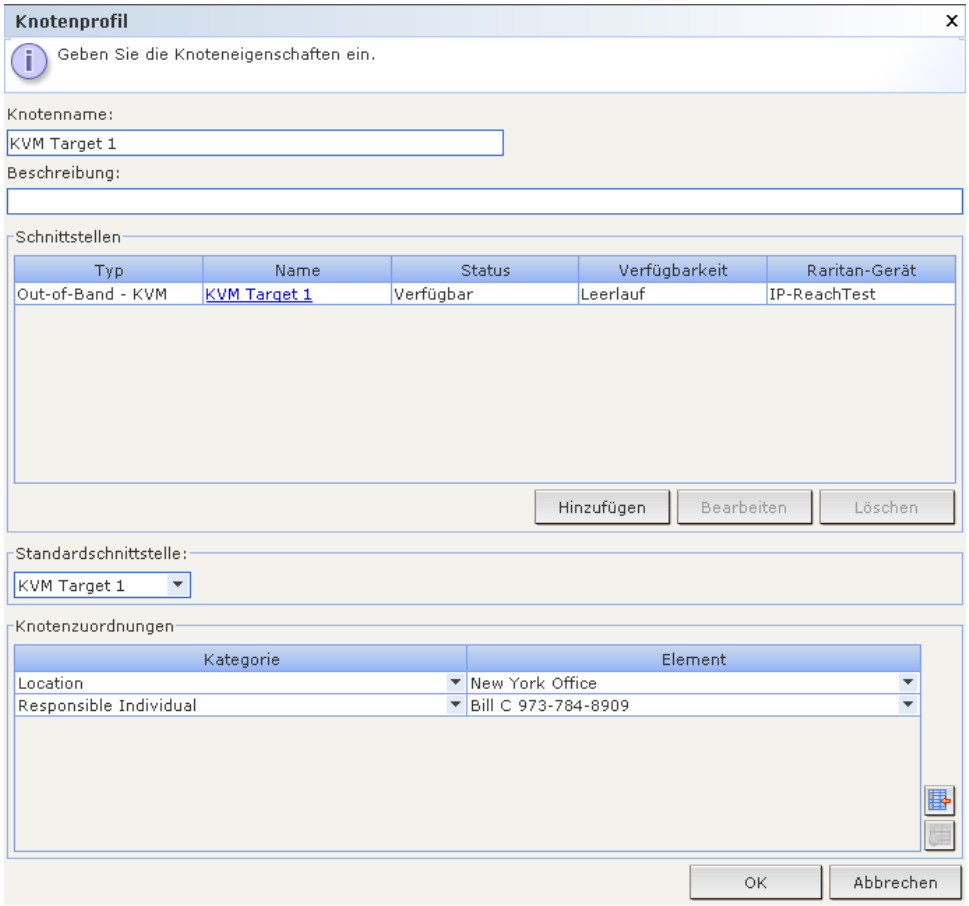


Abbildung 72 Fenster Knoten bearbeiten

2. Geben Sie bei Bedarf einen neuen Namen für den Knoten im Feld **Knotenname** ein. Alle Knotennamen in CC-SG müssen eindeutig sein.
3. Sie können auch eine neue kurze Beschreibung für diesen Knoten in das Feld **Beschreibung** eingeben.
4. Klicken Sie im Fensterbereich **Schnittstellen** auf **Hinzufügen**, um eine neue Schnittstelle hinzuzufügen. Weitere Informationen finden Sie im Abschnitt **Schnittstellen hinzufügen** oben.
5. Wählen Sie in der Tabelle **Schnittstellen** einen vorhandenen Knoten aus, und klicken Sie auf **Bearbeiten** oder **Löschen**, um diese Schnittstelle des Knotens zu bearbeiten oder zu löschen. Weitere Informationen finden Sie oben in den Abschnitten **Schnittstellen bearbeiten** oder **Schnittstellen löschen**.
6. Sie können eine Liste mit **Kategorien** und **Elementen** konfigurieren, um diesen Knoten besser beschreiben und verwalten zu können. Eine Kategorie bietet die Möglichkeit, einen Knoten zu klassifizieren, und ein Element stellt einen bestimmten Wert für die Klassifizierung dar. Stellt der Knoten beispielsweise einen PC aus der Technikabteilung dar, könnte für eine Kategorie „Abteilung“ das Element „Technik“ ausgewählt werden.
   So konfigurieren Sie **Kategorien** und **Elemente** für den Knoten:
   a. Doppelklicken Sie für jede **Kategorie** in der Liste, der Sie einen Wert zuweisen möchten, auf das Feld **Element**. Das Feld wird als Dropdown-Menü angezeigt.
   b. Klicken Sie auf das Dropdown-Menü, und wählen Sie den gewünschten Wert **Element** aus. Wählen Sie **Keine** aus, wenn Sie diese Kategorie nicht verwenden möchten.

   Wenn die gewünschten Werte für **Kategorie** oder **Element** nicht angezeigt werden, können Sie über das Menü **Zuordnungen** weitere hinzufügen. Weitere Informationen zum Erstellen von Kategorien und Elementen finden Sie in **Kapitel 4: Erstellen von Zuordnungen**.
7. Klicken Sie auf **OK**, wenn Sie die Konfiguration des Knotens abgeschlossen haben.

Knoten löschen

Wenn Sie einen Knoten löschen, wird dieser aus der Liste **Knoten** entfernt. Der Knoten steht Benutzern dann nicht mehr zur Verfügung. Außerdem werden alle Schnittstellen und Zuordungen entfernt.

So löschen Sie Knoten:

1. Klicken Sie links auf die Registerkarte **Knoten**.
2. Klicken Sie mit der rechten Maustaste auf den Knoten, den Sie löschen möchten, und klicken Sie dann auf **Knoten löschen**. Im Fenster **Knoten löschen** wird der Name des ausgewählten Knotens angezeigt.

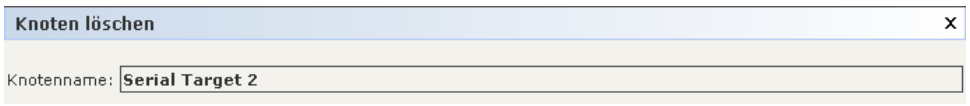


Abbildung 73 Knoten löschen

3. Klicken Sie zum Löschen des Knotens auf **OK**, oder klicken Sie auf **Abbrechen**, um den Vorgang ohne Löschen abzubrechen.

Chat

Chat bietet Benutzern, die mit einem Knoten verbunden sind, die Möglichkeit, miteinander zu kommunizieren. Sie müssen mit einem Knoten verbunden sein, um eine Chatsitzung für den Knoten zu starten. Nur Benutzer, die mit demselben Knoten verbunden sind, können miteinander chatten.

So nehmen Sie an einer Chatsitzung teil:

1. Klicken Sie links auf die Registerkarte **Knoten**.
2. Klicken Sie mit der rechten Maustaste auf den Knoten, mit dem Sie zurzeit verbunden sind, und wählen Sie **Chat** aus. Klicken Sie dann auf **Chatsitzung starten**, falls noch keine Sitzung verfügbar ist. Es wird eine Chatsitzung erstellt.

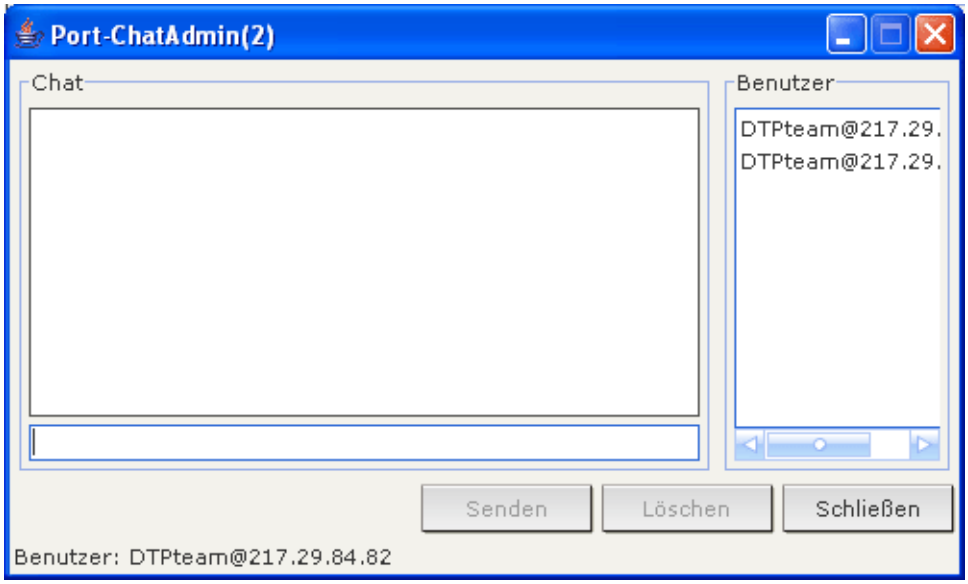


Abbildung 74 Chatsitzung für einen Knoten

   Ist bereits eine Chatsitzung verfügbar, klicken Sie mit der rechten Maustaste auf den Knoten, wählen Sie **Chat** und dann **Chatsitzung anzeigen** aus, um der Chatsitzung beizutreten.
   Das Fenster mit der Chatsitzung wird in den Nachrichtenfeldern links und eine Liste der Benutzer in dieser Chatsitzung rechts angezeigt.

3. Geben Sie eine Nachricht in das Feld für neue Nachrichten (unten links) ein, und drücken Sie die <**Eingabetaste**> oder klicken Sie auf **Senden**. Die Nachricht wird für alle Benutzer im Chatfeld (oben links) angezeigt.
4. Klicken Sie auf **Löschen**, um Nachrichten zu löschen, die Sie in das Feld für neue Nachrichten eingegeben, jedoch nicht gesendet haben. Das Chatfeld wird durch den Löschvorgang nicht gelöscht.
5. Klicken Sie auf **Schließen**, um die Chatsitzung zu beenden oder zu verlassen.
6. Sie werden gefragt, ob Sie die Chatsitzung schließen möchten. Klicken Sie auf **Ja**, um diese Chatsitzung für alle Teilnehmer zu schließen, oder auf **Nein**, um die Chatsitzung zu verlassen jedoch für andere nicht zu schließen.

Sie können die Chatsitzung für alle Teilnehmer auch über die Registerkarte **Knoten** schließen. Klicken Sie mit der rechten Maustaste auf den Knoten mit der Chatsitzung, wählen Sie **Chat** und dann **Chatsitzung beenden** aus.

Knotengruppen

Mithilfe von Knotengruppen können Administratoren logische Gruppen von Knoten entweder willkürlich oder auf den Kategorien und Elementen basierend erstellen. Diese werden dann beim Erstellen von Zugriffsrichtlinien verwendet. Weitere Informationen zum Erstellen von Knotengruppen und Anwenden von Gruppen auf Richtlinien finden Sie in **Kapitel 8: Richtlinien**.

Klicken Sie zum Anzeigen des Fensters **Knotengruppen** mit der rechten Maustaste in die Knotenliste, und wählen Sie **Knotengruppen** aus.

Kapitel 7: Hinzufügen und Verwalten von Benutzern und Benutzergruppen

Benutzer stellen die einzelnen Benutzer und Administratoren dar, die eine Verbindung zu CC-SG herstellen, um auf Knoten zuzugreifen und Geräte zu verwalten. **Benutzergruppen** sind Organisationseinheiten, die einen Satz von Rechten für die Benutzermitglieder festlegen. Benutzer selbst haben keine Berechtigungen. Im Allgemeinen müssen alle Benutzer einer Benutzergruppe angehören.

CC-SG verwaltet eine eigene zentralisierte Benutzerliste und Benutzergruppenliste zur Authentifizierung und Autorisierung, die in diesem Kapitel beschrieben wird. Bei der Verwendung externer Authentifizierungsschemas (beispielsweise RADIUS oder Active Directory) müssen trotzdem Benutzergruppen und Richtlinien (siehe **Kapitel 8: Richtlinien**) für CC-SG erstellt werden. Die Konfiguration von CC-SG zur Verwendung externer Authentifizierung wird in **Kapitel 9: Remoteauthentifizierung** beschrieben.

Benutzerstruktur

Klicken Sie auf die Registerkarte **Benutzer**, um die Benutzerstruktur anzuzeigen.

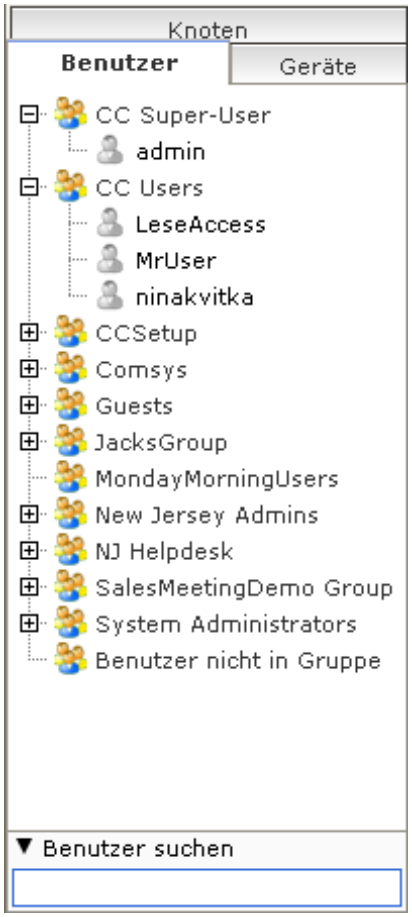


Abbildung 75 Benutzerstruktur

In der Benutzerstruktur werden alle Benutzergruppen und Benutzer in CC-SG angezeigt. Benutzer sind unter den Benutzergruppen angeordnet, denen sie zugewiesen sind. Benutzergruppen mit zugeordneten Benutzern werden in der Liste mit dem Symbol + angezeigt. Wenn Sie auf das Symbol klicken, wird die Liste der Benutzermitglieder ein- oder ausgeblendet. Aktive Benutzer, die zurzeit bei CC-SG angemeldet sind, werden in Fettdruck dargestellt.

Mithilfe der Benutzerstruktur können Sie in der Struktur nach Benutzern suchen. Sie können die Suchmethode über den Bildschirm **Mein Profil** konfigurieren, der später in diesem Kapitel beschrieben wird.

Spezielle Benutzergruppen

In CC-SG sind standardmäßig drei Benutzergruppen konfiguriert: **CC-Superuser**, **Systemadministratoren** und **CC Users**.

Die CC-Superuser-Gruppe

Die CC-Superuser-Gruppe verfügt über alle Verwaltungs- und Zugriffsberechtigungen. Nur ein Benutzer kann Mitglied dieser Gruppe sein. Der Standard-Benutzername lautet **admin**. Sie können den Standard-Benutzernamen ändern. Die CC-Superuser-Gruppe kann nicht gelöscht werden. Sie können die der CC-Superuser-Gruppe zugewiesenen Berechtigungen nicht ändern, keine weiteren Mitglieder hinzufügen oder den einzigen Benutzer der Gruppe löschen. Für das Mitglied der CC-Superuser-Gruppe sind immer sichere Kennwörter aktiviert.

Systemadministratorgruppe

Die **Systemadministratorgruppe** verfügt über alle Verwaltungs- und Zugriffsberechtigungen. Im Gegensatz zur CC-Superuser-Gruppe können Sie die Berechtigungen ändern und Mitglieder hinzufügen oder löschen.

CC Users-Gruppe

Die **CC Users-Gruppe** verfügt über In-Band- und Out-of-Band-Knotenzugriff. Sie können die Berechtigungen ändern und Mitglieder hinzufügen oder löschen.

Benutzer nicht in Gruppe

Benutzer nicht in Gruppe verfügt über keine Berechtigungen und Benutzer können in dieser Gruppe weder erstellt werden noch manuell in die Gruppe verschoben werden. Benutzer werden dieser Gruppe zugeordnet, wenn Sie aus allen vorhandenen Benutzergruppen entfernt werden.

Wichtig! Viele Befehle in diesem Kapitel können nur ausgewählt werden, wenn zuvor die entsprechende Benutzergruppe oder der Benutzer ausgewählt wurde.

Viele der in diesem Abschnitt beschriebenen Befehle in der Menüleiste können aufgerufen werden, indem Sie mit der rechten Maustaste auf eine Benutzergruppe oder einen Benutzer klicken und aus dem angezeigten Kontextmenü einen Befehl auswählen.

Benutzergruppen hinzufügen

Wenn Sie zunächst Benutzergruppen erstellen, können Sie Benutzer beim Hinzufügen einfacher organisieren. Beim Erstellen einer Benutzergruppe wird dieser Benutzergruppe ein Satz an Berechtigungen zugewiesen. Benutzer, die dieser Gruppe zugewiesen werden, erben diese Berechtigungen. Wenn Sie beispielsweise eine Gruppe erstellen und dieser die Berechtigung **Benutzermanagement** zuweisen, können alle Benutzer dieser Gruppe die Befehle im Menü **Benutzermanager** anzeigen und ausführen. Weitere Informationen zu den Berechtigungen finden Sie in **Anhang D: Benutzergruppenberechtigungen**.

Das Konfigurieren von Benutzergruppen umfasst vier Schritte:

- Name und Beschreibung für die Gruppe eingeben
- Berechtigungen für die Benutzergruppe auswählen
- Schnittstellentypen auswählen, die Benutzer für den Zugriff auf Knoten verwenden können
- Richtlinien auswählen, die beschreiben, auf welche Knoten die Benutzergruppe zugreifen kann

So erstellen Sie eine neue Benutzergruppe:

1. Wählen Sie im Menü **Benutzer** die Option **Benutzergruppenmanager** und dann **Benutzergruppe hinzufügen** aus. Das Fenster **Benutzergruppe hinzufügen** wird angezeigt.

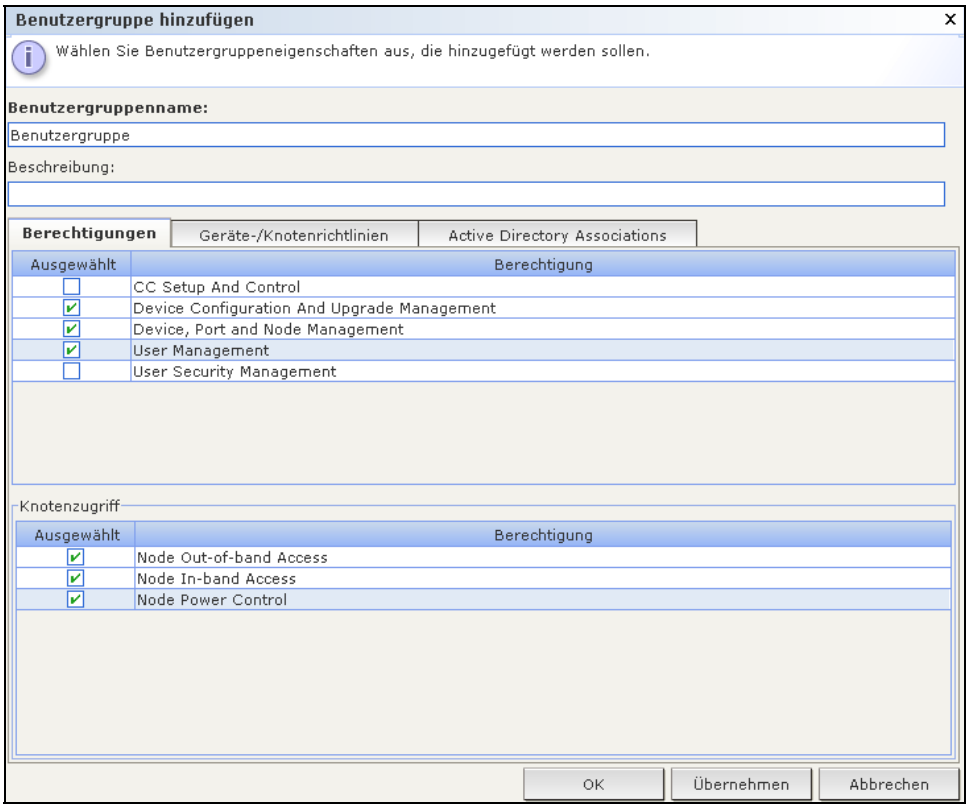


Abbildung 76 Fenster Benutzergruppe hinzufügen

2. Geben Sie einen neuen Benutzergruppennamen in das Feld **Benutzergruppenname** ein. Benutzergruppennamen müssen eindeutig sein.
3. Sie können auch eine kurze Beschreibung für die Gruppe in das Feld **Beschreibung** eingeben.
4. Klicken Sie auf die Registerkarte **Berechtigungen**.
5. Markieren Sie die Kontrollkästchen für die Berechtigungen, die Sie der Benutzergruppe zuweisen möchten.
6. Unter der Berechtigungstabelle wird der Bereich **Knotenzugriff** mit Berechtigungen für drei Arten des Knotenzugriffs angezeigt: **Out-of-Band-Zugriff**, **In-Band-Zugriff** und **Stromversorgung für Knoten steuern**. Markieren Sie das Kontrollkästchen für die Art des Knotenzugriffs, die Sie der Benutzergruppe zuweisen möchten.

7. Klicken Sie auf die Registerkarte **Geräte-/Knotenrichtlinien**. Eine Tabelle mit Richtlinien wird angezeigt.

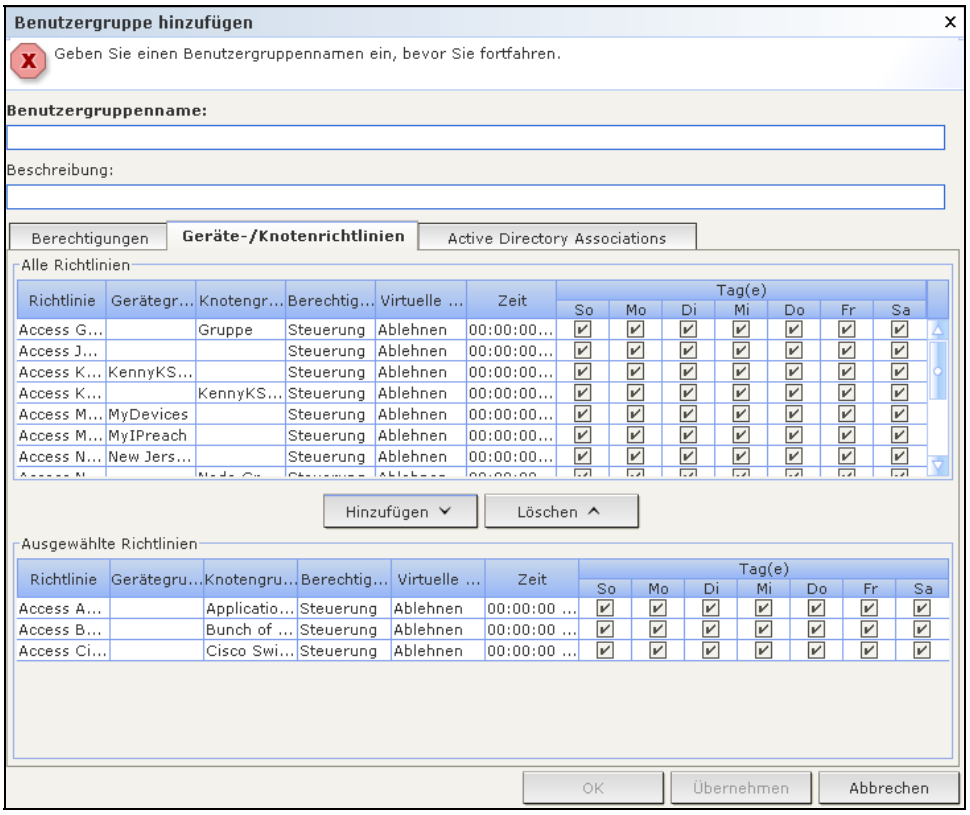


Abbildung 77 Registerkarte Richtlinien im Fenster Benutzergruppe hinzufügen

In der Tabelle **Alle Richtlinien** werden alle Richtlinien für CC-SG angezeigt. Jede Richtlinie stellt eine Regel dar, die den Zugriff auf eine Knotengruppe zulässt oder verweigert. Weitere Informationen zu Richtlinien und der Erstellung von Richtlinien finden Sie in **Kapitel 8: Richtlinien**.

8. Wählen Sie in der Liste **Alle Richtlinien** die Richtlinie aus, die Sie der Benutzergruppe zuweisen möchten, und klicken Sie auf **Hinzufügen**, um die Richtlinie in die Liste **Ausgewählte Richtlinien** zu verschieben. Mithilfe von Richtlinien in der Liste **Ausgewählte Richtlinien** erhalten Benutzer Zugriff auf den Knoten (oder auf Geräte), die durch diese Richtlinie gesteuert werden, oder der Zugriff wird verweigert.
9. Wiederholen Sie diesen Schritt, um der Benutzergruppe weitere Richtlinien zuzuweisen.
10. Wenn Sie dieser Gruppe den Zugriff auf alle verfügbaren Knoten gewähren möchten, wählen Sie in der Liste **Alle Richtlinien** die Option **Full Access Policy** (Richtlinie für unbeschränkten Zugriff) aus, und klicken Sie auf **Hinzufügen**.
11. Wählen Sie zum Löschen einer Richtlinie in der Benutzergruppe den Namen der Richtlinie in der Liste **Ausgewählte Richtlinien** aus, und klicken Sie auf **Löschen**.
12. Wenn Sie alle gewünschten Richtlinien für diese Gruppe konfiguriert haben, klicken Sie auf **Übernehmen**, um diese Gruppe zu speichern und eine weitere zu erstellen, oder auf **OK**, um die Benutzergruppe zu speichern, ohne weitere zu erstellen. Wenn Sie auf **Übernehmen** klicken, wiederholen Sie die Schritte in diesem Abschnitt, um weitere Benutzergruppen hinzuzufügen.

Benutzergruppen bearbeiten

Bearbeiten Sie eine Benutzergruppe, um die vorhandenen Berechtigungen und Richtlinien der Gruppe zu ändern.

***Hinweis**: Sie können die Berechtigungen und Richtlinien der Gruppen **CC-SuperUser** und **Benutzer nicht in Gruppe** nicht bearbeiten.*

So bearbeiten Sie Gruppen:

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf der Registerkarte **Benutzer** auf eine Benutzergruppe. Das **Benutzergruppenprofil** wird angezeigt.

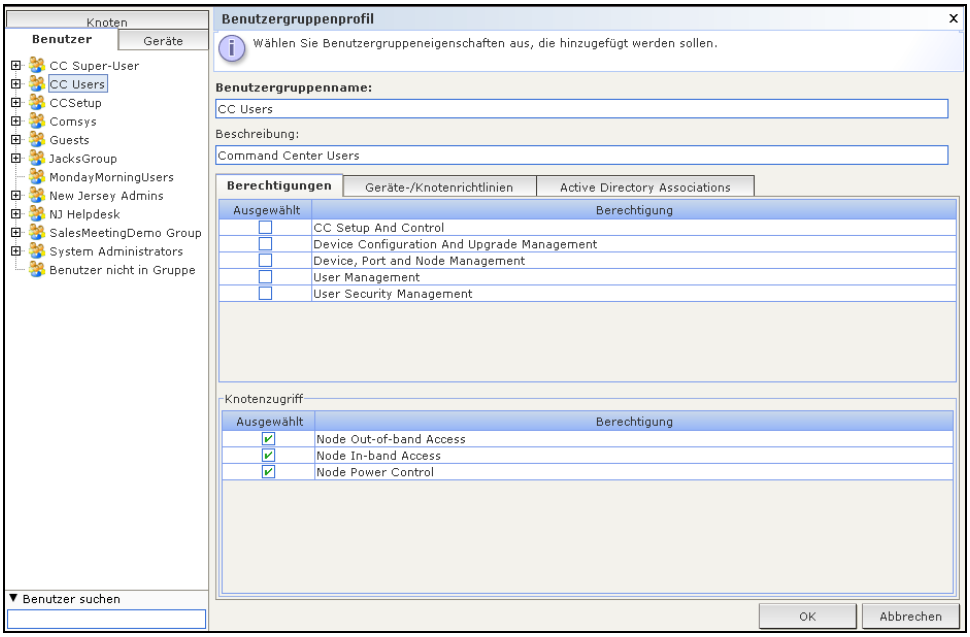


Abbildung 78 Ausgewählte Gruppen bearbeiten

3. Geben Sie bei Bedarf einen neuen Benutzergruppennamen in das Feld **Benutzergruppenname** ein.
4. Sie können auch eine neue Beschreibung für die Benutzergruppe in das Feld **Beschreibung** eingeben.
5. Klicken Sie auf die Registerkarte **Berechtigungen**.
6. Markieren Sie die Kontrollkästchen für die Berechtigungen, die Sie der Benutzergruppe zuweisen möchten. Heben Sie die Markierung einer Berechtigung auf, um sie aus der Gruppe zu entfernen.
7. Klicken Sie im Bereich **Knotenzugriff** auf das Dropdown-Menü jeder Schnittstelle, über die diese Gruppe zugreifen darf, und wählen Sie **Steuerung** aus.
8. Klicken Sie auf das Dropdown-Menü jeder Schnittstelle, über die diese Gruppe nicht zugreifen darf, und wählen Sie **Ablehnen** aus.
9. Klicken Sie auf die Registerkarte **Richtlinien**. Es werden zwei Tabellen mit Richtlinien angezeigt.
10. Wählen Sie jede Richtlinie, die Sie der Gruppe hinzufügen möchten, unter **Alle Richtlinien** aus, und klicken Sie auf **Hinzufügen**, um sie in die Liste **Ausgewählte Richtlinien** zu verschieben. Mithilfe von Richtlinien in der Liste **Ausgewählte Richtlinien** erhalten Benutzer Zugriff auf den Knoten (oder auf Geräte), die durch diese Richtlinie gesteuert werden, oder der Zugriff wird verweigert.

11. Wählen Sie zum Löschen einer Richtlinie aus der Benutzergruppe den Namen der Richtlinie in der Liste **Ausgewählte Richtlinien** aus, und klicken Sie auf **Löschen**.
12. Wenn Sie alle Richtlinien für diese Gruppe konfiguriert haben, klicken Sie auf **OK**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen zu verwerfen.

Benutzergruppe löschen

Wenn Sie eine Benutzergruppe löschen, wird diese Gruppe aus CC-SG entfernt. Benutzer dieser gelöschten Gruppe bleiben Mitglied der anderen Gruppen, denen sie angehören. Sind die Benutzer der gelöschten Gruppe in keinen weiteren Gruppen enthalten, werden sie der Gruppe **Benutzer nicht in Gruppe** zugewiesen, die über keine Berechtigungen verfügt.

So löschen Sie Benutzergruppen:

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf der Registerkarte **Benutzer** auf die Benutzergruppe, die gelöscht werden soll.
3. Wählen Sie im Menü **Benutzer** die Option **Benutzergruppenmanager** und dann **Benutzergruppe löschen** aus. Das Fenster **Benutzergruppe löschen** wird angezeigt.

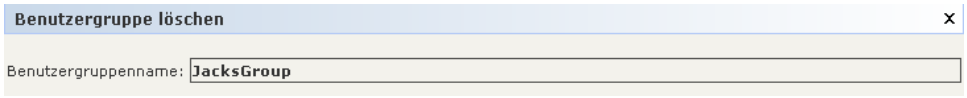


Abbildung 79 Benutzergruppen löschen

4. Klicken Sie zum Löschen der Benutzergruppe auf **OK**, oder klicken Sie auf **Abbrechen**, um den Vorgang ohne Löschen abzubrechen.

Wenn Sie auf **OK** klicken, wird eine Statusmeldung angezeigt, um den erfolgreichen Löschvorgang der Gruppe zu bestätigen.

Benutzer hinzufügen

Weisen Sie Gruppen Benutzer zu, um dem Benutzer Zugriffsberechtigungen in CC-SG zuzuweisen. Die Fähigkeit eines Benutzers, auf Knoten zuzugreifen oder Geräte zu verwalten, hängt davon ab, welcher Benutzergruppe er angehört.

So fügen Sie Benutzer hinzu:

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf der Registerkarte **Benutzer** auf die Benutzergruppe, der Sie einen Benutzer hinzufügen möchten. (Sie müssen zum Hinzufügen von Benutzern eine Gruppe auswählen.)
3. Wählen Sie im Menü **Benutzer** die Option **Benutzermanager** und dann **Benutzer hinzufügen** aus. Das Fenster **Benutzer hinzufügen** wird angezeigt.

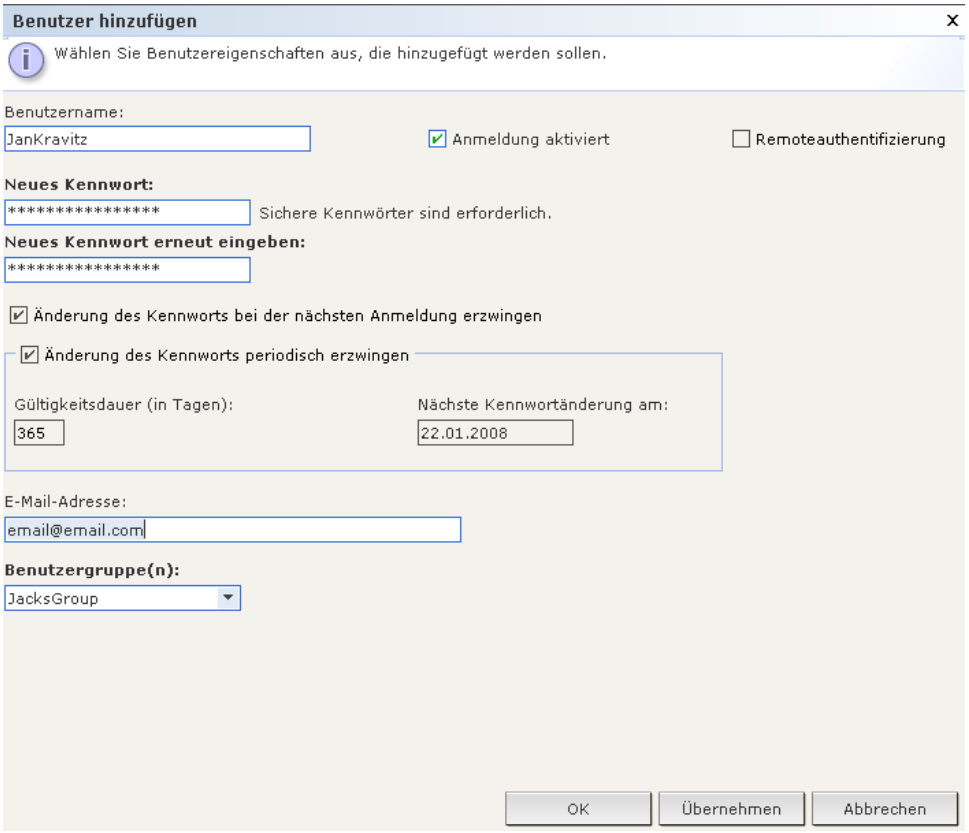


Abbildung 80 Benutzer hinzufügen

4. Geben Sie im Feld **Benutzername** den Benutzernamen des Benutzer ein, der hinzugefügt werden soll. Dieser Name wird für die Anmeldung bei CC-SG verwendet.
5. Markieren Sie das Kontrollkästchen **Anmeldung aktiviert**, wenn der Benutzer über die Anmeldeberechtigung für CC-SG verfügen soll.
6. Markieren Sie das Kontrollkästchen **Remoteauthentifizierung** nur, wenn der Benutzer mithilfe eines externen Servers wie TACACS+, RADIUS, LDAP oder AD authentifiziert werden soll. Wenn Sie die Remoteauthentifizierung verwenden, benötigen Sie kein Kennwort, und die Felder **Neues Kennwort** und **Neues Kennwort erneut eingeben** sind deaktiviert.
7. Geben Sie in die Felder **Neues Kennwort** und **Neues Kennwort erneut eingeben** das Kennwort ein, das der Benutzer zur Anmeldung in CC-SG verwenden soll.

***Hinweis**: Sind sichere Kennwörter aktiviert, muss das eingegebene Kennwort den definierten Regeln entsprechen. In der Informationszeile oben im Bildschirm wird eine Nachricht mit den Kennwortanforderungen angezeigt. Weitere Informationen zu sicheren Kennwörtern finden Sie in **Kapitel 12: Erweiterte Administration**.*

8. Markieren Sie das Kontrollkästchen **Änderung des Kennworts bei der nächsten Anmeldung erzwingen**, wenn der Benutzer gezwungen werden soll, das zugewiesene Kennwort bei der nächsten Anmeldung zu ändern.
9. Markieren Sie das Kontrollkästchen **Änderung des Kennworts periodisch erzwingen**, wenn Sie angeben möchten, wie oft der Benutzer zur Kennwortänderung gezwungen werden soll.
    a. Falls das Feld **Gültigkeitsdauer (in Tagen)** markiert ist, geben Sie die Anzahl von Tagen ein, die der Benutzer dasselbe Kennwort verwenden kann, bevor eine Änderung erzwungen wird.
10. Geben Sie die E-Mail-Adresse des Benutzers in das Feld **E-Mail-Adresse** ein. Sie wird zum Senden der Benutzerbenachrichtigungen verwendet.
11. Wenn Sie die Gruppe ändern möchten, der Sie diesen Benutzer hinzufügen, klicken Sie auf das Dropdown-Menü **Benutzergruppen**, und wählen Sie eine neue Gruppe aus.
12. Wenn Sie die Konfiguration dieses Benutzers abgeschlossen haben, klicken Sie auf **Übernehmen**, um diesen Benutzer hinzuzufügen und einen weiteren zu erstellen. Sie können auch auf **OK** klicken, um den Benutzer hinzuzufügen ohne weitere zu erstellen. Die erstellten Benutzer werden auf der Registerkarte **Benutzer** unter den Benutzergruppen angezeigt, denen sie zugewiesen sind.

Benutzer bearbeiten

So bearbeiten Sie Benutzer:

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf das Symbol + neben der Benutzergruppe, die den Benutzer enthält, den Sie bearbeiten möchten.
3. Klicken Sie auf den Benutzer, den Sie bearbeiten möchten. Das **Benutzerprofil** wird angezeigt.

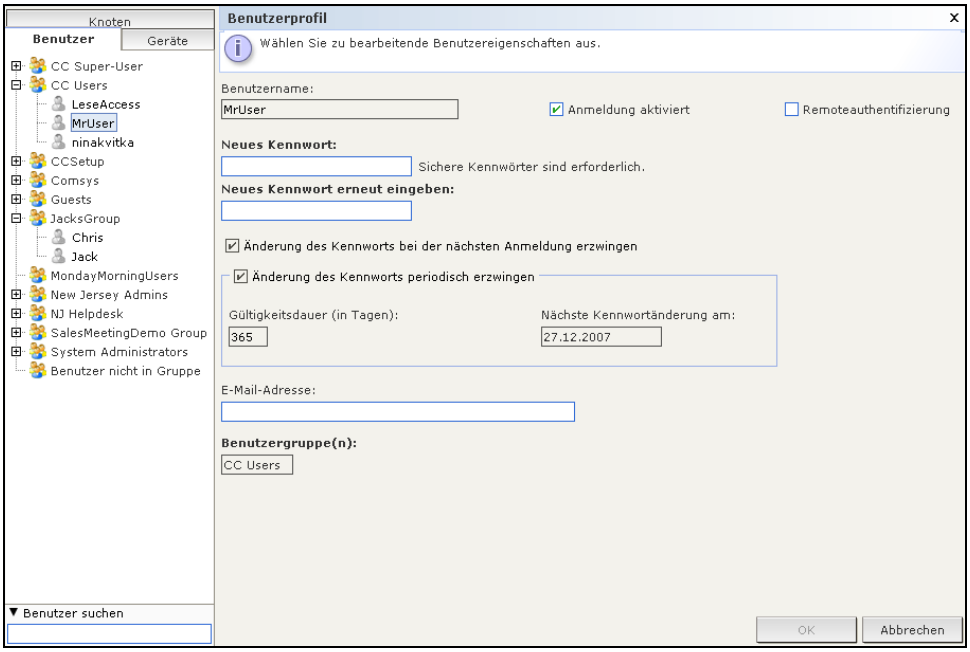


Abbildung 81 Ausgewählte Benutzer bearbeiten

4. Deaktivieren Sie **Anmeldung aktiviert**, wenn dieser Benutzer sich nicht bei CC-SG anmelden darf. Aktivieren Sie **Anmeldung aktiviert**, wenn sich dieser Benutzer bei CC-SG anmelden darf.
5. Markieren Sie das Kontrollkästchen **Remoteauthentifizierung** nur, wenn der Benutzer mithilfe eines externen Servers wie TACACS+, RADIUS, LDAP oder AD authentifiziert werden soll. Wenn Sie die Remoteauthentifizierung verwenden, benötigen Sie kein Kennwort, und die Felder **Neues Kennwort** und **Neues Kennwort erneut eingeben** sind deaktiviert.
6. Geben Sie in die Felder **Neues Kennwort** und **Neues Kennwort erneut eingeben** ein neues Kennwort ein, um das Benutzerkennwort zu ändern.

Hinweis: *Sind sichere Kennwörter aktiviert, muss das eingegebene Kennwort den definierten Regeln entsprechen. In der Informationszeile oben im Bildschirm werden die Kennwortanforderungen angezeigt. Weitere Informationen zu sicheren Kennwörtern finden Sie in* ***Kapitel 12: Erweiterte Administration****.*

7. Markieren Sie das Kontrollkästchen **Änderung des Kennworts bei der nächsten Anmeldung erzwingen**, wenn der Benutzer gezwungen werden soll, das zugewiesene Kennwort bei der nächsten Anmeldung zu ändern.
8. Geben Sie in das Feld **E-Mail-Adresse** eine neue E-Mail-Adresse ein, um die vom Benutzer konfigurierte E-Mail-Adresse hinzuzufügen oder zu ändern. Sie wird zum Senden der Benutzerbenachrichtigungen verwendet.
9. Wenn Sie den Benutzer bearbeitet haben, klicken Sie auf **OK**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen zu verwerfen.

Hinweis: *Durch das Bearbeiten eines Benutzers können Sie die Gruppe, der dieser Benutzer angehört, nicht ändern. Weitere Informationen finden Sie unter* ***Benutzer der Gruppe hinzufügen****.*

Benutzer löschen

Wenn Sie einen Benutzer löschen, wird dieser Benutzer aus CC-SG entfernt. Sie können dadurch Konten löschen, die nicht mehr benötigt werden.

So löschen Sie Benutzer:

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf das Symbol + neben der Benutzergruppe, die den Benutzer enthält, den Sie löschen möchten.
3. Klicken Sie auf den Benutzer, den Sie löschen möchten.
4. Wählen Sie im Menü **Benutzer** die Option **Benutzermanager** und dann **Benutzer löschen** aus. Das Fenster **Benutzer löschen** wird angezeigt.

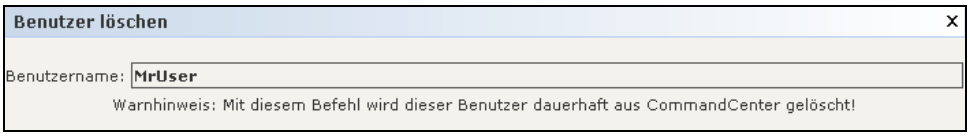


Abbildung 82 Benutzer löschen

5. Klicken Sie auf **OK**, um den Benutzer aus CC-SG zu löschen, oder auf **Abbrechen**, um den Benutzer nicht zu löschen.

Hinweis: *Dieser Befehl löscht alle Instanzen des Benutzers. Dies gilt auch, wenn der Benutzer mehreren Benutzergruppen angehört. Weitere Informationen zum Entfernen eines Benutzers aus einer Gruppe finden Sie unter* ***Benutzer aus Gruppe löschen****.*

Benutzer der Gruppe zuweisen

Verwenden Sie diesen Befehl, um vorhandene Benutzer einer Gruppe zuzuweisen, der sie nicht angehören. Benutzer, die auf diese Art und Weise zugewiesen werden, werden der neuen Gruppe hinzugefügt und sind weiterhin Mitglieder ihrer bereits bestehenden Gruppen. Sie können einen Benutzer mit diesem Befehl in Verbindung mit **Benutzer aus Gruppe löschen** (siehe unten) verschieben.

So weisen Sie einen Benutzer einer Gruppe zu:

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf die Benutzergruppe, der Sie Benutzer zuweisen möchten.
3. Wählen Sie im Menü **Benutzer** die Option **Benutzergruppenmanager** und dann **Benutzer der Gruppe zuweisen** aus. Das Fenster **Benutzer der Gruppe zuweisen** wird angezeigt.

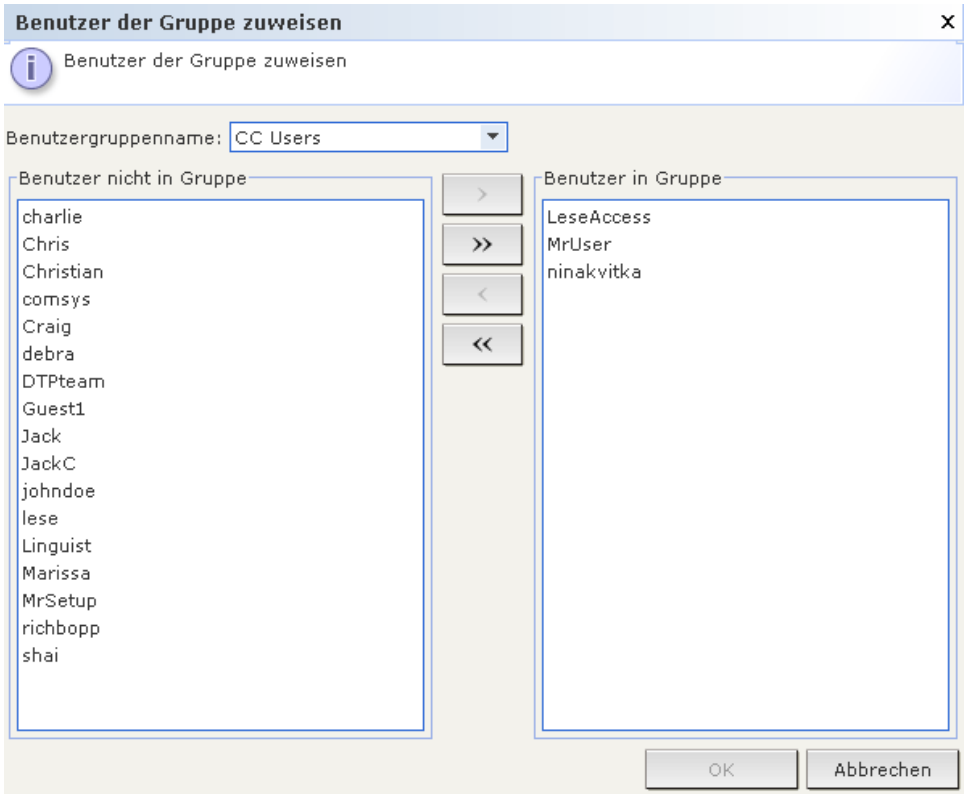


Abbildung 83 Fenster Benutzer der Gruppe hinzufügen

4. Benutzer, die keiner Zielgruppe zugewiesen werden, werden in der Liste **Benutzer nicht in Gruppe** angezeigt. Wählen Sie die Benutzer, die Sie hinzufügen möchten, in dieser Spalte aus, und klicken Sie auf die Schaltfläche >, um sie in die Liste **Benutzer in Gruppen** zu verschieben.
5. Klicken Sie auf die Schaltfläche >>, um alle Benutzer, die sich nicht in der Gruppe befinden, in die Liste **Benutzer in Gruppen** zu verschieben.
6. Sie können Mitglieder aus der Zielgruppe entfernen, indem Sie die entsprechenden Benutzer in der Liste **Benutzer in Gruppen** auswählen und auf die Schaltfläche < klicken.
7. Klicken Sie auf die Schaltfläche <<, um alle Benutzer in der Liste **Benutzer in Gruppen** zu löschen.
8. Wenn Sie alle Benutzer in die entsprechenden Spalten verschoben haben, klicken Sie auf **OK**. Die Benutzer in der Liste **Benutzer in Gruppen** werden zur ausgewählten Benutzergruppe hinzugefügt.

Benutzer aus Gruppe löschen

Mit diesem Befehl entfernen Sie einen Benutzer aus der Gruppe, in der er ausgewählt ist. Dieser Befehl entfernt den Benutzer nicht aus anderen Gruppen und löscht den Benutzer nicht aus CC-SG.

So löschen Sie einen Benutzer in einer Gruppe:

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf das Symbol + neben einer Benutzergruppe, die den Benutzer enthält, den Sie löschen möchten.

3. Klicken Sie auf den Benutzer, den Sie löschen möchten.
4. Wählen Sie im Menü **Benutzer** die Option **Benutzermanager** und dann **Benutzer aus Gruppe löschen** aus. Das Fenster **Benutzer löschen** zeigt den Benutzer und die Gruppe an, aus der der Benutzer gelöscht wird.

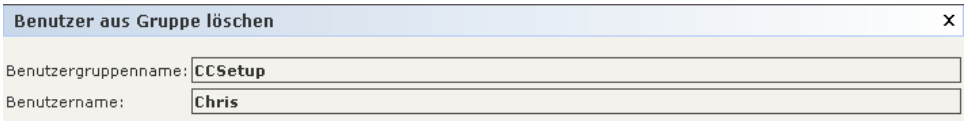


Abbildung 84 Benutzer aus Gruppe löschen

5. Klicken Sie auf **OK**, um den Benutzer aus der Gruppe zu löschen, oder auf **Abbrechen**, um den Benutzer nicht zu löschen.

***Hinweis**: Wenn Sie einen Benutzer aus einer Gruppe löschen und dieser keiner weiteren Gruppe angehört, wird der Benutzer in die Gruppe **Benutzer nicht in Gruppe** verschoben.*

Weitere Benutzer- und Benutzergruppenfunktionen

Mein Profil

Unter **Mein Profil** können Benutzer Kontoinformationen anzeigen, einige Details ändern und die Einstellungen zur Verwendung anpassen. Es ist die einzige Möglichkeit, den Kontonamen des Kontos **admin** zu ändern.

So bearbeiten Sie Ihr Profil:

1. Klicken Sie im Menü **Secure Gateway** auf **Mein Profil**. Der Bildschirm **Mein Profil** wird mit Informationen zu Ihrem Konto angezeigt.

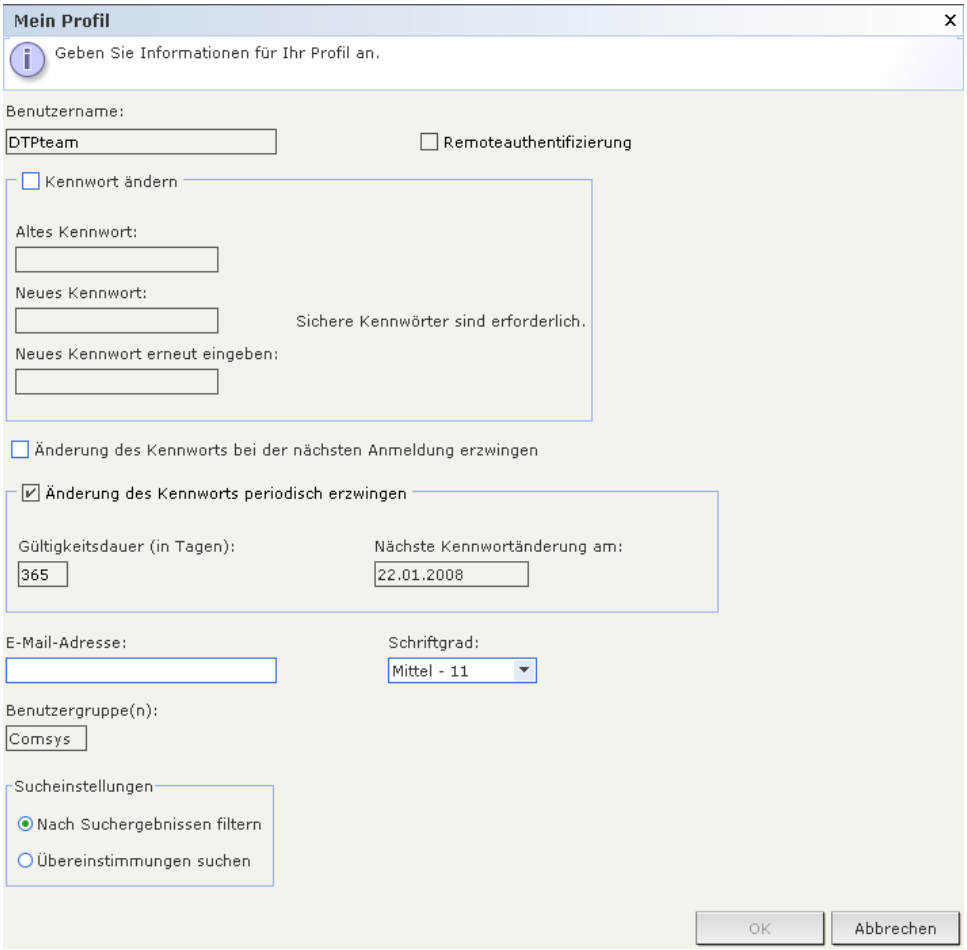


Abbildung 85 Fenster Mein Profil

2. Wenn Sie mit dem Konto **admin** angemeldet sind, können Sie einen neuen Namen in das Feld **Benutzername** eingeben, um den Namen Ihres Kontos zu ändern.

3. Markieren Sie die Option **Kennwort ändern**, wenn Sie Ihr Kennwort ändern möchten.
   a. Geben Sie das aktuelle Kennwort im Feld **Altes Kennwort** ein.
   b. Geben Sie das neue Kennwort im Feld **Neues Kennwort** ein. Eine Nachricht wird angezeigt, wenn sichere Kennwörter erforderlich sind.
   c. Bestätigen Sie das neue Kennwort im Feld **Neues Kennwort erneut eingeben**.
4. Geben Sie eine neue Adresse in das Feld **E-Mail-Adresse** ein, um die Adresse hinzuzufügen oder zu ändern, die CC-SG für Benachrichtigungen verwendet.
5. Klicken Sie auf das Dropdown-Menü **Schriftgrad**, um den Schriftgrad für den standardmäßigen CC-SG-Client anzupassen.
6. Wählen Sie im Bereich **Sucheinstellungen** eine bevorzugte Methode zur Suche nach Knoten, Benutzern und Geräten aus.
   - **Nach Suchergebnissen filtern**: Benutzer können Platzhalter verwenden und nur die Knoten, Benutzer oder Geräte anzeigen, die den Suchkriterien entsprechen.
   - **Übereinstimmungen suchen**: Unterstützt keine Platzhalter, und die ähnlichste Entsprechung für Knoten, Benutzer oder Geräte wird beim Eingeben angezeigt. Die Liste ist auf die Elemente beschränkt, die nach Klicken auf **Suchen** den Suchkriterien entsprechen.
7. Wenn Sie Ihr Profil bearbeitet haben, klicken Sie auf **OK**, um die Änderungen zu speichern, oder auf **Abbrechen**, um die Änderungen zu verwerfen.

Benutzer abmelden

Mit diesem Befehl können Sie aktive Benutzer bei CC-SG abmelden. Sie können damit auch alle aktiven Benutzer einer Benutzergruppe abmelden.

So melden Sie Benutzer ab:

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf das Symbol + neben einer Benutzergruppe mit Benutzern, die Sie abmelden möchten.
3. Klicken Sie auf den Benutzer, den Sie abmelden möchten. Halten Sie zum Abmelden mehrerer Benutzer die **Strg**-Taste gedrückt, während Sie weitere Benutzer durch Klicken auswählen.
4. Wählen Sie im Menü **Benutzer** die Option **Benutzermanager** und dann **Benutzer abmelden** aus. Der Bildschirm **Benutzer abmelden** wird mit den ausgewählten Benutzern angezeigt.
5. Klicken Sie auf **OK**, um die Benutzer bei CC-SG abzumelden, oder auf **Abbrechen**, um die Benutzer nicht abzumelden.

So melden Sie alle Benutzer einer Benutzergruppe ab:

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf die Benutzergruppe, die die Benutzer enthält, die Sie abmelden möchten. Halten Sie zum Abmelden mehrerer Benutzergruppen die **Strg**-Taste gedrückt, während Sie weitere Benutzergruppen durch Klicken auswählen.
3. Wählen Sie im Menü **Benutzer** die Option **Benutzergruppenmanager** und dann **Benutzer abmelden** aus. Der Bildschirm **Benutzer abmelden** wird mit den aktiven Benutzern der ausgewählten Gruppen angezeigt.
4. Klicken Sie auf **OK**, um die Benutzer bei CC-SG abzumelden, oder auf **Abbrechen**, um die Benutzer nicht abzumelden.

Massenkopieren

Sie können mit **Massenkopieren** Zeit sparen, indem Sie die Berechtigungen und Richtlinien eines Benutzers für andere vorhandene Benutzer kopieren. Verschieben Sie sie dazu einfach in die Benutzergruppen des ausgewählten Benutzers. So verwenden Sie Massenkopieren:

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf das Symbol + neben einer Benutzergruppe, die den Benutzer enthält, den Sie kopieren möchten.
3. Klicken Sie auf den Benutzer, den Sie kopieren möchten.
4. Wählen Sie im Menü **Benutzer** die Option **Benutzermanager** und dann **Massenkopieren** aus. Das Fenster **Massenkopieren** wird angezeigt.

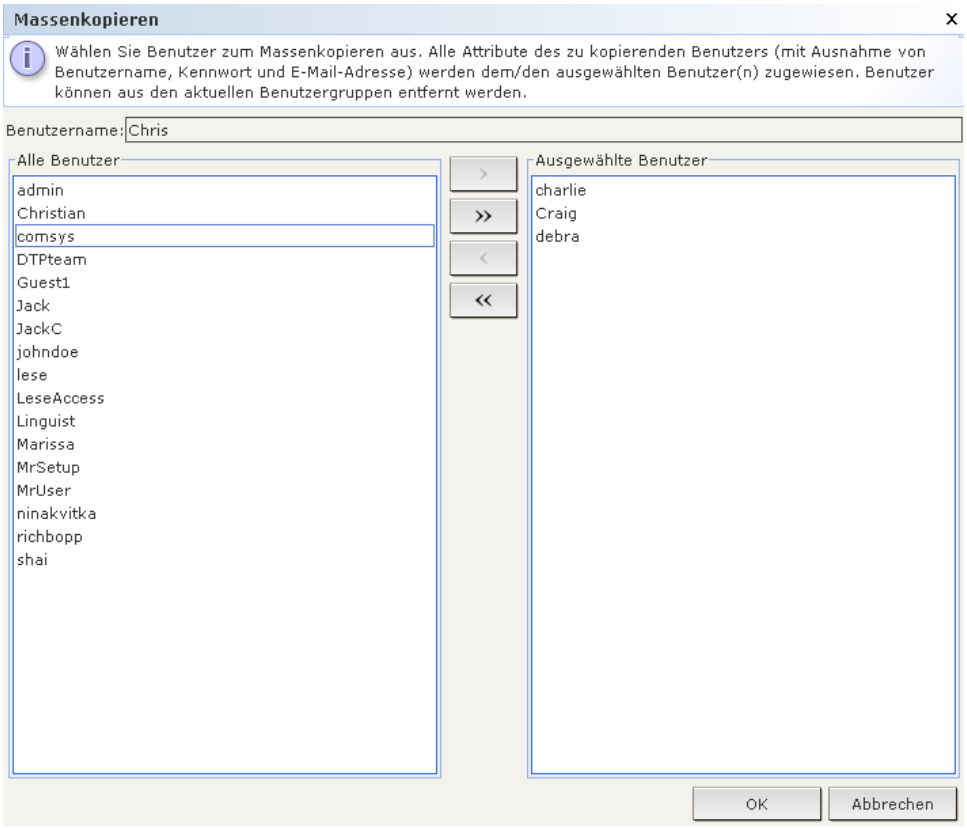


Abbildung 86 Fenster Massenkopieren

5. Wählen Sie in der Liste **Alle Benutzer** die Benutzer aus, die die Berechtigungen und Richtlinien des im Feld **Benutzername** angezeigten Benutzers übernehmen sollen.
6. Klicken Sie auf die Schaltfläche > (Pfeil nach rechts), um einen Benutzernamen in die Liste **Ausgewählte Benutzer** zu verschieben.
7. Klicken Sie auf die Schaltfläche >>, um alle Benutzer in die Liste **Ausgewählte Benutzer** zu verschieben.
8. Sie können einen Benutzer aus der Liste **Ausgewählte Benutzer** löschen, indem Sie den Benutzer auswählen und auf die Schaltfläche < klicken.
9. Klicken Sie auf die Schaltfläche <<, um alle Benutzer in der Liste **Benutzer in Gruppen** zu löschen.
10. Klicken Sie auf **OK**, um die Benutzereigenschaften zu kopieren. Kopierte Benutzer werden aus den vorhandenen Gruppen in die Gruppen verschoben, denen der ausgewählte Benutzer angehört.

Diese Seite wurde absichtlich leer gelassen.

Kapitel 8: Richtlinien

Zugriff anhand von Richtlinien steuern

Das Konfigurieren neuer Richtlinien, um einen Benutzerzugriff auf Knoten bereitzustellen, ist zwar optional, jedoch wird es zur effektiven Verwendung der Zugriffssteuerung von CC-SG dringend empfohlen. Wenn Sie allen Benutzern Zugriff auf alle Knoten gewähren möchten, können Sie einfach allen Benutzergruppen die Richtlinie mit unbeschränktem Zugriff zuweisen.

Wenn Sie den Zugriff der Benutzer auf Knoten steuern möchten, müssen Sie Richtlinien erstellen, um Regeln für den Zugriff festzulegen. Wie alle Berechtigungen werden Richtlinien den Benutzergruppen zugewiesen, damit diese Zugriffsregeln für alle Benutzer in der Gruppe gelten.

Wenn Sie den **Setup-Assistenten** (siehe **Kapitel 3: Konfigurieren von CC-SG mit dem Setup-Assistenten**) abgeschlossen haben, wurden bereits einige grundlegende Richtlinien erstellt. Sie können diese Richtlinien dann auf vorhandene Benutzergruppen anwenden. Wenn Sie den **Setup-Assistenten** nicht verwendet oder die gewünschten Richtlinien nicht erstellt haben, sollten Sie die Anweisungen unten befolgen. Folgendes wird erläutert:

- Erstellen von Knotengruppen, um die Knoten zu verwalten, für die Sie Zugriffsregeln erstellen möchten
- Erstellen von Gerätegruppen, wenn Sie Zugriffsregeln für Raritan-Geräte erstellen möchten, die als Schnittstellen für Knoten dienen
- Erstellen einer Richtlinie für einen Knoten (oder ein Gerät), die angibt, wann der Zugriff auf den Knoten erfolgen darf
- Anwenden dieser Richtlinie auf eine Benutzergruppe

Richtlinienübersicht

Das folgende Diagramm ist eine visuelle Darstellung, wie Sicherheit mit CC-SG implementiert wird:

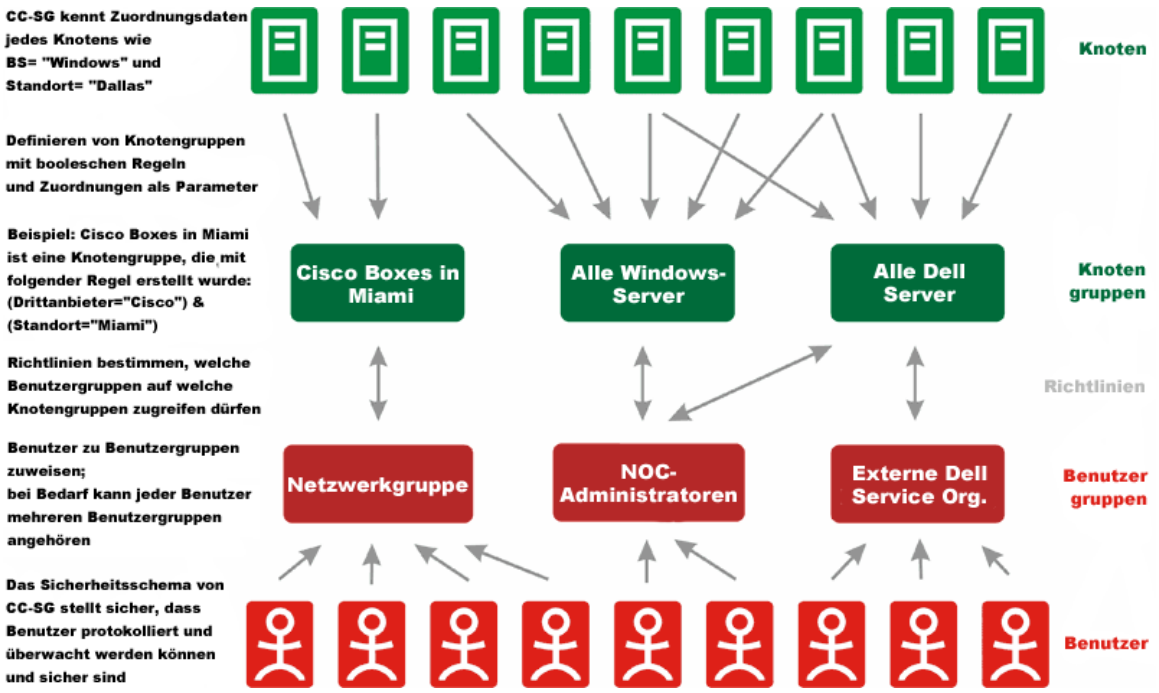


Abbildung 87 Richtlinienübersicht

Knotengruppen

Knotengruppen werden zur Verwaltung von mehreren Knoten verwendet. Diese Gruppe dient als Basis für eine Richtlinie, die den Zugriff auf diese Knotengruppe zulässt oder verweigert. Knoten können willkürlich oder anhand von gemeinsamen Attributen gruppiert werden.

Wenn Sie den Zuordnungsmanager zum Erstellen von Kategorien und Elementen für Knoten verwenden, werden einige Mittel zum Verwalten von Konten mit gemeinsamen Attributen erstellt. CC-SG erstellt automatisch Zugriffsrichtlinien basierend auf diesen Elementen. Weitere Informationen zum Erstellen von Kategorien und Elementen finden Sie in **Kapitel 4: Zuordnungen**.

So zeigen Sie vorhandene Knotengruppen an:

Klicken Sie im Menü **Zuordnungen** auf **Knotengruppe**. Das Fenster **Knotengruppenmanager** wird angezeigt. Die Liste der vorhandenen Knotengruppen wird links angezeigt, und Details der ausgewählten Knotengruppe werden im Hauptfenster angezeigt.

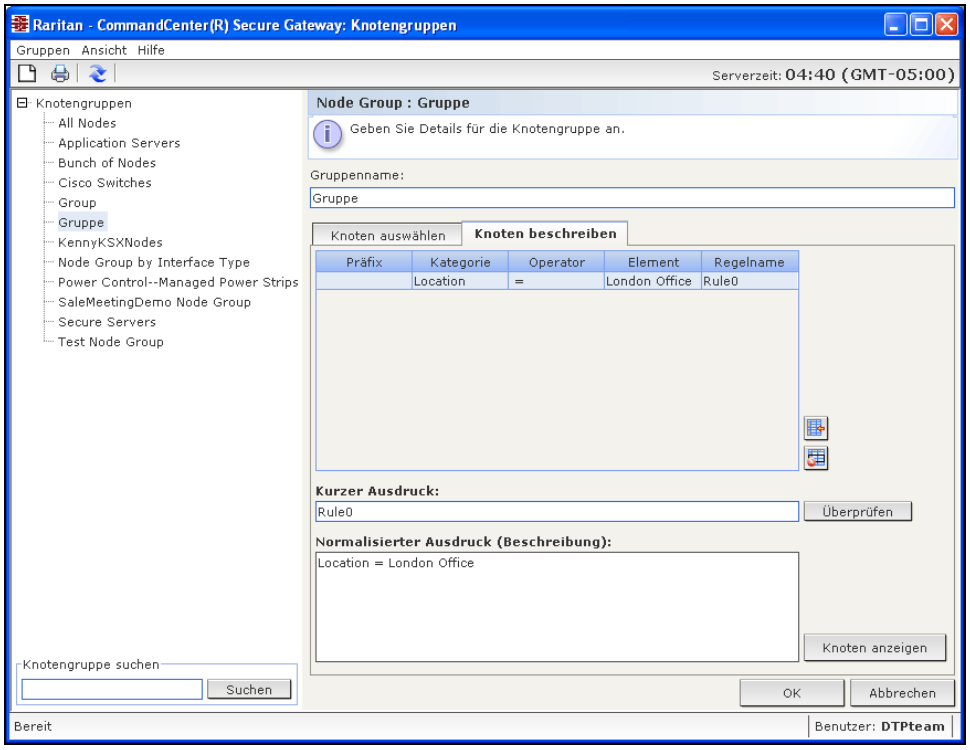


Abbildung 88 Knotengruppenmanager

1. Eine Liste der vorhandenen Knotengruppen wird links angezeigt. Klicken Sie auf eine Knotengruppe, um die Details dieser Gruppe im Knotengruppenmanager anzuzeigen.
   Die Gruppe wurde willkürlich zusammengestellt. Die Registerkarte **Knoten auswählen** wird mit einer Liste der Knoten angezeigt, die der Gruppe angehören oder nicht angehören.
   Wurde die Gruppe basierend auf gemeinsamen Attributen gebildet, werden auf der Registerkarte **Knoten beschreiben** die Regeln angezeigt, die die Auswahl der Knoten für die Gruppe bestimmt haben.
2. Geben Sie zur Suche eines Knotens in der Knotengruppenliste unten in der Liste einen Suchbegriff in das Feld **Suchen** ein. Klicken Sie dann auf **Suchen**. Die Suchmethode wird über den Bildschirm **Mein Profil** konfiguriert. Weitere Informationen finden Sie in **Kapitel 7: Benutzer und Benutzergruppen**.

3. Wenn Sie eine Gruppe anzeigen, die auf auf Attributen basiert, können Sie über **Knoten anzeigen** eine Liste der Knoten anzeigen, die der Knotengruppe zugeordnet sind. Im Fenster **Knoten in der Knotengruppe** werden die Knoten und ihre Attribute angezeigt.

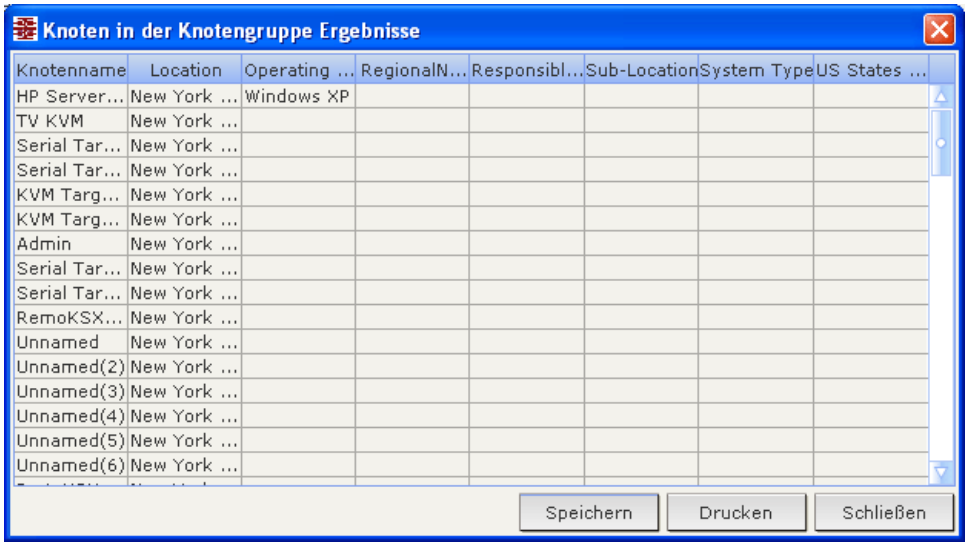


Abbildung 89 Knoten in einer Gruppe, die auf Attributen basiert

Knotengruppen hinzufügen

So fügen Sie eine neue Knotengruppe hinzu:

1. Klicken Sie im Menü **Zuordnungen** auf **Knotengruppe**. Das Fenster **Knotengruppenmanager** wird angezeigt.
2. Wählen Sie im Menü **Gruppen** die Option **Hinzufügen** aus. Eine Vorlage einer Knotengruppe wird angezeigt.
3. Geben Sie in das Feld **Gruppenname** einen Namen für die Knotengruppe ein, die Sie erstellen möchten.

Sie haben zwei Möglichkeiten, Knoten einer Gruppe hinzuzufügen: **Knoten auswählen** und **Knoten beschreiben**. Über **Knoten auswählen** können Sie willkürlich bestimmen, welche Knoten der Gruppe zugeordnet werden sollen. Wählen Sie die Knoten dazu einfach in der Liste der verfügbaren Knoten aus. Mithilfe der Methode **Knoten beschreiben** können Sie Regeln zum Beschreiben von Knoten festlegen. Knoten, die der Beschreibung entsprechen, werden der Gruppe hinzugefügt.

Knoten auswählen

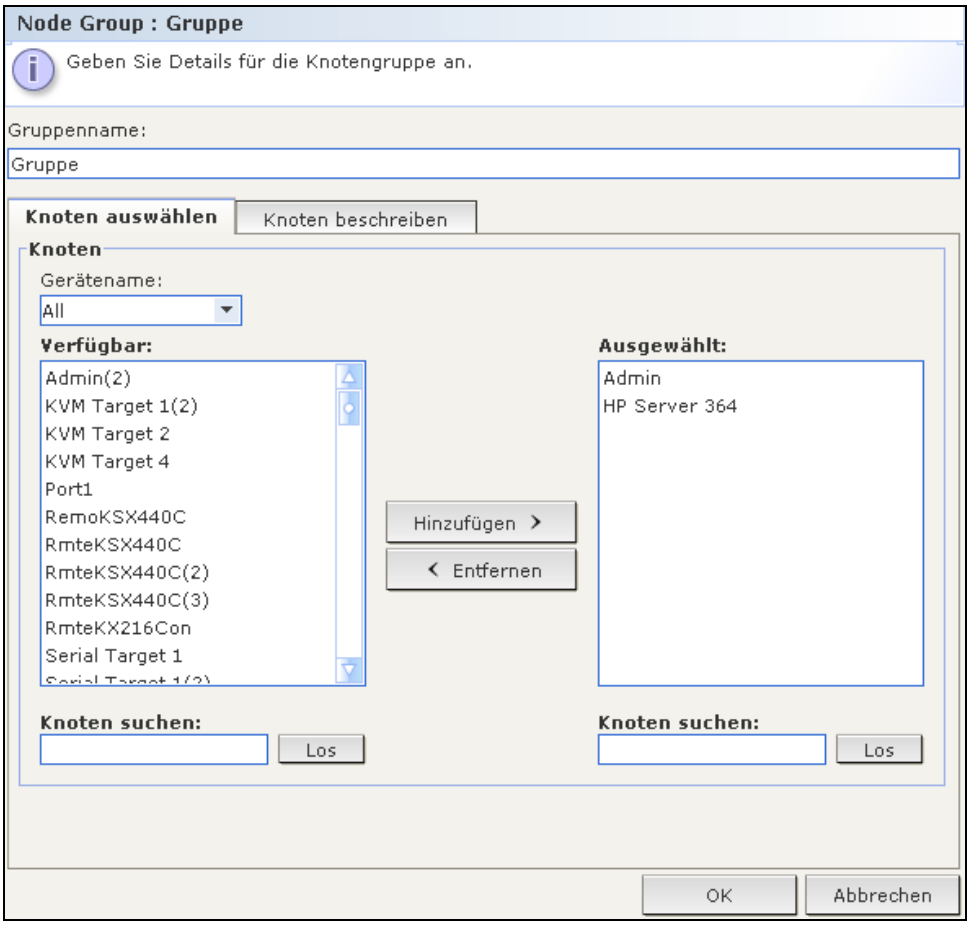


Abbildung 90 Knoten über Knoten auswählen hinzufügen

1. Klicken Sie auf die Registerkarte **Knoten auswählen**.
2. Klicken Sie auf das Dropdown-Menü **Gerätename**, und wählen Sie ein Gerät aus, wenn Sie die Liste **Verfügbar** nach den Knoten durchsuchen möchten, die über Schnittstellen zu diesem Gerät verfügen.
3. Wählen Sie in der Liste **Verfügbar** den Knoten aus, den Sie der Gruppe hinzufügen möchten, und klicken Sie dann auf **Hinzufügen**, um den Knoten in die Liste **Ausgewählt** zu verschieben. Knoten in der Liste **Ausgewählt** werden der Gruppe hinzugefügt.
4. Wählen Sie zum Löschen eines Knotens aus der Gruppe den Knotennamen in der Liste **Ausgewählt** aus, und klicken Sie auf **Löschen**.
5. Sie können den Knoten in der Liste **Verfügbar** oder **Ausgewählt** suchen. Geben Sie den Suchbegriff in das Feld unter der Liste ein, und klicken Sie auf **Los**.
6. Wenn Sie wissen, dass Sie eine Richtlinie erstellen möchten, die jederzeit Zugriff auf die Knoten dieser Gruppe erlaubt, markieren Sie **Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen**.
7. Wenn Sie alle Knoten zur Gruppe hinzugefügt haben, klicken Sie auf **Hinzufügen**, um die Knotengruppe zu erstellen. Die Gruppe wird der Liste der Knotengruppen links hinzugefügt.

Knoten beschreiben

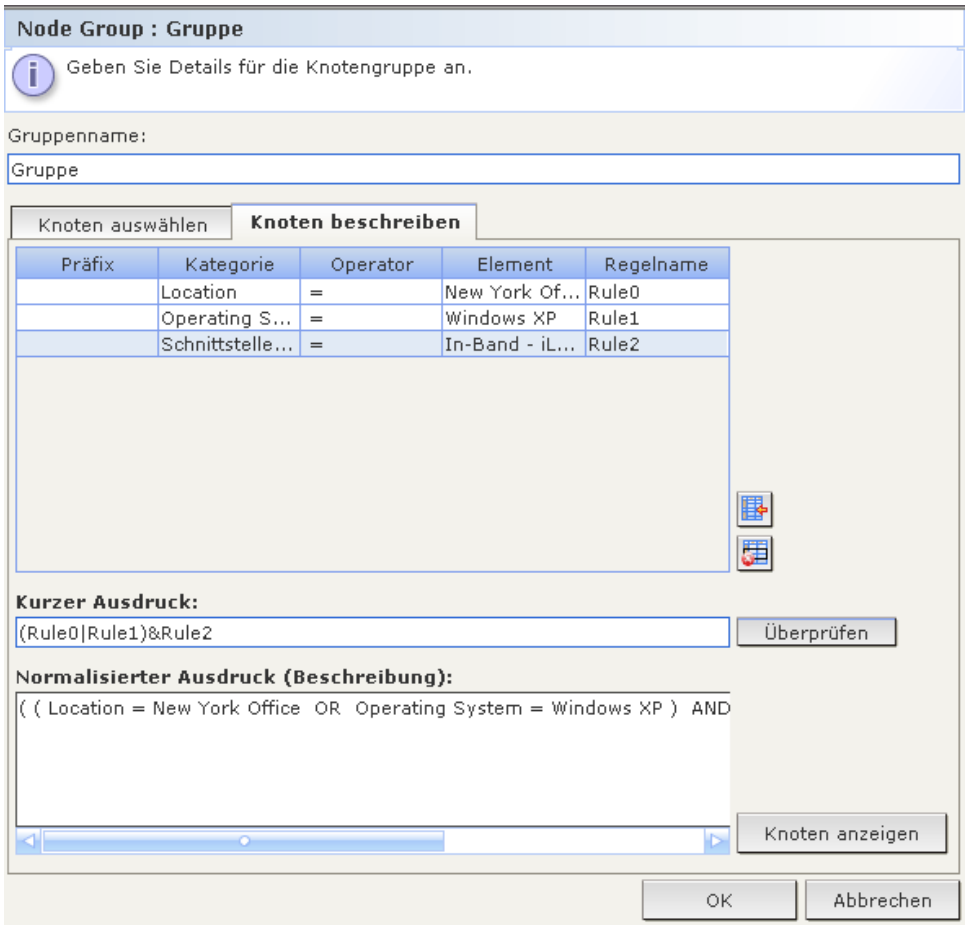


Abbildung 91 Knotengruppe mit mehreren Regeln beschreiben

1. Klicken Sie auf die Registerkarte **Knoten auswählen**.
2. Klicken Sie auf das Symbol  , um eine Zeile in die Tabelle für eine neue Regel einzufügen. Regeln nehmen die Form eines Ausdrucks an, der mit Knoten verglichen werden kann.
3. Doppelklicken Sie auf jede Spalte in der Zeile, um für die entsprechende Zeile ein Dropdown-Menü anzuzeigen. Wählen Sie dann den entsprechenden Wert für jede Komponente aus:
   - **Präfix**: Feld leer lassen oder **NOT** auswählen. Wenn **NOT** ausgewählt ist, sucht diese Regel nach Werten, die dem Ausdruck nicht entsprechen.
   - **Kategorie**: Wählen Sie ein Attribut aus, das in der Regel bewertet wird. Es sind alle Kategorien verfügbar, die Sie im **Zuordnungsmanager** erstellt haben. Außerdem sind **Knotenname** und **Schnittstelle** enthalten.
   - **Operator**: Wählen Sie einen Vergleichsvorgang, der zwischen Kategorien und Elementen durchgeführt werden soll. Es stehen drei Operatoren zur Verfügung: = (ist gleich), **LIKE** (zum Suchen des Elements in einem Namen) und <> (ist nicht gleich).
   - **Element**: Wählen Sie einen Wert für das Kategorieattribut zum Vergleich aus. Hier werden nur Elemente dargestellt, die mit der ausgewählten Kategorie verknüpft sind. (Beispiel: wenn eine Kategorie „Abteilung“ bewertet wird, werden Elemente mit der Bezeichnung „Standort“ nicht angezeigt).
   - **Regelname**: Der Name, der der Regel in dieser Zeile zugewiesen wurde. Sie können diese Werte nicht bearbeiten. Verwenden Sie diese Werte, um Beschreibungen im Feld **Kurzer Ausdruck** einzugeben.

   Die Beispielregel `Abteilung = Technik` beschreibt alle Knoten, bei denen die **Kategorie** „Abteilung“ auf „Technik“ eingestellt ist. Dies geschieht genau dann, wenn Sie die Zuordnungen während des Vorgangs **Knoten hinzufügen** konfigurieren.

4. Wenn Sie eine weitere Regel hinzufügen möchten, klicken Sie auf das Symbol zum Einfügen einer neuen Zeile  , und nehmen Sie die entsprechenden Konfigurationen vor. Wenn Sie mehrere Regeln konfigurieren, können Sie genauere Beschreibungen anfertigen, indem Sie mehrere Kriterien zur Bewertung von Knoten bereitstellen.
5. Markieren Sie die Regeln, die gelöscht werden sollen, in der Tabelle, und klicken Sie auf **Zeile(n) entfernen**.
6. Die Tabelle mit Regeln stellt nur Kriterien zur Bewertung von Knoten bereit. Definieren Sie eine Beschreibung für die Knotengruppe, indem Sie die Regeln nach **Regelname** zum Feld **Kurzer Ausdruck** hinzufügen. Erfordert die Beschreibung nur eine Regel, geben Sie einfach den Namen der Regel in das Feld ein. Werden mehrere Regeln bewertet, geben Sie die Regeln in das Feld mithilfe logischer Operatoren ein, um die Regeln in ihrer Beziehung zueinander zu beschreiben:
   - **&** - der UND Operator. Ein Knoten muss die Regeln auf beiden Seiten dieses Operators für die Beschreibung (oder den Abschnitt einer Beschreibung) erfüllen, um als wahr bewertet zu werden.
   - | - der ODER Operator. Ein Knoten muss nur eine Regel auf einer Seite dieses Operators für die Beschreibung (oder den Abschnitt einer Beschreibung) erfüllen, um als wahr bewertet zu werden.
   - **(** und **)** – Gruppierungsoperatoren. Die Beschreibung wird in einen Unterabschnitt aufgeteilt, der in Klammern steht. Der Abschnitt innerhalb der Klammern wird bewertet, bevor die restliche Beschreibung mit dem Knoten verglichen wird. Gruppen in Klammern können in einer anderen Gruppe in Klammern verschachtelt werden.

   Beispiel: Wenn Sie Knoten beschreiben möchten, die zur Technikabteilung gehören, muss die Regel wie folgt aussehen: `Abteilung = Technik`. Dies ist dann Regel0. Geben Sie dann Regel0 in das Feld **Kurzer Ausdruck** ein.

   Ein weiteres Beispiel: Wenn Sie eine Knotengruppe beschreiben möchten, die zur Technikabteilung gehört ODER den Standort „Philadelphia“ aufweist und festlegen möchten, dass alle Geräte mindestens über 1 GB Speicher verfügen müssen, dann müssen Sie drei Regeln erstellen. `Abteilung = Technik` (Regel0) `Standort = Philadelphia` (Regel1) `Speicher = 1GB` (Regel2). Diese Regeln müssen in Relation zueinander gesetzt werden. Da der Knoten entweder der Technikabteilung angehören oder den Standort „Philadelphia“ aufweisen kann, verwenden Sie den ODER Operator **|**, um die beiden zu verbinden: `Regel0|Regel1`. Dieser Vergleich wird zuerst durchgeführt, indem er in Klammern eingeschlossen wird: `(Regel0|Regel1)`. Da die Knoten beide diesen Vergleich erfüllen UND 1 GB Speicher aufweisen müssen, wird der UND Operator **&** verwendet, um diesen Abschnitt mit Regel2 zu verbinden: `(Regel0|Regel1)&Regel2`. Geben Sie diesen Ausdruck in das Feld **Kurzer Ausdruck** ein.

7. Klicken Sie auf **Überprüfen**, wenn eine Beschreibung im Feld **Kurzer Ausdruck** enthalten ist. Wurde die Beschreibung fehlerhaft gebildet, wird ein Warnhinweis angezeigt. Wurde die Beschreibung richtig gebildet, wird eine normalisierte Form des Ausdrucks im Feld **Normalisierter Ausdruck** angezeigt.
8. Klicken Sie auf **Knoten anzeigen**, um anzuzeigen, welche Knoten diese Anforderungen erfüllen. Ein Ergebnisfenster **Knoten in der Knotengruppe** wird mit den Knoten angezeigt, die durch den aktuellen Ausdruck gruppiert werden. Sie können dadurch prüfen, ob die Beschreibung richtig geschrieben wurde. Ist dies nicht der Fall, können Sie zur Regeltabelle oder dem Feld **Kurzer Ausdruck** wechseln, um Anpassungen vorzunehmen.
9. Wenn Sie wissen, dass Sie eine Richtlinie erstellen möchten, die jederzeit Zugriff auf die Knoten dieser Gruppe erlaubt, markieren Sie **Richtlinie mit unbeschränktem Zugriff für Gruppe erstellen**.
10. Wenn Sie alle Knoten der Gruppe beschrieben haben, klicken Sie auf **Hinzufügen**, um die Knotengruppe zu erstellen. Die Gruppe wird der Liste der Knotengruppen links hinzugefügt.

Knotengruppe bearbeiten

Sie können eine Knotengruppe bearbeiten, um die Mitgliedschaft oder Beschreibung der Gruppe zu ändern. So bearbeiten Sie Knotengruppen:

1. Klicken Sie im Menü **Zuordnungen** auf **Knotengruppe**. Das Fenster **Knotengruppenmanager** wird angezeigt.

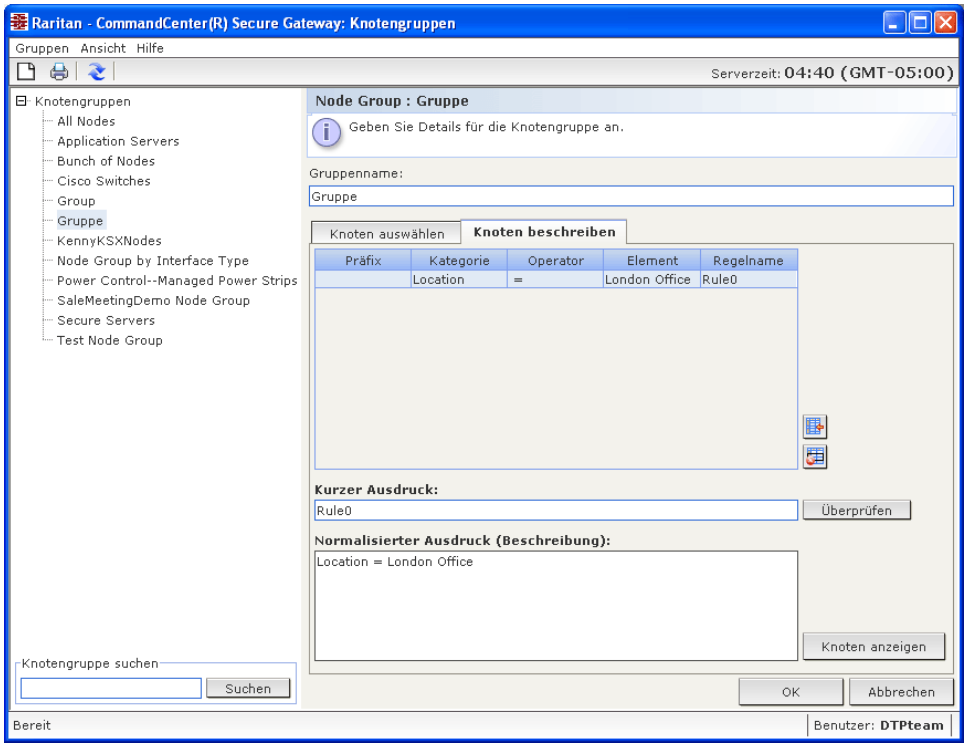


Abbildung 92 Knotengruppen bearbeiten

2. Klicken Sie in der Knotengruppenliste links auf den Knoten, den Sie bearbeiten möchten. Die Details des Knotens werden im Fenster **Knotengruppen** angezeigt.
3. Weitere Informationen zum Konfigurieren von Knotengruppen finden Sie in den Abschnitten **Knoten auswählen** oder **Knoten beschreiben** oben.
4. Klicken Sie auf **OK**, wenn Sie die Knotengruppe bearbeitet haben.

Knotengruppe löschen

1. Klicken Sie im Menü **Zuordnungen** auf **Knotengruppe**. Das Fenster **Knotengruppenmanager** wird angezeigt.
2. Klicken Sie in der Knotengruppenliste links auf den Knoten, den Sie löschen möchten.
3. Klicken Sie im Menü **Gruppen** auf **Löschen**.

Gerätegruppen

Gerätegruppen funktionieren ähnlich wie Knotengruppen, jedoch werden Gerätegruppen verwendet, um Raritan-Geräte in Sätze zur Verwaltung durch Richtlinien zu organisieren.

Weitere Informationen finden Sie in **Kapitel 5: Hinzufügen von Geräten und Gerätegruppen, Gerätegruppenmanager**.

Richtlinienmanager

Nachdem Sie Knoten- und Gerätegruppen erstellt haben, können Sie diese als Basis zum Erstellen einer Zugriffsrichtlinie verwenden. Diese Regel gibt an, ob Benutzer auf die Knoten oder Geräte in der Gruppe (oder Gerätegruppe) zugreifen dürfen und für welche Zeiträume diese Regel gilt.

Richtlinie hinzufügen

So erstellen Sie Richtlinien:

1. Klicken Sie im Menü **Zuordnungen** auf **Richtlinien**. Das Fenster **Richtlinienmanager** wird angezeigt.

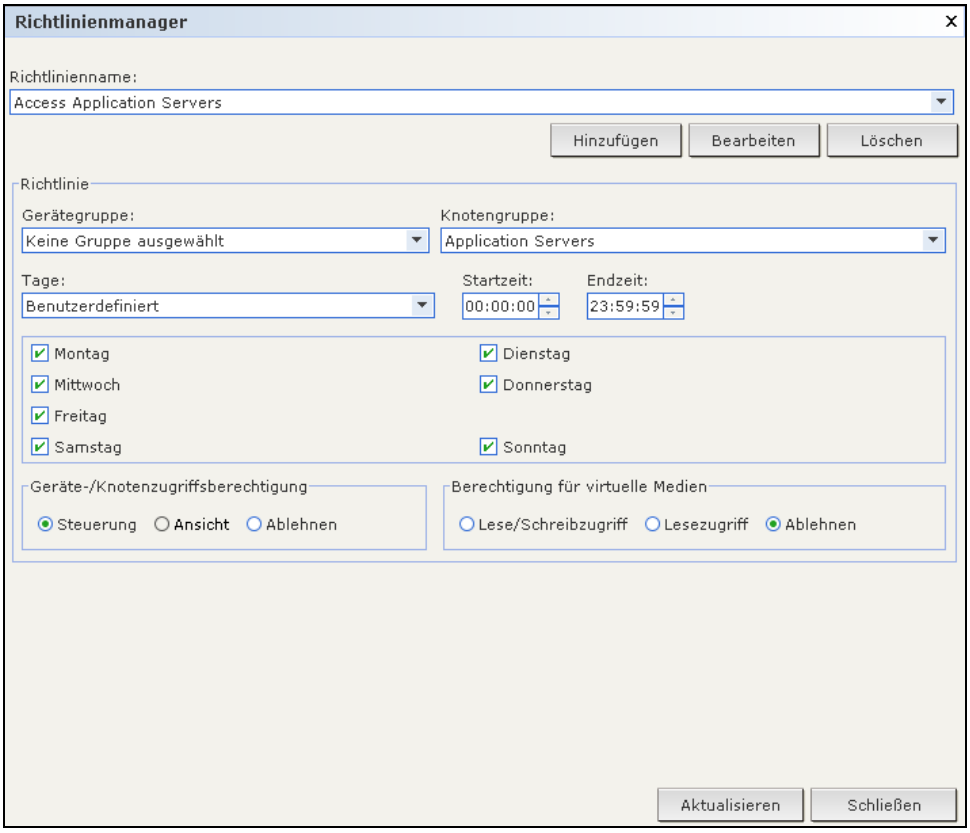


Abbildung 93 Richtlinienmanager

2. Klicken Sie auf **Hinzufügen**. Geben Sie den Namen der Richtlinie in das Dialogfeld ein.

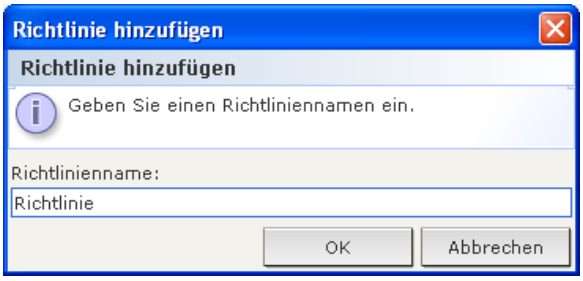


Abbildung 94 Richtlinien hinzufügen

3. Geben Sie den Namen der neuen Richtlinie im Feld **Richtlinienname** ein.
4. Klicken Sie auf **OK**. Die neue Richtlinie wird im Bildschirm **Richtlinienmanager** zur Liste **Richtlinienname** hinzugefügt.
5. Klicken Sie auf den Pfeil der Dropdown-Liste **Gerätegruppe**, und wählen Sie die Gerätegruppe aus, für die diese Richtlinie den Zugriff steuern soll.
   Klicken Sie auf den Pfeil der Dropdown-Liste **Knotengruppe**, und wählen Sie die Knotengruppe aus, für die diese Richtlinie den Zugriff steuern soll.
   Bezieht sich die Richtlinie nur auf eine Gruppenart, müssen Sie nur einen Wert für die Gruppe auswählen.
6. Klicken Sie auf den Pfeil der Dropdown-Liste **Tage**, und wählen Sie aus, an welchen Wochentagen diese Richtlinie gelten soll: **Alle** Tage, **Wochentag** (nur Montag bis Freitag) und **Wochenende** (nur Samstag und Sonntag) oder **Benutzerdefiniert** (wählen Sie bestimmte Tage aus).
   a. Wählen Sie **Benutzerdefiniert** aus, um die gewünschten Tage auszuwählen. Die Kontrollkästchen für die einzelnen Tage werden wählbar.
   b. Markieren Sie die Kontrollkästchen für die Tage, an denen die Richtlinie gelten soll.
7. Geben Sie in das Feld **Startzeit** die Uhrzeit ein, die als Startzeit für diese Richtlinie gelten soll. Die Uhrzeit muss im 24-Stundenformat eingegeben werden.
8. Geben Sie in das Feld **Endzeit** die Uhrzeit ein, die als Endzeit für diese Richtlinie gelten soll. Die Uhrzeit muss im 24-Stundenformat eingegeben werden.
9. Wählen Sie im Feld **Geräte-/Knotenzugriffsberechtigung** die Option **Steuerung** aus, um diese Richtlinie so zu definieren, dass sie den Zugriff auf ausgewählte Knoten oder Gerätegruppen zu den angegebenen Uhrzeiten und Tagen zulässt. Wählen Sie **Ablehnen** aus, um diese Richtlinie so zu definieren, dass sie den Zugriff auf ausgewählte Knoten oder Gerätegruppen zu den angegebenen Uhrzeiten und Tagen verweigert.
10. Klicken Sie auf **Aktualisieren**, um die neue Richtlinie zu CC-SG hinzuzufügen. Bestätigen Sie die Nachricht mit **Ja**.

Hinweis: *Wenn Sie eine Richtlinie erstellen, die den Zugriff auf eine Knoten- oder Gerätegruppe verweigert (**Ablehnen**), müssen Sie auch eine Richtlinie erstellen, die den Zugriff auf die ausgewählten Knoten- oder Gerätegruppen zulässt (**Steuerung**). Benutzer erhalten nicht automatisch die Rechte **Steuerung**, wenn die Richtlinie zum **Ablehnen** nicht verwendet wird.*

Richtlinien bearbeiten

Beim Bearbeiten von Richtlinien wirken sich die Änderungen nicht auf Benutzer aus, die zu dem Zeitpunkt bei CC-SG angemeldet sind. Die Änderungen werden beim nächsten Anmeldevorgang aktiviert. Wenn Sie sicherstellen müssen, dass die Änderungen vorher übernommen werden, müssen Sie in den Wartungsmodus wechseln und die Richtlinien dann bearbeiten. Wenn Sie in den Wartungsmodus wechseln, werden alle angemeldeten Benutzer bei CC-SG abgemeldet, bis Sie den Wartungsmodus verlassen. Danach können sich die Benutzer erneut anmelden. Weitere Informationen finden Sie in **Kapitel 11: Systemwartung, Wartungsmodus**.

So bearbeiten Sie Richtlinien:

1. Klicken Sie im Menü **Zuordnungen** auf **Richtlinien**. Das Fenster **Richtlinienmanager** wird angezeigt.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Richtlinienname**, und wählen Sie die Richtlinien, die Sie bearbeiten möchten, in der Liste aus.
3. Klicken Sie zum Bearbeiten des Namens der Richtlinie auf **Bearbeiten**. Das Fenster **Richtlinie bearbeiten** wird angezeigt. Geben Sie einen neuen Namen für die Richtlinie in das Feld ein, und klicken Sie auf **OK**, um den Namen der Richtlinie zu ändern.
4. Klicken Sie auf den Pfeil der Dropdown-Liste **Gerätegruppe**, und wählen Sie die Gerätegruppe aus, für die diese Richtlinie den Zugriff steuern soll.
   Klicken Sie auf den Pfeil der Dropdown-Liste **Knotengruppe**, und wählen Sie die Knotengruppe aus, für die diese Richtlinie den Zugriff steuern soll.
   Bezieht sich die Richtlinie nur auf eine Gruppenart, müssen Sie nur einen Wert für diese Art auswählen.

5. Klicken Sie auf den Pfeil der Dropdown-Liste **Tage**, und wählen Sie aus, an welchen Wochentagen diese Richtlinie gelten soll: **Alle** Tage, **Wochentag** (nur Montag bis Freitag) und **Wochenende** (nur Samstag und Sonntag) oder **Benutzerdefiniert** (wählen Sie bestimmte Tage aus).
    a. Wählen Sie **Benutzerdefiniert** aus, um die gewünschten Tage auszuwählen. Die Kontrollkästchen für die einzelnen Tage werden wählbar.
    b. Markieren Sie die Kontrollkästchen für die Tage, an denen die Richtlinie gelten soll.
6. Geben Sie in das Feld **Startzeit** die Uhrzeit ein, die als Startzeit für diese Richtlinie gelten soll. Die Uhrzeit muss im 24-Stundenformat eingegeben werden.
7. Geben Sie in das Feld **Endzeit** die Uhrzeit ein, die als Endzeit für diese Richtlinie gelten soll. Die Uhrzeit muss im 24-Stundenformat eingegeben werden.
8. Wählen Sie im Feld **Geräte-/Knotenzugriffsberechtigung** die Option **Steuerung** aus, um diese Richtlinie so zu definieren, dass sie den Zugriff auf ausgewählte Knoten oder Gerätegruppen zu den angegebenen Uhrzeiten und Tagen zulässt. Wählen Sie **Ablehnen** aus, um diese Richtlinie so zu definieren, dass sie den Zugriff auf ausgewählte Knoten oder Gerätegruppen zu den angegebenen Uhrzeiten und Tagen verweigert.
9. Wenn Sie **Steuerung** im Feld **Geräte-/Knotenzugriffsberechtigung** ausgewählt haben, wird der Abschnitt **Berechtigung für virtuelle Medien** aktiv dargestellt. Wenn Sie diese Richtlinie so definieren möchten, dass **Berechtigung für virtuelle Medien** zugelassen ist, wählen Sie die Berechtigung **Lese/Schreibzugriff** oder **Lesezugriff** aus. Wenn Sie diese Richtlinie so definieren möchten, dass **Berechtigung für virtuelle Medien** nicht zugelassen ist, wählen Sie **Ablehnen** aus.
10. Klicken Sie auf **Aktualisieren**, um die Änderungen der Richtlinie zu speichern. Bestätigen Sie die Nachricht mit **Ja**.

Richtlinien löschen

So löschen Sie Richtlinien:

1. Klicken Sie im Menü **Zuordnungen** auf **Richtlinien**. Das Fenster **Richtlinienmanager** wird angezeigt.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Richtlinienname**, und wählen Sie die Richtlinien, die gelöscht werden soll, in der Liste aus.
3. Klicken Sie auf **Löschen**, und dann in der Bestätigungsnachricht auf **Ja**.

Richtlinien auf Benutzergruppen anwenden

Richtlinien müssen Benutzergruppen zugewiesen werden, bevor sie wirksam werden. Nachdem eine Richtlinie einer Benutzergruppe zugewiesen wurde, wird der Zugriff der Gruppenmitglieder durch diese Richtlinie bestimmt. Weitere Informationen zum Zuweisen von Richtlinien zu Benutzergruppen finden Sie in **Kapitel 7: Hinzufügen und Verwalten von Benutzern und Benutzergruppen**.

Kapitel 9: Konfigurieren der Remoteauthentifizierung

Authentifizierung und Autorisierung (AA)

CC-SG-Benutzer können lokal authentifiziert und in CC-SG autorisiert werden, oder die Authentifizierung kann mithilfe der folgenden unterstützten Verzeichnisserver remote durchgeführt werden:

- Microsoft Active Directory (AD)
- Lightweight Directory Access Protocol (LDAP) von Netscape
- TACACS+
- RADIUS

Zur externen Authentifizierung kann eine beliebige Anzahl an RADIUS, TACACS+ und LDAP Remoteservern verwendet werden. Sie können beispielsweise drei Active Directory-Server, zwei iPlanet- (LDAP) Server und drei RADIUS-Server konfigurieren.

Authentifizierungsfluss

Ist die Remoteauthentifizierung aktiviert, werden bei der Authentifizierung und Autorisierung folgende Schritte durchgeführt:

1. Der Benutzer meldet sich mit seinem Benutzernamen und Kennwort bei CS-SG an.
2. CC-SG stellt eine Verbindung zum externen Server her und übermittelt den Benutzernamen und das Kennwort.
3. Der Benutzername und das Kennwort werden entweder akzeptiert oder zurückgewiesen und zurückgesendet. Bei einer zurückgewiesenen Authentifizierung schlägt die Anmeldung fehl.
4. Ist die Authentifizierung erfolgreich, wird die lokale Autorisierung durchgeführt. CC-SG prüft, ob der eingegebene Benutzername einer Gruppe entspricht, die in CC-SG erstellt oder von Active Directory importiert wurde, und die Berechtigungen über die zugewiesene Richtlinie gewährt.

Ist die Remoteauthentifizierung deaktiviert, werden die Authentifizierung und Autorisierung lokal in CC-SG durchgeführt.

Benutzerkonten

Benutzerkonten müssen dem Authentifizierungsserver zur Remoteauthentifizierung hinzugefügt werden. Außer bei der Verwendung von Active Directory für die Authentifizierung und Autorisierung, erfordern alle Authentifizierungsserver, dass Benutzer in CC-SG erstellt werden. Der Benutzername, der beim Authentifizierungsserver verwendet wird, muss mit dem bei CC-SG übereinstimmen; die Kennwörter dürfen jedoch voneinander abweichen. Das lokale CC-SG-Kennwort wird nur verwendet, wenn die Remoteauthentifizierung deaktiviert ist. Weitere Informationen zum Hinzufügen von Benutzern, für die die Remoteauthentifizierung gilt, finden Sie in **Kapitel 7: Hinzufügen und Verwalten von Benutzern und Benutzergruppen**.

***Hinweis**: Bei der Verwendung der Remoteauthentifizierung müssen sich die Benutzer an den Administrator wenden, wenn sie ihr Kennwort auf dem Remoteserver ändern möchten. Kennwörter können in CC-SG für Benutzer, bei denen die Remoteauthentifizierung verwendet wird, nicht geändert werden.*

Definierte Namen für LDAP und Active Directory

Die Konfiguration von Benutzern auf LDAP- oder Active Directory-Servern, für die die Remoteauthentifizierung verwendet wird, erfordert die Eingabe von Benutzernamen und das Suchen im Format für definierte Namen. Das vollständige DN-Format wird unter **RFC2253** beschrieben. Im Rahmen dieses Dokuments müssen Sie wissen, wie Sie definierte Namen eingeben und in welcher Reihenfolge die Komponenten des Namens aufgeführt werden sollten.

Die Angabe eines definierten Namens für Active Directory sollte nach der folgenden Struktur erfolgen, Sie müssen jedoch nicht beides, **Allgemeiner Name** und **Organisationseinheit**, eingeben:

```
common name (cn), organizational unit (ou), domain component (dc)
```

Die Angabe eines DN für Netscape LDAP und eDirectory LDAP sollte nach dem folgenden Schema erfolgen:

```
user id (uid), organizational unit (ou), organization (o)
```

Benutzername

Bei der Authentifizierung von CC-SG-Benutzern auf einem Active Directory-Server durch die Angabe von **cn=administrator,cn=users,dc=xyz,dc=com** in **username** erhalten die Benutzer Zugriff mithilfe dieser Angaben, wenn ein CC-SG einer importierten AD-Gruppe zugewiesen ist. Beachten Sie, dass Sie mehrere allgemeine Namen, Organisationseinheiten und Domänenkomponenten festlegen können.

Basis-DN

Sie können auch einen DN (Distinguished Name) eingeben, um festzulegen, wo die Suche für Benutzer beginnt. Geben Sie einen DN im Feld **Basis-DN** ein, um einen Active Directory-Container festzulegen, in dem die Benutzer gefunden werden können. Die Eingabe von **ou=DCAdmins,ou=IT,dc=xyz,dc=com** führt beispielsweise zu einer Suche unter allen Benutzern in den Organisationseinheiten **DCAdmins** und **IT** und der Domäne **xyz.com**.

AD-Konfigurationen

AD-Modul zu CC-SG hinzufügen

CC-SG unterstützt die Authentifizierung und Autorisierung von Benutzern, die von einem AD-Domänencontroller importiert wurden, ohne dass die Benutzer lokal in CC-SG definiert werden müssen. Benutzer können somit ausschließlich auf dem AD-Server verwaltet werden. Sobald Ihr AD-Server als Modul in CC-SG konfiguriert wurde, kann CC-SG alle Domänenkontroller nach einer bestimmten Domäne durchsuchen. Sie können Ihre AD-Module mit Ihren AD-Servern in CC-SG synchronisieren, um sicherzustellen, dass CC-SG über die aktuellsten Autorisierungsinformationen hinsichtlich Ihrer AD-Benutzergruppen verfügt.

Wichtig: Erstellen Sie entsprechende AD-Benutzergruppen und weisen Sie AD-Benutzer zu, bevor Sie diesen Vorgang starten. Vergewissern Sie sich außerdem, dass Sie das CC-SG DNS- und Domänensuffix im Konfigurationsmanager konfiguriert haben. Weitere Informationen finden Sie in Kapitel 12: Konfigurationsmanager.

So fügen Sie AD-Module zu CC-SG hinzu:

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Auf dem Bildschirm **Sicherheitsmanager** wird die Registerkarte **Allgemein** angezeigt.
2. Klicken Sie auf **Hinzufügen...**, um das Fenster **Modul hinzufügen** zu öffnen.

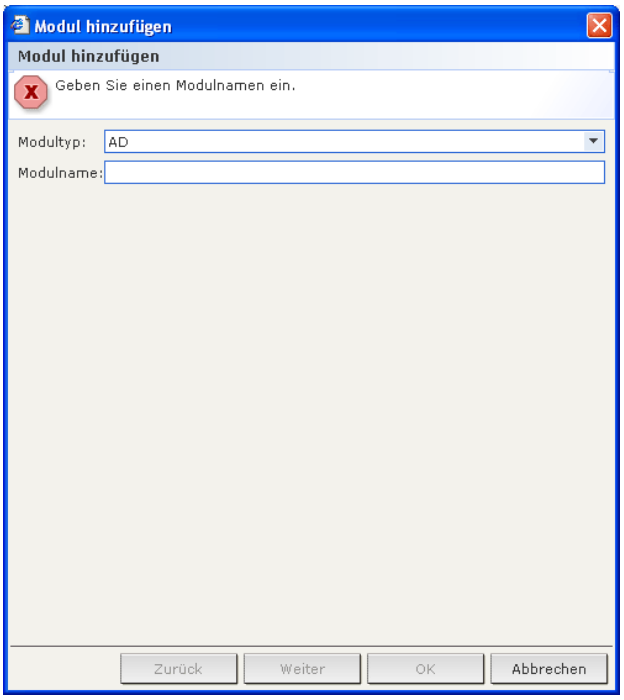


Abbildung 95 Modul hinzufügen

3. Klicken Sie auf das Dropdown-Menü **Modultyp**, und wählen Sie AD in der Liste aus.
4. Geben Sie den Namen des AD-Servers in das Feld **Modulname** ein. Der Modulname ist optional und wird nur angegeben, um dieses AD-Servermodul von anderen zu unterscheiden, die Sie in CC-SG konfigurieren. Der Name wird nicht mit dem tatsächlichen AD-Servernamen verknüpft.
5. Klicken Sie auf **Weiter**. Die Registerkarte **Allgemein** wird angezeigt.

Allgemeine AD-Einstellungen

Auf der Registerkarte **Allgemein** können Sie Informationen hinzufügen, damit CC-SG den AD-Server abfragen kann.

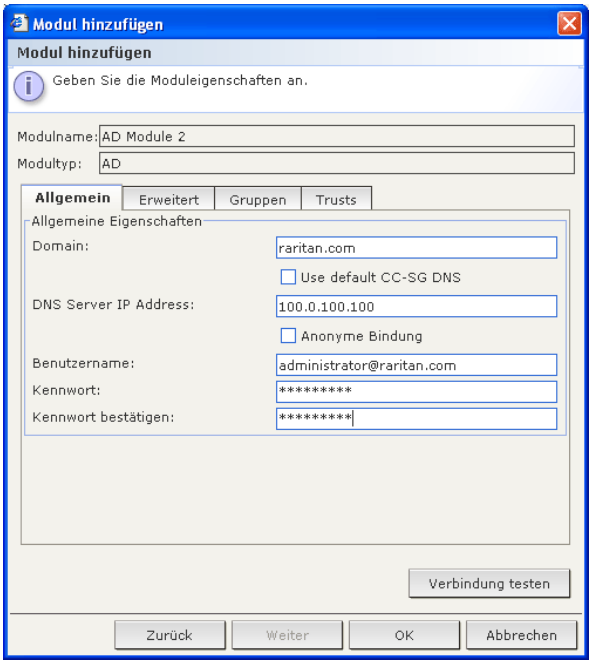


Abbildung 96 Allgemeine AD-Einstellungen

1. Geben Sie die AD-Domäne zum Abfragen in das Feld **Domäne** ein. Ist die AD-Domäne beispielsweise in der Domäne xyz.com installiert, geben Sie **xyz.com** in das Feld **Domäne** ein. CC-SG und der AD-Server, den Sie abfragen möchten, müssen entweder in derselben Domäne oder in verschiedenen Domänen konfiguriert sein, die sich vertrauen.

***Hinweis**: CC-SG fragt alle bekannten Domänencontroller nach der angegebenen Domäne ab.*

2. Geben Sie die IP-Adresse des DNS-Servers in das Feld **IP-Adresse des DNS-Servers** ein. Sie können auch das Kontrollkästchen **Use default CC-SG DNS (Standard-CC-SG-DNS verwenden)** markieren, um den DNS zu verwenden, der im Abschnitt des Konfigurationsmanagers in CC-SG konfiguriert ist. Weitere Informationen finden Sie in **Kapitel 12: Konfigurationsmanager**.
3. Aktivieren Sie **Anonyme Verbindung**, wenn Sie ohne Festlegung eines Benutzernamens und Kennworts eine Verbindung mit dem AD-Server herstellen möchten. Wenn Sie diese Option verwenden, sollten Sie sicherstellen, dass der AD-Server anonyme Abfragen zulässt.

***Hinweis**: Standardmäßig lässt Windows 2003 KEINE anonymen Abfragen zu. Windows 2000 Server lassen bestimmte anonyme Funktionen zu, wenn die Abfrageergebnisse auf den Berechtigungen für jedes Objekt beruhen.*

4. Wenn Sie keine anonyme Verbindung verwenden, geben Sie den Benutzernamen des Benutzerkontos ein, den Sie für die Abfrage des AD-Servers verwenden möchten. Halten Sie sich im Feld **Benutzername** an folgendes Format: **username@domain.com**. Der angegebene Benutzer muss über die Berechtigung verfügen, Suchabfragen in der AD-Domäne durchführen zu können. Der Benutzer kann beispielsweise einer Gruppe im Acitve Directory angehören, für die **Group scope** (Gruppenumfang) auf **Global** und **Group type** (Gruppentyp) auf **Security** (Sicherheit) gesetzt ist.
5. Geben Sie in die Felder **Kennwort** und **Kennwort bestätigen** das Kennwort für das Benutzerkonto ein, das Sie für die Abfrage des AD-Servers verwenden möchten.

6. Klicken Sie auf **Verbindung testen**, um die Verbindung zum Active Directory-Server mit den angegebenen Parametern zu testen. Sie sollten eine Bestätigung über eine erfolgreiche Verbindung erhalten. Wird die Bestätigungsmeldung nicht angezeigt, prüfen Sie die Einstellungen sorgfältig auf Fehler, und versuchen Sie es erneut.
7. Klicken Sie auf **Weiter**. Die Registerkarte **Erweitert** wird angezeigt.

Erweiterte AD-Einstellungen

1. Wenn Sie die erweiterten Einstellungen konfigurieren möchten, klicken Sie auf die Registerkarte **Erweitert**.

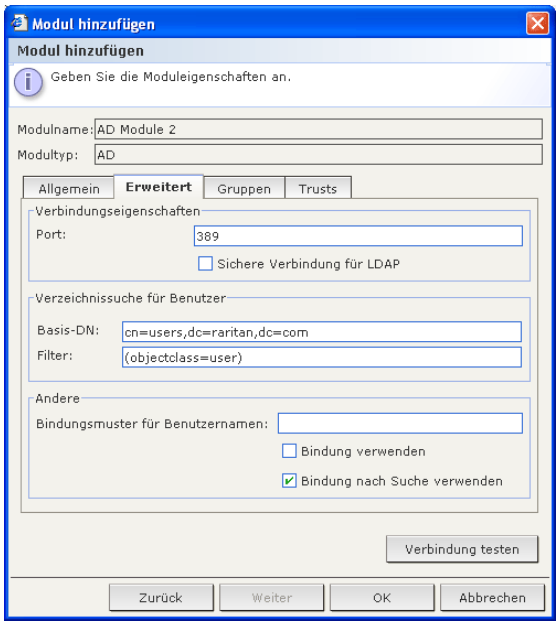


Abbildung 97 Erweiterte AD-Einstellungen

2. Geben Sie die Portnummer ein, die der AD-Server überwacht. Der Standardport lautet **389**. Wenn Sie sichere Verbindungen für LDAP verwenden (Schritt 3, unten) müssen Sie diesen Port ggf. ändern. Der Standardport für sichere LDAP-Verbindungen lautet **636**.
3. Aktivieren Sie **Sichere Verbindung für LDAP**, wenn Sie einen sicheren Kanal für die Verbindung verwenden möchten. Ist das Feld markiert, verwendet CC-SG zur Verbindung mit AD LDAP über SSL. Diese Option wird ggf. nicht von Ihrer AD-Konfiguration unterstützt.
4. Legen Sie einen **Basis-DN** (Verzeichnisebene/Eintrag) fest, unter dem die Authentifizierungssuchabfrage ausgeführt wird. CC-SG kann eine rekursive Suche vom Basis-DN nach unten durchführen.

BEISPIEL	BESCHREIBUNG
dc=raritan,dc=com	Die Abfrage für den Benutzereintrag wird für die gesamte Verzeichnisstruktur durchgeführt.
cn=Administrators,cn=Users,dc=raritan,dc=com	Die Abfrage für den Benutzereintrag wird nur im Unterverzeichnis „Administrators” (Eintrag) durchgeführt.

5. Geben Sie die Attribute eines Benutzers im Feld **Filter** ein, damit die Suchabfrage auf die Einträge beschränkt wird, die diese Kriterien erfüllen. Der Filter ist standardmäßig **objectclass=user**, d. h., dass nur Einträge vom Typ **user** durchsucht werden.

6. Geben Sie die Art und Weise für die Durchführung der Abfrage für den Benutzereintrag an. Wenn Sie **Bindung verwenden** markieren, versucht CC-SG mit dem Benutzernamen und dem Kennwort, die mit dem Applet bereitgestellt wurden, direkt eine Verbindung bzw. **Bindung** mit dem Active Directory-Server herzustellen. Ist das Muster des Benutzernamens jedoch unter **Benutzernamenmuster binden** angegeben, wird das Muster mit dem Benutzernamen vereint, der im Applet angegeben ist, und der vereinte Benutzername wird für die Verbindung zum AD-Server verwendet.
   Beispiel: Ist **cn={0},cn=Users,dc=raritan,dc=com** und **TestUser** im Applet angegeben, verwendet CC-SG **cn=TestUser,cn-Users,dc=raritan,dc=com** für die Verbindung zum AD-Server. Markieren Sie die Option **Bindung verwenden** nur, wenn der Benutzer, der sich über das Applet anmeldet, über die Berechtigungen verfügt, Abfragen an den AD-Server zu senden.
7. Aktivieren Sie **Bindung nach Suche verwenden**, um mit dem Benutzernamen und dem Kennwort, die auf der Registerkarte **Allgemein** festgelegt wurden, eine Verbindung mit dem Active Directory-Server herzustellen. Der Eintrag wird in dem angegebenen Basis-DN gesucht. Treffer treten auf, wenn die bestimmten Filterkriterien übereinstimmen und das Attribut „BerndKontoname" dem Benutzernamen entspricht, der im Applet angegeben wurde. Dann wird die zweite Verbindung oder **Bindung** mit dem Benutzernamen und Kennwort versucht, die im Applet angegeben sind. Durch diese zweite Verbindung wird sichergestellt, dass der Benutzer das richtige Kennwort angegeben hat.
8. Klicken Sie auf **Weiter**. Die Registerkarte **Gruppen** wird angezeigt.

AD-Gruppeneinstellungen

Auf der Registerkarte **Gruppen** können Sie den Speicherort angeben, von dem Sie AD-Benutzergruppen importieren möchten.

Wichtig: Sie müssen Gruppeneinstellungen angeben, bevor Sie Gruppen von AD importieren können.

1. Klicken Sie auf die Registerkarte **Gruppen**.

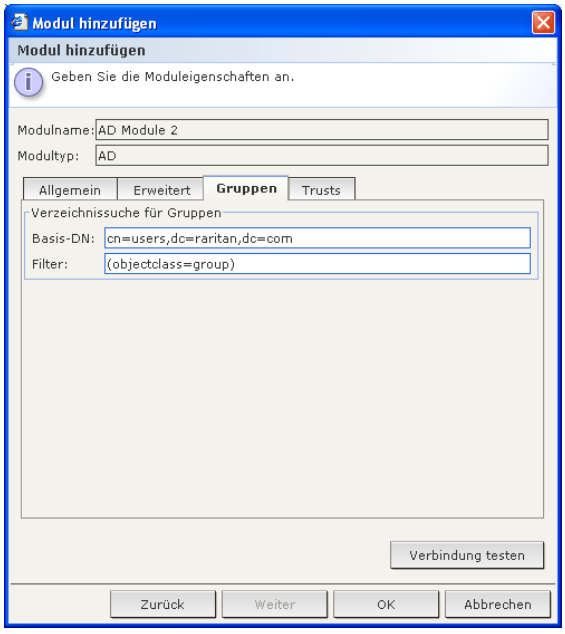


Abbildung 98 AD-Gruppeneinstellungen

2. Legen Sie einen **Basis-DN** (Verzeichnisebene/Eintrag) fest, unter dem die Gruppen, die den zu authentifizierenden Benutzer enthalten, gesucht werden.

BEISPIEL	BESCHREIBUNG
dc=raritan,dc=com	Die Abfrage für den Benutzer in der Gruppe wird für die gesamte Verzeichnisstruktur durchgeführt.
cn=Administrators,cn=Users,dc=raritan,dc=com	Die Abfrage für den Benutzer in der Gruppe wird nur im Unterverzeichnis „Administrators“ (Eintrag) durchgeführt.

3. Geben Sie die Attribute eines Benutzers im Feld **Filter** ein, damit die Suchabfrage für den Benutzer in der Gruppe auf die Einträge beschränkt wird, die diese Kriterien erfüllen. Wenn Sie beispielsweise **cn=Groups,dc=raritan,dc=com** als den Basis-DN und (**objectclass=group**) als Filter angeben, werden alle Einträge zurückgegeben, die sich im Eintrag **Groups** befinden und den Typ **group** aufweisen.
4. Klicken Sie auf **Weiter**. Die Registerkarte **Trusts** (Vertrauen) wird angezeigt.

AD-Vertrauenseinstellungen

Auf der Registerkarte **Trusts** (Vertrauen) können Sie Vertrauensbeziehungen zwischen dieser neuen AD-Domäne und vorhandenen Domänen einrichten. Eine Vertrauensbeziehung bietet authentifizierten Benutzern verschiedener Domänen den Zugriff auf Ressourcen. Vertrauensbeziehungen können eingehend, ausgehend, bidirektional oder deaktiviert sein. Sie sollten Vertrauensbeziehungen einrichten, wenn AD-Module, die verschiedene Gesamtstrukturen in AD darstellen, auf die Informationen anderer Gesamtstrukturen zugreifen sollen.

1. Klicken Sie auf die Registerkarte **Trusts** (Vertrauen). Wenn Sie mehrere AD-Domänen konfiguriert haben, werden alle anderen Domänen auf der Registerkarte **Trusts** (Vertrauen) aufgeführt.

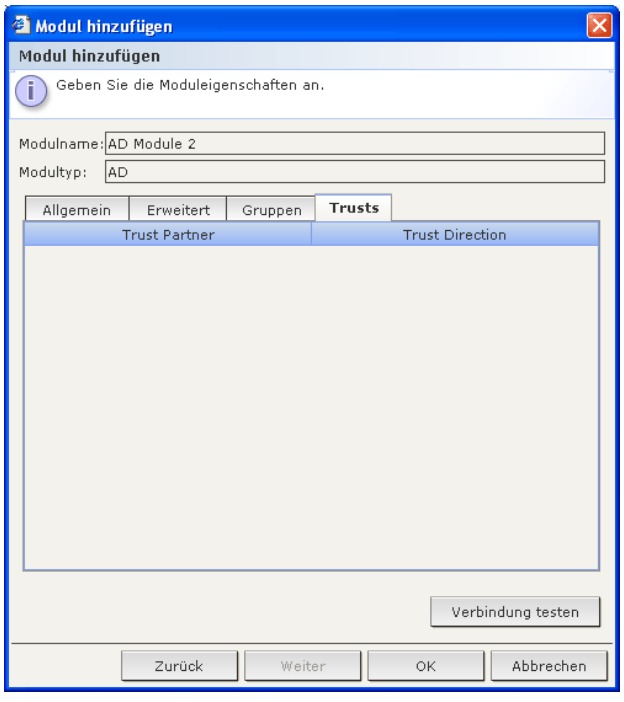


Abbildung 99 AD-Vertrauenseinstellungen

2. Klicken Sie für jede Domäne in der Spalte **Trust Partner** (Vertrauenspartner) auf das Dropdown-Menü **Trust Direction** (Vertrauensrichtung), und wählen Sie die Richtung für das Vertrauen zwischen den Domänen aus. Vertrauensrichtungen werden in allen AD-Modulen aktualisiert, wenn Sie Änderungen an einem AD-Modul vornehmen.
    - **Incoming** (Eingehend): Informationen, die von anderen Domänen eingehen, sind vertrauenswürdig. In der Abbildung oben würde AD-Modul 2 den Informationen trauen, die von AD-Modul 1 eingehen.
    - **Outgoing** (Ausgehend): Informationen, die an die ausgewählten Domänen gesendet werden, sind vertrauenswürdig. In der Abbildung oben würde AD-Modul 1 den Informationen trauen, die von AD-Modul 2 eingehen.
    - **Bidirectional** (Bidirektional): Informationen aus beiden Richtungen jeder Domäne sind vertrauenswürdig.
    - **Disabled** (Deaktiviert): Unter den Domänen findet kein Informationsaustausch statt.
3. Klicken Sie auf **Übernehmen**, um die Änderungen zu speichern. Klicken Sie dann auf **OK**, um das AD-Modul zu speichern und das Fenster zu schließen.

AD-Module bearbeiten

Nachdem Sie AD-Module konfiguriert haben, können Sie sie jederzeit bearbeiten.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**.
2. Wählen Sie das AD-Modul aus, das Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
3. Klicken Sie auf jede Registerkarte des Fensters **Modul bearbeiten**, um die konfigurierten Einstellungen anzuzeigen. Nehmen Sie bei Bedarf Änderungen vor. Weitere Informationen finden Sie unter **Allgemeine AD-Einstellungen**, **Erweiterte AD-Einstellungen**, **AD-Gruppeneinstellungen** und **AD-Vertrauenseinstellungen**.
4. Wenn Sie die Verbindungsinformationen ändern, klicken Sie auf **Verbindung testen**, um die Verbindung zum AD-Server mit den festgelegten Parametern zu testen. Sie sollten eine Bestätigung über eine erfolgreiche Verbindung erhalten. Wird die Bestätigungsmeldung nicht angezeigt, prüfen Sie die Einstellungen sorgfältig auf Fehler, und versuchen Sie es erneut.
5. Klicken Sie zum Speichern der Änderungen auf **OK**. Sie müssen die von Ihnen geänderten AD-Benutzergruppen synchronisieren. Sie können auch alle AD-Module synchronisieren, um alle Gruppen und Benutzer in allen Modulen zu synchronisieren. Weitere Informationen finden Sie unter **AD-Benutzergruppen synchronisieren** und **Alle AD-Module synchronisieren**.

AD-Benutzergruppen importieren

Sie müssen Gruppeneinstellungen im AD-Modul angeben, bevor Sie Gruppen vom AD-Server importieren können. Weitere Informationen zu AD-Gruppeneinstellungen finden Sie auf Seite 110. Nachdem Sie Änderungen an den importierten Gruppen oder Benutzern vorgenommen haben, müssen Sie die geänderten AD-Benutzergruppen synchronisieren. Sie können auch alle AD-Module synchronisieren, um alle Gruppen und Benutzer in allen Modulen zu synchronisieren. Weitere Informationen finden Sie unter **AD-Benutzergruppen synchronisieren** und **Alle AD-Module synchronisieren**.

***Hinweis**: Vergewissern Sie sich, dass Sie das CC-SG DNS und Domänensuffix im Konfigurationsmanager konfiguriert haben, bevor Sie AD-Benutzergruppen importieren. Weitere Informationen finden Sie in **Kapitel 12: Konfigurationsmanager**.*

1. Klicken Sie im Menü **Administration** auf **Sicherheit**.
2. Wählen Sie die AD-Module zum Importieren von AD-Benutzergruppen aus.
3. Klicken Sie auf **Gruppen importieren…**, um eine Liste der Benutzergruppenwerte abzurufen, die auf dem AD-Server gespeichert sind. Befinden sich noch nicht alle Benutzergruppen in CC-SG, können Sie diese hier importieren und ihnen Zugriffsrichtlinien zuweisen.

4. Markieren Sie die Kontrollkästchen neben den Gruppen, die Sie in CC-SG importieren möchten. Klicken Sie auf eine Spaltenüberschrift, um die Liste der Benutzergruppen nach den Daten in der Spalte zu sortieren. Geben Sie zur Suche nach Benutzergruppen einen Suchbegriff in das Feld **Suche für Gruppen** ein, und klicken Sie auf **Los**. Klicken Sie auf **Alles auswählen**, um alle Benutzergruppen zum Importieren auszuwählen. Klicken Sie auf **Gesamte Auswahl aufheben**, um die Auswahl aller Benutzergruppen aufzuheben.
5. Klicken Sie in der Spalte **Richtlinien** auf das Feld, und wählen Sie eine CC-SG-Zugriffsrichtlinie in der Liste aus, um die Richtlinie der ausgewählten Gruppe zuzuweisen. Diese Richtlinien sollten bereits erstellt sein. Weitere Informationen finden Sie in Kapitel 8: Richtlinien.
6. Klicken Sie auf **Importieren**, um die ausgewählten Benutzergruppen zu importieren.
7. Klicken Sie zum Überprüfen, dass die Gruppe ordnungsgemäß importiert wurde, und zum Anzeigen der Rechte dieser gerade importierten Gruppe auf die Registerkarte **Benutzer**. Wählen Sie dann die importierte Gruppe aus, um das Fenster **Benutzergruppenprofil** anzuzeigen. Prüfen Sie die Daten auf den Registerkarten **Berechtigungen** und **Geräte-/Knotenrichtlinien**. Klicken Sie auf die Registerkarte **Active Directory Associations** (Active Directory-Zuordnungen), um die Daten für das AD-Modul anzuzeigen, das mit der Benutzergruppe verknüpft ist.

AD-Benutzergruppen synchronisieren

Beim Synchronisieren von AD-Benutzergruppen ruft CC-SG die Gruppen für das ausgewählte AD-Modul ab, vergleicht die Namen mit den Benutzergruppen, die von AD importiert wurden, und ermittelt die Übereinstimmungen. Die Ergebnisse werden in CC-SG angezeigt, und Sie können auswählen, welche Sie importieren möchten. Dadurch wird sichergestellt, dass CC-SG die aktuellen AD-Benutzergruppendaten importiert hat. CC-SG synchronisiert außerdem täglich alle AD-Module automatisch. Weitere Informationen finden Sie unter **AD-Synchronisierungszeitpunkt festlegen**.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**.
2. Wählen Sie das AD-Modul aus, dessen Benutzergruppen mit dem AD-Server synchronisiert werden sollen.
3. Klicken Sie auf **Synchronize AD User Groups** (AD-Benutzergruppen synchronisieren).
4. Eine Bestätigung wird angezeigt, sobald alle importieren Benutzergruppen des ausgewählten Moduls erfolgreich synchronisiert wurden.

Alle AD-Module synchronisieren

Wenn Sie alle AD-Module synchronisieren, ruft CC-SG die Benutzergruppen für alle konfigurierten AD-Module ab, vergleicht die Namen mit den Benutzergruppen, die in CC-SG importiert wurden, und aktualisiert den lokalen CC-SG-Cache. Der lokale CC-SG-Cache enthält alle Domänencontroller für jede Domäne, alle Benutzergruppen für alle Module sowie die Benutzerdaten für alle bekannten AD-Benutzer. Wurden Benutzergruppen aus dem AD-Modul gelöscht, entfernt CC-SG sie auch aus dem lokalen Cache. Dadurch wird sichergestellt, dass CC-SG über die aktuellen AD-Benutzergruppendaten verfügt.

1. Sie müssen in den Wartungsmodus wechseln, wenn Sie alle AD-Module synchronisieren möchten. Im Wartungsmodus werden alle Benutzer bei CC-SG abgemeldet. Klicken Sie im Menü **Systemwartung** auf **Wartungsmodus** und dann auf **Wartungsmodus starten**.
2. Geben Sie im Fenster **Wartungsmodus starten** in die entsprechenden Felder die Nachricht für Benutzer ein, die bei CC-SG abgemeldet werden, sowie die Dauer in Minuten, bis CC-SG in den Wartungsmodus wechselt. Klicken Sie dann auf **OK**.
3. Klicken Sie im Bestätigungsfeld auf **OK**.
4. Beim Starten des CC-SG-Wartungsmodus wird eine zweite Bestätigungsnachricht angezeigt. Klicken Sie auf **OK**.
5. Wenn CC-SG sich im Wartungsmodus befindet, klicken Sie im Menü **Administration** auf **Sicherheit**.

6. Klicken Sie auf **Synchronize all AD Modules** (Alle AD-Module synchronisieren).

Abbildung 100 Alle AD-Module synchronisieren

7. Nachdem alle AD-Module erfolgreich synchronisiert wurden, wird eine Bestätigungsmeldung angezeigt.
8. Verlassen Sie den Wartungsmodus, indem Sie im Menü **Systemwartung** auf **Wartungsmodus** und dann auf **Wartungsmodus beenden** klicken.
9. Klicken Sie im angezeigten Bildschirm auf **OK**. Beim Verlassen des CC-SG-Wartungsmodus wird eine zweite Bestätigungsnachricht angezeigt. Klicken Sie auf **OK**.

AD-Synchronisierungszeitpunkt festlegen

Standardmäßig synchronisiert CC-SG alle konfigurierten AD-Module täglich um 23:30 Uhr. Sie können die Uhrzeit für diese automatische Synchronisierung ändern.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**.
2. Klicken Sie unten im Feld **AD Synchronization Time** (AD-Synchronisierungszeitpunkt) auf die Pfeile nach oben oder unten, um die Uhrzeit auszuwählen, zu der CC-SG die tägliche Synchronisierung der AD-Module ausführen soll.

Abbildung 101 Alle AD-Module synchronisieren

3. Klicken Sie auf **Update Synchroniszation Time** (Synchonisierungszeitpunkt aktualisieren), um die Änderungen zu speichern.

AD-Konfiguration – Aktualisierung von CC-SG 3.0.2

Wenn Sie CC-SG von 3.0.2 auf 3.1 aktualisiert haben, müssen Sie Ihre AD-Module erneut konfigurieren, bevor sich Ihre AD-Benutzer bei CC-SG anmelden können. CC-SG 3.1 erfordert, dass für jedes AD-Modul ein DNS- und Domänenname festgelegt wird. Durch diese Konfiguration kann CC-SG alle Domänencontroller einer bestimmten Domäne abfragen.

Wichtig: CC-SG befindet sich nach der Aktualisierung auf 3.1 im Wartungsmodus. Sie müssen sich daher mit dem CC-Superuser-Konto anmelden, um diese Aktion durchführen zu können. Das Standardkonto des CC-Superuser zur Systemaktualisierung von 3.0.2 lautet ccroot/raritan0.

So konfigurieren Sie AD-Module erneut:

1. Klicken Sie im Menü **Administration** auf **Sicherheit**.
2. Wählen Sie das AD-Modul aus, das Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
3. Geben Sie auf der Registerkarte **Allgemein** den DNS- und Domänennamen für die AD-Module in die entsprechenden Felder ein. Weitere Informationen finden Sie unter **Allgemeine AD-Einstellungen**.
4. Klicken Sie auf **Verbindung testen**, um die Verbindung zum Active Directory-Server mit den angegebenen Parametern zu testen. Sie sollten eine Bestätigung über eine erfolgreiche Verbindung erhalten. Wird die Bestätigungsmeldung nicht angezeigt, prüfen Sie die Einstellungen sorgfältig auf Fehler, und versuchen Sie es erneut.
5. Klicken Sie zum Speichern der Änderungen auf **OK**.

6. Wenn Sie erweiterte, Gruppen- oder Vertrauenseinstellungen konfigurieren möchten, müssen Sie auf die entsprechende Registerkarte klicken, um die Optionen anzuzeigen. Weitere Informationen finden Sie unter **Erweiterte AD-Einstellungen**, **AD-Gruppeneinstellungen** und **AD-Vertrauenseinstellungen**. Klicken Sie zum Speichern der Änderungen auf **OK**.
7. Wiederholen Sie diese Schritte, um alle AD-Module erneut zu konfigurieren.
8. Nachdem Sie alle AD-Module erneut konfiguriert haben, können Sie Ihre importieren AD-Benutzergruppen mit den AD-Servern synchronisieren. Weitere Informationen finden Sie unter **AD-Benutzergruppen synchronisieren**.
9. Nachdem Sie die AD-Benutzergruppen jedes Moduls synchronisiert haben, sollten Sie alle AD-Module synchronisieren. Weitere Informationen finden Sie unter **Alle AD-Module synchronisieren**. Abhängig von der AD-Konfiguration kann die Synchronisierung bis zu 30 Sekunden pro Domänencontroller dauern. Sind einige Domänencontroller während der Synchronisation offline, kann der Vorgang länger dauern.

Hinweis: *Weitere Informationen dazu, wie CC-SG 3.1 die Synchronisation von AD-Benutzergruppen durchführt, finden Sie in den folgenden Abschnitten:* ***Alle AD-Module synchronisieren*** *und* ***AD-Synchronisierungszeitpunkt festlegen****. Weitere Informationen zum Generieren von Berichten mit Informationen zu AD-Benutzergruppen finden Sie in* ***Kapitel 10: Erstellen von Berichten, AD-Benutzergruppenbericht****.*

LDAP-Modul (Netscape) zu CC-SG hinzufügen

Nach dem Starten von CC-SG und der Eingabe eines Benutzernamens und Kennworts wird eine Abfrage entweder über CC-SG oder direkt an den LDAP-Server weitergeleitet. Stimmen der Benutzername und das Kennwort mit denjenigen im LDAP-Verzeichnis überein, wird der Benutzer authentifiziert. Der Benutzer wird dann für die lokalen Benutzergruppen auf dem LDAP-Server autorisiert.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Auf dem Bildschirm **Sicherheitsmanager** wird die Registerkarte **Allgemein** angezeigt.
2. Klicken Sie auf **Hinzufügen...**, um das Fenster **Modul hinzufügen** zu öffnen.

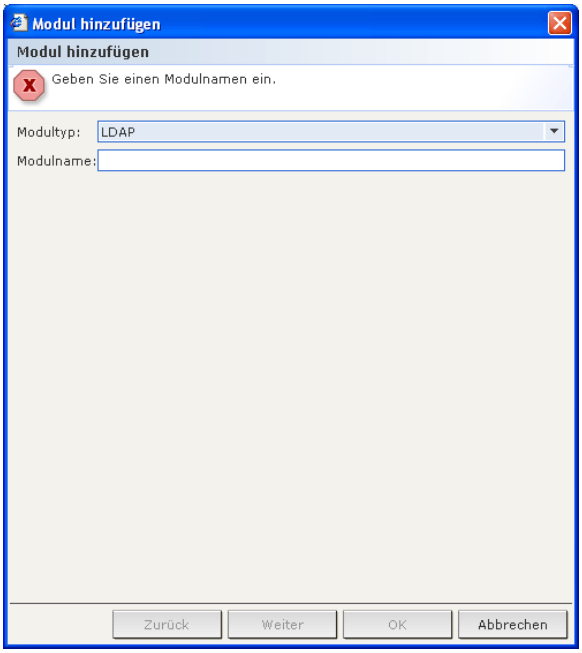


Abbildung 102 LDAP-Modul hinzufügen

3. Klicken Sie auf das Dropdown-Menü **Modultyp**, und wählen Sie LDAP in der Liste aus.
4. Geben Sie den Namen des LDAP-Servers in das Feld **Modulname** ein.
5. Klicken Sie auf **Weiter**. Die Registerkarte **Allgemein** wird angezeigt.

Allgemeine LDAP-Einstellungen

1. Klicken Sie auf die Registerkarte **Allgemein**.

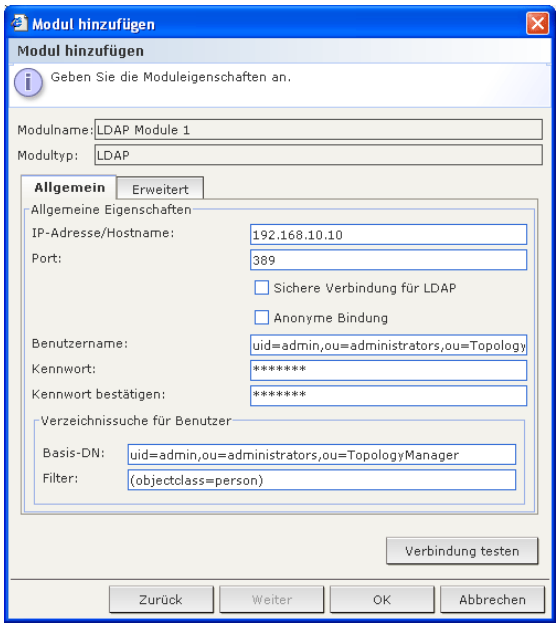


Abbildung 103 Allgemeine LDAP-Einstellungen

2. Geben Sie die IP-Adresse oder den Hostnamen des LDAP-Servers im Feld IP-Adresse/Hostname ein. Die Regeln zur Vergabe von Hostnamen sind unter **Terminologie/Abkürzungen** in **Kapitel 1: Einleitung** beschrieben.
3. Geben Sie den Portwert im Feld **Port** ein. Der Standardport lautet 389.
4. Markieren Sie **Sichere Verbindung für LDAP**, wenn Sie einen sicheren LDAP-Server verwenden.
5. Markieren Sie die Option **Anonyme Verbindung**, wenn Ihr LDAP-Server anonyme Abfragen zulässt. Sie müssen bei anonymen Verbindungen keinen Benutzernamen und kein Kennwort eingeben.

***Hinweis**: Standardmäßig lässt Windows 2003 KEINE anonymen Abfragen zu. Windows 2000 Server lassen bestimmte anonyme Funktionen zu, wenn die Abfrageergebnisse auf den Berechtigungen für jedes Objekt beruhen.*

6. Wenn Sie keine anonyme Verbindung verwenden, geben Sie einen Benutzernamen in das Feld **Benutzername** ein. Geben Sie einen DN (Distinguished Name) ein, um die Berechtigungen festzulegen, die beim Abfragen des LDAP-Servers verwendet werden. Geben Sie für den DN den allgemeinen Namen, die Organisationseinheit und Domäne ein. Geben Sie beispielsweise **uid=admin,ou=Administrators,ou=TopologyManagement,o=NetscapeRoot** ein. Trennen Sie die Werte durch Komma, verwenden Sie vor oder nach dem Komma jedoch keine Leerstellen. Die Werte können Leerstellen enthalten (z. B. **Command Center**).
7. Geben Sie das Kennwort in die Felder **Kennwort** und **Kennwort bestätigen** ein.
8. Geben Sie einen DN (Distinguished Name) im Feld **Basis-DN** ein, um anzugeben, wo die Suche nach Benutzern anfangen soll. Mit dem Wert **ou=Administrators,ou=TopologyManagement,o=NetscapeRoot** werden beispielsweise alle Organisationseinheiten der Domäne durchsucht.
9. Sie können die Suche auf bestimmte Objekttypen beschränken, indem Sie einen Wert im Feld **Filter** eingeben. Der Wert **(objectclass=person)** schränkt die Suche beispielsweise auf Personenobjekte ein.

10. Klicken Sie auf **Verbindung testen**, um den LDAP-Server mit den vorhandenen Parametern zu testen. Sie sollten eine Bestätigung über eine erfolgreiche Verbindung erhalten. Ist dies nicht der Fall, prüfen Sie die Einstellungen sorgfältig auf Fehler, und versuchen Sie es erneut.
11. Klicken Sie auf **Weiter**, um die Registerkarte **Erweitert** anzuzeigen und die erweiterten Konfigurationsoptionen für den LDAP-Server einzustellen.

Erweiterte LDAP-Einstellungen

1. Klicken Sie auf die Registerkarte **Erweitert**.

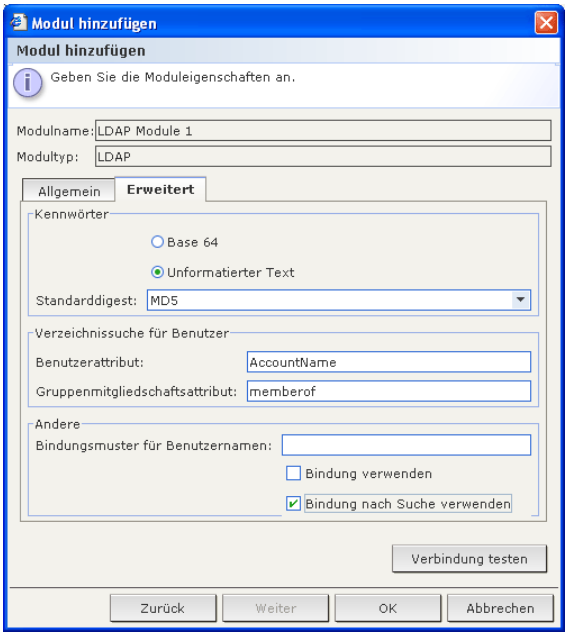


Abbildung 104 Erweiterte LDAP-Einstellungen

2. Klicken Sie auf das Optionsfeld **Base 64**, wenn das Kennwort verschlüsselt an den LDAP-Server gesendet werden soll. Klicken Sie auf das Optionsfeld **Unformatierter Text**, wenn das Kennwort unverschlüsselt an den LDAP-Server gesendet werden soll.
3. Klicken Sie auf das Dropdown-Menü **Standarddigest**, und wählen Sie die Standardverschlüsselung für Benutzerkennwörter aus.
4. Geben Sie die Parameter für die Benutzer- und Gruppenmitgliedschaftsattribute in die Felder **Benutzerattribute** und **Gruppenmitgliedschaftsattribute** ein. Diese Werte sollten Sie aus Ihrem LDAP-Verzeichnisschema abrufen.
5. Geben Sie das Bindungsmuster im Feld **Benutzernamenmuster binden** ein.
6. Aktivieren Sie **Bindung verwenden**, wenn CC-SG den Benutzernamen und das Kennwort, die bei der Anmeldung eingegeben wurden, zur Authentifizierung an den LDAP-Server senden soll. Ist **Bindung verwenden** nicht aktiviert, sucht CC-SG auf dem LDAP-Server nach dem Benutzernamen. Wird der Name gefunden, ruft CC-SG das LDAP-Objekt ab und vergleicht das zugeordnete Kennwort lokal mit dem eingegebenen Kennwort.
7. Auf einigen LDAP-Servern kann das Kennwort nicht als Teil des LDAP-Objekts abgerufen werden. Aktivieren Sie **Bindung nach Suche verwenden**, damit CC-SG das Kennwort wieder an das LDAP-Objekt bindet und es zur Authentifizierung an den Server zurücksendet.
8. Klicken Sie zum Speichern der Änderungen auf **OK**.

Konfigurationseinstellungen für Sun One LDAP (iPlanet)

Beispiel für Parametereinstellungen bei Verwendung eines Sun One LDAP-Server zur Remoteauthentifizierung:

PARAMETERNAME	SUN ONE LDAP-PARAMETER
IP-Adresse/Hostname:	**<IP-Adresse des Verzeichnisservers>**
Benutzername	**CN=<Gültige Benutzer-ID>**
Kennwort	***<Kennwort>***
Basis-DN	**O=<Organisation>**
Filter	**(objectclass=person)**
Kennwörter (Fenster Erweitert)	**Unformatierter Text**
Standarddigest für Kennwort (Erweitert):	**SHA**
Bindung verwenden	**Deaktiviert**
Bindung nach Suche verwenden	**Aktiviert**

Konfigurationseinstellungen für OpenLDAP (eDirectory)

Verwenden Sie bei einem OpenLDAP-Server für die Remoteauthentifizierung das folgende Beispiel:

PARAMETERNAME	OPEN LDAP-PARAMETER
IP-Adresse/Hostname:	**<IP-Adresse des Verzeichnisservers>**
Benutzername	**CN=<Gültige Benutzer-ID>, O=<Organisation>**
Kennwort	**<Kennwort>**
Benutzerbasis	**O=accounts, O=<Organisation>**
Benutzerfilter	**(objectclass=person)**
Kennwörter (Fenster Erweitert)	**Base64**
Standarddigest für Kennwort (Erweitert):	**Crypt**
Bindung verwenden	**Deaktiviert**
Bindung nach Suche verwenden	**Aktiviert**

LDAP-Zertifikateinstellungen

Mithilfe der LDAP-Zertifikateinstellungen können Sie ein LDAP-Zertifikat hochladen. Sie können außerdem hochgeladene Zertifikate annehmen oder ablehnen.

1. Klicken Sie auf die Registerkarte **Erweitert**.
2. Klicken Sie auf **Durchsuchen**, navigieren Sie zur Zertifikatdatei, die Sie hochladen möchten, und klicken Sie auf **Öffnen**.
3. Klicken Sie auf **Annehmen**, damit CC-SG dem Zertifikat vertraut. Klicken Sie auf **Ablehnen**, um das Zertifikat zu entfernen.
4. Wenn Sie ein Zertifikat löschen möchten, wählen Sie dieses aus, und klicken Sie auf **Löschen**.
5. Klicken Sie zum Speichern der Änderungen auf **OK**.

TACACS+-Module hinzufügen

CC-SG-Benutzer, für die ein TACACS+-Server und Remoteauthentifizierung verwendet wird, müssen auf dem TACACS+-Server und in CC-SG erstellt werden. Der Benutzername, der für den TACACS+-Server verwendet wird, muss mit dem für CC-SG übereinstimmen; die Kennwörter dürfen jedoch voneinander abweichen. Weitere Informationen zum Hinzufügen von Benutzern, für die die Remoteauthentifizierung gilt, finden Sie in **Kapitel 7: Hinzufügen und Verwalten von Benutzern und Benutzergruppen**.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Auf dem Bildschirm **Sicherheitsmanager** wird die Registerkarte **Allgemein** angezeigt.
2. Klicken Sie auf **Hinzufügen...**, um das Fenster **Modul hinzufügen** zu öffnen.

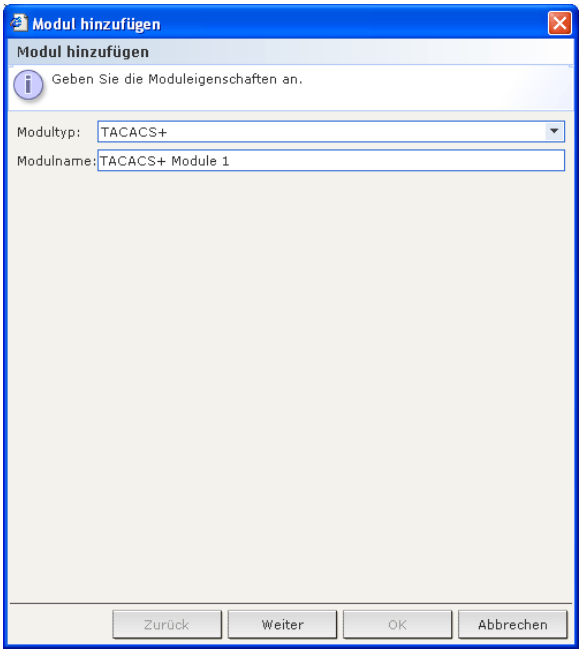


Abbildung 105 TACACS+-Modul hinzufügen

3. Klicken Sie auf das Dropdown-Menü **Modultyp**, und wählen Sie TACACS+ in der Liste aus.
4. Geben Sie den Namen des TACACS+-Servers in das Feld **Modulname** ein.
5. Klicken Sie auf **Weiter**. Die Registerkarte **Allgemein** wird angezeigt.

Allgemeine TACACS+-Einstellungen

1. Geben Sie die IP-Adresse oder den Hostnamen des TACACS+-Servers im Feld **IP-Adresse/Hostname** ein. Die Regeln zur Vergabe von Hostnamen werden unter **Terminologie/Abkürzungen** in **Kapitel 1: Einleitung** beschrieben.

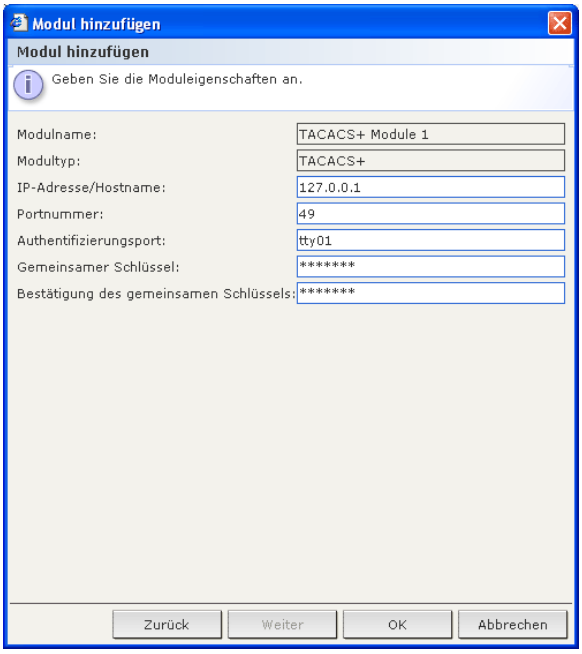


Abbildung 106 Allgemeine TACACS+-Einstellungen

2. Geben Sie die Portnummer in das Feld **Portnummer** ein, die der TACACS+-Server überwacht. Der Standardport lautet **49**.
3. Geben Sie den Authentifizierungsport im Feld **Authentifizierungsport** ein.
4. Geben Sie den gemeinsamen Schlüssel in die Felder **Gemeinsamer Schlüssel** und **Bestätigung des gemeinsamen Schlüssels** ein.
5. Klicken Sie zum Speichern der Änderungen auf **OK**.

RADIUS-Module hinzufügen

CC-SG-Benutzer, für die ein RADIUS-Server und Remoteauthentifizierung verwendet wird, müssen auf dem RADIUS-Server und in CC-SG erstellt werden. Der Benutzername, der für den RADIUS-Server verwendet wird, muss mit dem für CC-SG übereinstimmen, die Kennwörter dürfen jedoch voneinander abweichen. Weitere Informationen zum Hinzufügen von Benutzern, für die die Remoteauthentifizierung gilt, finden Sie in **Kapitel 7: Hinzufügen und Verwalten von Benutzern und Benutzergruppen**.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Auf dem Bildschirm **Sicherheitsmanager** wird die Registerkarte **Allgemein** angezeigt.
2. Klicken Sie auf **Hinzufügen...**, um das Fenster **Modul hinzufügen** zu öffnen.

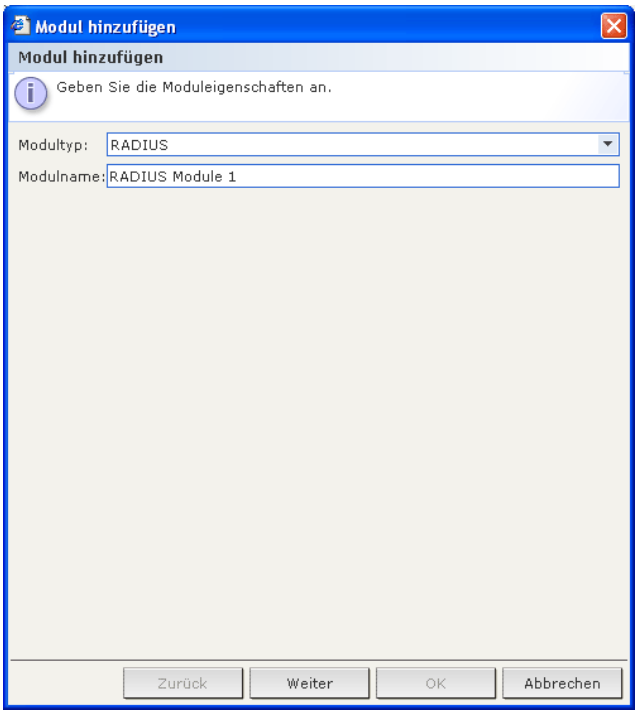


Abbildung 107 Registerkarte Modul hinzufügen des Sicherheitsmanagers

3. Klicken Sie auf das Dropdown-Menü **Modultyp**, und wählen Sie RADIUS in der Liste aus.
4. Geben Sie den Namen des RADIUS-Servers in das Feld **Modulname** ein.
5. Klicken Sie auf **Weiter**. Die Registerkarte **Allgemein** wird angezeigt.

Allgemeine RADIUS-Einstellungen

1. Klicken Sie auf die Registerkarte **Allgemein**.

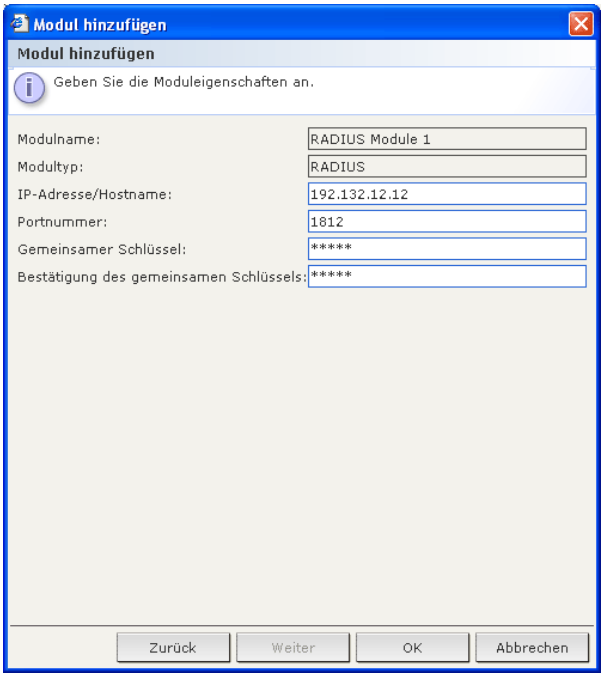


Abbildung 108 RADIUS-Server festlegen

2. Geben Sie die IP-Adresse oder den Hostnamen des RADIUS-Servers im Feld **IP-Adresse/Hostname** ein. Die Regeln zur Vergabe von Hostnamen sind unter **Terminologie/Abkürzungen** in **Kapitel 1: Einleitung** beschrieben.
3. Geben Sie die Portnummer im Feld **Portnummer** ein. Der Standardport lautet **1812**.
4. Geben Sie den Authentifizierungsport im Feld **Authentifizierungsport** ein.
5. Geben Sie den gemeinsamen Schlüssel in die Felder **Gemeinsamer Schlüssel** und **Bestätigung des gemeinsamen Schlüssels** ein.
6. Klicken Sie zum Speichern der Änderungen auf **OK**.

Zwei-Faktoren-Authentifizierung mit RADIUS

Mithilfe eines RSA RADIUS-Servers, der die Zwei-Faktoren-Authentifizierung in Verbindung mit einem RSA-Authentifizierungsmanager verwendet, kann CC-SG die Zwei-Faktoren-Authentifizierung mit dynamischen Token nutzen.

In dieser Umgebung melden sich Benutzer bei CC-SG an, indem sie ihren Benutzernamen in das Feld **Benutzername** eingeben. Dann geben Benutzer ihre festgelegten Kennwörter und einen Wert für den dynamischen Token in das Feld **Kennwort** ein.

Die dazu notwendige Konfiguration des RADIUS-Servers und des Authentifizierungsmanagers würde den Rahmen dieses Dokuments sprengen. CC-SG wird wie bei der standardmäßigen RADIUS-Remoteauthentifizierung (wie oben beschrieben) konfiguriert. CC-SG sollte so konfiguriert werden, dass es auf den RADIUS-Server verweist. Weitere Informationen finden Sie in **Anhang G: Zwei-Faktoren-Authentifizierung**.

Module für die Authentifizierung und Autorisierung festlegen

Nachdem Sie alle externen Server in CC-SG als Module hinzugefügt haben, legen Sie fest, ob CC-SG jeden dieser Server für die Authentifizierung, Autorisierung oder beides verwenden soll.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Klicken Sie im Fenster **Sicherheitsmanager** auf die Registerkarte **Allgemein**. Alle konfigurierten externen Authentifizierung- und Autorisierungsserver werden im Bereich für externe AA-Server angezeigt.
2. Markieren Sie für jeden Server das Kontrollkästchen **Authentifizierung**, wenn CC-SG den Server zur Authentifizierung von Benutzern verwenden soll.
3. Markieren Sie für jeden Server das Kontrollkästchen **Autorisierung**, wenn CC-SG den Server zur Autorisierung von Benutzern verwenden soll. Nur AD-Server können zur Autorisierung verwendet werden.
4. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Reihenfolge für externe AA-Server festlegen

Auf der Registerkarte **Allgemein** können Sie die Reihenfolge festlegen, in der CC-SG die konfigurierten externen AA-Server abfragt. Wenn die erste aktivierte Option nicht verfügbar ist, probiert CC-SG die zweite Option aus, dann die dritte usw., bis der Vorgang erfolgreich ist.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Klicken Sie im Fenster **Sicherheitsmanager** auf die Registerkarte **Allgemein**.

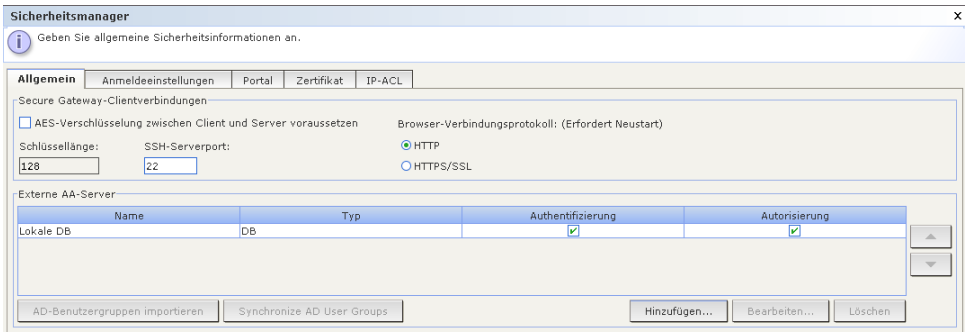


Abbildung 109 Registerkarte Allgemein des Sicherheitsmanagers

2. Im Bereich **Externe AA-Server** werden alle verfügbaren Authentifizierungs- und Autorisierungsoptionen für CC-SG angezeigt. Wählen Sie in der Liste einen Namen aus, und klicken Sie auf die Pfeile nach oben und nach unten, um die Reihenfolge der Verwendung festzulegen.
3. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Diese Seite wurde absichtlich leer gelassen.

Kapitel 10: Erstellen von Berichten

Berichte können durch Klicken auf die Spaltenüberschriften sortiert werden. Klicken Sie auf eine Spaltenüberschrift, um die Berichtsdaten nach den Werten in der Spalte zu sortieren. Die Daten werden in aufsteigender Reihenfolge alphabetisch, numerisch oder chronologisch angezeigt. Klicken Sie erneut auf die Spaltenüberschrift, um die Daten in absteigender Reihenfolge zu sortieren.

Sie können die Spaltenbreite in allen Berichten anpassen. Positionieren Sie Ihren Mauszeiger auf der Spaltentrennung in der obersten Zeile, bis der Mauszeiger als Pfeil mit zwei Spitzen angezeigt wird. Klicken Sie und ziehen Sie den Pfeil nach links oder rechts, um die Spaltenbreite anzupassen.

Der Sortierungswert und die Spaltenbreite, die Sie verwendet haben, werden das nächste Mal, wenn Sie sich anmelden und CC-SG-Berichte ausführen, als Standardansicht angezeigt. Sie können in allen Berichten auf eine Zeile doppelklicken, um weitere Berichtsdetails anzuzeigen.

***Hinweis**: Sie können in allen Berichten die **Strg.**-Taste halten und klicken, um die Markierung einer Zeile aufzuheben.*

Überwachungslistenbericht

Der Bericht **Überwachungsliste** enthält Überwachungsprotokolle und Informationen über den Zugriff auf CC-SG. Sie finden darin Informationen über das Hinzufügen, Bearbeiten oder Löschen von Geräten oder Ports und andere Änderungen.

CC-SG verwaltet eine Überwachungsliste für die folgenden Ereignisse:

- Starten von CC-SG
- Beenden von CC-SG
- Anmeldungen von Benutzern bei CC-SG
- Abmeldungen von Benutzern bei CC-SG
- Herstellen einer Knotenverbindung durch Benutzer

1. Klicken Sie im Menü **Berichte** auf **Überwachungsliste**. Das Fenster **Überwachungsliste** wird angezeigt.

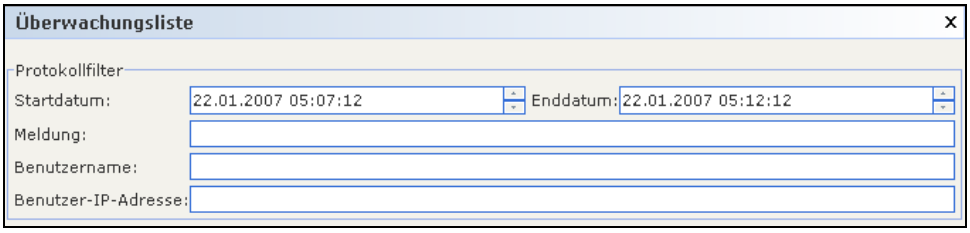


Abbildung 110 Fenster Überwachungsliste

2. Legen Sie den Datumsbereich für den Bericht in den Feldern **Startdatum** und **Enddatum** fest. Klicken Sie auf jede Komponente des Standarddatums (Monat, Tag, Jahr, Stunde, Minute, Sekunde), um sie auszuwählen, und legen Sie den gewünschten Wert fest, indem Sie auf die Pfeile nach oben und nach unten klicken.
3. Sie können die Daten im Bericht einschränken, indem Sie weitere Parameter in die Felder **Meldung**, **Benutzername** und **Benutzer-IP-Adresse** eingeben.

- Wenn Sie den Bericht auf Meldungstexte einschränken möchten, die mit einer Aktivität verknüpft sind, geben Sie den Text in das Feld **Meldung** ein.
- Wenn Sie den Bericht auf bestimmte Benutzeraktivitäten einschränken möchten, geben Sie den Benutzernamen in das Feld **Benutzername** ein.
- Wenn Sie den Bericht auf bestimmte IP-Adressen-Aktivitäten einschränken möchten, geben Sie die IP-Adresse des Benutzers in das Feld **Benutzer-IP-Adresse** ein.

4. Klicken Sie auf **OK**, um den Bericht auszuführen. Der Bericht wird erstellt, und es werden die Daten zu den Aktivitäten angezeigt, die während des angegebenen Zeitraums aufgetreten sind und allen angegebenen Parametern entsprechen.

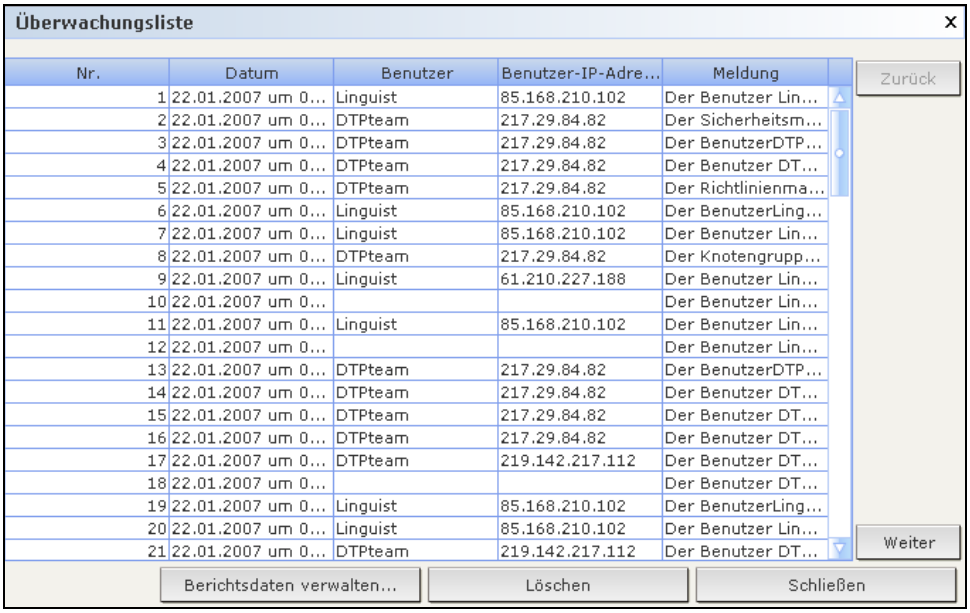


Abbildung 111 Bericht Überwachungsliste

- Klicken Sie auf **Weiter** oder **Zurück**, um im Bericht zu navigieren.
- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Löschen**, um die Protokolldateien zu löschen, die im Bericht verwendet wurden.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Fehlerprotokollbericht

CC-SG speichert Fehlermeldungen in verschiedenen Fehlerprotokolldateien, die aufgerufen und zum Beheben von Problemen verwendet werden können.

1. Klicken Sie im Menü **Berichte** auf **Fehlerprotokoll**. Das Fenster **Fehlerprotokoll** wird angezeigt.

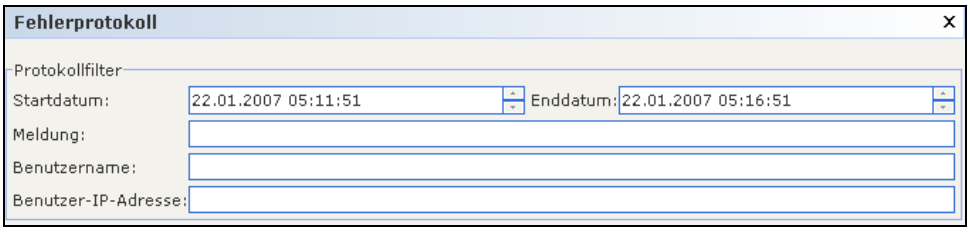


Abbildung 112 Fenster Fehlerprotokoll

2. Legen Sie den Datumsbereich für den Bericht in den Feldern **Startdatum** und **Enddatum** fest. Klicken Sie auf jede Komponente des Standarddatums (Monat, Tag, Jahr, Stunde, Minute, Sekunde), um sie auszuwählen, und legen Sie den gewünschten Wert fest, indem Sie auf die Pfeile nach oben und nach unten klicken.
3. Sie können die Daten im Bericht einschränken, indem Sie weitere Parameter in die Felder **Meldung**, **Benutzername** und **Benutzer-IP-Adresse** eingeben.

- Wenn Sie den Bericht auf Meldungstexte einschränken möchten, die mit einer Aktivität verknüpft sind, geben Sie den Text in das Feld **Meldung** ein.
- Wenn Sie den Bericht auf bestimmte Benutzeraktivitäten einschränken möchten, geben Sie den Benutzernamen in das Feld **Benutzername** ein.
- Wenn Sie den Bericht auf bestimmte IP-Adressen-Aktivitäten einschränken möchten, geben Sie die IP-Adresse des Benutzers in das Feld **Benutzer-IP-Adresse** ein.

4. Klicken Sie auf **OK**, um den Bericht auszuführen. Der Bericht wird erstellt, und es werden die Daten zu den Aktivitäten angezeigt, die während des angegebenen Zeitraums aufgetreten sind und allen angegebenen Parametern entsprechen.

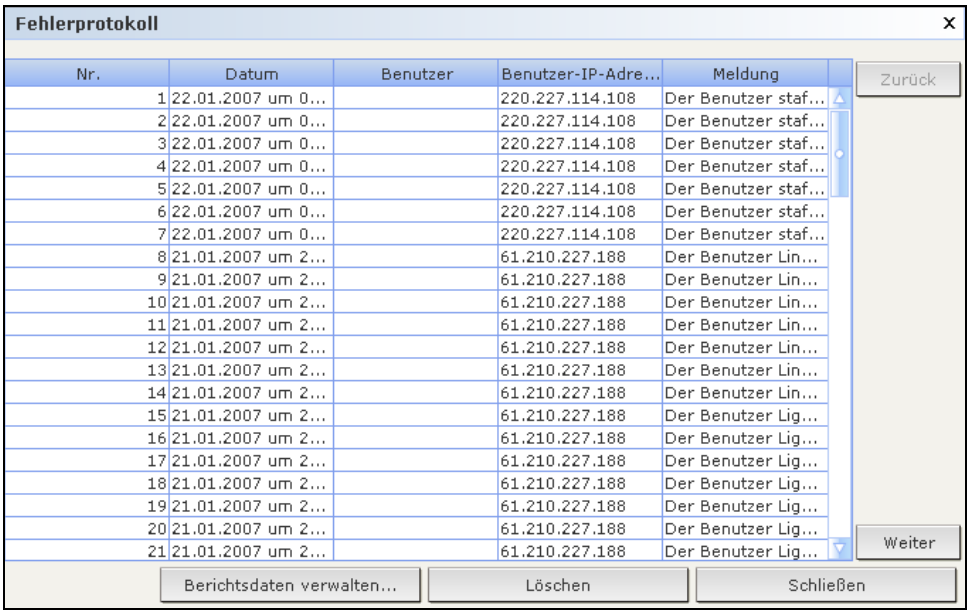


Abbildung 113 Bericht Fehlerprotokoll

- Klicken Sie auf **Weiter** oder **Zurück**, um im Bericht zu navigieren.
- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Löschen**, um die Protokolldateien zu löschen, die im Bericht verwendet wurden.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Zugriffsbericht

Führen Sie den Bericht **Zugriff** aus, um folgende Informationen anzuzeigen: alle Geräte und Ports, auf die zugegriffen wurde, den Zeitpunkt des Zugriffs und den Benutzer, der zugegriffen hat.

1. Klicken Sie im Menü **Berichte** auf **Zugriffsbericht.** Das Fenster **Zugriffsbericht** wird angezeigt.

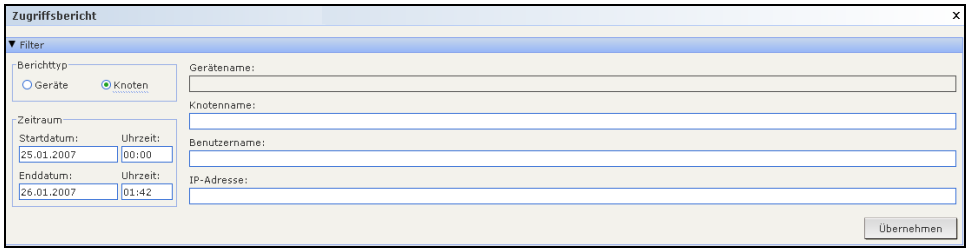
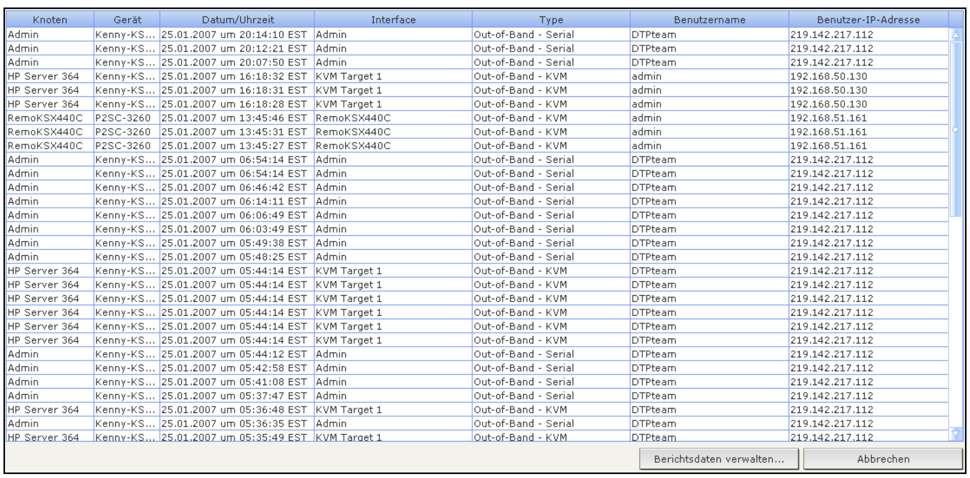


Abbildung 114 Fenster Zugriffsbericht

2. Legen Sie den Datumsbereich für den Bericht in den Feldern **Startdatum** und **Enddatum** fest. Klicken Sie auf jede Komponente des Standarddatums (Monat, Tag, Jahr, Stunde, Minute, Sekunde), um sie auszuwählen, und legen Sie den gewünschten Wert fest, indem Sie auf die Pfeile nach oben und nach unten klicken.
3. Sie können die Daten im Bericht einschränken, indem Sie weitere Parameter in die Felder **Meldung**, **Gerätename**, **Portname**, **Benutzername** und **Benutzer-IP-Adresse** eingeben.

- Wenn Sie den Bericht auf Meldungstexte einschränken möchten, die mit einer Aktivität verknüpft sind, geben Sie den Text in das Feld **Meldung** ein.
- Wenn Sie den Bericht auf ein bestimmtes Gerät beschränken möchten, geben Sie den Gerätenamen in das Feld **Gerätename** ein.
- Wenn Sie den Bericht auf einen bestimmten Port beschränken möchten, geben Sie den Portnamen in das Feld **Portname** ein.
- Wenn Sie den Bericht auf bestimmte Benutzeraktivitäten einschränken möchten, geben Sie den Benutzernamen in das Feld **Benutzername** ein.
- Wenn Sie den Bericht auf bestimmte IP-Adressen-Aktivitäten einschränken möchten, geben Sie die IP-Adresse des Benutzers in das Feld **Benutzer-IP-Adresse** ein.

4. Klicken Sie auf **OK**, um den Bericht auszuführen. Der Bericht wird erstellt und es werden die Daten zu den Zugriffen angezeigt, die während des angegebenen Zeitraums aufgetreten sind und allen angegebenen Parametern entsprechen.



Knoten	Gerät	Datum/Uhrzeit	Interface	Type	Benutzername	Benutzer-IP-Adresse
Admin	Kenny-KS...	25.01.2007 um 20:14:10 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 20:12:21 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 20:07:50 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
HP Server 364	Kenny-KS...	25.01.2007 um 16:18:32 EST	KVM Target 1	Out-of-Band - KVM	admin	192.168.50.130
HP Server 364	Kenny-KS...	25.01.2007 um 16:18:31 EST	KVM Target 1	Out-of-Band - KVM	admin	192.168.50.130
HP Server 364	Kenny-KS...	25.01.2007 um 16:18:28 EST	KVM Target 1	Out-of-Band - KVM	admin	192.168.50.130
RemoKSX440C	P2SC-3260	25.01.2007 um 13:45:46 EST	RemoKSX440C	Out-of-Band - KVM	admin	192.168.51.161
RemoKSX440C	P2SC-3260	25.01.2007 um 13:45:31 EST	RemoKSX440C	Out-of-Band - KVM	admin	192.168.51.161
RemoKSX440C	P2SC-3260	25.01.2007 um 13:45:27 EST	RemoKSX440C	Out-of-Band - KVM	admin	192.168.51.161
Admin	Kenny-KS...	25.01.2007 um 06:54:14 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 06:54:14 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 06:46:42 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 06:14:11 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 06:06:49 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 06:03:49 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 05:49:38 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 05:48:25 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
HP Server 364	Kenny-KS...	25.01.2007 um 05:44:14 EST	KVM Target 1	Out-of-Band - KVM	DTPteam	219.142.217.112
HP Server 364	Kenny-KS...	25.01.2007 um 05:44:14 EST	KVM Target 1	Out-of-Band - KVM	DTPteam	219.142.217.112
HP Server 364	Kenny-KS...	25.01.2007 um 05:44:14 EST	KVM Target 1	Out-of-Band - KVM	DTPteam	219.142.217.112
HP Server 364	Kenny-KS...	25.01.2007 um 05:44:14 EST	KVM Target 1	Out-of-Band - KVM	DTPteam	219.142.217.112
HP Server 364	Kenny-KS...	25.01.2007 um 05:44:14 EST	KVM Target 1	Out-of-Band - KVM	DTPteam	219.142.217.112
HP Server 364	Kenny-KS...	25.01.2007 um 05:44:14 EST	KVM Target 1	Out-of-Band - KVM	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 05:44:12 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 05:42:58 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 05:41:08 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 05:37:47 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
HP Server 364	Kenny-KS...	25.01.2007 um 05:36:48 EST	KVM Target 1	Out-of-Band - KVM	DTPteam	219.142.217.112
Admin	Kenny-KS...	25.01.2007 um 05:36:35 EST	Admin	Out-of-Band - Serial	DTPteam	219.142.217.112
HP Server 364	Kenny-KS...	25.01.2007 um 05:35:49 EST	KVM Target 1	Out-of-Band - KVM	DTPteam	219.142.217.112

Berichtsdaten verwalten... Abbrechen

Abbildung 115 Zugriffsbericht

- Klicken Sie auf **Weiter** oder **Zurück**, um im Bericht zu navigieren.
- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Löschen**, um die Protokolldateien zu löschen, die im Bericht verwendet wurden.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Verfügbarkeitsbericht

Der Verfügbarkeitsbericht enthält den Status aller Verbindungen und zeigt die Namen und IP-Adressen von Geräten an. Dieser Bericht vermittelt einen vollständigen Überblick über alle verfügbaren Geräte im System und enthält nützliche Informationen für die Problembehandlung.

1. Klicken Sie im Menü **Berichte** auf **Verfügbarkeitsbericht**. Der **Verfügbarkeitsbericht** wird erstellt.

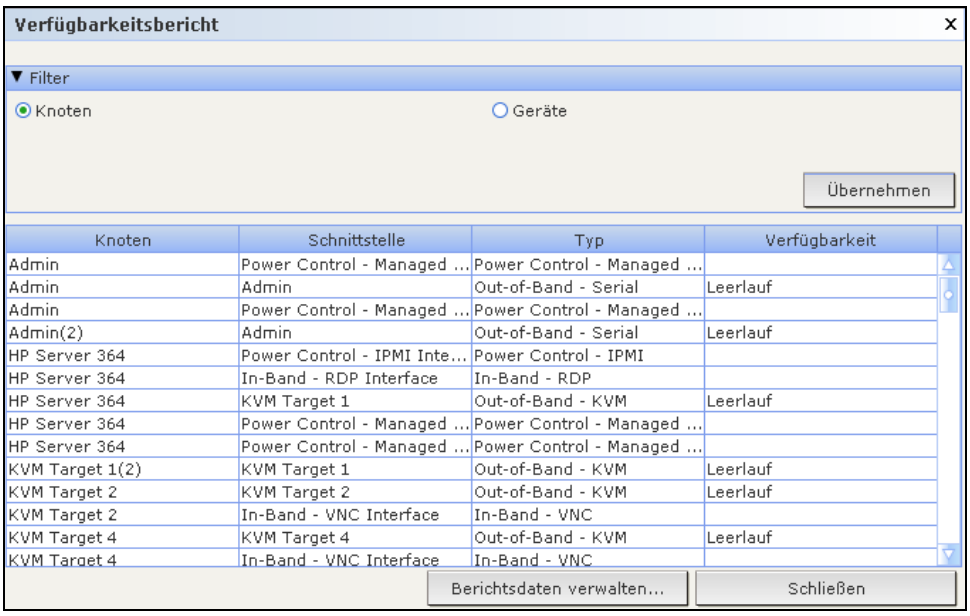


Abbildung 116 Verfügbarkeitsbericht

- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Bericht „Aktive Benutzer“

Der Bericht **Aktive Benutzer** enthält alle aktuellen Benutzer und Benutzersitzungen. Sie können aktive Benutzer im Bericht auswählen und bei CC-SG abmelden.

1. Klicken Sie im Menü **Berichte** auf **Benutzer** und dann auf **Aktive Benutzer**. Der Bericht **Aktive Benutzer** wird erstellt.

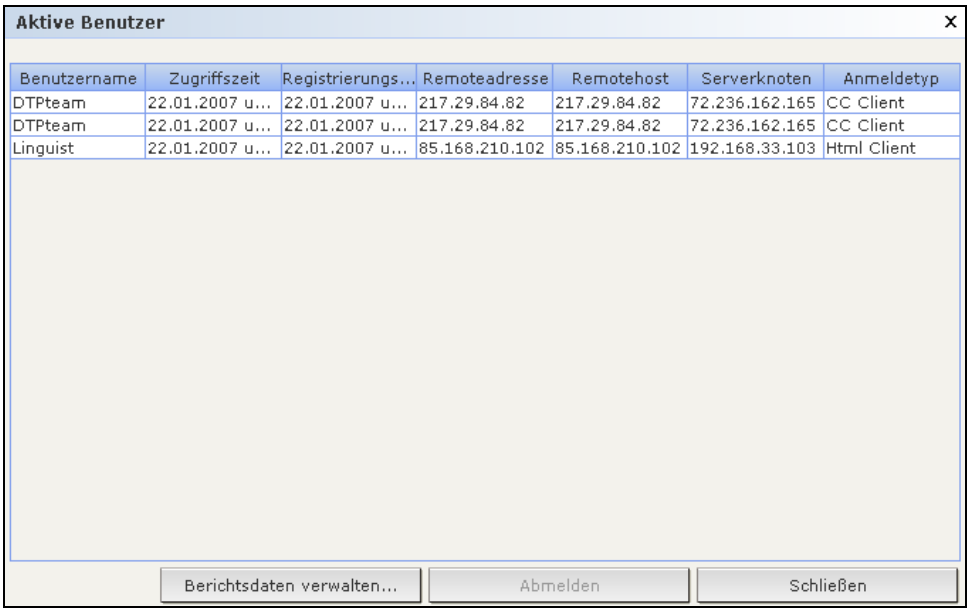


Abbildung 117 Bericht Aktive Benutzer

- Wählen Sie zum Abmelden eines Benutzers während einer aktiven Sitzung in CC-SG den Benutzernamen aus, und klicken Sie auf **Abmelden**.
- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Bericht „Gesperrte Benutzer“

Der Bericht **Gesperrte Benutzer** zeigt die Benutzer an, die zurzeit in CC-SG gesperrt sind, da zu viele fehlerhafte Anmeldeversuche aufgetreten sind. Sie können die Sperre für Benutzer in diesem Bericht aufheben. Weitere Informationen zu Sperreinstellungen finden Sie in **Kapitel 12: Erweiterte Administration, Sperreinstellungen**.

1. Klicken Sie im Menü **Berichte** auf **Benutzer** und dann auf **Gesperrte Benutzer**.

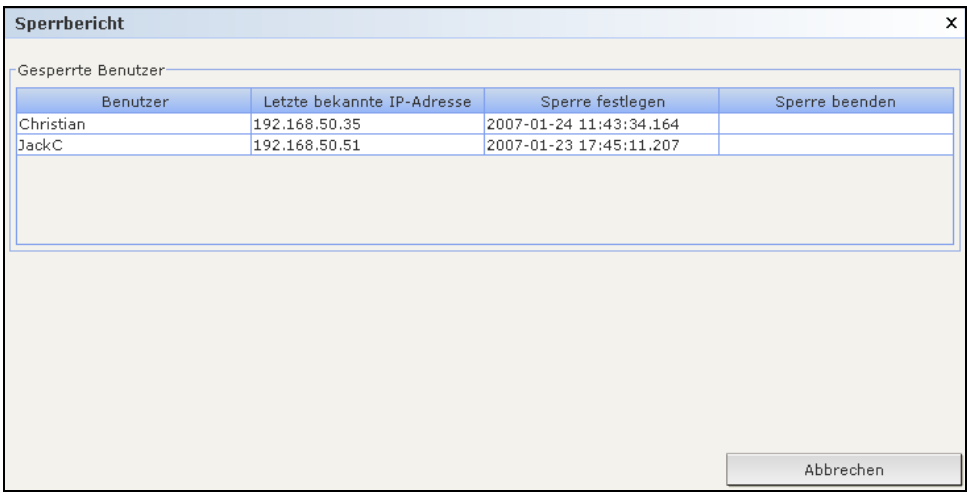


Abbildung 118 Bericht Gesperrte Benutzer

- Sie können die Sperre für Benutzer aufheben, die in CC-SG gesperrt sind, indem Sie den gewünschten Benutzernamen auswählen und auf **Benutzersperre aufheben** klicken.
- Klicken Sie auf **Abbrechen**, um den Bericht zu schließen.

Benutzerdatenbericht

Der Benutzerdatenbericht enthält bestimmte Daten über alle Benutzer in der CC-SG-Datenbank.

1. Klicken Sie im Menü **Berichte** auf **Benutzer** und dann auf **Benutzerdaten**. Der Bericht **Alle Benutzerdaten** wird erstellt.

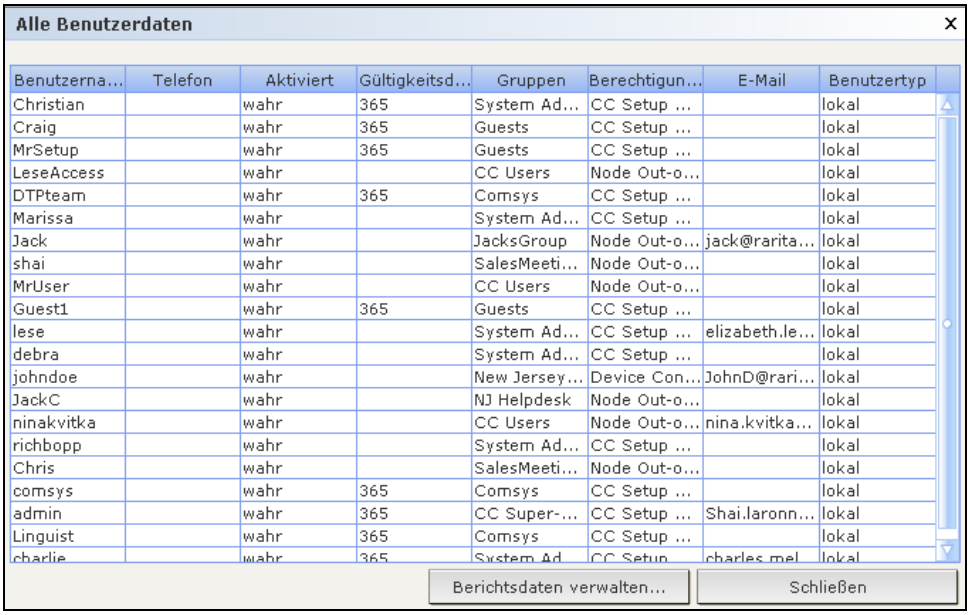


Abbildung 119 Bericht Alle Benutzerdaten

- Im Feld **Benutzername** werden die Benutzernamen aller CC-SG-Benutzer angezeigt.
- Im Feld **Telefon** werden die Rückrufnummer für Benutzer angezeigt, die nur bei Benutzern von CC-SG G1-Systemen verfügbar sind, die ein Modem umfassen.
- Das Feld **Aktiviert** enthält den Wert **wahr**, wenn der Benutzer sich bei CC-SG anmelden darf, bzw. **falsch**, wenn der Benutzer sich nicht bei CC-SG anmelden darf. Dies hängt davon ab, ob das Kontrollkästchen **Anmeldung aktiviert** im Benutzerprofil markiert ist. Weitere Informationen finden Sie in **Kapitel 7: Hinzufügen und Verwalten von Benutzern und Benutzergruppen, Benutzer hinzufügen**.
- Im Feld **Gültigkeitsdauer des Kennworts** wird die Anzahl von Tagen angezeigt, die der Benutzer dasselbe Kennwort verwenden kann, bevor es geändert werden muss. Weitere Informationen finden Sie in **Kapitel 7: Hinzufügen und Verwalten von Benutzern und Benutzergruppen, Benutzer hinzufügen**.
- Im Feld **Gruppen** werden die Benutzergruppen angezeigt, denen der Benutzer angehört.
- Im Feld **Berechtigungen** werden die CC-SG-Berechtigungen angezeigt, die dem Benutzer zugewiesen wurden. Weitere Informationen finden Sie in **Anhang C: Benutzergruppenberechtigungen**.
- Im Feld **E-Mail** wird die E-Mail-Adresse des Benutzers angezeigt, die im Benutzerprofil angegeben wurde.
- Im Feld **Benutzertyp** wird abhängig von der Zugriffsmethode des Benutzers **Lokal** oder **Remote** angezeigt.
- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Bericht „Benutzer in Gruppen“

Der Bericht **Benutzer in Gruppen** enthält Informationen über die Benutzer und Gruppen, denen sie zugeordnet sind.

1. Klicken Sie im Menü **Berichte** auf **Benutzer** und dann auf **Benutzer in Gruppen**. Der Bericht **Benutzer in Gruppen** wird erstellt.

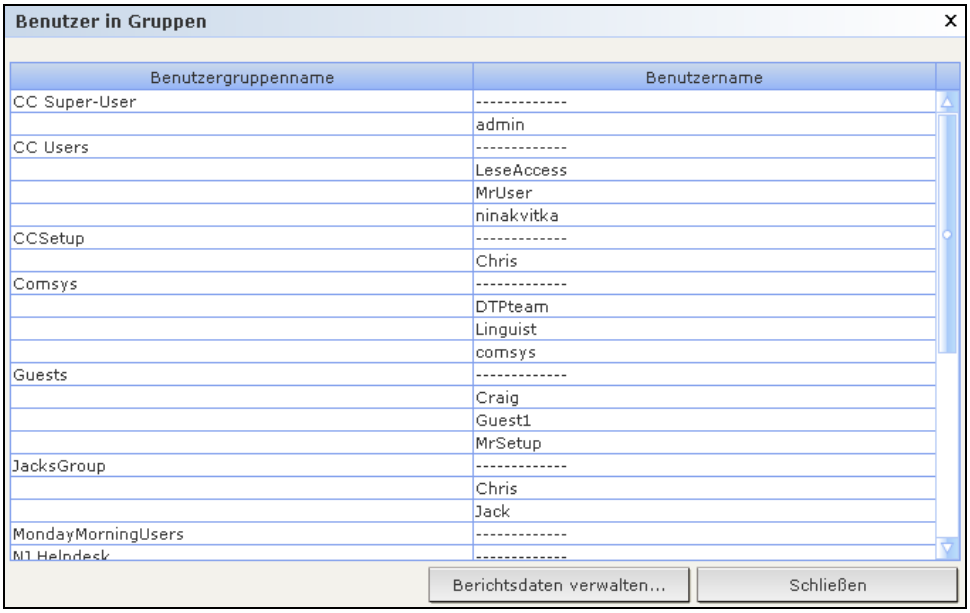


Abbildung 120 Bericht Benutzer in Gruppen

- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Gruppendatenbericht

Der Bericht **Gruppendaten** enthält Benutzer-, Knoten- und Gerätegruppeninformationen. Sie können in nur einem Fenster die Namen und Beschreibungen von Benutzergruppen, die Namen von Knotengruppen und die Namen von Gerätegruppen anzeigen.

1. Klicken Sie im Menü **Berichte** auf **Benutzer** und dann auf **Gruppendaten**. Der Bericht **Gruppen** wird erstellt.

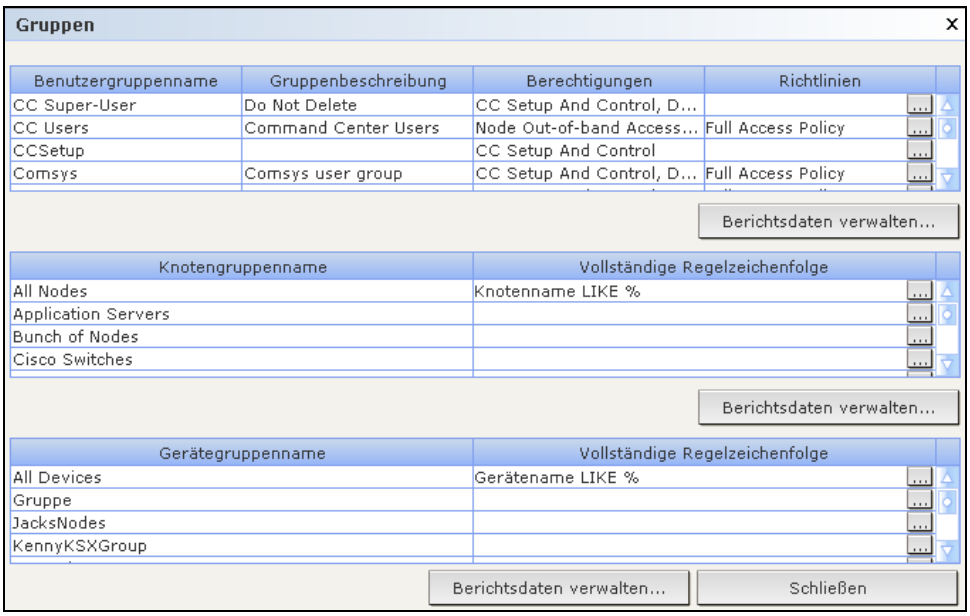


Abbildung 121 Bericht Gruppen

- Klicken Sie auf **Berichtdaten verwalten...**, um den Berichtsabschnitt zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.
- Klicken Sie auf die Schaltfläche **…** neben einer Zeile, um entweder die mit der Benutzergruppe verknüpften Richtlinien, die Knotenliste, die der Knotengruppenregel entspricht, oder die Geräteliste anzuzeigen, die der Gerätegruppenregel entspricht.

AD-Benutzergruppenbericht

Im AD-Benutzergruppenbericht werden alle Benutzer in Gruppen angezeigt, die von Active Directory-Servern, die zur Authentifizierung und Autorisierung konfiguriert wurden, in CC-SG importiert wurden. Der Bericht enthält keine Benutzer, die lokal (über CC-SG) zu den AD-Benutzergruppen hinzugefügt wurden.

1. Klicken Sie im Menü **Berichte** auf **Benutzer** und dann auf **AD-Benutzergruppenbericht**. Das Fenster **AD-Benutzergruppenbericht** wird angezeigt.
2. In der Liste **AD-Server** werden alle AD-Server aufgeführt, die in CC-SG zur Authentifizierung und Autorisierung konfiguriert wurden. Markieren Sie die Kontrollkästchen jedes AD-Servers, den CC-SG im Bericht berücksichtigen soll.
3. Im Bereich **AD-Benutzergruppen** enthält die Liste **Verfügbar** alle Benutzergruppen, die über AD-Server, die in der Liste **AD-Server** markiert wurden, in CC-SG importiert wurden. Wählen Sie die Benutzergruppen aus, die im Bericht enthalten sein sollen, und klicken Sie auf **Hinzufügen**, um die Benutzergruppen in die Liste **Ausgewählt** zu verschieben.

4. Klicken Sie auf **Übernehmen**. Der Bericht **AD-Benutzergruppe** wird erstellt.

- Klicken Sie auf **Berichtdaten verwalten...**, um den Berichtsabschnitt zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Anlagenverwaltungsbericht

Der Anlagenverwaltungsbericht enthält Daten zu Geräten, die zurzeit von CC-SG verwaltet werden.

1. Klicken Sie im Menü **Berichte** auf **Geräte** und dann auf **Anlagenverwaltungsbericht.** Der **Anlagenverwaltungsbericht** wird für alle Geräte erzeugt.
2. Wenn Sie die Berichtsdaten nach Gerätetyp filtern möchten, klicken Sie den Pfeil der Dropdown-Liste **Gerätetyp**, wählen Sie in der Liste einen Gerätetyp aus, und klicken Sie auf **Übernehmen**. Der Bericht wird erneut mit dem ausgewählten Filter generiert.

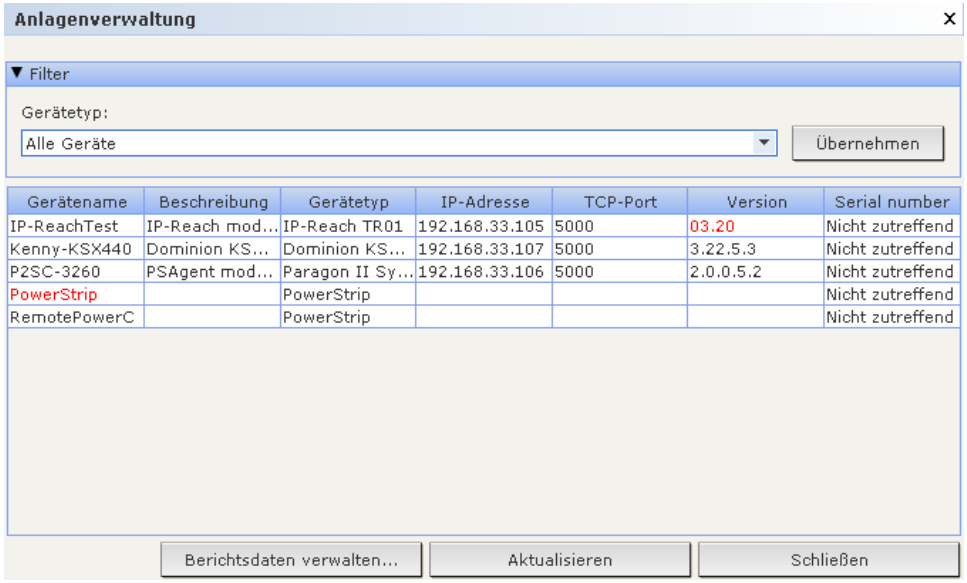


Abbildung 122 Anlagenverwaltungsbericht

- Bei Geräten, deren Version nicht der Kompatibilitätsmatrix entsprechen, wird der Text im Feld **Gerätename** rot angezeigt.
- Klicken Sie auf **Berichtdaten verwalten...**, um den Berichtsabschnitt zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Aktualisieren**, um einen neuen Bericht zu generieren. Dies kann abhängig von der Systemkonfiguration einige Minuten dauern.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Knotenanlagebericht

Der Knotenanlagebericht zeigt den Knotennamen, Schnittstellennamen und -typ, Gerätenamen und -typ und die Knotengruppe für alle Knoten an, die in CC-SG verwaltet werden. Sie können auch Filter für den Bericht verwenden, damit nur Daten für Knoten angezeigt werden, die bestimmten Werten für Knotengruppe, Schnittstellentyp, Gerätetyp oder Gerät entsprechen.

1. Klicken Sie im Menü **Berichte** auf **Knoten** und dann auf **Knotenanlagebericht**. Der Bildschirm **Knotenanlagebericht** wird angezeigt.

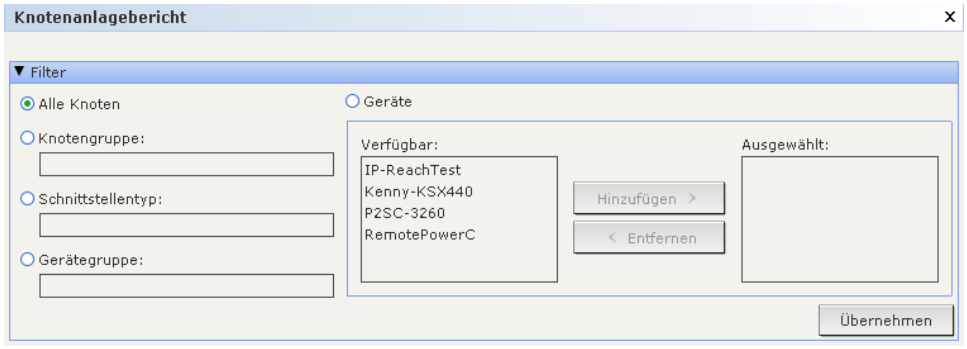


Abbildung 123 Bildschirm Knotenanlagebericht

2. Klicken Sie auf das Optionsfeld, das den Filterkriterien entspricht, die Sie für den Bericht verwenden möchten: **Alle Knoten**, **Knotengruppe**, **Gerätegruppe** oder **Geräte**.
   - Wenn Sie **Knotengruppe**, **Schnittstellentyp** oder **Gerätegruppe** ausgewählt haben, klicken Sie auf den entsprechenden Pfeil der Dropdown-Liste, und wählen Sie in der Liste einen Parameter aus.
   - Wenn Sie **Geräte** ausgewählt haben, wählen Sie in der Liste **Verfügbar** die Geräte aus, deren Knotenanlagen im Bericht enthalten sein sollen. Klicken Sie dann auf **Hinzufügen**, um Sie in die Liste **Ausgewählt** zu verschieben.
3. Klicken Sie zum Erstellen des Berichts auf **Übernehmen**. Der **Knotenanlagebericht** wird erstellt.

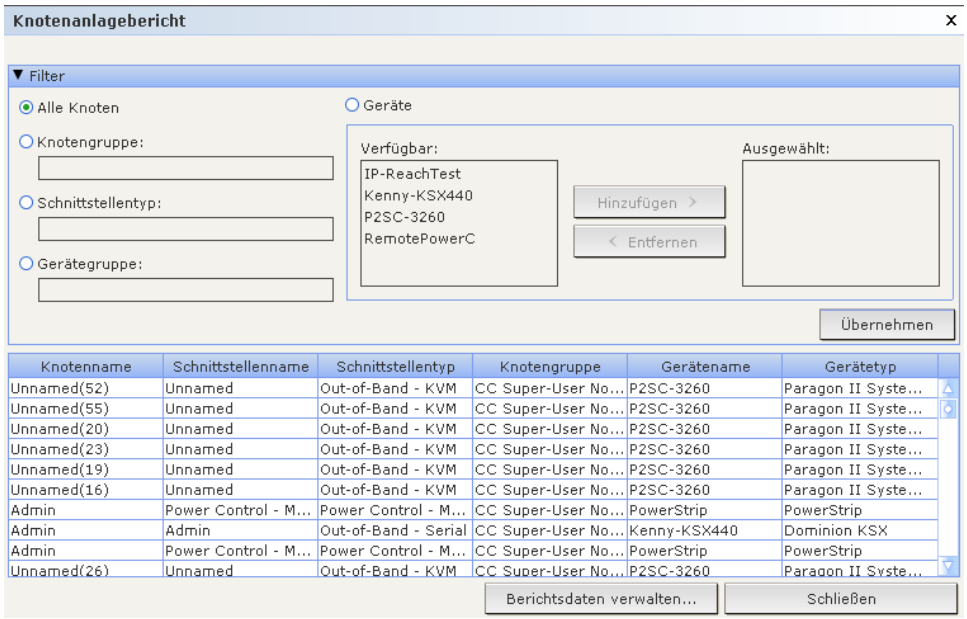


Abbildung 124 Knotenanlagebericht

- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Bericht „Aktive Knoten“

Der Bericht **Aktive Knoten** enthält den Namen und Typ jeder aktiven Schnittstelle, den aktuellen Benutzer, einen Zeitstempel und die Benutzer-IP-Adresse für jeden Knoten mit einer aktiven Verbindung. Sie können die Liste der aktiven Knoten und getrennten Knoten in diesem Bericht anzeigen.

1. Klicken Sie im Menü **Berichte** auf **Knoten** und dann auf **Aktive Knoten**. Der Bericht **Aktive Knoten** wird erstellt, falls aktive Knoten vorhanden sind.

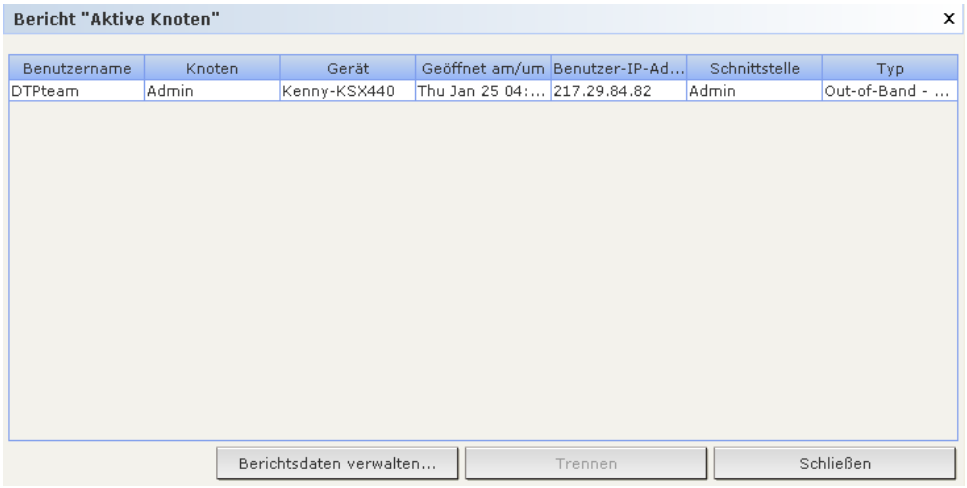


Abbildung 125 Bericht Aktive Knoten

- Sie können einen Knoten von einer aktuellen Sitzung trennen. Wählen Sie dazu den entsprechenden Knoten aus, und klicken Sie auf **Trennen**.
- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Knotenerstellungsbericht

Der Knotenerstellungsbericht führt alle Knotenerstellungs-Versuche auf, die in einem bestimmten Zeitfenster erfolgreich durchgeführt oder fehlgeschlagen sind. Sie können festlegen, ob Sie alle derartigen Versuche oder nur solche Versuche anzeigen möchten, bei denen potenziell doppelte Knoten erstellt wurden.

1. Klicken Sie im Menü **Berichte** auf **Knoten** und dann auf **Knotenerstellung**. Der Bildschirm **Knotenerstellung** wird angezeigt.

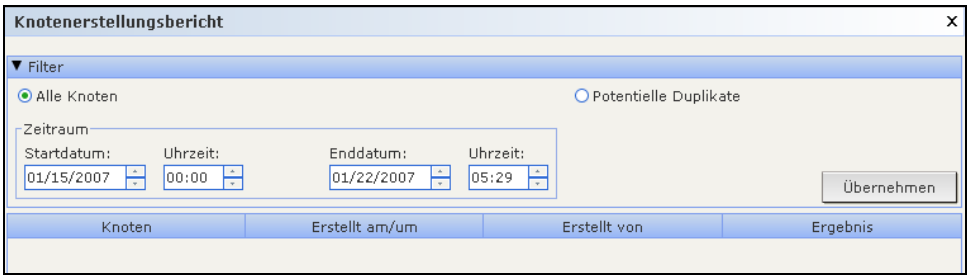


Abbildung 126 Bildschirm Knotenerstellungsbericht

2. Legen Sie den Datumsbereich für den Bericht in den Feldern **Startdatum** und **Enddatum** fest. Klicken Sie auf jede Komponente des Standarddatums (Monat, Tag, Jahr, Stunde, Minute, Sekunde), um sie auszuwählen, und legen Sie den gewünschten Wert fest, indem Sie auf die Pfeile nach oben und nach unten klicken.
3. Markieren Sie das Kontrollkästchen **Potentielle Duplikate**, damit nur Knoten im Bericht angezeigt werden, die als potenzielle Duplikate gekennzeichnet wurden.
4. Klicken Sie auf **Übernehmen**. Der Knotenerstellungsbericht wird erstellt.

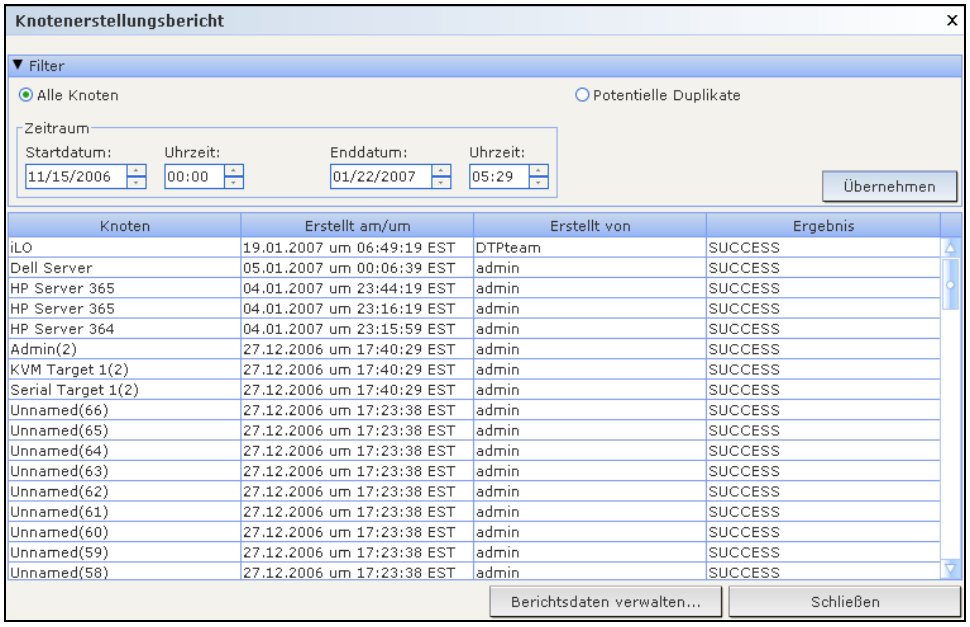


Abbildung 127 Knotenerstellungsbericht

- Im Ergebnisfeld wird **Erfolg**, **Fehlgeschlagen** oder **Potenzielle Duplikate** angezeigt, um den Status nach dem Knotenerstellungs-Versuch zu beschreiben.
- Klicken Sie auf **Berichtdaten verwalten...**, um den Berichtsabschnitt zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Portabfragebericht

Im Bericht **Port abfragen** werden alle Ports nach Portstatus aufgelistet.

1. Klicken Sie im Menü **Berichte** auf **Ports** und dann auf **Port abfragen**. Das Fenster **Port abfragen** wird angezeigt.

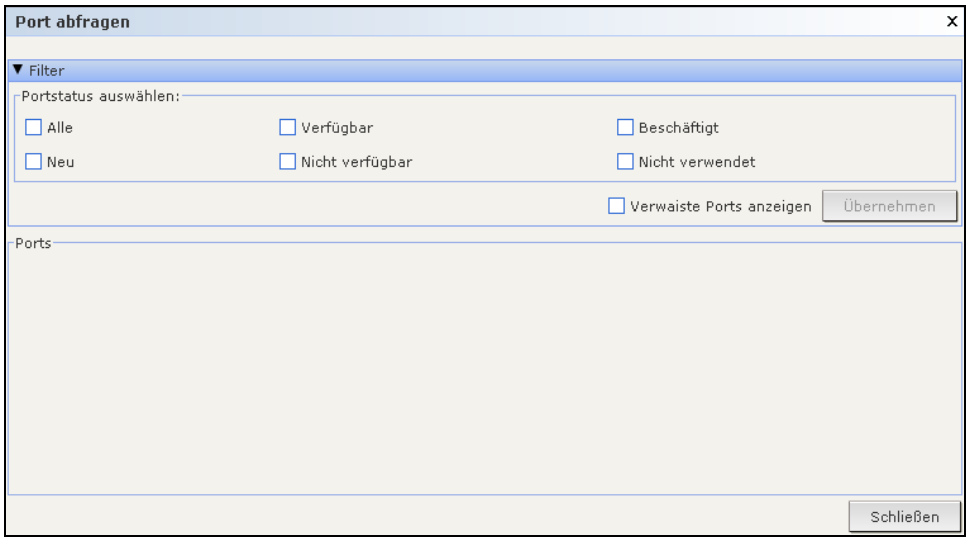


Abbildung 128 Fenster Port abfragen

2. Markieren Sie im Bereich **Portstatus auswählen** die Kontrollkästchen, die dem Portstatus entsprechen, der im Bericht enthalten sein soll. Markieren Sie mehrere Kontrollkästchen und klicken anschließend auf **Übernehmen**, werden alle Ports mit allen ausgewählten Statuszuständen angezeigt.

PORTSTATUS	DEFINITION
Alle	Alle Portstatuszustände.
Neu	Der Port ist verfügbar (die physische Verbindung zum Zielserver ist hergestellt), er ist jedoch nicht konfiguriert.
Nicht verwendet	Der Port ist nicht verfügbar (die physische Verbindung zum Zielserver ist nicht hergestellt), und er ist nicht konfiguriert.
Verfügbar	Der Port ist konfiguriert, und eine Verbindung zum Port ist möglich.
Nicht verfügbar	Die Verbindung zum Port ist nicht möglich, da das Gerät ausgeschaltet und nicht verfügbar ist.
Beschäftigt	Ein Benutzer ist mit diesem Port verbunden.

3. Markieren Sie das Kontrollkästchen **Verwaiste Ports anzeigen** in Verbindung mit einem oder mehreren Portstatuszuständen, um Ports anzuzeigen, die den ausgewählten Portstatus aufweisen und verwaist sind. Ein verwaister Port kann entstehen, wenn ein CIM- oder Zielserver im Paragon-System entfernt oder (manuell oder unbeabsichtigt) abgeschaltet wird. Weitere Informationen hierzu finden Sie im **Benutzerhandbuch für Paragon II-Geräte** von Raritan.

4. Klicken Sie zum Erstellen des Berichts auf **Übernehmen**.

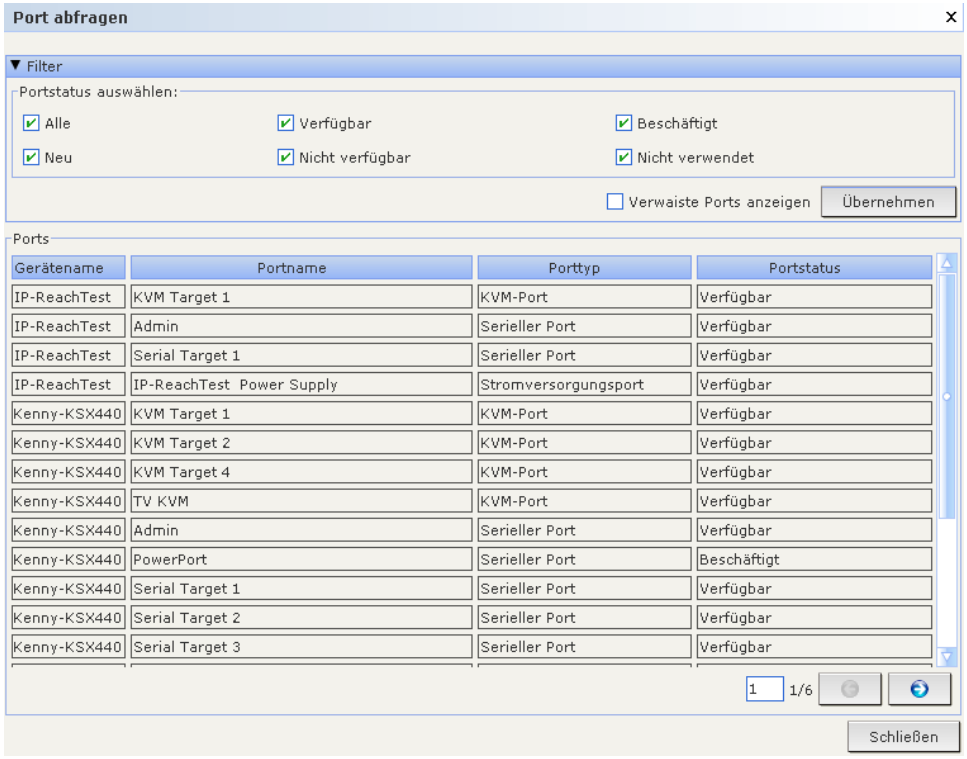


Abbildung 129 Bericht Port abfragen

- Klicken Sie auf die Pfeile unten rechts im Bericht, um in Berichten mit mehreren Seiten zu navigieren.
- Klicken Sie neben einem neuen oder nicht verwendeten Port im Bericht auf **Konfigurieren**, um ihn zu konfigurieren.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Bericht „Aktive-Ports“

Der Bericht **Aktive Ports** enthält alle derzeit verwendeten Out-of-Band-Ports. Sie können die Liste der aktiven und getrennten Ports in diesem Bericht anzeigen.

1. Klicken Sie im Menü **Berichte** auf **Ports** und dann auf **Aktive Ports**. Der Bericht **Aktive Ports** wird erstellt.

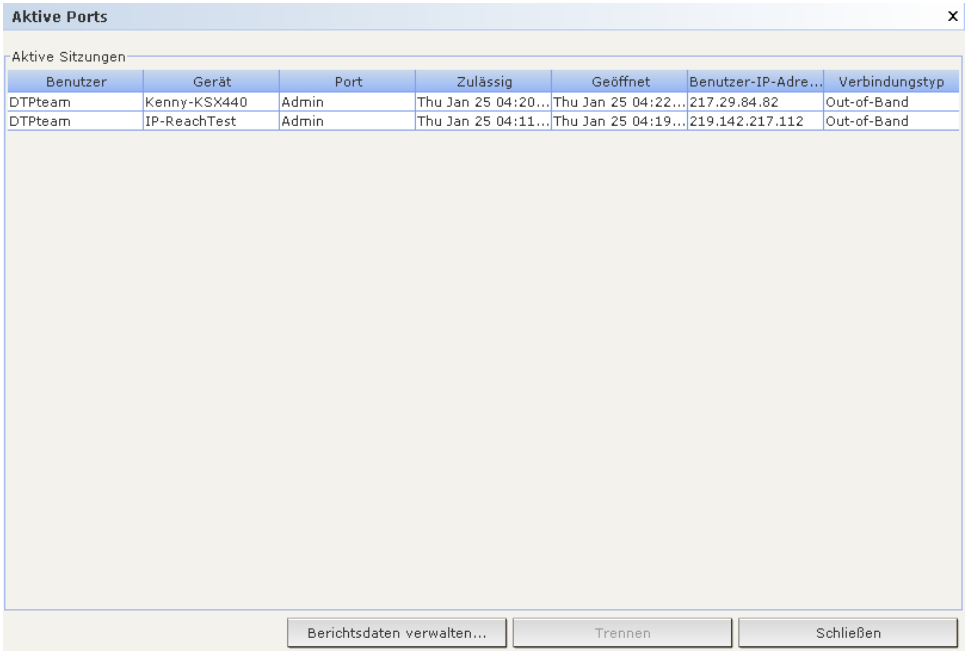


Abbildung 130 Bericht Aktive Ports

- Sie können einen Port von einer aktuellen Sitzung trennen. Wählen Sie dazu den entsprechenden Port aus, und klicken Sie auf **Trennen**.
- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.
- Klicken Sie auf **Schließen**, um den Bericht zu schließen.

Geplante Berichte

Geplante Berichte sind Berichte, die im Aufgabenmanager geplant wurden. Geplante Berichte können im HTML-Format angezeigt werden. Weitere Informationen finden Sie in **Kapitel 12: Erweiterte Administration**.

1. Klicken Sie im Menü **Berichte** auf **Geplante Berichte**.
2. Klicken Sie auf **Berichte abrufen**, um die vollständige Liste aller geplanten Berichte anzuzeigen, die von allen Besitzern erstellt wurden. Standardmäßig werden alle Berichte angezeigt, die eine Stunde vor der aktuellen Uhrzeit geplant wurden.
3. Sie können angezeigte Berichte filtern, indem Sie einen bestimmten **Berichttyp** wie **Aktive Ports** oder **Berichtseigentümer** auswählen. Sie können auch die Start- und Enddaten in den Feldern **Berichte erstellt zwischen** ändern, indem Sie jede Komponente des Standarddatums (Monat, Tag, Jahr, Stunde, Minute, Sekunde) zur Auswahl anklicken und über die Pfeiltasten den gewünschten Wert einstellen. Sie können einen **Berichtnamen** eingeben, um nach dem Namen zu filtern. Geben Sie eine Phrase oder Teilphrase des Namens ein. Bei der Übereinstimmung wird die Groß- und Kleinschreibung nicht berücksichtigt, und Platzhalter sind nicht erlaubt.
4. Klicken Sie auf **Berichte abrufen**, um die gefilterte Liste anzuzeigen.
5. Zum Anzeigen eines Berichts markieren Sie diesen in der Liste, und klicken Sie auf **Bericht anzeigen**.
6. Klicken Sie auf **Schließen**, um den Bericht zu schließen.

CC-NOC-Synchronisation-Bericht

Im CC-NOC-Synchronisation-Bericht werden alle Ziele sowie die IP-Adressen aufgeführt, die CC-SG abonniert und die von CC-NOC nach einem bestimmten Erkennungsdatum überwacht werden. Außerdem werden hier alle neuen Ziele angezeigt, die im konfigurierten Bereich erkannt werden. Weitere Informationen finden Sie unter **Ein CC-NOC hinzufügen** in **Kapitel 12: Erweiterte Administration**. Sie können in diesem Bericht auch Ziele aus der CC-SG-Datenbank löschen.

1. Klicken Sie im Menü **Berichte** auf **CC-NOC-Synchronisation**.
2. Wählen Sie einen Wert für **Datum zuletzt erkannt** aus, und klicken Sie auf **Ziele abrufen**. Die Ziele, die an dem oder vor dem **Datum zuletzt erkannt** ermittelt wurden, werden unter **Erkannte Ziele** angezeigt.

- Wenn Sie ein Ziel aus der CC-SG-Datenbank löschen möchten, wählen Sie das entsprechende Ziel aus, und klicken Sie auf **Leeren**.
- Wenn Sie eine Liste mit Zielen aus der CC-SG-Datenbank löschen möchten, klicken Sie auf **Alle leeren**.
- Klicken Sie auf **Berichtsdaten verwalten...**, um den Bericht zu speichern oder zu drucken. Klicken Sie auf **Speichern**, um die auf der aktuellen Berichtsseite angezeigten Datensätze in einer CSV-Datei zu speichern, oder auf **Alle speichern**, um alle Datensätze zu speichern. Klicken Sie auf **Drucken**, um die auf der aktuellen Berichtsseite angezeigten Datensätze zu drucken, oder auf **Alle drucken**, um alle Datensätze zu drucken. Klicken Sie zum Schließen des Fensters auf **Schließen**.

Kapitel 11: Systemwartung

Wartungsmodus

Dieser Modus schränkt den Zugriff auf CC-SG ein, damit Administratoren bestimmte Aufgaben ohne Unterbrechung durchführen können. Aufgaben können über die Benutzeroberfläche oder über eine SSH-Befehlszeilenschnittstelle über Clients wie Putty, OpenSSH Client usw. durchgeführt werden. Weitere Informationen finden Sie in **Kapitel 12: Erweiterte Administration, SSH-Zugriff**.

Aktuelle Benutzer mit Ausnahme des Administrators, der den Wartungsmodus startet, werden benachrichtigt und nach Ablauf der konfigurierbaren Zeitspanne abgemeldet. Im Wartungsmodus können sich andere Administratoren bei CC-SG anmelden, andere Benutzer können sich jedoch nicht anmelden. Wenn der Wartungsmodus für CC-SG gestartet oder beendet wird, werden SNMP-Traps erzeugt.

***Hinweis**: Der Wartungsmodus steht nur in Standalone-CC-SG-Einheiten und nicht in einer Clusterkonfiguration zur Verfügung. CC-SG kann nur im Wartungsmodus aktualisiert werden.*

Geplante Aufgaben und der Wartungsmodus

Geplante Aufgaben können nicht durchgeführt werden, wenn sich CC-SG im Wartungsmodus befindet. Weitere Informationen zu geplanten Aufgaben finden Sie in **Kapitel 12: Erweiterte Administration, Aufgabenmanager**. Beendet CC-SG den Wartungsmodus, werden geplante Aufgaben so schnell wie möglich ausgeführt.

Wartungsmodus starten

So starten Sie den Wartungsmodus:

1. Klicken Sie im Menü **Systemwartung** auf **Wartungsmodus** und dann auf **Wartungsmodus starten**.

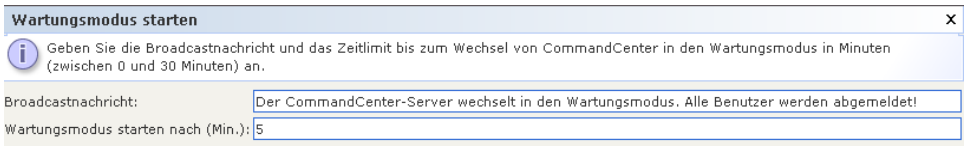


Abbildung 131 Wartungsmodus starten

2. Geben Sie eine **Broadcastnachricht** ein, oder übernehmen Sie die Standardnachricht. Diese Nachricht wird allen angemeldeten Benutzern angezeigt. Sie weist darauf hin, dass sie abgemeldet werden, sobald CC-SG in den Wartungsmodus wechselt.
3. Geben Sie einen Zeitrahmen (in Minuten) in das Feld **Wartungsmodus starten nach (Min)** ein. Dieser Zeitraum verstreicht, bevor CC-SG in den Wartungsmodus wechselt. Der Zeitrahmen kann zwischen **0** und **30** Minuten liegen, wobei **0** bedeutet, dass der Wartungsmodus sofort gestartet wird.
4. Klicken Sie auf **OK**.

Wartungsmodus beenden

So beenden Sie den Wartungsmodus:

1. Klicken Sie im Menü **Systemwartung** auf **Wartungsmodus**.
2. Klicken Sie auf **Wartungsmodus beenden**. Der Bildschirm **Wartungsmodus beenden** wird angezeigt.
3. Klicken Sie auf **OK**, um den Wartungsmodus zu beenden.

Eine Nachricht wird angezeigt, dass CC-SG den Wartungsmodus verlassen hat. Benutzer können jetzt wieder normal auf CC-SG zugreifen.

CC-SG sichern

Vor der Sicherung von CC-SG sollten Sie in den Wartungsmodus wechseln.

1. Klicken Sie im Menü **Systemwartung** auf **Sicherungsknoten**. Das Fenster **CommandCenter sichern** wird angezeigt.

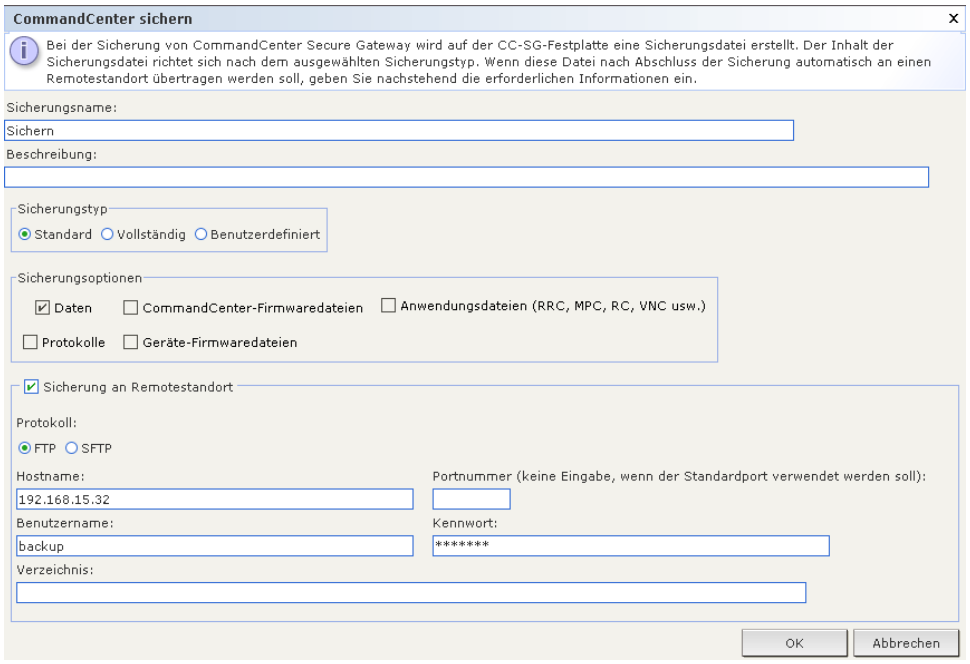


Abbildung 132 Bildschirm CommandCenter sichern

2. Geben Sie einen Namen für diese Sicherung im Feld **Sicherungsname** ein.
3. Sie können auch eine kurze Beschreibung für die Sicherung in das Feld **Beschreibung** eingeben.
4. Wählen Sie einen **Sicherungstyp** aus.
   - **Benutzerdefiniert**: Sie können angeben, welche Komponenten zur Sicherung hinzugefügt werden sollen, indem Sie sie im Bereich **Sicherungsoptionen** unten markieren. Markieren Sie jede der folgenden Optionen, um sie in der Sicherung einzuschließen.
     - **Daten**: CC-SG-Konfiguration, Geräte- und Knotenkonfiguration und Benutzerdaten. (Standard)
     - **Protokolle**: Fehlerprotokolle und Ereignisberichte, die unter CC-SG gespeichert sind.
     - **CC-SG-Firmwaredateien**: Gespeicherte Firmwaredateien, die zur Aktualisierung des CC-SG-Servers verwendet werden.
     - **Geräte-Firmwaredateien**: Gespeicherte Firmwaredateien, die zur Aktualisierung von CC-SG verwalteten Raritan-Geräten verwendet werden.
     - **Anwendungsdateien**: Gespeicherte Anwendungen, die von CC-SG verwendet werden, um Benutzer mit Knoten zu verbinden.
   - **Vollständig**: Erstellt eine Sicherung aller **Daten**, **Protokolle**, **Firmware-** und **Anwendungsdateien**, die in CC-SG gespeichert sind. Dieses Verfahren erzeugt die größte Sicherungsdatei.
   - **Standard**: Die Sicherung enthält nur wichtige **Daten** in CC-SG. Diese Sicherung umfasst CC-SG-Konfigurationsinformationen, Geräte- und Knotenkonfigurationen und Benutzerkonfigurationen. Dieses Verfahren erzeugt die kleinste Sicherungsdatei.
5. Wenn Sie eine Kopie dieser Sicherungsdatei auf einem externen Server speichern möchten, markieren Sie **Sicherung an Remotestandort**.

a. Wählen Sie ein **Protokoll**, das für die Verbindung zum Remoteserver verwendet wird (entweder **FTP** oder **SFTP**).
b. Geben Sie die IP-Adresse oder den Hostnamen des Servers im Feld **Hostname** ein.
c. Wenn Sie für das ausgewählte Protokoll nicht den Standardport (FTP: 21, SFTP: 22) verwenden, geben Sie den verwendeten Kommunikationsport in das Feld **Portnummer** ein.
d. Geben Sie einen Benutzernamen für den Remoteserver in das Feld **Benutzername** ein.
e. Geben Sie ein Kennwort für den Remoteserver in das Feld **Kennwort** ein.
f. Geben Sie im Feld **Verzeichnis** das Verzeichnis an, das zum Speichern der Sicherung auf dem Remoteserver verwendet werden soll.

6. Klicken Sie auf **OK**.

Eine Meldung zum Bestätigen der CC-SG-Sicherung wird angezeigt. Die Sicherungsdatei wird im CC-SG-Dateisystem gespeichert. Ist das Kontrollkästchen **Sicherung an Remotestandort** markiert, wird sie auch auf einem Remoteserver gespeichert. Diese Sicherung kann später wiederhergestellt werden.

Wiederherstellen von CC-SG

1. Klicken Sie im Menü **Systemwartung** auf **Wiederherstellen**. Der Bildschirm **CommandCenter wiederherstellen** wird mit einer Tabelle mit Sicherungssitzungen für CC-SG angezeigt. Die Tabelle enthält auch die Sicherungsart, das Sicherungsdatum, die Beschreibung, welche CC-SG-Version verwendet wurde, sowie die Größe der Sicherungsdatei.

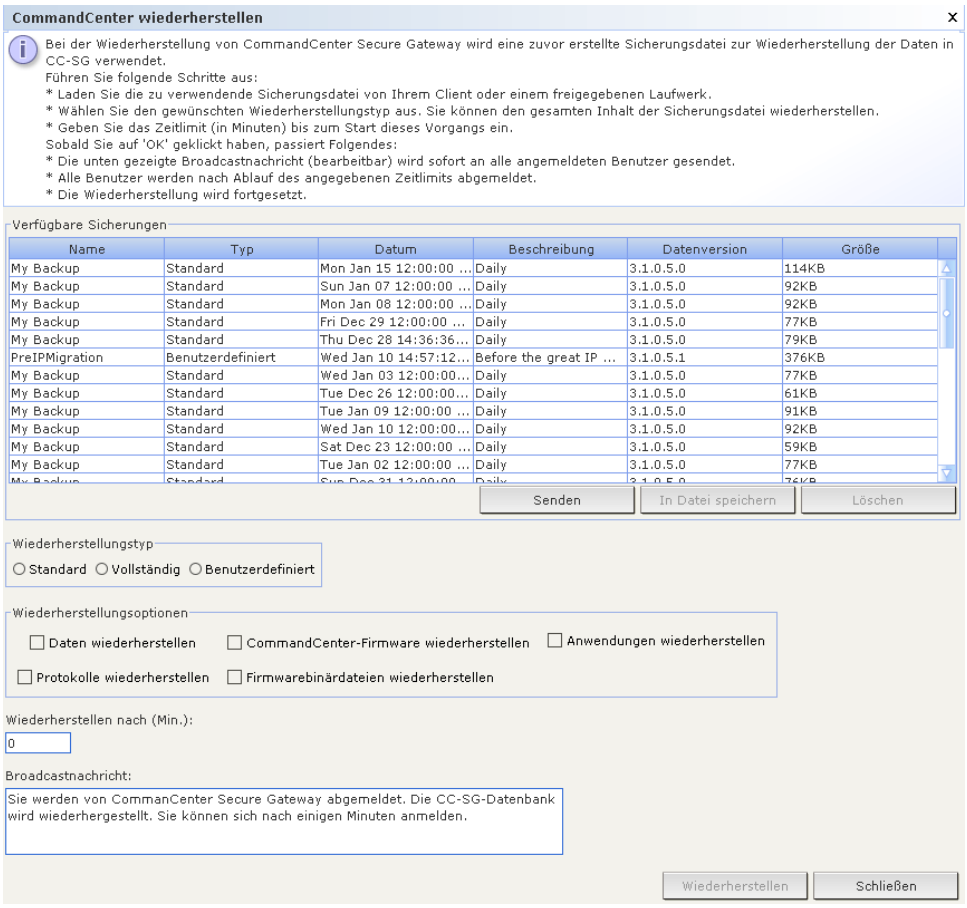


Abbildung 133 Bildschirm CommandCenter wiederherstellen

2. Wenn Sie eine Sicherung wiederherstellen möchten, die nicht auf dem CC-SG-System gespeichert wurde, müssen Sie diese zunächst zur Verfügung stellen. Klicken Sie auf **Upload**. Ein Dialogbildschirm wird angezeigt. Sie können die Datei überall im Netzwerk des Client abrufen.
   a. Suchen Sie nach der Sicherungsdatei, und wählen Sie sie im Dialogfenster aus.
   b. Klicken Sie auf **Öffnen**, um diese Datei an CC-SG zu senden.
   c. Nach Abschluss wird die Sicherungsdatei in der Tabelle **Verfügbare Sicherungen** angezeigt.
3. Wählen Sie die Sicherung, die Sie wiederherstellen möchten, in der Tabelle **Verfügbare Sicherungen** aus.
4. Wählen Sie ggf.die Art der Wiederherstellung für diese Sicherung aus:

- **Standard**: Nur wichtige **Daten** werden auf CC-SG wiederhergestellt. Diese Sicherung umfasst CC-SG-Konfigurationsinformationen, Geräte- und Knotenkonfigurationen und Benutzerkonfigurationen.
- **Vollständig**: Stellt alle **Daten**, **Protokolle**, **Firmware-** und **Anwendungsdatei** wieder her, die sich in der Sicherungsdatei befinden. Dies setzt voraus, dass für die Datei eine vollständige Sicherung durchgeführt wurde.
- **Benutzerdefiniert**: Sie können angeben, welche Komponenten der Sicherung auf CC-SG wiederhergestellt werden sollen, indem Sie sie im Bereich **Sicherungsoptionen** unten markieren. Markieren Sie jede der folgenden Optionen, um sie in der Wiederherstellung einzuschließen.
  a. **Daten**: CC-SG-Konfiguration, Geräte- und Knotenkonfiguration und Benutzerdaten.
  b. **Protokolle**: Fehlerprotokolle und Ereignisberichte, die unter CC-SG gespeichert sind.
  c. **CC-SG-Firmwaredateien**: Gespeicherte Firmwaredateien, die zur Aktualisierung des CC-SG-Servers verwendet werden.
  d. **Geräte-Firmwaredateien**: Gespeicherte Firmwaredateien, die zur Aktualisierung von CC-SG verwalteten Raritan-Geräten verwendet werden.
  e. **Anwendungsdateien**: Gespeicherte Anwendungen, die von CC-SG verwendet werden, um Benutzer mit Knoten zu verbinden.

5. Geben Sie in das Feld **Wiederherstellen nach (Min)** die Minuten von 0 bis 60 ein, die verstreichen sollen, bevor CC-SG die Wiederherstellung durchführt. Dadurch erhalten die Benutzer die Möglichkeit, ihre Arbeiten abzuschließen und sich abzumelden.
6. Geben Sie in das Feld **Broadcastnachricht** eine Nachricht ein, die andere CC-SG-Benutzer darüber informiert, dass eine Wiederherstellung durchgeführt wird.
7. Klicken Sie auf **Wiederherstellen**.

Wenn Sie auf **Wiederherstellen** klicken, wartet CC-SG den im Feld **Wiederherstellen nach (Min)** angegebenen Zeitraum, bevor die Konfiguration der ausgewählten Sicherung wiederhergestellt wird. Während der Wiederherstellung werden alle anderen Benutzer abgemeldet.

Sicherungsdateien speichern und löschen

Sie können Sicherungen, die auf dem CC-SG-System gespeichert sind, im Bildschirm **CommandCenter wiederherstellen** speichern und löschen. Durch das Speichern von Sicherungen können Sie eine Kopie der Sicherungsdatei auf einem anderen PC verwahren. Durch das Löschen von Sicherungen, die nicht mehr benötigt werden, können Sie Speicherplatz in CC-SG sparen.

So speichern Sie Sicherungen:

1. Wählen Sie in der Tabelle **Verfügbare Sicherungen** eine Sicherung aus, die Sie auf Ihrem PC speichern möchten.
2. Klicken Sie auf **In Datei speichern**. Ein Speicherdialog wird angezeigt.

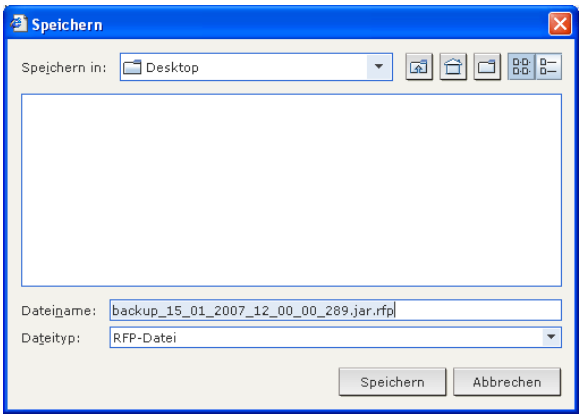


Abbildung 134 Sicherungsdateien speichern

3. Legen Sie zum Speichern Ihrer CC-SG-Sicherungsdatei einen Speicherort fest. Klicken Sie dann auf **Speichern**. Die Sicherungsdatei wird auf Ihren Client-PC kopiert.

So löschen Sie eine Sicherung:

1. Wählen Sie in der Tabelle **Verfügbare Sicherungen** die Sicherung zum Löschen aus.
2. Klicken Sie auf **Löschen**. Ein Bestätigungsfeld wird angezeigt.
3. Klicken Sie auf **OK**, um die Sicherung im CC-SG-System zu löschen, oder auf **Abbrechen**, um die Sicherung nicht zu löschen. Nach dem Löschvorgang wird die Sicherungsdatei aus CC-SG entfernt.

Hinweis: *Speichern und Wiederherstellen kann dazu verwendet werden, eine Sicherungsdatei von einer CC-SG-Einheit auf eine andere zu verschieben. Speichern und Löschen kann dazu verwendet werden, ein sicheres Archiv mit CC-SG-Sicherungen zu verwalten, ohne das vollständige Archiv auf dem System zu speichern.*

CC-SG zurücksetzen

Sie können den Befehl **CommandCenter zurücksetzen** verwenden, um die CC-SG-Datenbankdaten zu leeren. Die Systemkonfigurationsdaten wie die IP-Adresse von CC-SG werden dadurch nicht zurückgesetzt. Folgendes wird durchgeführt: CC-SG-Datenbank zurücksetzen, SNMP-Konfiguration zurücksetzen, auf Standardfirmware zurücksetzen, Standardfirmware in CC-SG-Datenbank laden und die Diagnosekonsole auf Standardwerte zurücksetzen.

1. Klicken Sie im Menü **Systemwartung** auf **Zurücksetzen**.

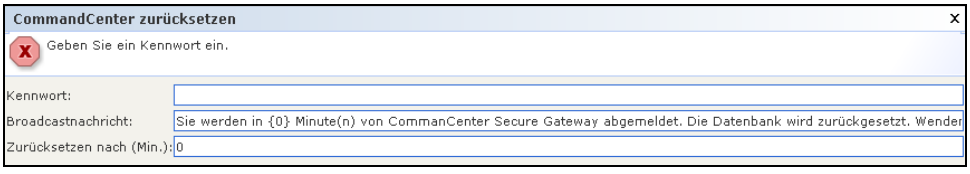


Abbildung 135 Fenster CommandCenter zurücksetzen

2. Geben Sie Ihr CC-SG-**Kennwort** ein.
3. Übernehmen Sie die aktuelle **Broadcastnachricht**, oder erstellen Sie eine eigene Nachricht.
4. Geben Sie in das Feld **Zurücksetzen nach (Min)** die Minuten von 0 bis 60 ein, die verstreichen sollen, bevor der Zurücksetzungsvorgang von CC-SG durchgeführt werden soll. Der Standardwert ist 0, d. h. die CC-SG-Einheit wird sofort zurückgesetzt.
5. Klicken Sie auf **OK**, um Ihre CC-SG-Einheit zurückzusetzen. Eine Meldung zum Bestätigen des Zurücksetzens wird angezeigt.

Wichtig: Durch den Befehl **Zurücksetzen** wird die CC-SG-Datenbank geleert. Alle Geräte, Knoten, Ports und Benutzer werden gelöscht. Bei der Authentifizierung wird wieder die lokale DB verwendet. Sie sollten eine Sicherheitskopie von CC-SG erstellen, bevor Sie **Zurücksetzen** verwenden.

CC-SG neu starten

Mit dem Befehl **Neu starten** wird die CC-SG-Software erneut gestartet. Durch den CC-SG-Neustart werden alle aktiven Benutzer bei CC-SG abgemeldet.

Hinweis: *Durch den Neustart wird CC-SG nicht aus- und eingeschaltet. Wenn Sie CC-SG neu hochfahren möchten, müssen Sie auf die Diagnostic Console zugreifen oder den Betriebsschalter am Gerät selbst verwenden.*

---

1. Klicken Sie im Menü **Systemwartung** auf **Neu starten**. Das Fenster **CommandCenter neu starten** wird angezeigt.

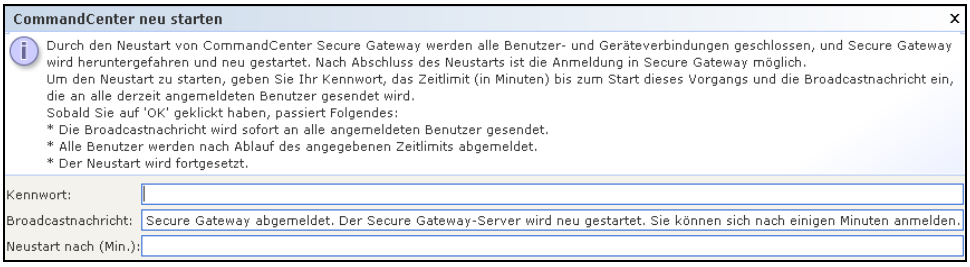


Abbildung 136 Fenster CommandCenter neu starten

2. Geben Sie Ihr Kennwort im Feld **Kennwort** ein.
3. Übernehmen Sie die Standardnachricht, oder geben Sie im Feld **Broadcastnachricht** für alle derzeit mit Sitzungen verbundenen Benutzer eine Warnmeldung ein. Teilen Sie beispielsweise mit, wie viel Zeit den Benutzern zum Abschließen ihrer Aufgaben bleibt, und weisen Sie sie darauf hin, wann CC-SG wieder einsatzbereit sein wird. Beim Neustarten von CC-SG werden alle Benutzerverbindungen getrennt.
4. Geben Sie in das Feld **Neustart nach (Min)** die Minuten von 0 bis 60 ein, die verstreichen sollen, bevor CC-SG einen Neustart durchführt.
5. Klicken Sie auf **OK**, um CC-SG neu zu starten. Klicken Sie auf **Abbrechen**, um das Fenster ohne Neustart zu schließen. Nach dem Neustarten von CC-SG wird Ihre Broadcastnachricht angezeigt.
6. Klicken Sie auf **OK**, um CC-SG neu zu starten. Nach dem Neustart ist CC-SG betriebsbereit.

CC-SG aktualisieren

Der Befehl **Aktualisieren** wird verwendet, um die Firmware von CC-SG auf eine neue Version zu aktualisieren. Bevor Sie CC-SG aktualisieren, sollten Sie die neuste Firmwaredatei auf Ihrem Client-PC speichern. Firmwaredaten finden Sie im Support-Bereich der Raritan-Website: **http://www.raritan.com/support/sup_upgrades.aspx**

Sie sollten vor der Aktualisierung eine Sicherung von CC-SG anlegen.

***Hinweis**: Wenn Sie mit einem CC-SG-Cluster arbeiten, müssen Sie zuerst das Cluster entfernen und jeden Knoten einzeln aktualisieren.*

1. Klicken Sie im Menü **Systemwartung** auf **Wartungsmodus**, und dann auf **Wartungsmodus starten**, um den Wartungsmodus für CC-SG zu starten. Sie können CC-SG nur auf diese Art und Weise aktualisieren. Weitere Informationen finden Sie in diesem Kapitel unter **Wartungsmodus**.
2. Wenn sich CC-SG im Wartungsmodus befindet, klicken Sie im Menü **Systemwartung** auf **Aktualisieren**. Das Fenster **CommandCenter aktualisieren** wird angezeigt.

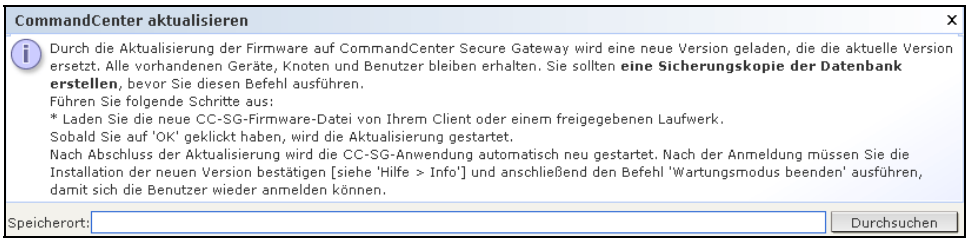


Abbildung 137 Fenster CommandCenter aktualisieren

3. Klicken Sie auf **Durchsuchen**, wechseln Sie zur CC-SG-Firmwaredatei, wählen Sie diese aus, und klicken Sie auf **Öffnen**.
4. Klicken Sie auf **OK**, um die Firmwaredatei an CC-SG zu senden.
5. Nachdem die Firmwaredatei an CC-SG gesendet wurde, erhalten Sie eine Nachricht. Dadurch wird angezeigt, dass CC-SG die Datei erhalten und den Aktualisierungsvorgang gestartet hat. Dazu werden alle Benutzer bei CC-SG abgemeldet. Klicken Sie auf **OK**, um CC-SG zu verlassen und den Neustart durchzuführen.
6. Sie müssen ca. 8 Minuten warten, während CC-SG neu startet. Schließen Sie Ihr Browserfenster, und löschen Sie den Browser-Cache.
7. Öffnen Sie nach 8 Minuten ein neues Browserfenster, und starten Sie CC-SG. Wählen Sie **Info zu Raritan Secure Gateway** im Menü **Hilfe** aus. Prüfen Sie im angezeigten Fenster die Versionsnummer, um sicherzustellen, dass die Aktualisierung erfolgreich war. Wurde die Version nicht aktualisiert, wiederholen Sie die Schritte oben. War die Aktualisierung erfolgreich, fahren Sie mit dem nächsten Schritt fort.
8. CC-SG befindet sich noch im **Wartungsmodus**, d. h. die meisten Benutzer können sich nicht anmelden. Verlassen Sie den Wartungsmodus, indem Sie im Menü **Systemwartung** auf **Wartungsmodus** und dann auf **Wartungsmodus beenden** klicken. Klicken Sie auf **OK**.

CC-SG herunterfahren

Zum Herunterfahren von CC-SG werden folgende Methoden empfohlen. Wenn Sie CC-SG herunterfahren, wird die CC-SG-Software heruntergefahren, die CC-SG-Einheit wird jedoch nicht ausgeschaltet.

1. Klicken Sie im Menü **Systemwartung** auf **CommandCenter herunterfahren**. Das Fenster **CommandCenter herunterfahren** wird angezeigt.

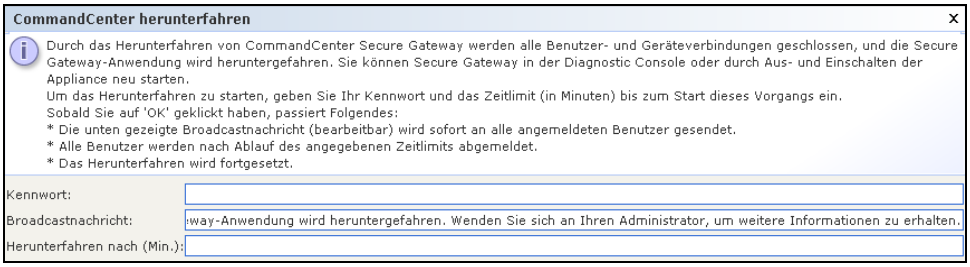


Abbildung 138 Fenster CommandCenter herunterfahren

2. Geben Sie Ihr Kennwort im Feld **Kennwort** ein.
3. Übernehmen Sie die Standardnachricht, oder geben Sie im Feld **Broadcastnachricht** für alle derzeit mit Sitzungen verbundenen Benutzer eine Meldung ein. Teilen Sie den Benutzern beispielsweise mit, wie viel Zeit ihnen zum Abschließen ihrer Aufgaben bleibt, und weisen Sie sie darauf hin, wann CC-SG wieder einsatzbereit sein wird. Beim Herunterfahren von CC-SG werden alle Benutzerverbindungen getrennt.
4. Geben Sie in das Feld **Herunterfahren nach (Min)** die Minuten von 0 bis 60 ein, die verstreichen sollen, bevor CC-SG heruntergefahren wird.
5. Klicken Sie auf **OK**, um CC-SG herunterzufahren, oder auf **Abbrechen**, um das Fenster ohne Herunterfahren von CC-SG zu schließen. Nach dem Herunterfahren wird das CC-SG-Anmeldefenster angezeigt.

Hinweis: *Nachdem CC-SG heruntergefahren wurde, sind alle Benutzer abgemeldet und wechseln zum Anmeldebildschirm. Benutzer können sich erst wieder Anmelden, wenn Sie CC-SG, wie im nächsten Abschnitt beschrieben, wieder neu gestartet haben.*

CC-SG nach dem Herunterfahren neu starten

Nach dem Herunterfahren von CC-SG gibt es zwei Möglichkeiten, die Einheit neu zu starten:

1. Über die Diagnostic Console: Weitere Informationen finden Sie unter **Diagnostic Console** in **Kapitel 12: Erweiterte Administration**.
2. Schalten Sie die CC-SG-Einheit aus und dann wieder ein.

CC-SG-Sitzung beenden

Abmelden

Wenn Sie CC-SG am Ende einer Sitzung beenden oder die Datenbank aktualisieren möchten (falls während Ihrer Anmeldung Änderungen vorgenommen wurden), melden Sie sich bei CC-SG ab, und melden Sie sich dann wieder an.

1. Klicken Sie im Menü **Secure Gateway** auf **Abmelden**. Das Fenster **Abmelden** wird angezeigt.
2. Klicken Sie auf **Ja**, um sich bei CC-SG abzumelden, oder auf **Nein**, um das Fenster zu schließen. Nach dem Abmelden wird das CC-SG-Anmeldefenster angezeigt.
3. Melden Sie sich erneut bei CC-SG an, oder klicken Sie auf **Beenden**, um CC-SG vollständig herunterzufahren.

CC-SG beenden

Sie können CC-SG jederzeit beenden.

1. Klicken Sie im Menü **Secure Gateway** auf **Beenden**. Das Fenster **Beenden** wird angezeigt.
2. Klicken Sie zum Beenden von CC-SG auf **Ja**, oder klicken Sie auf **Nein**, um das Fenster **Beenden** zu schließen und weiterzuarbeiten.

Kapitel 12: Erweiterte Administration

Setup-Assistent

Der **Setup-Assistent** hilft Administratoren bei einigen häufigen Aufgaben in CC-SG: Zuordnungen erstellen, Raritan-Geräte einrichten, Benutzergruppen und Benutzer erstellen. Weitere Informationen zum **Setup-Assistent** finden Sie in **Kapitel 3: Konfigurieren von CC-SG mit dem Setup-Assistenten**.

Tipp des Tages einrichten

Über den Tipp des Tages können Secure Gateway-Administratoren für alle Benutzer eine Nachricht anzeigen, sobald diese sich anmelden. Damit sie den Tipp des Tages konfigurieren können, müssen Administratoren über die Berechtigung **CC Setup and Control** verfügen.

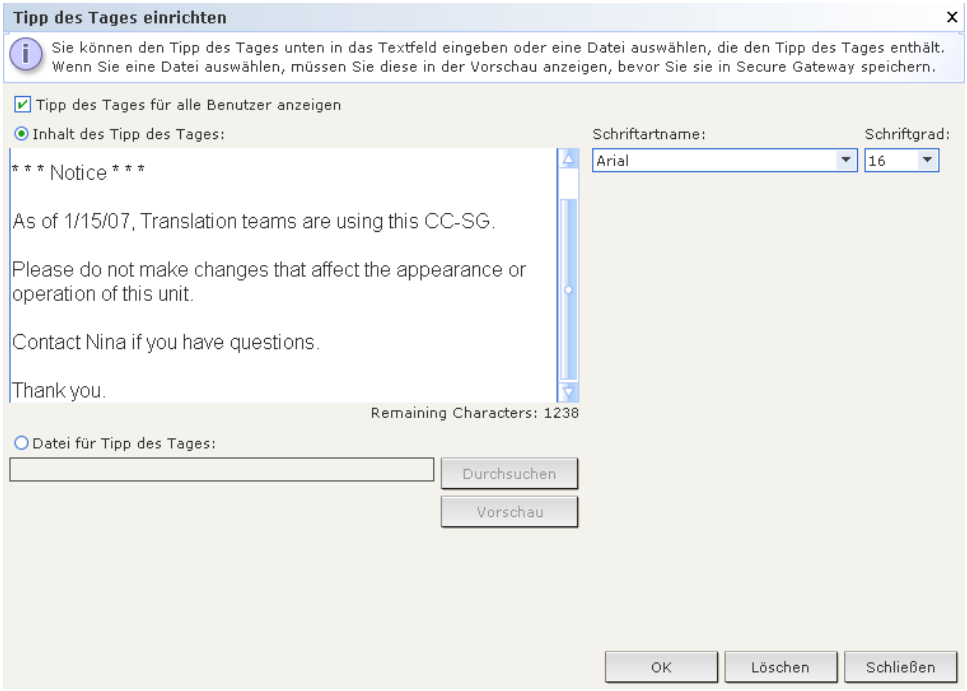


Abbildung 139 Tipp des Tages konfigurieren

1. Klicken Sie im Menü **Administration** auf **Tipp des Tages einrichten**. Der Bildschirm für den Tipp des Tages wird angezeigt.
2. Markieren Sie das Kontrollkästchen **Tipp des Tages für alle Benutzer anzeigen**, wenn die Nachricht allen Benutzern nach dem Anmelden angezeigt werden soll.
3. Markieren Sie das Kontrollkästchen **Inhalt des Tipp des Tages**, wenn Sie eine Nachricht in CC-SG eingeben möchten, oder markieren Sie **Datei für Tipp des Tages**, wenn Sie eine vorhandene Datei mit der Nachricht laden möchten.

   Bei Markierung von **Inhalt des Tipp des Tages**:
   a. Geben Sie eine Nachricht in das Dialogfeld ein.
   b. Klicken Sie auf das Dropdown-Menü **Schriftartname**, und wählen Sie die Schriftart zur Anzeige der Nachricht aus.
   c. Klicken Sie auf das Dropdown-Menü **Schriftgrad**, und wählen Sie den Schriftgrad zur Anzeige der Nachricht aus.

   Bei Markierung von **Datei für Tipp des Tages**:
   a. Klicken Sie auf **Durchsuchen**, um die Datei zu suchen.
   b. Wählen Sie die Datei im Dialogfenster aus, und klicken Sie auf **Öffnen**.
   c. Klicken Sie auf **Vorschau**, um den Inhalt der Datei anzuzeigen.

4. Klicken Sie auf **Löschen**, wenn Sie den Inhalt des Feldes **Inhalt des Tipp des Tages** oder den Pfad der **Datei für Tipp des Tages** löschen möchten.
5. Klicken Sie auf **OK**, um Ihre Einstellungen in CC-SG zu speichern.

Anwendungsmanager

Der Anwendungsmanager bietet eine Möglichkeit für Administratoren, CC-SG Zugriffsanwendungen hinzuzufügen, vorhandene Anwendungen zu bearbeiten und die Standardanwendung für den Zugriff auf Knoten auf Raritan-Geräten festzulegen.

1. Klicken Sie im Menü **Administration** auf **Anwendungen**. Das Fenster **Anwendungsmanager** wird angezeigt.

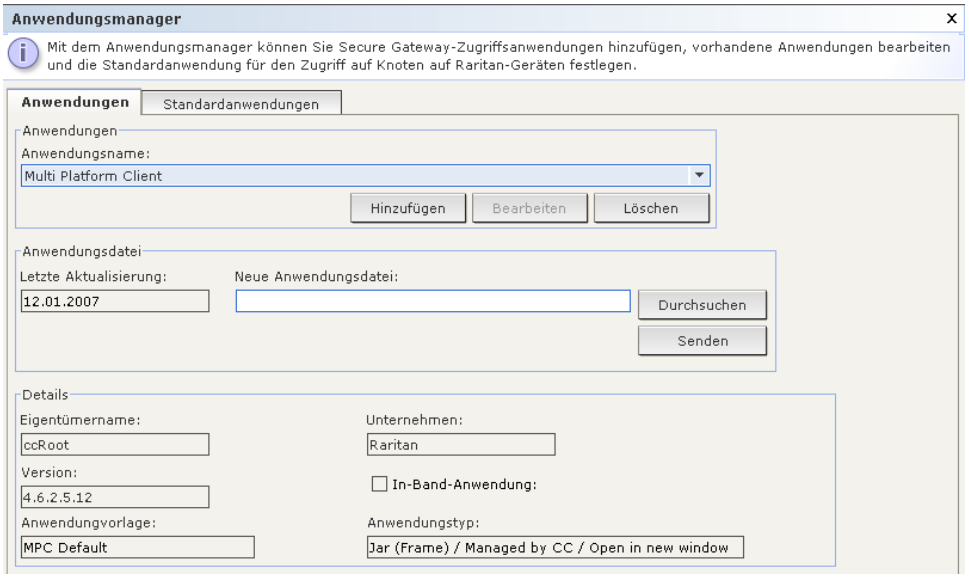


Abbildung 140 Registerkarte Anwendungen im Anwendungsmanager

Anwendungen hinzufügen, bearbeiten und löschen

Klicken Sie im Anwendungsmanager auf die Registerkarte **Anwendungen**, um eine Anwendung hinzuzufügen, zu bearbeiten oder zu löschen.

So fügen Sie Anwendungen hinzu:

1. Klicken Sie auf der Registerkarte **Anwendungen** im Bereich **Anwendungen** auf **Hinzufügen**. Das Fenster **Anwendung hinzufügen** wird angezeigt.

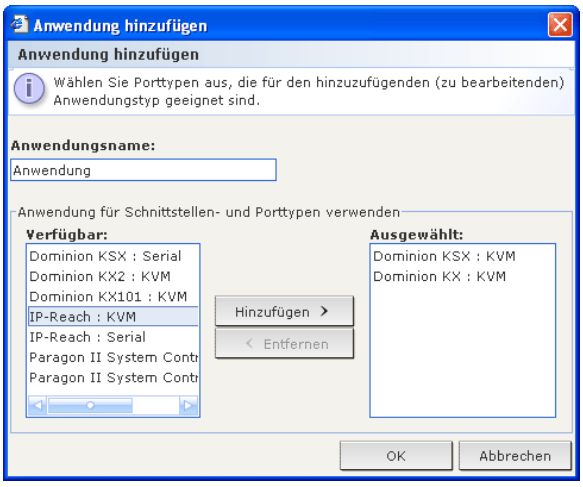


Abbildung 141 Anwendung hinzufügen

2. Geben Sie den Namen der Anwendung im Feld **Anwendungsname** ein.

3. Wählen Sie in der Liste **Verfügbar** die Raritan-Geräte für die Anwendung aus, und klicken Sie auf **Hinzufügen**, um sie der Liste **Ausgewählt** hinzuzufügen. Nachdem die Anwendung hinzugefügt wurde, können die Geräte in der Liste **Ausgewählt** auf diese Anwendung zugreifen. Bietet ein Gerät KVM- und seriellen Zugriff, wird es für beide Methoden aufgeführt.
4. Sie können Geräte entfernen, damit sie nicht mehr mit der Anwendung verwendet werden können. Wählen Sie dazu das Gerät in der Liste **Ausgewählt** aus, und klicken Sie auf **Löschen**.
5. Klicken Sie auf **OK**, wenn die entsprechenden Geräte zur Arbeit mit der Anwendung ausgewählt wurden. Das Fenster **Öffnen** wird angezeigt.
6. Suchen Sie im Fenster **Öffnen** nach Ihrer Anwendungsdatei (normalerweise eine JAR- oder CAB-Datei), wählen Sie die Datei aus, und klicken Sie auf **Öffnen**.

Die ausgewählte Anwendung wird dann in CC-SG geladen.

So bearbeiten Sie Anwendungen:

1. Wählen Sie die Anwendung auf der Registerkarte **Anwendungen** im Bereich **Anwendungen** im Dropdown-Menü **Anwendungsname** aus. Informationen zur ausgewählten Anwendung werden im Bereich **Details** der Registerkarte angezeigt.
2. Je nach der Anwendung können einige dieser Daten konfiguriert werden. Konfigurieren Sie Paramenter bei Bedarf im Bereich **Details**.
3. Klicken Sie auf **Bearbeiten**. Das Fenster **Anwendung bearbeiten** wird angezeigt.
4. Wählen Sie ggf. in der Liste **Verfügbar** weitere Raritan-Geräte für die Anwendung aus, und klicken Sie auf **Hinzufügen**, um sie der Liste **Ausgewählt** hinzuzufügen.
5. Sie können Geräte auch entfernen, damit sie nicht mehr mit der Anwendung verwendet werden können. Wählen Sie dazu das Gerät in der Liste **Ausgewählt** aus, und klicken Sie auf **Löschen**.
6. Klicken Sie auf **OK**, wenn die entsprechenden Geräte zur Arbeit mit der Anwendung ausgewählt wurden.

So löschen Sie Anwendungen:

1. Wählen Sie die Anwendung auf der Registerkarte **Anwendungen** im Bereich **Anwendungen** im Dropdown-Menü **Anwendungsname** aus. Informationen zur ausgewählten Anwendung werden im Bereich **Details** der Registerkarte angezeigt.
2. Klicken Sie zum Löschen der Anwendung auf **Löschen**. Eine Bestätigungsmeldung wird angezeigt.
3. Klicken Sie zum Bestätigen auf **Ja** und zum Abbrechen ohne Löschen der Anwendung auf **Nein**.

Standardanwendungen

Klicken Sie auf die Registerkarte **Standardanwendungen**, um die aktuellen Standardanwendungen für verschiedene Schnittstellen- und Porttypen anzuzeigen und zu bearbeiten. Hier aufgeführte Anwendungen werden als Standard bei der Konfiguration eines Knotens für den Zugriff über eine ausgewählte Schnittstelle festgelegt.

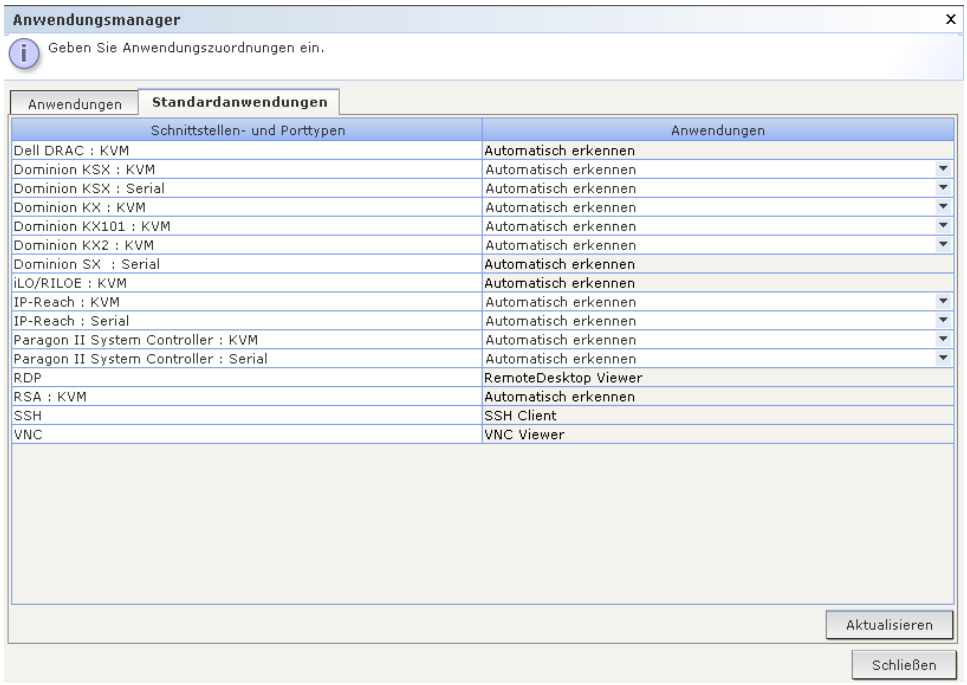


Abbildung 142 Liste der Standardanwendungen

So bearbeiten Sie die Standardanwendung eines Schnittstellen- oder Porttyps:

1. Wählen Sie die Zeile für den Schnittstellen- oder Porttyp aus.
2. Doppelklicken Sie auf die **Anwendung**, die in der Zeile aufgeführt ist. Der Wert wird in einem Dropdown-Menü angezeigt. Abgeblendete Werte können nicht bearbeitet werden.
3. Wählen Sie im Dropdown-Menü eine Standardanwendung aus, die für die Verbindung zu hervorgehobenen Schnittstellen- oder Porttypen verwendet werden soll. Wenn Sie **Automatisch erkennen** auswählen, erkennt CC-SG die Anwendung basierend auf dem Clientbrowser automatisch.
4. Nachdem alle Standardanwendungen konfiguriert wurden, klicken Sie auf **Aktualisieren**, um die Änderungen in CC-SG zu speichern.

Sie können jederzeit auf **Schließen** klicken, um den **Anwendungsmanager** zu schließen.

Firmwaremanager

CC-SG speichert Firmware für Raritan-Geräte, damit die gesteuerten Geräte aktualisiert werden können. Der Firmwaremanager wird verwendet, um die Geräte-Firmwaredateien an CC-SG zu senden oder in CC-SG zu löschen.

Upload

Verwenden Sie diesen Befehl, um verschiedene Firmwareversionen ins System zu laden. Wenn neue Firmwareversionen verfügbar sind, werden sie auf der Website von Raritan veröffentlicht.

1. Klicken Sie im Menü **Administration** auf **Firmware**. Das Fenster **Firmwaremanager** wird angezeigt.

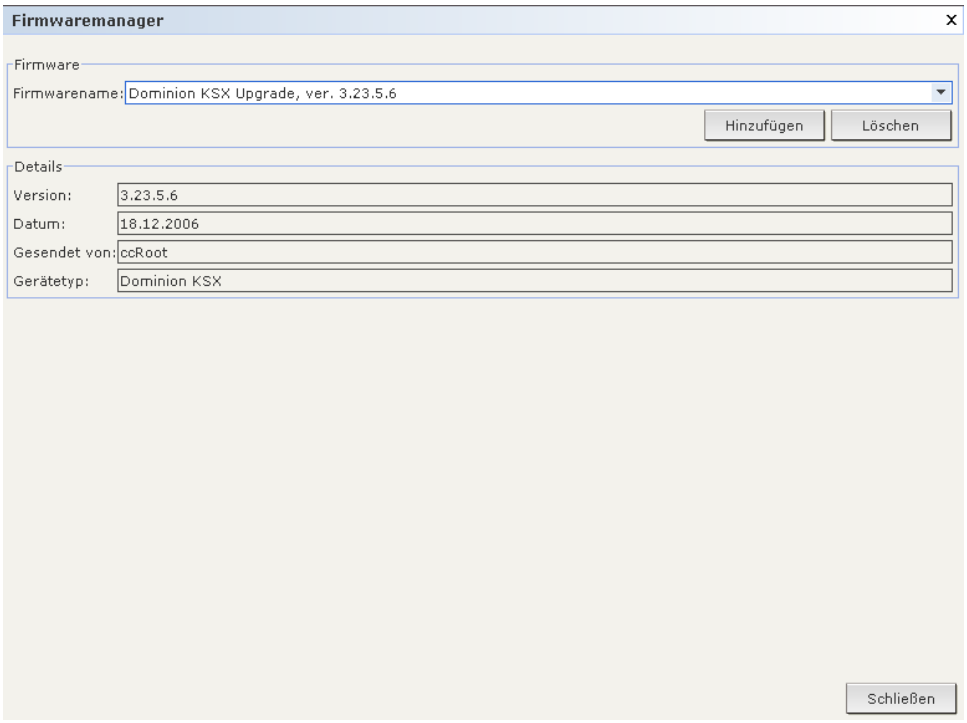


Abbildung 143 Fenster Firmwaremanager

2. Klicken Sie auf **Hinzufügen**, um eine neue Firmwaredatei hinzuzufügen. Ein Suchfenster wird angezeigt.

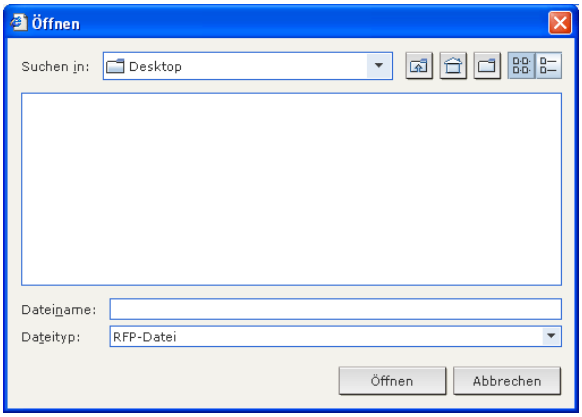


Abbildung 144 Suchfenster für Firmware

3. Klicken Sie auf die Dropdown-Liste **Suchen in**, und suchen Sie die auf Ihrem System gespeicherte Firmwaredatei. Wenn Sie die Firmware gefunden haben, wählen Sie sie aus, und klicken Sie auf **Öffnen**. Nach dem Hinzufügen wird der Firmwarename im Feld **Firmwarename** im Firmwaremanager angezeigt.

Firmware löschen

1. Klicken Sie im Menü **Administration** auf **Firmware**. Das Fenster **Firmwaremanager** wird angezeigt.
2. Klicken Sie auf die Dropdown-Liste **Firmwarename**, und wählen Sie die zu löschende Firmware aus.
3. Klicken Sie auf **Löschen**. Das Fenster **Firmware löschen** wird angezeigt.

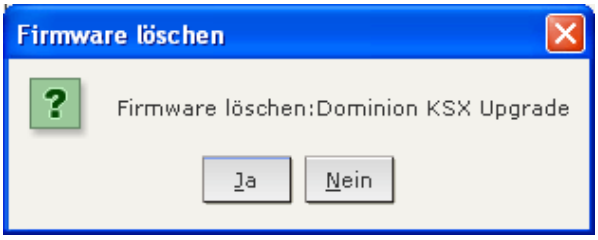


Abbildung 145 Fenster Firmware löschen

4. Klicken Sie zum Löschen der Firmware auf **Ja**, oder klicken Sie auf **Nein**, um das Fenster zu schließen.
5. Klicken Sie zum Schließen des Fensters **Firmwaremanager** auf **Schließen**.

Konfigurationsmanager

Im Konfigurationsmanager werden einige der CC-SG-Haupteinstellungen wie Netzwerkkonfiguration verwaltet.

Netzwerkkonfiguration

1. Klicken Sie im Menü **Administration** auf **Konfiguration**. Das Fenster **Konfigurationsmanager** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Netzwerksetup**.

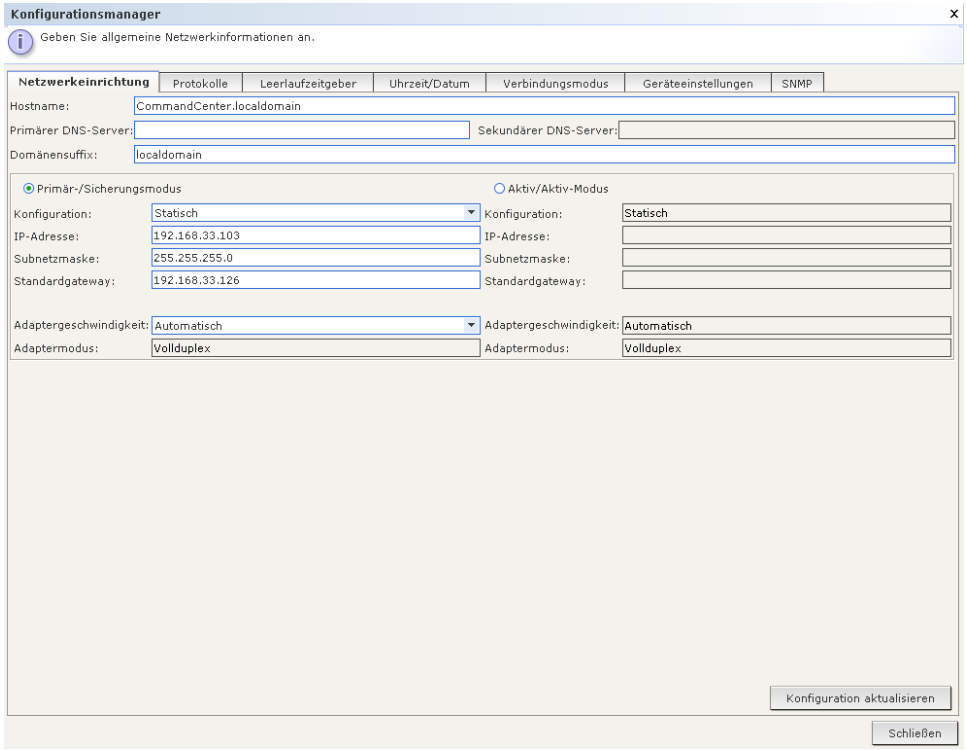


Abbildung 146 Registerkarte Netzwerksetup des Fensters Konfigurationsmanager

3. Geben Sie den CC-SG-Hostnamen im **Hostname** ein. Weitere Informationen finden Sie in den Regeln zur Vergabe von Hostnamen oder in Kapitel 1 dieses Handbuchs. Nachdem **Konfiguration aktualisieren** ausgewählt wurde, wird das Feld aktualisiert. Der vollständig qualifizierte Domänenname (FQDN, Fully-Qualified Domain Name) wird angezeigt, wenn ein Domänenserver und ein Domänensuffix konfiguriert wurden.
4. Klicken Sie auf **Primär-/Sicherungsmodus** oder **Aktiv/Aktiv-Modus**. CC-SG bietet zwei Netzwerkkarten (NICs). Die NICs auf einer G1- oder V1-Einheit sind hinten am Gerät von links nach rechts wie folgt beschriftet:

MODELL	NIC GANZ LINKS (PRIMÄRE SCHNITTSTELLE)	NIC GANZ RECHTS
G1	LAN1	LAN0
V1	LAN1	LAN2

Die NICs auf einer E1-Einheit unterscheiden sich wie folgt:

MODELL	NIC OBEN (PRIMÄRE SCHNITTSTELLE)	NIC UNTEN
E1	LAN1	LAN2

Eine Schnittstelle kann einzeln oder es können beide Schnittstellen gleichzeitig verwendet werden. Zur einfachen Darstellung wird im Folgenden LAN1 als NIC links und LAN2 als NIC rechts bezeichnet. Einige interne Diagnosen und Nachrichten bezeichnen diese Schnittstellen ggf. als „eth0“ und „eth1“.

Hinweis: *Werden beide Schnittstellen getrennt, wird CC-SG neu gestartet.*

A. Wählen Sie die Option **Primär-/Sicherungsmodus** aus, um Ausfallsicherung und Redundanz für das Netzwerk zu implementieren. In diesem Modus ist nur eine NIC zurzeit aktiv, und nur eine Zuweisung einer Netzwerk-IP-Adresse ist möglich.

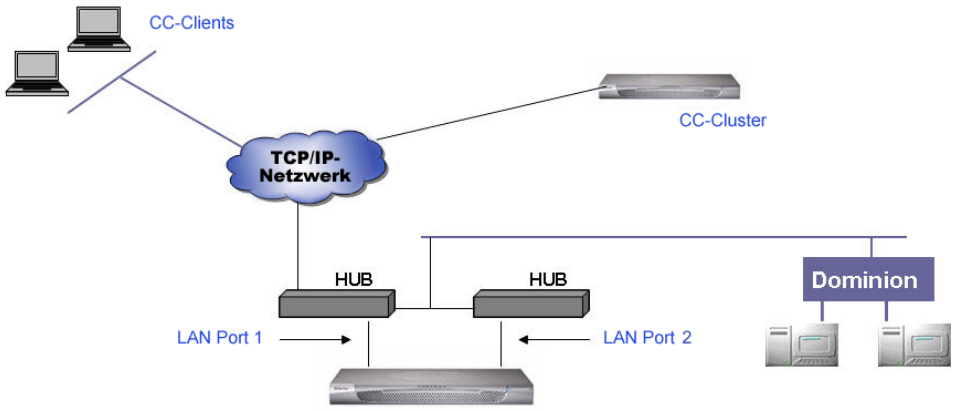


Abbildung 147 Primär-/Sicherungsmodus

Normalerweise sind beide NICs mit demselben LAN-Subnetzwerk verbunden. Es werden jedoch ggf. verschiedene Switches (oder Hubs) für bessere Zuverlässigkeit verwendet. Werden beide NICs verwendet, bietet dies ein bestimmtes Maß an Netzwerkredundanz. Ist beispielsweise LAN1 angeschlossen und erhält ein Verbindungsintegritätssignal, verwendet CC-SG diese NIC für die Kommunikation. Fällt LAN1 aus und ist LAN2 angeschlossen, migriert CC-SG die (ggf. von DHCP) zugewiesene IP-Adresse auf LAN2. LAN2 wird verwendet, bis LAN1 wieder instand gesetzt wurde und dienstbereit ist. In diesem Fall verwendet CC-SG wieder LAN1.

Solange eine Schnittstelle einsatzbereit ist, sollte ein PC-Client keine Dienstunterbrechung bei Ausfällen feststellen. CC-SG behält dieselbe logische IP-Adresse und versucht, die Kommunikationskanäle und vorhandenen Sitzungen aufrecht zu erhalten, falls Netzwerkausfälle auftreten. Die Kommunikation (z. B. PC-Client, Raritan Geräteverwaltung, Cluster Peer usw.) wird über diesen einen Kommunikationskanal durchgeführt, der von beiden NICs erhalten wird.

B. Wählen Sie den **Aktiv/Aktiv-Modus**, wenn spezielle Netzwerkbedingungen vorliegen. Dies gilt besonders, wenn Sie über zwei Netzwerke verfügen und Routing ggf. nicht vorhanden ist. Ist die Netzwerksicherheit wichtig und verwenden Sie proxyartige Implementierungen, sollten Sie diesen Modus ebenfalls auswählen.

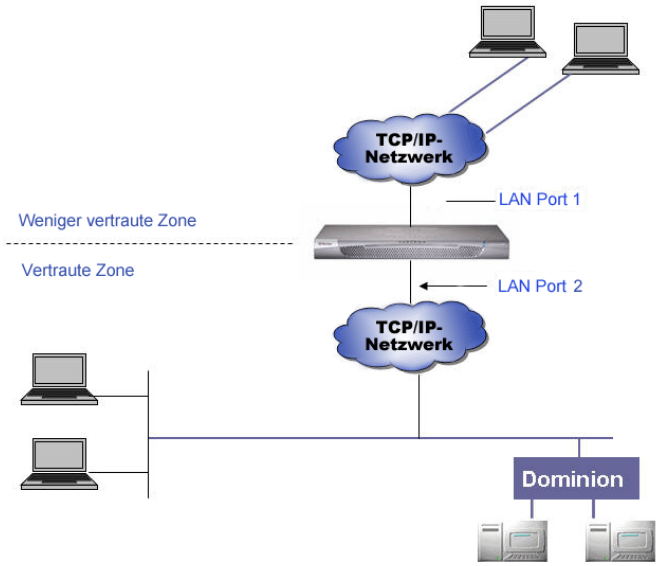


Abbildung 148 Aktiv/Aktiv-Netzwerk

In diesem Modus arbeitet CC-SG als „Router“ oder „Verkehrspolizist“ zwischen zwei getrennten IP-Domänen. Dies gilt besonders, wenn der **Proxymodus** verwendet wird. (Weitere Informationen finden Sie unter **Verbindungsmodus** in diesem Kapitel.) Im Proxymodus ist der **Aktiv/Aktiv**-Modus erforderlich, damit PC-Client-Sitzungen, für die Proxys eingesetzt werden, von CC-SG an die entsprechenden Knoten weitergeleitet werden. Es wird empfohlen, dass Raritan-gesteuerte Geräte mit LAN1 verbunden werden, während PC-Client-Verbindungen, für die Proxys verwendet werden, mit LAN2 verbunden werden. Beide NICs sollten sich in getrennten Subnetzwerken befinden. Wenn Sie jedoch DHCP verwenden, ist dies ggf. nicht möglich, und die Konfiguration wird nicht unterstützt. Geben Sie bei der Konfiguration beider NICs eine standardmäßige Gateway-Adresse für nur eine NIC ein, und lassen Sie die andere leer.

Fällt eine NIC aus, versucht CC-SG, das Paket über die andere NIC basierend auf der aktuellen IP-Routing-Tabelle weiterzuleiten. Dieser Routing-Versuch schlägt ggf. fehl, besonders, wenn eine Firewall verwendet wird. Werden weitere Routen benötigt, können sie in der Diagnostic Console hinzugefügt werden. Weitere Informationen finden Sie unter **Static Routes bearbeiten (Network Interfaces)** in diesem Kapitel.

***Hinweis**: Clustering kann im **Aktiv/Aktiv**-Modus nicht konfiguriert werden.*

5. Klicken Sie auf die Dropdown-Liste **Konfiguration**, und wählen Sie **DHCP** oder **Statisch** in der Liste aus. Wenn Sie **DHCP** auswählen, müssen Sie sicherstellen, dass Ihr DHCP-Server richtig konfiguriert wurde. Geben Sie dann einen Hostnamen ein. DNS-Informationen, Domänensuffix, IP-Adresse, Standardgateway und Subnetzmaske werden automatisch ausgefüllt, wenn Sie **Konfiguration aktualisieren** auswählen. Mithilfe dieser Informationen wird CC-SG dynamisch beim DNS-Server registriert, wenn dieser dynamische Aktualisierungen annimmt. Nach der erfolgreichen Registrierung können Sie über den Hostnamen auf CC-SG zugreifen, da die IP-Adresse bei der Verwendung von DHCP ggf. nicht bekannt ist.

   Wenn Sie **Static** auswählen, geben Sie die Daten für **IP Address**, **Subnet Mask**, **Default Gateway**, **Primary DNS** und **Secundary DNS** in die entsprechenden Felder ein. Geben Sie außerdem eine Zeichenfolge für Ihr Domänensetup im Feld **Domain Suffix** ein.
6. Klicken Sie auf die Dropdown-Liste **Adaptergeschwindigkeit**, und wählen Sie in der Liste eine Geschwindigkeit aus.

7. Wenn Sie **Auto** im Feld **Adapter Speed** ausgewählt haben, ist das Feld **Adapter Mode** deaktiviert und **Full Duplex** ist automatisch ausgewählt. Wenn Sie eine andere Adaptergeschwindigkeit als Auto ausgewählt haben, klicken Sie auf den Pfeil der Dropdown-Liste **Adapter Mode**, und wählen Sie einen Duplexmodus in der Liste aus.
8. Wenn Sie den Modus **Active/Active** auswählen, konfigurieren Sie die zweite Netzwerkschnittstelle mithilfe der Schritte 5 bis 7.
9. Klicken Sie auf **Konfiguration aktualisieren**, um das Netzwerksetup Ihres Systems zu aktualisieren.
10. Klicken Sie zum Schließen des Fensters **Konfigurationsmanager** auf **Schließen**.

Protokollkonfiguration

Auf der Registerkarte **Protokolle** können Sie CC-SG so konfigurieren, dass Berichte für externe Protokollserver erstellt werden. Sie können konfigurieren, welche Nachrichtenebene in jedem Protokoll enthalten sein soll.

So konfigurieren Sie die Protokollaktivitäten:

1. Klicken Sie im Menü **Administration** auf **Konfiguration**. Das Fenster **Konfigurationsmanager** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Protokolle**.

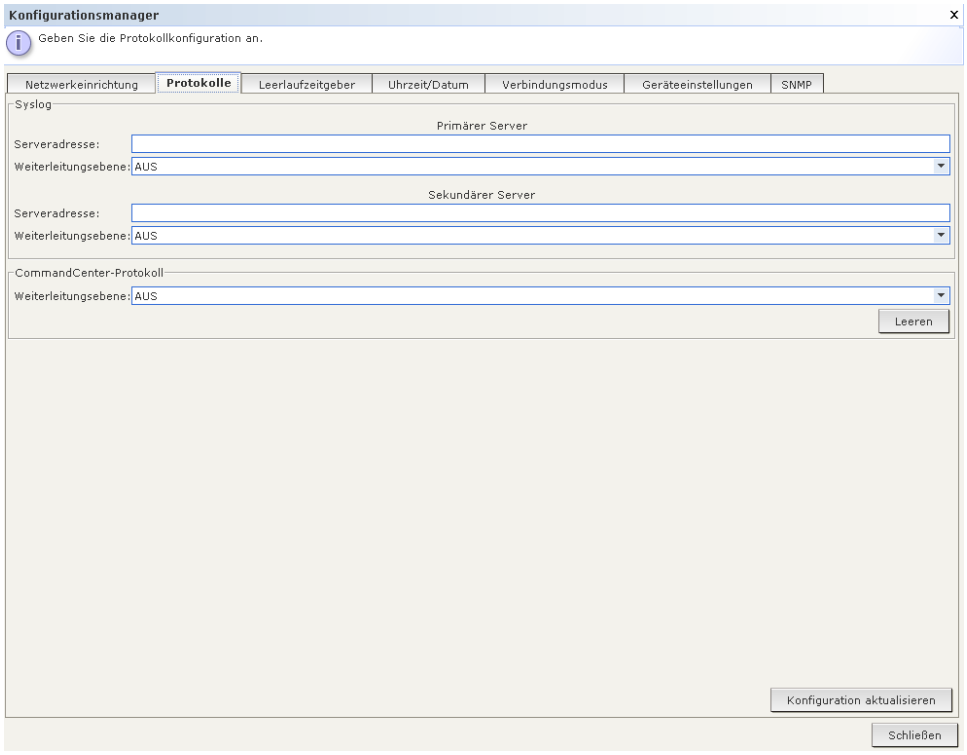


Abbildung 149 Registerkarte Protokolle des Fensters Konfigurationsmanager

3. Sie können in CC-SG einen externen Protokollserver angeben, indem Sie die IP-Adresse in das Feld **Serveradresse** unter **Primärer Server** eingeben.
4. Klicken Sie auf den Pfeil der Dropdown-Liste **Weiterleitungsebene**, und wählen Sie eine Ereignisebene mit entsprechendem Schweregrad aus. Alle Ereignisse dieser oder der darüber liegenden Ebenen werden an den Protokollserver weitergeleitet.
5. Sie können einen zweiten externen Protokollserver konfigurieren, indem Sie die Schritte 3 und 4 für die Felder unter **Sekundärer Server** wiederholen.
6. Klicken Sie unter **CommandCenter-Protokoll** auf das Dropdown-Menü **Weiterleitungsebene**, und wählen Sie eine Ebene aus. Alle Ereignisse auf dieser Ebene oder höher werden an das interne Protokoll von CC-SG weitergeleitet.
7. Klicken Sie nach Abschluss der Konfiguration der Protokolle auf **Konfiguration aktualisieren**, um die Einstellungen in CC-SG zu speichern.
8. Klicken Sie zum Schließen des Fensters **Konfigurationsmanager** auf **Schließen**.

Interne CC-SG-Protokolle leeren

Auf der Registerkarte **Protokolle** können Sie auch die CC-SG-Protokolle leeren. Durch diesen Befehl wird nur das CC-SG-Protokoll geleert. Ereignisse, die durch externe Protokollserver aufgezeichnet werden, werden nicht geleert.

1. Klicken Sie im Menü **Administration** auf **Konfiguration**. Das Fenster **Konfigurationsmanager** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Protokolle**.
3. Klicken Sie unten im Bildschirm auf **Leeren**. Ein Bestätigungsfenster wird angezeigt.
4. Klicken Sie auf **Ja**, um das CC-SG-Protokoll zu leeren.

***Hinweis**: Die Überwachungsliste und der Fehlerprotokollbericht basieren auf dem internen CC-SG-Protokoll. Wenn Sie das interne CC-SG-Protokoll leeren, werden diese beiden Berichte ebenfalls geleert.*

Konfiguration vom Leerlaufzeitgeber

Über diesen Bildschirm können Sie konfigurieren, wie lange eine Sitzung aktiv sein darf bevor sie abgemeldet wird.

1. Klicken Sie im Menü **Administration** auf **Konfiguration**. Das Fenster **Konfigurationsmanager** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Leerlaufzeitgeber**.

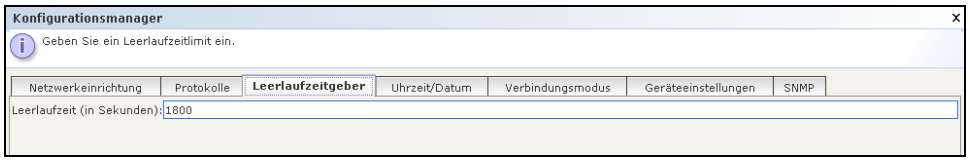


Abbildung 150 Registerkarte Leerlaufzeitgeber

3. Geben Sie das gewünschte Zeitlimit für den Leerlauf in das Feld **Leerlaufzeit** ein.
4. Klicken Sie auf **Konfiguration aktualisieren**, um Ihre Einstellungen in CC-SG zu speichern.

Konfiguration von Uhrzeit/Datum

Uhrzeit und Datum von CC-SG müssen korrekt verwaltet werden, um die Glaubwürdigkeit der Funktionen zur Geräteverwaltung zu gewährleisten.

Wichtig! Die Konfiguration von Uhrzeit/Datum wird zum Planen von Aufgaben im Aufgabenmanager verwendet. Weitere Informationen finden Sie in Kapitel 12: Erweiterte Administration, Aufgabenmanager. Die Zeit, die auf dem Client eingestellt ist, unterscheidet sich eventuell von der auf CC-SG eingestellten Zeit.

Nur der CC-Superuser und Benutzer mit ähnlichen Berechtigungen dürfen Uhrzeit und Datum konfigurieren.

1. Klicken Sie im Menü **Administration** auf **Konfiguration**, um das Fenster **Konfigurationsmanager** anzuzeigen.
2. Klicken Sie auf die Registerkarte **Datum/Uhrzeit**.

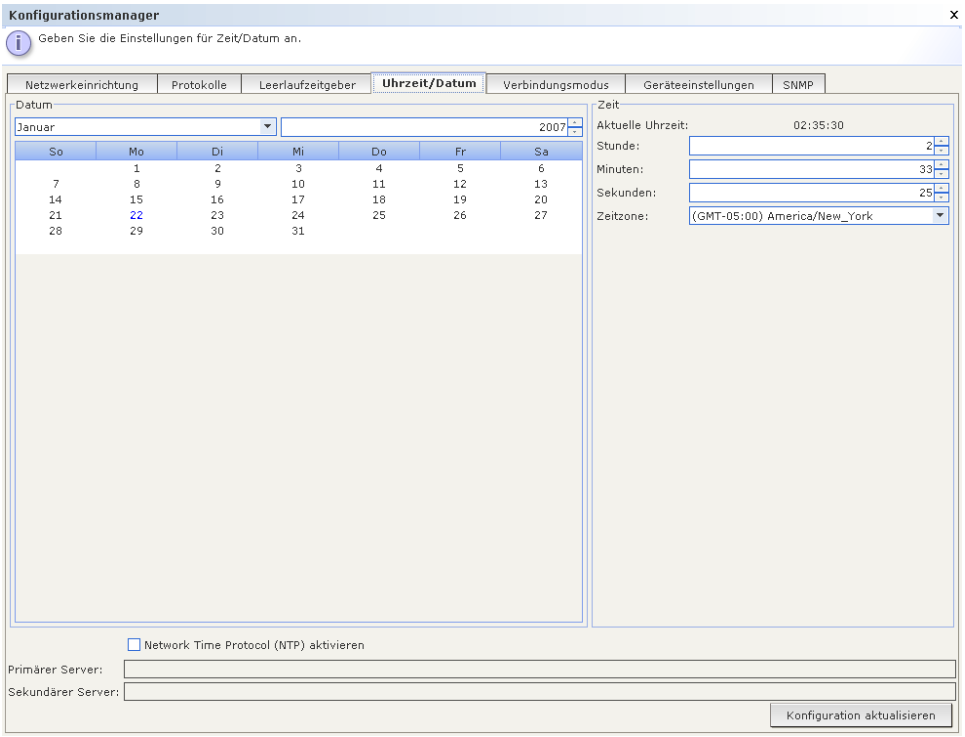


Abbildung 151 Registerkarte Uhrzeit/Datum des Fensters Konfigurationsmanager

a. **So stellen Sie das Datum und die Uhrzeit manuell ein: Datum**: Zum Einstellen des Datums klicken Sie auf den Pfeil neben der Dropdown-Liste und wählen darin den **Monat** aus. Wählen Sie das **Jahr** mit der Pfeil-nach-oben/unten-Schaltfläche aus, und klicken Sie im Kalenderbereich auf den **Tag**. **Uhrzeit**: Zum Einstellen der Uhrzeit klicken Sie auf die Pfeil-nach-oben/unten-Schaltfläche, um die **Stunde**, **Minuten** und **Sekunden** festzulegen. Klicken Sie anschließend auf die Dropdown-Liste **Zeitzone**, um die Zeitzone auszuwählen, in der CC-SG betrieben wird.

b. **So stellen Sie das Datum und die Uhrzeit mittels NTP ein**: Markieren Sie das Kontrollkästchen **Network Time Protocol aktivieren** unten im Fenster, und geben Sie die IP-Adresse für den **Primären NTP-Server** und **Sekundären NTP-Server** in die entsprechenden Felder ein.

Hinweis: *Zum Synchronisieren des Datums und der Uhrzeit von angeschlossenen Computern mit dem Datum und der Uhrzeit eines zugewiesenen NTP-Servers wird das Network Time Protocol (NTP) verwendet. Wird CC-SG mit NTP konfiguriert, kann es zur konsistenten Verwendung der korrekten Uhrzeit seine eigene Uhrzeit mit dem öffentlich verfügbaren NTP-Referenzserver synchronisieren.*

3. Klicken Sie auf **Konfiguration aktualisieren**, um die Uhrzeit- und Datumsänderungen auf CC-SG anzuwenden.
4. Klicken Sie auf **Aktualisieren**, um die neue Serverzeit im Feld **Aktuelle Uhrzeit** zu aktualisieren.
5. Klicken Sie im Menü **Wartung** auf **Neu starten**, um CC-SG neu zu starten.

***Hinweis**: In einer Clusterkonfiguration kann die Zeitzone nicht geändert werden.*

Modemkonfiguration

Verwenden Sie dieses Fenster, um über einen Client und eine Modemverbindung auf CC-SG G1 zuzugreifen. Diese Zugriffsmethode auf CC-SG kann in Notsituationen verwendet werden.

***Hinweis**: Für die V1- oder E1-Plattform steht kein Modem zur Verfügung und kann auch nicht konfiguriert werden.*

CC-SG konfigurieren

1. Klicken Sie im Menü **Administration** auf **Konfiguration**. Klicken Sie im Fenster **Konfigurationsmanager** auf die Registerkarte **Modem**.

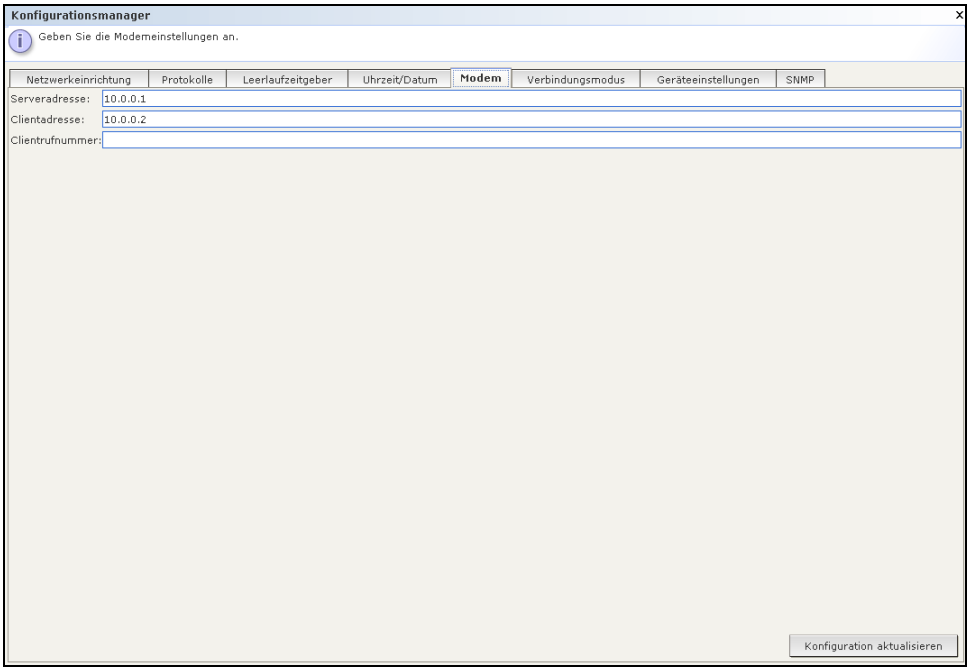


Abbildung 152 Registerkarte Modem des Fensters Konfigurationsmanager

2. Geben Sie die IP-Adresse von CC-SG in das Feld **Serveradresse** ein.
3. Geben Sie die IP-Adresse des Clients, der sich bei CC-SG einwählt, in das Feld **Clientadresse** ein.
4. Geben Sie bei der Verwendung von Rückrufen die Rückrufnummer, die CC-SG wählt, um eine Verbindung zum Client herzustellen, in das Feld **Clientrufnummer** ein.
5. Klicken Sie auf **Konfiguration aktualisieren**, um die Modeminformationen zu speichern.

Das Modem auf dem Client-PC konfigurieren

Verbinden Sie CC-SG G1 (mit integriertem Modem) mit einer Telefonleitung. Sie können die LAN-Kabel entfernen.

Verbinden Sie den Client, der sich einwählt, mit einem Modem (z. B. ein Computer mit Windows XP). Verbinden Sie das Client-Modem mit einer Telefonleitung. Starten Sie den Client-Computer neu, und das verbundene Modem wird als neue Hardware erkannt. Installieren Sie das Modem wie folgt auf dem Client, bei dem es sich hier um einen Client mit Windows XP handelt:

1. Wählen Sie **Systemsteuerung → Telefon- und Modemoptionen** aus.
2. Klicken Sie auf die Registerkarte **Modems**.

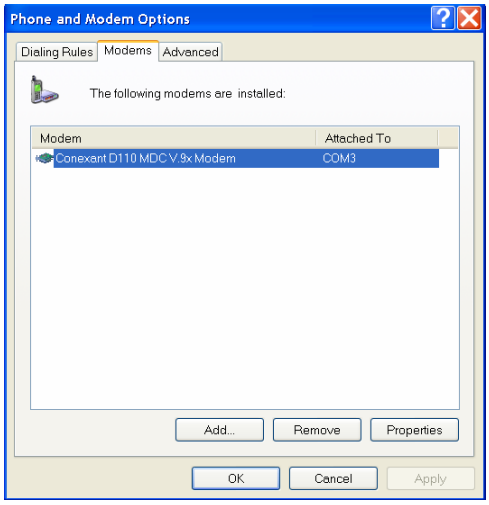


Abbildung 153 Registerkarte Modems

3. Klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Erweitert**.

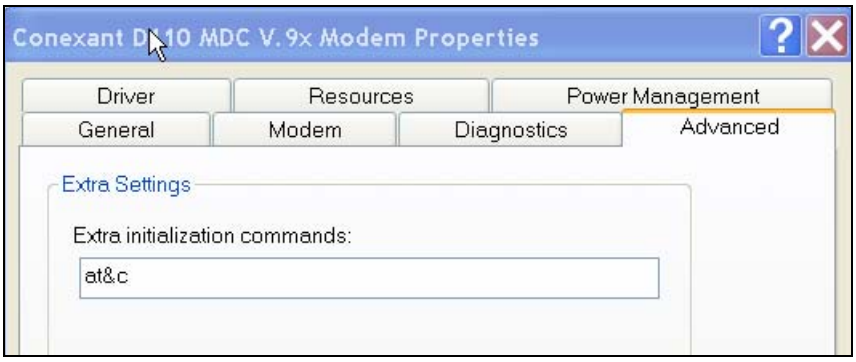


Abbildung 154 Weitere Initialisierungsbefehle

5. Geben Sie einen Initialisierungsbefehl im Feld **Weitere Initialisierungsbefehle** ein, der von Ihrem Modem zum Setzen des Kennzeichens „Carrier detection“ verwendet wird. Geben Sie beispielsweise **at&c** für ein SoftK56 Data Faxmodem ein. Dadurch schließt Windows den standardmäßigen Modemverbindungsvorgang nicht, wenn die Modemverbindung von der anderen (eingewählten) Seite getrennt wird. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

Modemverbindung konfigurieren

Im Folgenden wird gezeigt, wie eine eingehende Modemverbindung für CC-SG von einem Windows XP-Client erstellt wird:

1. Klicken Sie im Menü **Start** auf **Netzwerkumgebung**.
2. Klicken Sie mit der rechten Maustaste in das Fenster, und wählen Sie **Eigenschaften** aus.

3. Klicken Sie im Fenster **Netzwerkverbindungen** unter **Netzwerkaufgaben** auf **Neue Verbindung erstellen**.

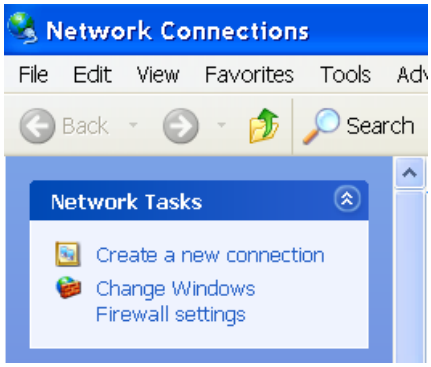


Abbildung 155 Neue Verbindung erstellen

4. Klicken Sie auf **Weiter**, **Verbindung mit dem Netzwerk am Arbeitsplatz herstellen**, **DFÜ-Verbindung**.
5. Geben Sie einen Namen für CC-SG ein (z. B. **CommandCenter**).

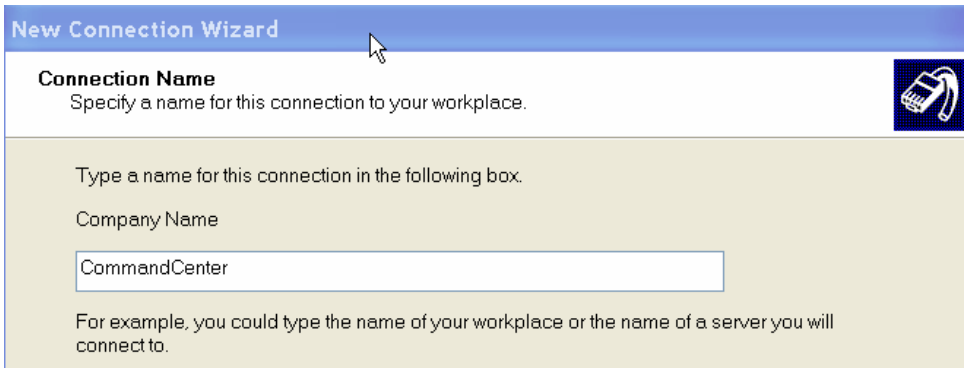


Abbildung 156 Verbindungsname

6. Geben Sie die Telefonnummer ein, die für die Verbindung zu CC-SG verwendet wird, und klicken Sie auf **Weiter**. Hierbei handelt es sich NICHT um die Nummer für Rückrufe, die als **Clientrufnummer** auf der Registerkarte **Modem** im **Konfigurationsmanager** in CC-SG konfiguriert wurde.

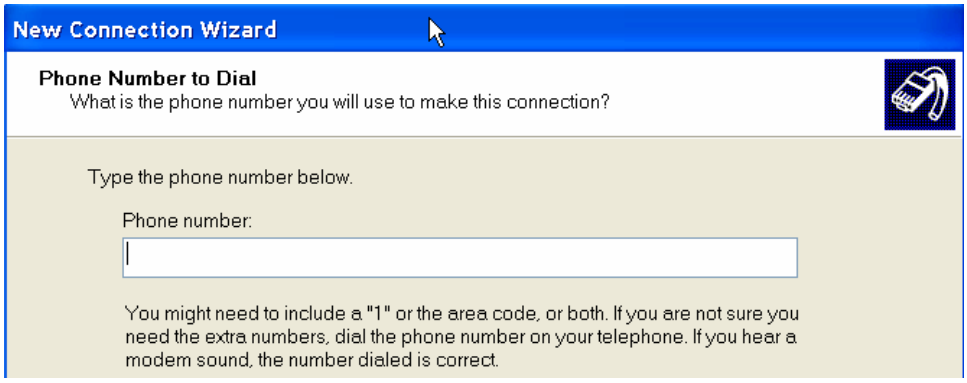


Abbildung 157 Telefonnummer zum Wählen

7. Eine Smartcard ist zum Einwählen bei CC-SG nicht nötig. Wenn Sie keine verwenden, klicken Sie für diese Verbindung auf **Eigene Smartcard nicht verwenden** und dann auf **Weiter**.
8. Im nächsten Fenster sollten Sie normalerweise **Eigene Verwendung** markieren, damit die Verbindung nur Ihnen zur Verfügung steht.
9. Klicken Sie im letzten Fenster auf **Fertig stellen**, um die Verbindungseinstellungen zu speichern.

Rückrufverbindung konfigurieren

Verwendet CC-SG eine Rückrufverbindung, müssen Sie eine Skriptdatei verwenden, die im Folgenden beschrieben wird. So stellen Sie die Skriptdatei für Rückrufe bereit:

1. Klicken Sie im Menü **Start** auf **Netzwerkumgebung**.
2. Klicken Sie unter **Netzwerkaufgaben** auf **Netzwerkverbindungen anzeigen**.
3. Klicken Sie mit der rechten Maustaste auf die Verbindung **CommandCenter** und dann auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Sicherheit**.

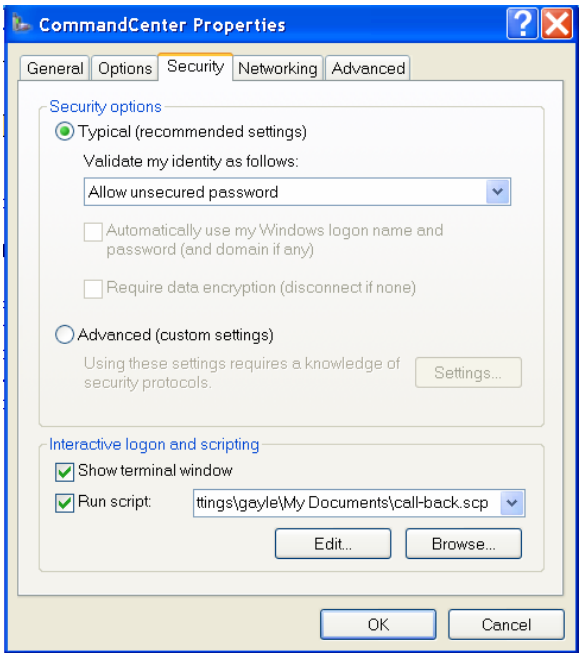


Abbildung 158 DFÜ-Skript angeben

5. Klicken Sie auf **Terminalfenster einblenden**.
6. Klicken Sie auf **Skript ausführen** und **Durchsuchen**, um das DFÜ-Skript (z. B. **call-back.scp**) einzugeben.
7. Klicken Sie auf **OK**.

Beispiel für eine Rückruf-Skriptdatei:

```
proc main
delay 1
waitfor "ogin:"
transmit "ccclient^M"
waitfor "client:"
transmit "dest^M"
waitfor "callback."
transmit "ATH^M"
waitfor "RING"
transmit "ATA^M"
waitfor "CONNECT"
waitfor "ogin:"
transmit "ccclient^M"
endproc
```

Mit CC-SG über ein Modem verbinden

So stellen Sie eine Verbindung zu CC-SG her:

1. Klicken Sie im Menü **Start** auf **Netzwerkumgebung**.
2. Klicken Sie unter **Netzwerkaufgaben** auf **Netzwerkverbindungen anzeigen**.
3. Doppelklicken Sie auf die Verbindung **CommandCenter**.

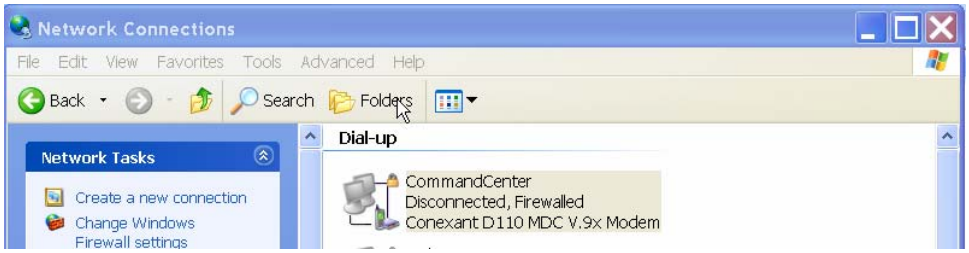


Abbildung 159 Verbindung zu CC-SG

4. Geben Sie den Benutzernamen **ccclient** und das Kennwort **cbupass** ein.

Abbildung 160 Benutzernamen und Kennwort eingeben

5. Geben Sie die Telefonnummer für die Verbindung zu CC-SG ein, falls diese noch nicht angezeigt wird. Es handelt sich NICHT um die Nummer für den Rückruf.
6. Klicken Sie auf **Wählen**. Bei Rückrufen wählt das Modem CC-SG an, und CC-SG wählt dann Ihren Client-PC an.

7. Ist **Terminalfenster einblenden** wie in diesem Kapitel in Abschnitt **Rückrufverbindung konfigurieren** beschrieben markiert, wird ein ähnliches Fenster wie unten angezeigt:

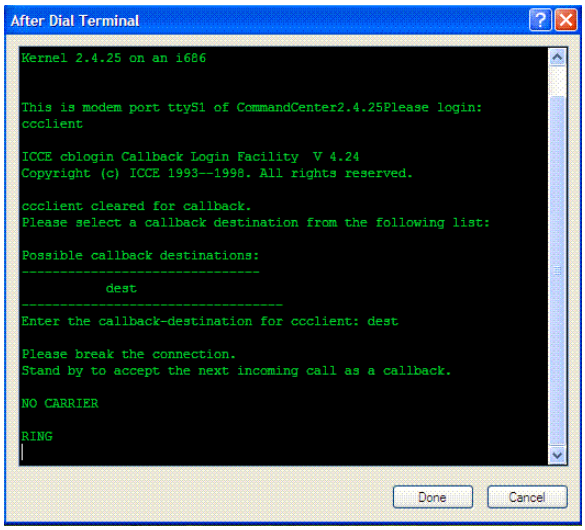


Abbildung 161 Terminal nach dem Wählen

8. Warten Sie eine oder zwei Minuten. Geben Sie dann in einem unterstützten Browser die IP-Adresse von CC-SG ein, die als **Serveradresse** auf der Registerkarte **Modem** im **Konfigurationsmanager** von CC-SG konfiguriert wurde, und melden Sie sich bei CC-SG an.

Verbindungsmodus

Wenn die Verbindung zu einem Knoten hergestellt wurde, können Daten mit diesem Knoten direkt weitergeleitet und zurückgegeben werden (**Direktmodus**), oder alle Daten können über Ihre CC-SG-Einheit geleitet werden (**Proxymodus**). Der **Proxymodus** erhöht zwar die Bandbreitenauslastung des CC-SG-Servers, Sie müssen jedoch nur die TCP-Ports des CC-SG (80, 443 und 2400) in der Firewall geöffnet lassen. Weitere Informationen finden Sie im Handbuch **Digitales Lösungskonzept von Raritan – Implementierungshandbuch**.

1. Klicken Sie im Menü **Administration** auf **Konfiguration**. Das Fenster **Konfigurationsmanager** wird angezeigt.

2. Klicken Sie auf die Registerkarte **Verbindungsmodus**.

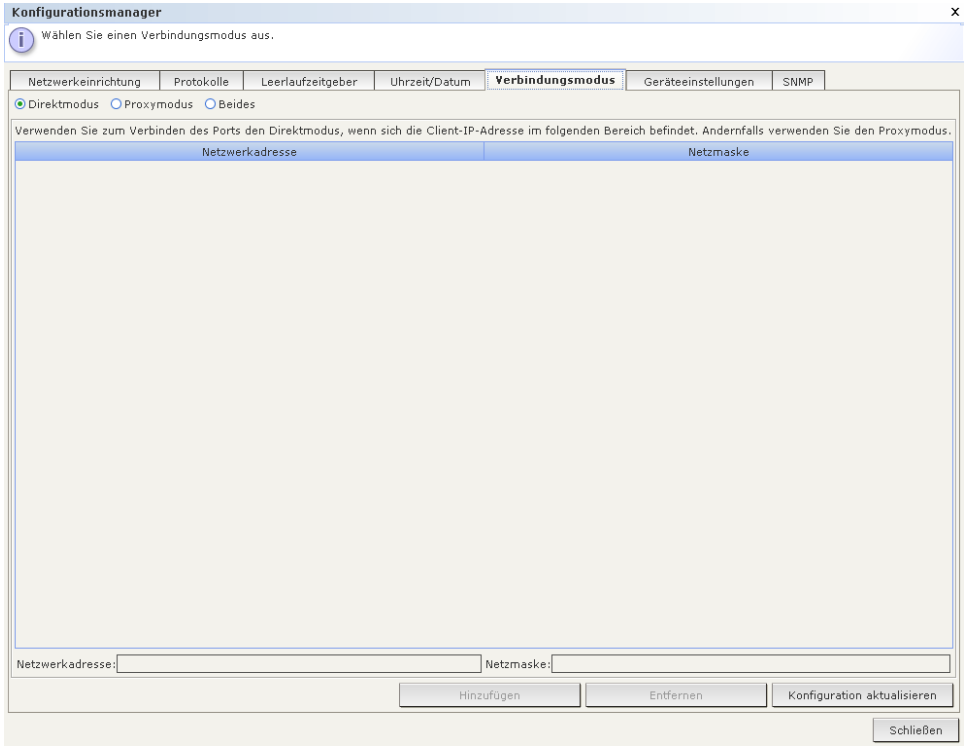


Abbildung 162 Registerkarte Verbindungsmodus des Fensters Konfigurationsmanager – Direktmodus

3. Klicken Sie auf das Optionsfeld neben dem von Ihnen bevorzugten Verbindungsmodus.
   a. Klicken Sie auf das Optionsfeld **Direktmodus**, um eine direkte Verbindung zu einem Gerät herzustellen.
   b. Klicken Sie auf das Optionsfeld **Proxymodus**, um eine Verbindung mit einem Gerät über die CC-SG-Einheit herzustellen.
   c. Klicken Sie auf das Optionsfeld **Beides**, wenn Sie zu einigen Geräten eine direkte Verbindung, zu anderen jedoch eine Verbindung über den **Proxymodus** herstellen möchten. Legen Sie dann die Einstellungen für die Geräte fest, die direkt verbunden werden sollen:
      i. Geben Sie die IP-Adresse des Clients im Feld **Netzwerkadresse** unten im Fenster ein.
      ii. Geben Sie die Netzmaske Ihres Clients im Feld **Netzmaske** ein.
      iii. Klicken Sie auf die Schaltfläche **Hinzufügen**, um die Netzadresse und die Maske zum Fenster hinzuzufügen. Möglicherweise müssen Sie die Bildlaufleiste rechts im Fenster verwenden, um die Schaltflächen **Hinzufügen/Entfernen/Aktualisieren** sehen zu können.

Geräteeinstellungen

1. Klicken Sie im Menü **Administration** auf **Konfiguration**. Das Fenster **Konfigurationsmanager** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Geräteeinstellungen**.

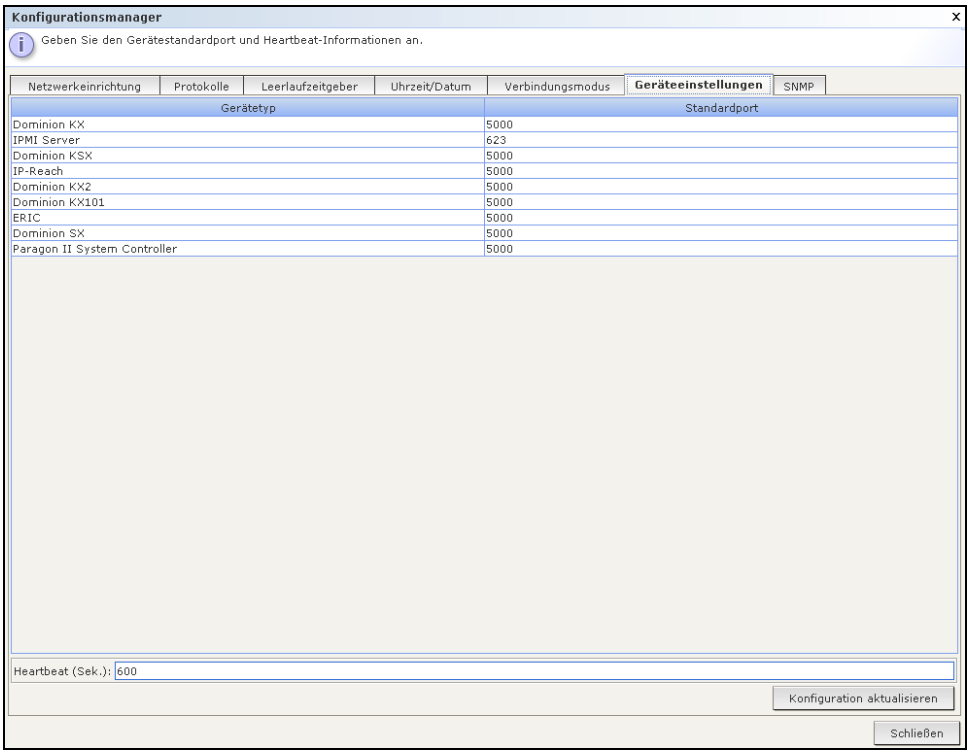


Abbildung 163 Fenster Konfigurationsmanager Geräteeinstellungen

3. Wählen Sie zum Aktualisieren des Standardports eines Geräts in der Tabelle einen **Gerätetyp** aus, und doppelklicken Sie auf den Wert **Standardport**. Geben Sie den neuen Wert für **Standardport** ein, und drücken Sie die **Eingabetaste**.
4. Zum Aktualisieren der Timeout-Dauer eines Geräts doppelklicken Sie unten im Fenster auf den Wert für **Heartbeat (Sek.)**. Geben Sie die neue Timeout-Dauer für dieses Gerät ein.
5. Klicken Sie zum Speichern der neuen Gerätewerte auf **Konfiguration aktualisieren**. Eine Meldung wird zur Bestätigung angezeigt, dass alle zugeordneten Geräteeinstellungen aktualisiert wurden.

SNMP

Mit Simple Network Management Protocol (SNMP) sendet CC-SG SNMP-Traps (Ereignisbenachrichtigungen) zu einem SNMP-Manager im Netzwerk. Nur ein auf SNMP-Infrastrukturen spezialisierter CC-SG-Administrator sollte die Konfiguration von CC-SG mit SNMP ausführen.

CC-SG unterstützt außerdem SNMP-Get/Set-Anfragen mit Unternehmensverwaltungslösungen von Drittanbietern wie HP OpenView. Zur Unterstützung dieser Anfragen müssen Sie SNMP-Agentenkennungsdaten angeben, wie beispielsweise die folgenden MIB-II Systemgruppenobjekte: sysContact, sysName und sysLocation. Weitere Informationen finden Sie unter RFC 1213. Diese Kennzeichen bieten Kontakt-, administrative und Standortinformationen für den verwalteten Knoten.

MIB-Dateien

Da CC-SG eigene Raritan-Traps sendet, müssen alle SNMP-Manager mit einer benutzerdefinierten MIB-Datei, die Raritan-Trap-Definitionen enthält, aktualisiert werden. Weitere Informationen finden Sie in **Anhang D: SNMP-Traps**. Diese benutzerdefinierte MIB-Datei befindet sich auf der CD, die mit Ihrer CC-SG-Einheit geliefert wurde, sowie unter **Firmwareaktualisierungen** unter **http://www.raritan.com/support**.

SNMP in CC-SG konfigurieren

1. Klicken Sie im Menü **Administration** auf **Konfiguration**. Das Fenster **Konfigurationsmanager** wird angezeigt.
2. Klicken Sie auf die Registerkarte **SNMP**.

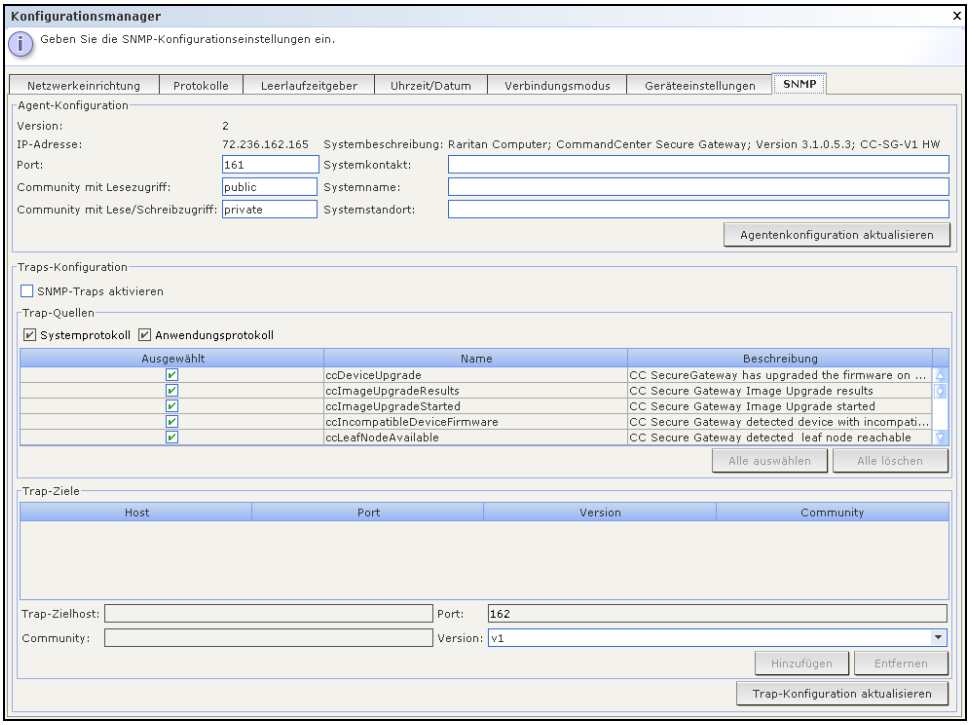


Abbildung 164 Fenster Konfigurationsmanager Geräteeinstellungen

3. Kennzeichnen Sie den SNMP-Agenten, der auf CC-SG ausgeführt wird, für Unternehmensverwaltungslösungen von Drittanbietern, indem Sie unter **Agent-Konfiguration** Informationen zum Agenten bereitstellen. Geben Sie einen **Port** für den Agenten ein. Der Standardwert ist **161**. Geben Sie eine Zeichenfolge für **Community mit Leseberechtigung** ein (Standardwert **public**) sowie eine für **Community mit Lese/Schreibzugriff** (Standardwert **private**). Mehrere Community-Zeichenfolgen sind erlaubt, müssen dann jedoch durch ein Komma getrennt werden. Geben Sie Werte für **Systemkontakt**, **Systemname** und **Systemstandort** ein, um Informationen zum verwalteten Knoten bereitzustellen.
4. Klicken Sie auf **Agentenkonfiguration aktualisieren**, um die SNMP-Agentenkennungsdaten zu speichern.
5. Markieren Sie unter **Traps-Konfiguration** das Kästchen **SNMP-Traps aktivieren**, damit SNMP-Traps über CC-SG an einen SNMP-Host gesendet werden können.
6. Aktivieren Sie die Kontrollkästchen neben den Traps, die von CC-SG an die SNMP-Hosts gesendet werden sollen:
   Unter **Trap-Quellen** finden Sie eine Liste der in zwei Kategorien unterteilten SNMP-Traps: **Systemprotokoll**-Traps, die Benachrichtigungen zum Status der CC-Einheit selbst enthalten, wie beispielsweise einen Festplattenfehler, und **Anwendungsprotokoll**-Traps für Benachrichtigungen, die von Ereignissen in der CC-Anwendung erstellt werden, wie beispielsweise Änderungen des Benutzerkontos. Zum Aktivieren von Traps nach Typ aktivieren Sie die Kontrollkästchen **Systemprotokoll** und **Anwendungsprotokoll**. Einzelne Traps können durch Aktivieren/Deaktivieren ihrer entsprechenden Kontrollkästchen aktiviert oder deaktiviert werden. Verwenden Sie **Alle auswählen** und **Alle löschen**, um alle Traps zu aktivieren oder alle Kontrollkästchen zu deaktivieren. Eine Liste der bereitgestellten SNMP-Traps finden Sie in den MIB-Dateien. Weitere Informationen finden Sie im Abschnitt **MIB-Dateien**.
7. Geben Sie im Fensterbereich **Trap-Ziele** die von SNMP-Hosts verwendete IP-Adresse vom **Trap-Zielhost** und die **Portnummer** ein. Der Standardport lautet **162**.

8. Geben Sie im Bereich **Trap-Ziele** eine Zeichenfolge für **Community** und die **Version** (**v1** oder **v2**) ein, die von SNMP-Hosts verwendet wird.
9. Klicken Sie auf **Hinzufügen**, um diesen Zielhost zur Liste der konfigurierten Hosts hinzuzufügen. Zum Entfernen eines Hosts aus der Liste wählen Sie den Host aus, und klicken Sie auf **Entfernen**. In dieser Liste können beliebig viele Manager festgelegt werden.
10. Klicken Sie nach dem Konfigurieren der SNMP-Traps und -Ziele auf **Trap-Konfiguration aktualisieren**.

Clusterkonfiguration

Ein CC-SG-Cluster verwendet zwei CC-SG-Konten: einen primären Knoten und einen sekundären Knoten, der zur Sicherheit dient, falls der primäre CC-SG-Knoten ausfällt. Für beide Knoten werden gemeinsame Daten für aktive Benutzer und Verbindungen verwendet, und alle Statusdaten werden zwischen den beiden Knoten repliziert. Die primären und sekundären Knoten in einem Cluster müssen dieselbe Softwareversion ausführen. Wird kein Name vom Benutzer definiert, weist CC-SG jedem Clusterknoten einen Standardnamen zu.

Geräte in einem CC-SG-Cluster müssen die IP-Adresse des primären Knotens von CC-SG kennen, damit sie diesen über Statusänderungen informieren können. Fällt der primäre Knoten aus, übernimmt der sekundäre Knoten sofort alle Funktionen des primären Knotens. Dafür ist eine Initialisierung der CC-SG-Anwendung und der Benutzersitzungen erforderlich. Alle vorhandenen Sitzungen, die vom primären Knoten des CC-SG ausgehen, werden beendet. Alle mit dem primären Knoten der CC-SG-Einheit verbundenen Geräte erkennen, dass der primäre Knoten nicht reagiert und reagieren auf Anforderungen des sekundären Knotens.

***Hinweis**: In einer Clusterkonfiguration kommuniziert nur das primäre CC-SG mit CC-NOC. Wechselt ein CC-SG in den primären Status, wird seine IP-Adresse mit der IP-Adresse des sekundären CC-SG an CC-NOC gesendet.*

Cluster erstellen

Bei einem Ausfall sollte der Administrator eine E-Mail an alle CC-SG-Benutzer senden, um sie zu benachrichtigen, die IP-Adresse des neuen primären CC-SG-Knotens zu verwenden.

Wichtig: Es wird empfohlen, Ihre Konfiguration auf beiden Knoten zu sichern, bevor Sie eine Clusterkonfiguration einrichten.

***Hinweis**: CC-SG muss für das Clustering die Netzwerkports im Modus **Primär/Sicherung** ausführen. Clustering funktioniert nicht, wenn die Konfiguration Aktiv/Aktiv ausgewählt wurde. Weitere Informationen finden Sie unter **Netzwerkkonfiguration** in diesem Kapitel.*

Primären CC-SG-Knoten einrichten

1. Klicken Sie im Menü **Administration** auf **Clusterkonfiguration**. Das Fenster **Clusterkonfiguration** wird angezeigt.

2. Klicken Sie auf **CommandCenter-Einheiten erkennen**, um alle CC-SG-Appliances in dem von Ihnen zurzeit verwendeten Subset zu durchsuchen und anzuzeigen. Sie können auch ein CC-SG (ggf. aus einem anderen Subnetz) hinzufügen, indem Sie unten im Fenster im Feld **CommandCenter-Adresse** eine IP-Adresse festlegen. Klicken Sie dann auf **CommandCenter hinzufügen**.

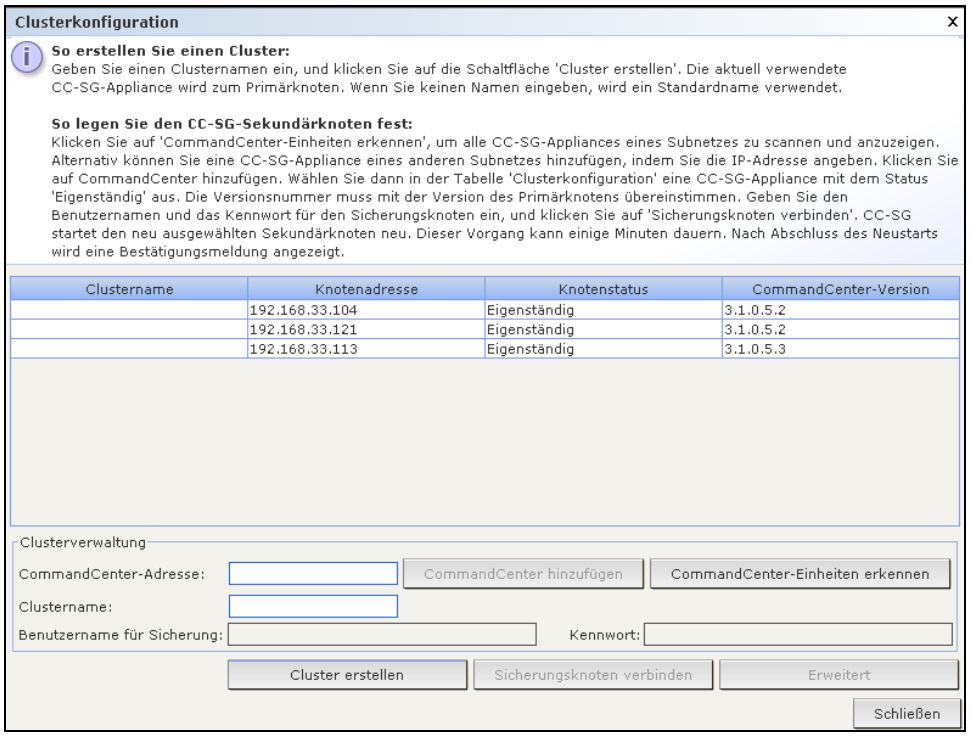


Abbildung 165 Fenster Clusterkonfiguration

3. Geben Sie im Feld **Clustername** einen Namen für dieses Cluster ein. Wenn Sie keinen Namen eingeben, wird beim Erstellen des Clusters ein Standardname wie **cluster192.168.51.124** bereitgestellt.
4. Klicken Sie auf **Cluster erstellen**.

5. Klicken Sie zum Fortfahren auf **Ja**. Das von Ihnen zurzeit verwendete CC-SG wird zum primären Knoten. Wenn Sie keinen Namen in das Feld **Clustername** eingegeben haben, wird ein Standardname bereitgestellt.

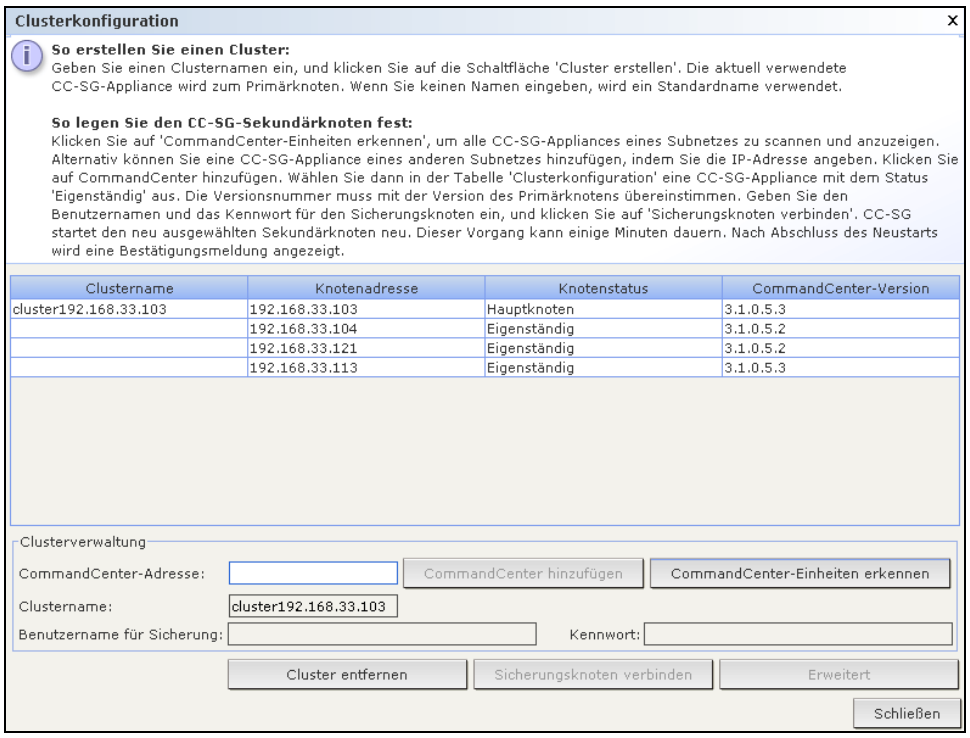


Abbildung 166 Clusterkonfiguration – Primärer Knotensatz

Sekundären CC-SG-Knoten einrichten

1. Klicken Sie auf **CommandCenter-Einheiten erkennen**, um alle CC-SG-Appliances in dem von Ihnen zurzeit verwendeten Subset zu durchsuchen und anzuzeigen. Sie können auch ein CC-SG (ggf. aus einem anderen Subnetz) hinzufügen, indem Sie unten im Fenster im Feld **CommandCenter-Adresse** eine IP-Adresse festlegen. Klicken Sie auf **CommandCenter hinzufügen**.

***Hinweis**: Wenn Sie ein Sicherungs-CC-SG aus einem anderen Subnetz oder Netzwerk hinzufügen, vermeiden Sie ggf. Probleme, die ein bestimmtes Netzwerk oder einen Standort betreffen.*

2. Wählen Sie zum Hinzufügen eines sekundären oder CC-SG-Sicherungsknotens eine CC-SG-Einheit mit dem Status **Eigenständig** in der Clusterkonfigurationstabelle aus. Die Versionsnummer muss mit der Version des Primärknotens übereinstimmen.
3. Geben Sie einen gültigen Benutzernamen und ein Kennwort für den Sicherungsknoten in die Felder **Benutzername für Sicherung** und **Kennwort** ein.
4. Klicken Sie auf **Sicherungsknoten verbinden**.
5. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**, um dem ausgewählten Knoten den Sekundärstatus zuzuweisen, oder klicken Sie zum Abbrechen auf **Nein**.

Wichtig! Wenn Sie den Verbindungsvorgang gestarten haben, sollten Sie wie in Schritt 6 unten angegeben keine weiteren Funktionen in CC-SG durchführen, bis der Verbindungsvorgang abgeschlossen ist.

6. Nachdem Sie auf **Ja** geklickt haben, startet CC-SG den neu ausgewählten sekundären Knoten erneut. Dieser Vorgang kann einige Minuten dauern. Nach Abschluss des Neustarts wird eine Bestätigungsmeldung angezeigt.

7. Klicken Sie im Menü **Administration** auf **Clusterkonfiguration**, um die aktualisierte Clusterkonfigurationstabelle anzuzeigen.

***Hinweis**: Besteht zwischen dem primären und sekundären Knoten keine Kommunikation mehr, übernimmt der sekundäre Knoten die Rolle des primären Knotens. Wird die Konnektivität wieder hergestellt, sind ggf. zwei primäre Knoten vorhanden. Sie sollten dann einen primären Knoten entfernen und als sekundären Knoten einrichten.*

Sekundären CC-SG-Knoten entfernen

1. Wenn Sie den Sekundärknotenstatus einer CC-SG-Einheit aufheben und diesen Status einer anderen Einheit in der Konfiguration zuweisen möchten, wählen Sie den entsprechenden Sekundärknoten von CC-SG aus, und klicken Sie auf **Sicherungsknoten entfernen**.
2. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **Ja**, um den Sekundärknotenstatus zu entfernen, oder auf **Nein**, um abzubrechen.

***Hinweis**: Wenn Sie auf **Sicherungsknoten entfernen** klicken, wird die Zuweisung des Sekundärknotens entfernt. Die CC-SG-Sekundäreinheit wird nicht aus der Konfiguration gelöscht.*

Primären CC-SG-Knoten entfernen

1. Wenn Sie den Primärknotenstatus einer CC-SG-Einheit aufheben und diesen Status einer neuen Einheit zuweisen möchten, wählen Sie den entsprechenden Primärknoten von CC-SG aus, und klicken Sie auf **Cluster entfernen**.
2. Wenn die Bestätigungsmeldung angezeigt wird, klicken Sie auf **Ja**, um den Primärknotenstatus zu entfernen, oder auf **Nein**, um abzubrechen.

***Hinweis**: Durch Klicken auf **Cluster entfernen** wird die Primäreinheit von CC-SG nicht aus der Konfiguration entfernt, sondern nur ihre Zuweisung als Primärknoten. **Cluster entfernen** ist nur möglich, wenn kein Sicherungsknoten vorhanden ist.*

Ausgefallenen CC-SG-Knoten wiederherstellen

Wenn ein Knoten ausfällt und Ausfallsicherheit eintritt, wird der ausgefallene Knoten im Status **Warten** wiederhergestellt.

1. Wählen Sie den Knoten im Wartestatus in der Clusterkonfigurationstabelle aus.
2. Durch Klicken auf **Warteknoten verbinden** fügen Sie den Knoten als Sicherungsknoten hinzu.
3. Eine Bestätigungsmeldung wird angezeigt. Klicken Sie auf **Ja**, um dem ausgewählten Knoten den Sekundärstatus zuzuweisen, oder klicken Sie zum Abbrechen auf **Nein**. Haben Sie auf **Ja** geklickt, müssen Sie warten, bis der Sekundärknoten, wie bei **Sicherungsknoten verbinden**, neu gestartet wird.

***Hinweis**: Befindet sich ein Knoten im Status **Warten**, kann er entweder im Modus **Eigenständig** oder im Modus **Sicherungsknoten** gestartet werden.*

Erweiterte Einstellungen einrichten

So konfigurieren Sie die erweiterten Einstellungen einer Clusterkonfiguration:

1. Markieren Sie den gerade erstellten Hauptknoten.
2. Klicken Sie auf **Erweitert**. Das Fenster **Erweiterte Einstellungen** wird angezeigt.

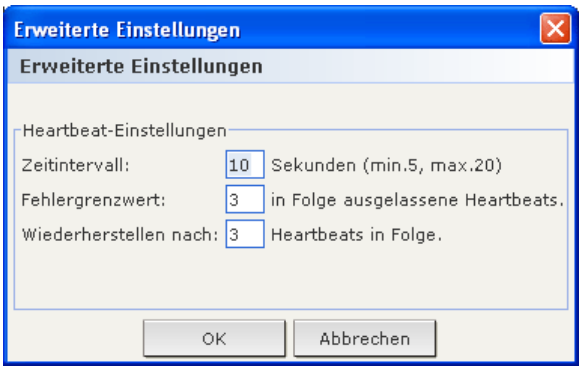


Abbildung 167 Clusterkonfiguration Erweiterte Einstellungen

3. Geben Sie bei **Zeitintervall** ein, wie oft CC-SG seine Verbindung mit dem anderen Knoten überprüfen soll.

***Hinweis**: Ein kurzes Zeitintervall erhöht den durch Heartbeat-Prüfungen verursachten Netzwerkverkehr. Cluster mit weit voneinander entfernt liegenden Knoten legen möglicherweise lange Intervalle fest.*

4. Geben Sie für **Fehlergrenzwert** die Anzahl der aufeinander folgenden Heartbeats an, die erfolgen muss, bevor ein CC-SG-Knoten als fehlgeschlagen eingestuft wird.
5. Geben Sie bei **Wiederherstellen nach** die Anzahl der aufeinander folgenden Heartbeats ein, die erfolgreich zurückgegeben werden muss, bevor eine fehlgeschlagene Verbindung als wiederhergestellt betrachtet wird.
6. Klicken Sie auf **OK**, um die Einstellungen zu speichern.

***Hinweis**: In einer Clusterkonfiguration kann die Zeitzone nicht geändert werden.*

Sicherheitskonfiguration

Der Sicherheitsmanager verwaltet, wie CC-SG Benutzern den Zugriff bereitstellt. Im Sicherheitsmanager können Sie Authentifizierungsmethoden, SSL-Zugriff, Regeln für sichere Kennwörter, Sperrregeln, das Anmeldeportal, Zertifikate und Zugriffssteuerungslisten konfigurieren.

Remoteauthentifizierung

Weitere Informationen zum Konfigurieren von Servern für die Remoteauthentifizierung finden Sie in **Kapitel 9: Konfigurieren der Remoteauthentifizierung**.

Sichere Clientverbindungen

Im Sicherheitsmanager können Sie Sicherheitseinstellungen für Clientverbindungen zu CC-SG konfigurieren.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Das Fenster **Sicherheitsmanager** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Allgemein**.

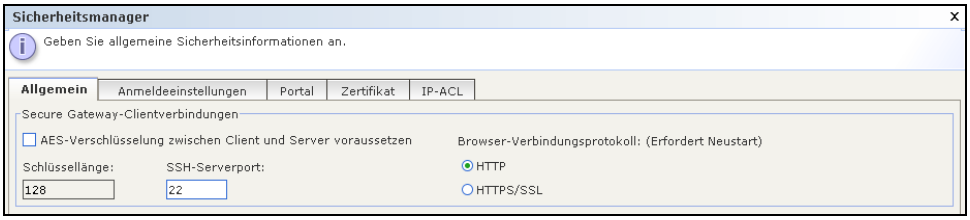


Abbildung 168 Sichere Clientverbindungen

3. Markieren Sie das Kontrollkästchen **AES-Verschlüsselung zwischen Client und Server voraussetzen**, wenn Sie AES-Verschlüsselung für Verbindungen zu CC-SG verwenden möchten. Geben Sie die Schlüssellänge zur Verschlüsselung in das Feld **Schlüssellänge** ein. Die standardmäßige Schlüssellänge ist **128**.
4. Geben Sie die Portnummer für den Zugriff auf CC-SG über SSH in das Feld **SSH-Serverport** ein. Weitere Informationen finden Sie in diesem Kapitel unter **SSH-Zugriff auf CC-SG**.
5. Klicken Sie auf das Optionsfeld **HTTP** oder **HTTP/SSL**, um das Browser-Verbindungsprotokoll für den Client zur Verbindung mit CC-SG auszuwählen. Sie müssen CC-SG neu starten, damit diese Einstellungen übernommen werden können.
6. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Anmeldeeinstellungen

Mit den **Anmeldeeinstellungen** können Sie die **Einstellungen für sichere Kennwörter** und **Sperreinstellungen** konfigurieren.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Das Fenster **Sicherheitsmanager** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Anmeldeeinstellungen**.

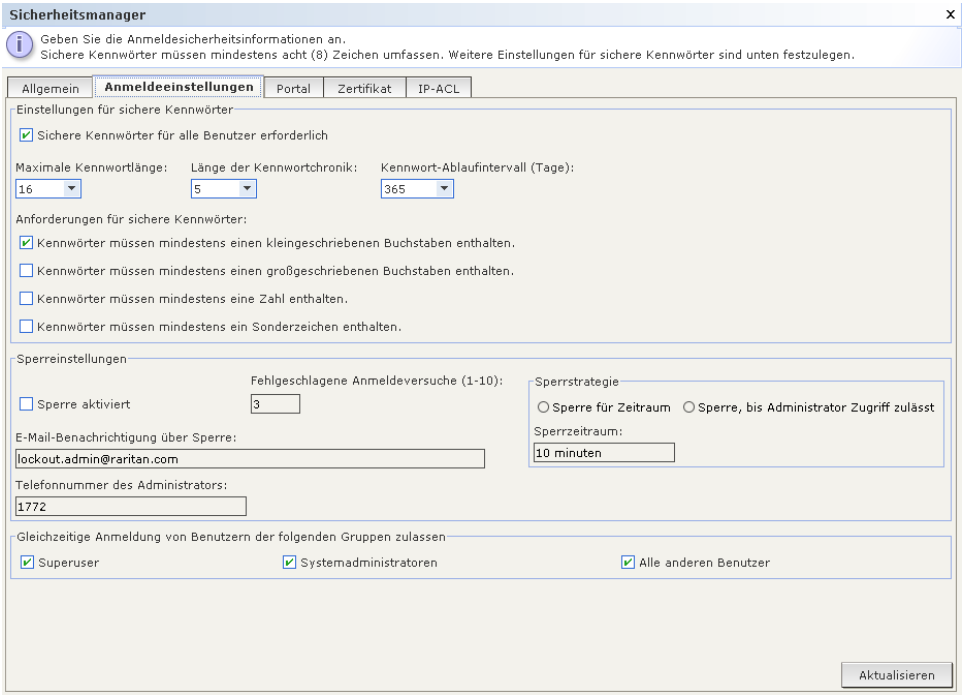


Abbildung 169 Anmeldeeinstellungen

Einstellungen für sichere Kennwörter

Regeln für sichere Kennwörter zwingen Benutzer beim Erstellen von Kennwörtern zur Beachtung von strikten Richtlinien. Diese erschweren das Erraten von Kennwörtern und tragen damit zur Erhöhung der Kennwortsicherheit bei. Sichere Kennwörter sind standardmäßig nicht in CC-SG aktiviert. Wenn Sie sichere Kennwörter verwenden möchten, muss ein Administrator das Kontrollkästchen **Sichere Kennwörter für alle Benutzer erforderlich** markieren.

***Hinweis**: Ein sicheres Kennwort, das alle Anforderungen für sichere Kennwörter umfasst, ist für den CC-Superuser grundsätzlich erforderlich.*

Nachdem das Feld aktiviert ist, können Administratoren die Felder im Bereich **Einstellungen für sichere Kennwörter** bearbeiten, um die Kennwortregeln anzupassen. Sichere Kennwörter müssen mindestens nach den folgenden Kriterien konfiguriert werden:

- **Minimale Kennwortlänge**: Alle Kennwörter müssen eine Mindestanzahl an Zeichen aufweisen. Klicken Sie auf das Dropdown-Menü, und wählen Sie die Mindestlänge für Kennwörter aus.
- **Länge der Kennwortchronik**: Klicken Sie auf das Dropdown-Menü, und wählen Sie aus, wie viele alte Kennwörter in der Chronik gespeichert werden sollen. Benutzer können Kennwörter in der Chronik nicht erneut verwenden, wenn sie ein neues Kennwort eingeben müssen. Ist die Kennwortchronik auf 5 festgelegt, können Benutzer keines ihrer letzten 5 Kennwörter verwenden.
- **Kennwort-Ablaufintervall**: Alle Kennwörter müssen nach einer bestimmten Anzahl an Tagen ablaufen. Klicken Sie auf das Dropdown-Menü, und wählen Sie die Anzahl von Tagen aus, die Kennwörter gültig sind. Nachdem ein Kennwort abgelaufen ist, müssen Benutzer beim nächsten Anmelden ein neues Kennwort eingeben.

Außerdem dürfen 4 aufeinander folgende Zeichen im Benutzernamen und Kennwort nicht übereinstimmen.

Der Administrator kann unter **Anforderungen für sichere Kennwörter** angeben, dass die Kennwortregeln weitere Bedingungen voraussetzen:

- Kennwörter müssen mindestens einen kleingeschriebenen Buchstaben enthalten.
- Kennwörter müssen mindestens einen großgeschriebenen Buchstaben enthalten.
- Kennwörter müssen mindestens eine Zahl enthalten.
- Kennwörter müssen mindestens ein Sonderzeichen (zum Beispiel ein Ausrufezeichen oder kaufmännisches Und) enthalten.

Wenn Sie die Konfiguration der Regeln für sichere Kennwörter abgeschlossen haben, klicken Sie zum Speichern der Einstellungen auf **Aktualisieren**. Alle ausgewählten Regeln sind kumulativ, d. h. alle Kennwörter müssen jedes vom Administrator konfigurierte Kriterium erfüllen. Nach der Konfiguration der Regeln für sichere Kennwörter müssen alle zukünftigen Kennwörter diese Kriterien erfüllen, und alle vorhandenen Benutzer müssen ihre Kennwörter beim nächsten Anmelden ändern, wenn die neuen Kriterien umfassender als die vorherigen sind. Die Regeln für sichere Kennwörter gelten nur für lokal gespeicherte Benutzerprofile. Die auf einem Authentifizierungsserver abgelegten Kennwortregeln müssen von diesem Authentifizierungsserver selbst verwaltet werden.

Raritan empfiehlt die Funktion **Tipp des Tages**, um Benutzer im Voraus davon zu unterrichten, dass die Regeln für sichere Kennwörter geändert und welche neuen Kriterien gelten werden.

Sperreinstellungen

Administratoren können CC-SG-, CC-NOC- und SSH-Benutzer nach einer festgelegten Anzahl von fehlgeschlagenen Anmeldeversuchen sperren. Dieses Feature gilt nur für Benutzer, die lokal von CC-SG authentifiziert und autorisiert werden und nicht für Benutzer, für die externe Server und Remoteauthentifizierung verwendet wird. Weitere Informationen finden Sie in Kapitel 9: Konfigurieren der Remoteauthentifizierung. Fehlgeschlagene Anmeldeversuche aufgrund von unzureichenden Benutzerlizenzen werden nicht berücksichtigt.

Hinweis: *Standardmäßig wird das Konto* **`admin`** *bei drei fehlgeschlagenen Anmeldeversuchen für fünf Minuten gesperrt. Für* **`admin`** *kann die Anzahl der fehlgeschlagenen Anmeldeversuche nicht konfiguriert werden, die für die Sperre verwendet wird.*

So konfigurieren Sie die Benutzersperre:

1. Markieren Sie **Sperre aktiviert**.
2. Die standardmäßige Anzahl für fehlgeschlagene Anmeldeversuche lautet **3**. Danach wird der Benutzer gesperrt. Sie können den Wert ändern, indem Sie eine Zahl zwischen **1** und **10** eingeben.
3. Wählen Sie eine Sperrstrategie aus:
   a. Wenn Sie **Sperre für Zeitraum** auswählen und einen Zeitraum in Minuten angeben, werden Benutzer gesperrt, bevor sie sich wieder anmelden können. Der Standardwert lautet **5** Minuten. Sie können jedoch einen Wert zwischen **1** Minute und **1440** Minuten (24 Stunden) auswählen. Ist die Zeit abgelaufen, kann sich der Benutzer wieder anmelden. Administratoren können während dieses Sperrzeitraums den Wert jederzeit überschreiben, sodass der Benutzer sich wieder bei CC-SG anmelden kann.
   b. Wenn Sie **Sperre, bis Administrator Zugriff zulässt** auswählen, sind die Benutzer gesperrt, bis ein Administrator die Sperre aufhebt. Weitere Informationen zum Aufheben von Benutzersperren finden Sie in **Kapitel 10: Erstellen von Berichten**.
4. Geben Sie eine E-Mail-Adresse im Feld **Benachrichtigung über Sperre** ein, damit eine Benachrichtigung an die Adresse gesendet und der Empfänger über die Sperre informiert werden kann. Ist das Feld leer, wird keine Benachrichtigung gesendet.
5. Geben Sie eine Telefonnummer im Feld **Telefonnummer des Administrators** ein, wenn der Administrator benachrichtigt werden soll.
6. Klicken Sie auf **Aktualisieren**, um die Konfigurationseinstellungen zu speichern.

Gleichzeitige Anmeldung von Benutzern zulassen

Diese Einstellungen lassen mehrere gleichzeitige CC-SG-Sitzungen mit demselben Benutzernamen zu.

1. Markieren Sie **Superuser**, wenn mehr als eine gleichzeitige Verbindung mit CC-SG für das Konto **admin** zulässig sein soll.
2. Markieren Sie **Systemadministratoren**, wenn gleichzeitige Anmeldungen mit Knoten der Benutzergruppe **Systemadministratoren** zulässig sein sollen.
3. Markieren Sie **Alle anderen Benutzer**, wenn gleichzeitige Anmeldungen für alle anderen Konten zulässig sein sollen.

Portal

Über Portaleinstellungen können Administratoren ein Logo und eine Zugriffsvereinbarung konfigurieren, die Benutzern beim Zugriff auf den Client angezeigt werden. So greifen Sie auf die Portaleinstellungen zu:

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Das Fenster **Sicherheitsmanager** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Portal**.

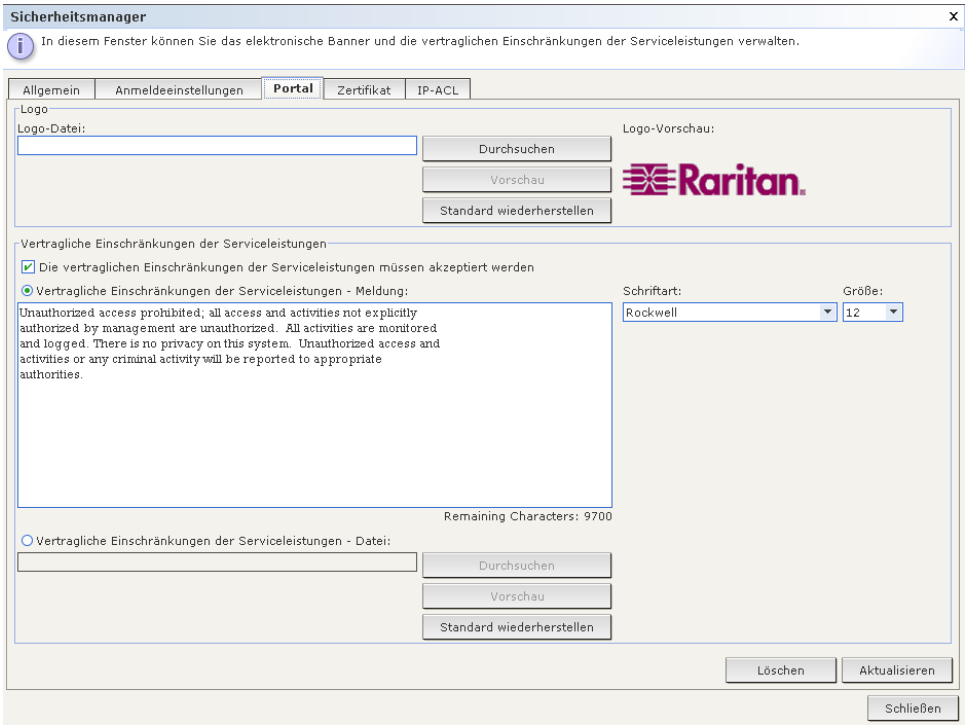


Abbildung 170 Portaleinstellungen

Logo

Sie können eine kleine Grafikdatei an CC-SG senden, die als Banner auf der Anmeldeseite verwendet wird. Die Logogröße darf maximal 998 x 170 Pixel betragen. So senden Sie das Logo:

1. Klicken Sie auf der Registerkarte **Portal** im Bereich **Logo** auf **Durchsuchen**. Ein Dialogbildschirm **Öffnen** wird angezeigt.
2. Wählen Sie die Grafikdatei aus, die Sie als Logo verwenden möchten, und klicken Sie auf **Öffnen**.
3. Sie können das Logo über **Vorschau** auch anzeigen. Die ausgewählte Grafikdatei wird rechts angezeigt.
4. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen am Logo in CC-SG zu speichern.

Vertragliche Einschränkungen der Serviceleistungen

Sie können links neben den Anmeldefeldern auf dem Anmeldebildschirm eine Nachricht anzeigen. Der Platz wurde für die vertraglichen Einschränkungen der Serviceleistungen oder eine Vereinbarung reserviert, die Benutzer vor dem Zugriff auf CC-SG annehmen müssen. Die Annahme der vertraglichen Einschränkungen der Serviceleistungen durch den Benutzer wird in den Protokolldateien und dem Überwachungslistenbericht erfasst.

1. Markieren Sie das Kontrollkästchen **Die vertraglichen Einschränkungen der Serviceleistungen müssen akzeptiert werden**, damit Benutzer das Kontrollkästchen für die Vereinbarung auf dem Anmeldebildschirm markieren müssen, bevor sie ihre Anmeldedaten eingeben können.
2. Markieren Sie das Kontrollkästchen **Vertragliche Einschränkungen der Serviceleistungen - Meldung:**, wenn Sie den Bannertext direkt eingeben möchten.
   a. Geben Sie die Meldung in das angezeigte Feld ein. Der Text darf höchstens 10.000 Zeichen umfassen.
   b. Klicken Sie auf das Dropdown-Menü **Schriftart**, und wählen Sie die Schriftart zur Anzeige der Nachricht aus.
   c. Klicken Sie auf das Dropdown-Menü **Schriftgrad**, und wählen Sie den Schriftgrad zur Anzeige der Nachricht aus.

   Markieren Sie **Vertragliche Einschränkungen der Serviceleistungen - Datei:**, wenn Sie eine Nachricht aus einer Textdatei (TXT) verwenden möchten.
   d. Klicken Sie auf **Durchsuchen**. Ein Fenster wird angezeigt.
   e. Wählen Sie im Fenster die Textdatei mit der Nachricht aus, die Sie verwenden möchten, und klicken Sie auf **Öffnen**. Der Text darf höchstens 10.000 Zeichen umfassen.
   f. Klicken Sie auf **Vorschau**, wenn Sie den Text in der Datei anzeigen möchten. Der Text wird im Feld für die Bannernachricht oben angezeigt.
3. Klicken Sie auf **Aktualisieren**, um Ihre Änderungen am Banner in CC-SG zu speichern.

Nachdem Sie die Einstellungen für das Logo und die vertraglichen Einschränkungen der Serviceleistungen aktualisiert haben, werden sie auf dem Anmeldebildschirm angezeigt, sobald ein Benutzer auf den Client zugreift.

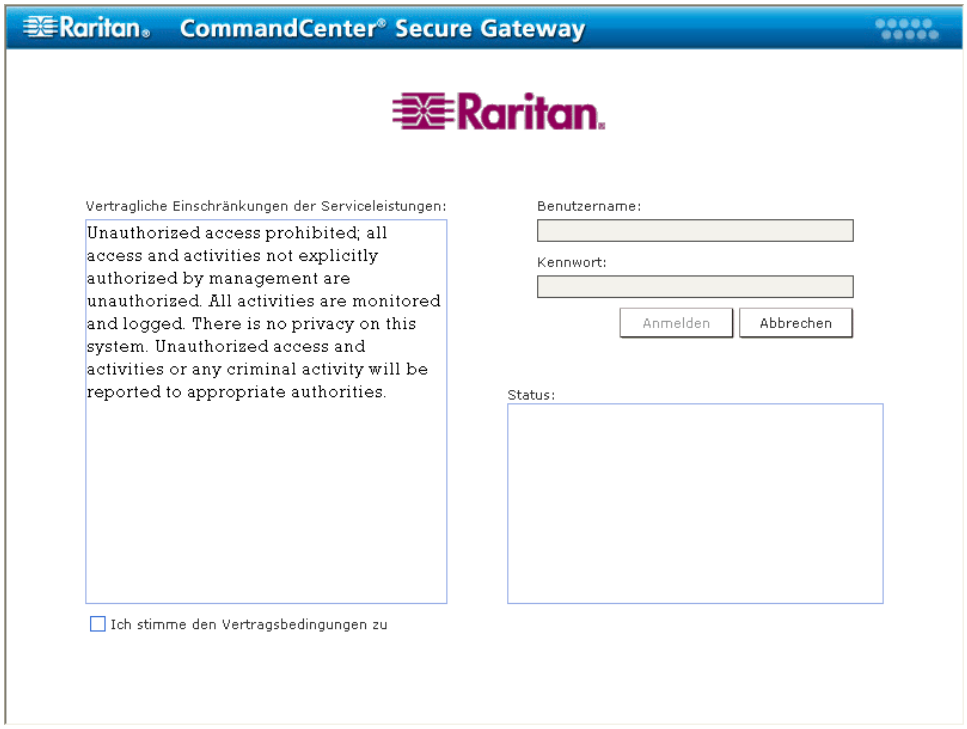


Abbildung 171 Anmeldeportal mit vertraglichen Einschränkungen der Serviceleistungen

Zertifikat

Mithilfe der Optionen in diesem Fenster können Sie eine Anforderung für die Zertifikatsignatur (auch CSR) erzeugen. Eine CSR ist eine Nachricht, die vom Bewerber an eine Zertifizierungsstelle übermittelt wird, um sich für ein digitales Identitätszertifikat zu bewerben. Bevor eine CSR erstellt wird, erzeugt der Bewerber zunächst ein Schlüsselpaar, wobei der private Schlüssel geheim gehalten wird. Die CSR enthält Informationen, mit deren Hilfe der Bewerber identifiziert wird (wie der Verzeichnisname bei einem X.509-Zertifikat), sowie den vom Bewerber ausgewählten öffentlichen Schlüssel.

***Hinweis**: Die Schaltfläche unten im Bildschirm zeigt abhängig von der ausgewählten Zertifikatsoption **Exportieren**, **Importieren** oder **Erzeugen** an.*

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Das Fenster **Sicherheitsmanager** wird angezeigt.
2. Klicken Sie auf die Registerkarte **Zertifikat**.

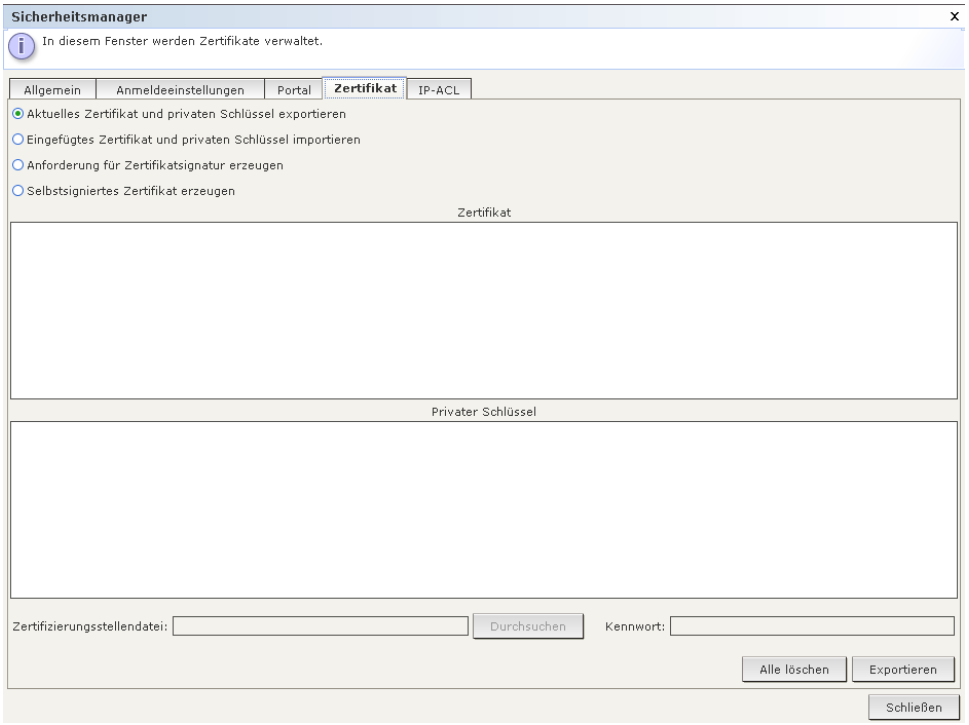


Abbildung 172 Registerkarte Zertifikat des Sicherheitsmanagers

Aktuelles Zertifikat und privaten Schlüssel exportieren

Klicken Sie auf **Aktuelles Zertifikat und privaten Schlüssel exportieren**. Das Zertifikat wird im Fensterbereich **Zertifikat** und der private Schlüssel im Fensterbereich **Privater Schlüssel** angezeigt. Kopieren Sie den Text in den Feldern **Zertifikat** und **Privater Schlüssel**, und übermitteln Sie ihn durch Klicken auf **Exportieren**.

Anforderung für Zertifikatsignatur erzeugen

Im folgenden Abschnitt wird erläutert, wie eine CSR und ein privater Schlüssel in CC-SG erzeugt werden. Die CSR wird an den Zertifikatserver übermittelt, der ein signiertes Zertifikat ausgibt. Außerdem wird ein Stammzertifikat vom Zertifikatserver exportiert und in einer Datei gespeichert. Das signierte Zertifikat, Stammzertifikat und der private Schlüssel werden dann importiert.

1. Klicken Sie auf **Anforderung für Zertifikatsignatur erzeugen** und dann auf **Erzeugen**. Das Fenster **Anforderung für Zertifikatsignatur erzeugen** wird angezeigt.
2. Geben Sie die erforderlichen Daten für die CSR in die Felder ein.

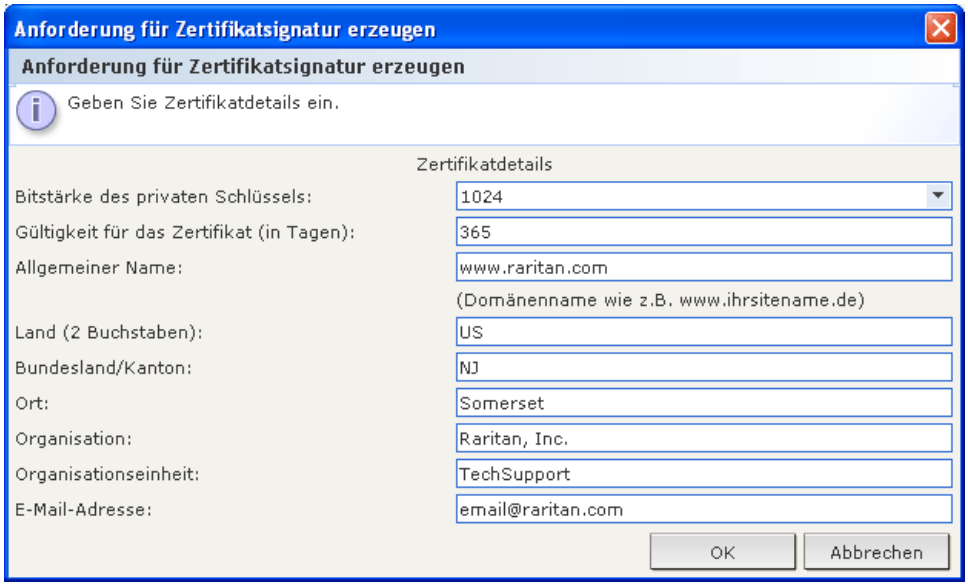


Abbildung 173 Fenster Anforderung für Zertifikatsignatur erzeugen

3. Klicken Sie zum Erzeugen der CSR auf **OK**, oder klicken Sie auf **Abbrechen**, um das Fenster zu schließen. Die CSR und der private Schlüssel werden in den entsprechenden Feldern im Fenster **Zertifikat** angezeigt.

Abbildung 174 Zertifikatsanforderung erzeugt

4. Öffnen Sie einen ASCII-Editor wie Editor, und kopieren Sie die CSR in eine Datei, die Sie dann mit der Erweiterung **.cer** speichern.
5. Öffnen Sie einen ASCII-Editor wie Editor, und kopieren Sie den privaten Schlüssel in eine Datei, die Sie dann als Textdatei speichern.
6. Übermitteln Sie die in Schritt 4 gespeicherte CSR-Datei (**.cer**) an den Zertifikatserver, um ein signiertes Zertifikat vom Server zu erhalten.
7. Laden Sie das Stammzertifikat vom Zertifikatserver herunter oder exportieren Sie es. Speichern Sie das Zertifikat dann in einer Datei mit der Erweiterung **.cer**. Dieses Zertifikat unterscheidet sich von dem signierten Zertifikat, das vom Zertifikatserver im nächsten Schritt ausgegeben wird.
8. Klicken Sie nach Erhalt des signierten Zertifikats vom Zertifikatserver auf **Eingefügtes Zertifikat und privaten Schlüssel importieren**.

9. Kopieren Sie das signierte Zertifikat in das Feld **Zertifikatsanforderung**. Fügen Sie den gespeicherten privaten Schlüssel in das Feld **Privater Schlüssel** ein.
10. Klicken Sie auf **Durchsuchen** neben **Zertifizierungsstellendatei:**, und wählen Sie die Stammzertifikatdatei aus, die in Schritt 6 gespeichert wurde.
11. Geben Sie **raritan** im Feld **Kennwort** ein, wenn die CSR von CC-SG erzeugt wurde. Wurde die CSR von einer anderen Anwendung erzeugt, verwenden Sie das Kennwort für diese Anwendung.

Hinweis: *Ist das importierte Zertifikat von einer Stamm- oder Substamm-Zertifizierungsstelle signiert, schlägt die Verwendung eines Stamm- oder Substamm-Zertifikats fehl. Sie können dieses Problem beheben, indem Sie das Stamm- und Substamm-Zertifikat in eine Datei kopieren und dann importieren.*

Selbstsigniertes Zertifikat erzeugen

Klicken Sie auf das Optionsfeld **Selbstsigniertes Zertifikat erzeugen** und anschließend auf **Erzeugen**. Das Fenster **Selbstsigniertes Zertifikat erzeugen** wird geöffnet. Geben Sie die erforderlichen Daten für das selbstsignierte Zertifikat in die Felder ein. Klicken Sie zum Erzeugen des Zertifikats auf **OK**, oder klicken Sie auf **Abbrechen**, um das Fenster zu schließen. Das Zertifikat und der private Schlüssel werden im Fenster **Zertifikat** verschlüsselt in den entsprechenden Feldern angezeigt.

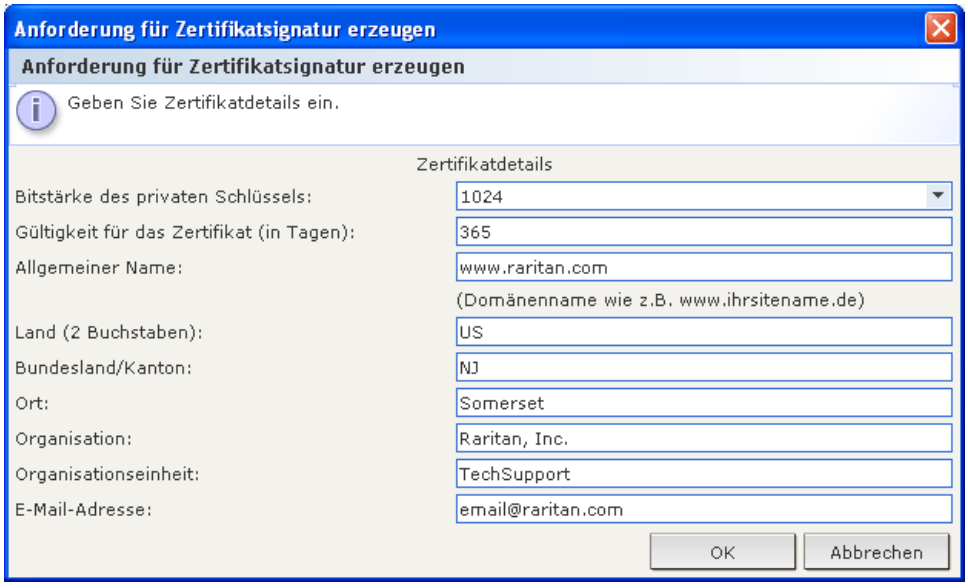


Abbildung 175 Fenster Selbstsigniertes Zertifikat erzeugen

IP-ACL

Diese Funktion schränkt den Zugriff auf CC-SG basierend auf IP-Adressen ein. Legen Sie eine IP-Zugriffssteuerliste (IP-ACL) fest, indem Sie einen IP-Adressenbereich; die Gruppe, für die dieser Bereich zutrifft, und eine Zulassen-/Verweigern-Berechtigung eingeben.

1. Klicken Sie im Menü **Administration** auf **Sicherheit**. Das Fenster **Sicherheitsmanager** wird angezeigt.

2. Klicken Sie auf die Registerkarte **IP-ACL**.

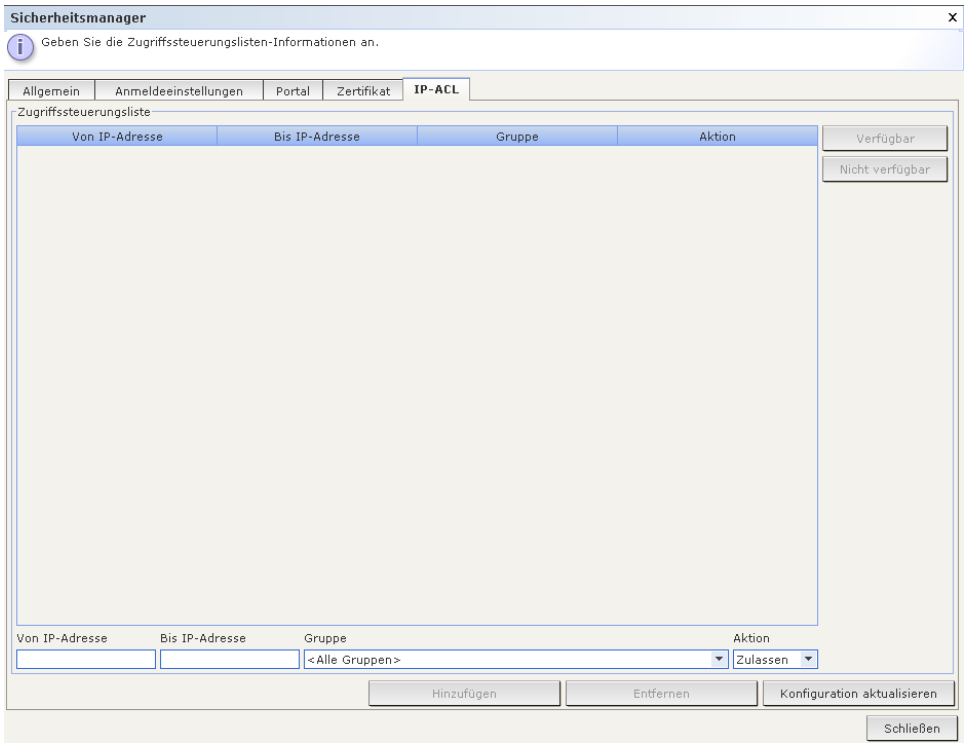


Abbildung 176 Registerkarte IP-ACL des Sicherheitsmanagers

3. Markieren Sie zum Ändern der Reihenfolge der Einträge in der **Zugriffssteuerungsliste** einen Eintrag, und klicken Sie auf **Nach oben** oder **Nach unten**. Die Verbindung von Benutzern wird entsprechend der ersten angewendeten Regel (von oben nach unten) gewährt oder verweigert.
4. Wenn Sie der Liste einen neuen Eintrag hinzufügen möchten, legen Sie einen Bereich fest, auf den die Regel angewendet werden soll. Geben Sie hierzu den Start-IP-Wert im Feld **Start-IP-Adresse** und den End-IP-Wert im Feld **End-IP-Adresse** ein.
5. Klicken Sie auf die Dropdown-Liste **Gruppe**, um eine Gruppe auszuwählen, auf die die Regel angewendet werden soll.
6. Klicken Sie auf die Dropdown-Liste **Aktion**, und gewähren oder verweigern Sie den Gruppenzugriff auf den IP-Adressbereich (**Zulassen** oder **Verweigern**).
7. Klicken Sie auf **Hinzufügen**, um die neue Regel der **Zugriffssteuerungsliste** hinzuzufügen.
8. Wenn Sie einen Eintrag entfernen möchten, wählen Sie ihn aus, und klicken Sie auf **Entfernen**.
9. Klicken Sie auf **Konfiguration aktualisieren**, um das System mit den neuen Zugriffssteuerungsregeln zu aktualisieren.

Benachrichtigungsmanager

Mit dem Benachrichtigungsmanager können Sie einen externen SMTP-Server so konfigurieren, dass Benachrichtigungen in CC-SG gesendet werden können. Benachrichtigungen werden verwendet, um Folgendes per E-Mail zu senden: geplante Berichte; Berichte, falls Benutzer gesperrt wurden, sowie Statusberichte erfolgreicher oder fehlgeschlagener geplanter Aufgaben. Weitere Informationen finden Sie unter **Aufgabenmanager** in diesem Kapitel. Nach der Konfiguration des SMTP-Servers können Sie eine Test-E-Mail an den festgelegten Empfänger senden und ihn über das Testergebnis informieren.

So konfigurieren Sie einen externen SMTP-Server:

1. Klicken Sie im Menü **Administration** auf **Benachrichtigungen**. Das Fenster **Benachrichtigungsmanager** wird angezeigt.

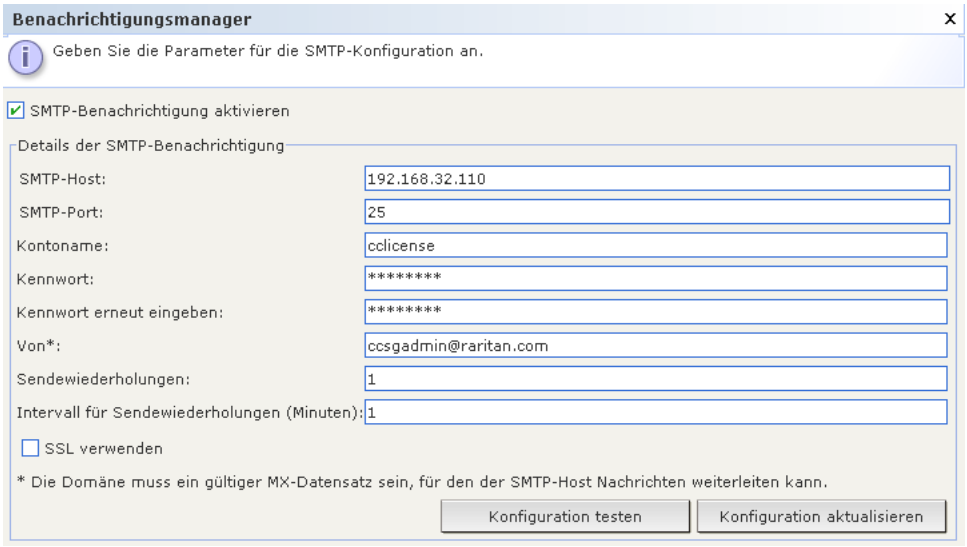


Abbildung 177 Benachrichtigungsmanager

2. Markieren Sie das Kontrollkästchen **SMTP-Benachrichtigung aktivieren**.
3. Geben Sie den SMTP-Host in das Feld **SMTP-Host** ein. Die Regeln zur Vergabe von Hostnamen werden unter **Terminologie/Abkürzungen** in **Kapitel 1: Einleitung** beschrieben.
4. Geben Sie eine gültige SMTP-Portnummer im Feld **SMTP-Port** ein.
5. Geben Sie einen gültigen Kontonamen in das Feld **Kontoname** ein, der zur Anmeldung beim SMTP-Server verwendet werden kann.
6. Geben Sie das Kennwort für das Konto in die Felder **Kennwort** und **Kennwort erneut eingeben** ein.
7. Geben Sie eine gültige E-Mail-Adresse im Feld **Von** ein, die kennzeichnet, dass die Nachricht von CC-SG ist.
8. Geben Sie in das Feld **Sendewiederholungen** die Anzahl von Wiederholungen ein, die die E-Mail erneut gesendet werden soll, falls der Vorgang fehlschlägt.
9. Geben Sie die Anzahl von Minuten von 1 bis 60 in das Feld **Intervall für Sendewiederholungen (Minuten)** ein, die verstreichen soll, bevor die E-Mail erneut gesendet wird.
10. Markieren Sie das Feld **SSL verwenden**, wenn Sie die E-Mail sicher über Secure Sockets Layer (SSL) senden möchten.
11. Klicken Sie auf **Konfiguration testen**, um eine Test-E-Mail an das angegebene SMTP-Konto zu senden. Sie sollten sicherstellen, dass die E-Mail empfangen wird.
12. Klicken Sie auf **Konfiguration aktualisieren**, um die Änderungen zu speichern.

Aufgabenmanager

Planen Sie tägliche, wöchentliche, monatliche oder jährliche CC-SG-Aufgaben mit dem Aufgabenmanager. Eine Aufgabe kann so geplant werden, dass sie nur einmal oder regelmäßig an einem bestimmten Wochentag oder in regelmäßigen Zeitabständen durchgeführt wird. Dazu gehören Gerätesicherungen alle drei Wochen an einem Freitag oder eine E-Mail jeden Montag an einen oder mehrere Empfänger.

***Hinweis**: Der Aufgabenmanager verwendet die Serverzeit, die in CC-SG zum Planen eingerichtet ist, und nicht die Zeit auf Ihrem Client-PC. Die Serverzeit wird oben rechts in jedem CC-SG-Bildschirm angezeigt.*

Aufgabenarten

Die folgenden Aufgaben können geplant werden:

- Gerätekonfiguration sichern (einzelne Geräte oder Gerätegruppen)
- Gerätekonfiguration wiederherstellen (gilt nicht für Gerätegruppen)
- Gerätekonfiguration kopieren (einzelne Geräte oder Gerätegruppen)
- Gerätefirmware aktualisieren (einzelne Geräte oder Gerätegruppen). Beachten Sie, dass die Firmware vor dem Planen dieser Aufgabe zur Verfügung gestellt werden muss.
- CC-SG sichern
- Gerät neu starten (gilt nicht für Gerätegruppen)
- Ausgangsport-Stromzufuhrverwaltung (Strom ein/aus/Ausgangsports ein-/ausschalten)
- Alle Berichte erzeugen (HTML- oder CSV-Format)
- Protokolle löschen

Aufeinander folgende Aufgaben planen

Sie können Aufgaben aufeinander folgend planen, um sicherzustellen, dass das erwartete Verhalten wirklich eingetreten ist. Sie können die Aufgabe „Gerätefirmware aktualisieren“ beispielsweise für eine bestimmte Gerätegruppe planen, dann direkt danach das Erstellen eines Anlagenverwaltungsberichts planen, um sicherzustellen, dass die richtige Version der Firmware verwendet wurde.

E-Mail-Benachrichtigungen

Nach dem Durchführen einer Aufgabe kann eine E-Mail-Nachricht an einen bestimmten Empfänger gesendet werden. Sie können im Benachrichtigungsmanager angeben, wo und wie die E-Mail gesendet wird (z. B. sicher über SSL). Weitere Informationen finden Sie unter **Benachrichtigungsmanager** in diesem Kapitel.

Geplante Berichte

Geplante Berichte werden per E-Mail an die festgelegten Empfänger gesendet.

Alle fertig gestellten Berichte werden in CC-SG 30 Tage lang gespeichert und können im HTML-Format über das Menü **Berichte** und **Gespeicherte Berichte anzeigen** aufgerufen werden. Weitere Informationen finden Sie in **Kapitel 10: Erstellen von Berichten, Geplante Berichte**.

Neue Aufgabe erstellen

So planen Sie eine neue Aufgabe:

1. Klicken Sie im Menü **Administration** auf **Aufgaben**. Das Fenster **Aufgabenmanager** wird angezeigt.

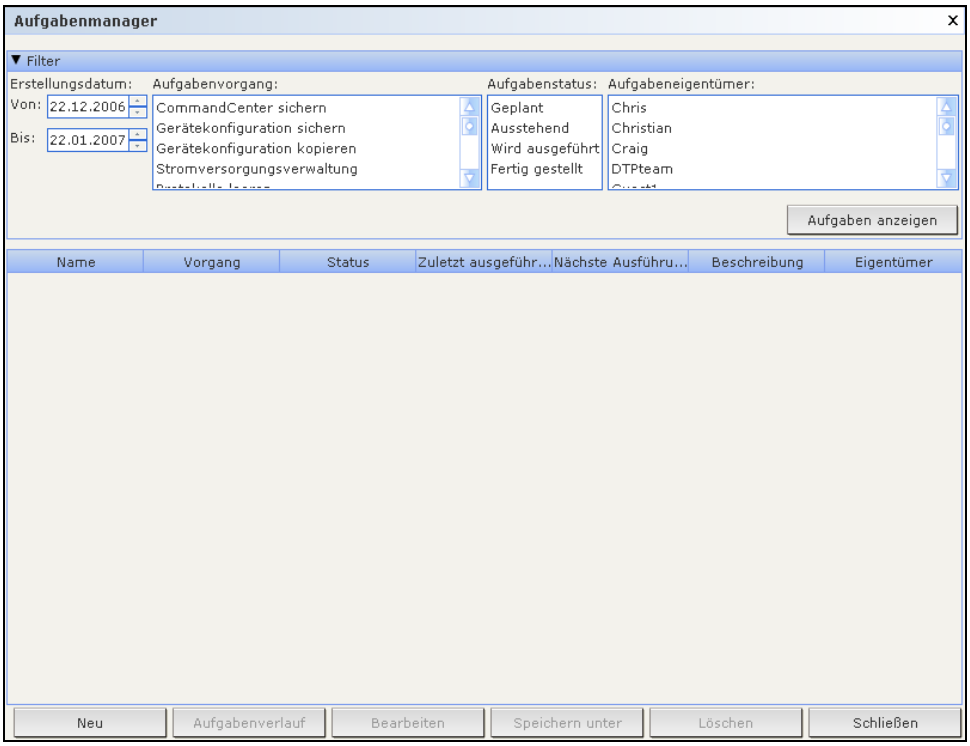


Abbildung 178 Aufgabenmanager

2. Klicken Sie auf **Neu**.
3. Geben Sie auf der Registerkarte **Hauptfenster** einen Namen (1-32 Zeichen, alphanumerische Zeichen oder Unterstriche, keine Leerstellen) und eine Beschreibung der Aufgabe ein.
4. Klicken Sie auf die Registerkarte **Aufgabendaten**.
5. Klicken Sie auf das Dropdown-Menü **Aufgabenvorgang**, und wählen Sie in der Liste die Aufgabe aus, die geplant werden soll (z. B. **Gerätefirmware aktualisieren**). Beachten Sie, dass die erforderlichen Felder von der ausgewählten Aufgabe abhängen.
6. Klicken Sie auf die Registerkarte **Serie**.
7. Klicken Sie im Feld **Zeitraum** auf das Optionsfeld, das dem Zeitraum entspricht, nach dem die geplante Aufgabe wieder ausgeführt werden soll.
   - **Einmal**: Wählen Sie über die Pfeile nach oben und unten die **Startzeit** für die Aufgabe aus.
   - **Periodisch**: Wählen Sie über die Pfeile nach oben und unten die **Startzeit** für die Aufgabe aus. Geben Sie im Feld **Wiederholungsanzahl** an, wie oft die Aufgabe ausgeführt werden soll. Geben Sie den Zeitraum im Feld **Wiederholungsintervall** ein, der zwischen Wiederholungen liegen soll. Klicken Sie auf das Dropdown-Menü, und wählen Sie die Zeiteinheit in der Liste aus.
   - **Täglich**: Klicken Sie auf das Optionsfeld neben **Täglich**, wenn die Aufgabe 7 Tage die Woche wiederholt werden soll. Klicken Sie auf das Optionsfeld neben **Werktags**, wenn die Aufgabe täglich von Montag bis Freitag wiederholt werden soll.
   - **Wöchentlich**: Wählen Sie über die Pfeile nach oben und unten aus, wie viele Wochen zwischen dem Ausführen der Aufgaben verstreichen sollen, und markieren Sie das Kontrollkästchen neben jedem Tag, an dem die Aufgabe in jeder Woche, in der sie ausgeführt wird, wiederholt werden soll.

- **Monatlich**: Geben Sie das Datum, an dem die Aufgabe ausgeführt werden soll, im Feld **Tage** ein, und markieren Sie das Kontrollkästchen neben jedem Monat, in dem die Aufgabe an dem bestimmten Datum wiederholt werden soll.
- **Jährlich**: Klicken Sie auf das Dropdown-Menü, und wählen Sie den Monat, in dem die Aufgabe ausgeführt werden soll, in der Liste aus. Wählen Sie über die Pfeile nach oben und unten den Tag im Monat aus, an dem die Aufgabe ausgeführt werden soll.

8. Bei den Aufgabenwerten **Täglich**, **Wöchentlich**, **Montlich** und **Jährlich** müssen Sie eine Start- und Endzeit für die Aufgabe im Bereich **Serienbereich** eingeben. Wählen Sie die Zeiten **Start um** und **Startdatum** über die Pfeile nach oben und unten aus. Klicken Sie auf das Optionsfeld neben **Kein Enddatum**, wenn die Aufgabe wie angegeben unbegrenzt ausgeführt werden soll. Sie können auch auf das Optionsfeld neben **Enddatum** klicken, und das Datum über die Pfeile nach oben und unten auswählen, ab dem die Aufgabe nicht mehr wiederholt wird.
9. Klicken Sie auf die Registerkarte **Wiederholen**.
10. Schlägt eine Aufgabe fehl, kann sie von CC-SG zu einem späteren Zeitpunkt wie auf der Registerkarte **Wiederholen** angegeben wiederholt werden. Geben Sie im Feld **Wiederholungsanzahl** an, wie oft CC-SG versuchen soll, die Aufgabe zu wiederholen. Geben Sie den Zeitraum, der zwischen Wiederholungen liegen soll, im Feld **Wiederholungsintervall** ein. Klicken Sie auf das Dropdown-Menü, und wählen Sie die Zeiteinheit in der Liste aus.

Wichtig: Wenn Sie eine Aufgabe zur Aktualisierung von SX- oder KX-Geräten planen, sollte das Wiederholungsintervall größer als 20 Minuten sein, da es ca. 20 Minuten dauert, diese Geräte erfolgreich zu aktualisieren.

11. Klicken Sie auf die Registerkarte **Benachrichtigung**.
12. Sie können E-Mail-Adressen angeben, die bei erfolgreichen oder fehlgeschlagenen Aufgaben eine Benachrichtigung erhalten. Standardmäßig wird die E-Mail-Adresse des Benutzers verwendet, der zurzeit angemeldet ist. Die E-Mail-Adressen der Benutzer werden im Benutzerprofil konfiguriert. Weitere Informationen finden Sie in **Kapitel 7: Hinzufügen und Verwalten von Benutzern und Benutzergruppen**. Um eine weitere E-Mail-Adresse hinzuzufügen, klicken Sie auf **Hinzufügen**, geben Sie die E-Mail-Adresse in das Fenster ein, und klicken Sie dann auf **OK**. Standardmäßig wird eine E-Mail gesendet, wenn die Aufgabe erfolgreich durchgeführt wurde. Markieren Sie das Kästchen **Bei Fehler**, um Empfänger über fehlgeschlagene Aufgaben zu unterrichten.
13. Klicken Sie auf **OK**, um die Aufgabe zu speichern.

Aufgaben, Aufgabendetails und Aufgabenverlauf anzeigen

So zeigen Sie eine Aufgabe an:

1. Klicken Sie im Menü **Administration** auf **Aufgaben**. Das Fenster **Aufgabenmanager** wird angezeigt.
2. Sie können nach Aufgaben suchen, indem Sie mit den Pfeiltasten nach oben und unten den Datumsbereich auswählen, in dem Sie suchen möchten. Sie können die Liste weiterhin filtern, indem Sie in jeder Liste eine oder mehrere (**Strg-Taste + klicken**) Aufgaben, Statusangaben oder Eigentümer auswählen. Klicken Sie auf **Aufgaben anzeigen**, um die gefilterte Liste der Aufgaben anzuzeigen.

- Zum Löschen von Aufgaben, wählen Sie die entsprechende Aufgabe aus, und klicken Sie auf **Löschen**.

***Hinweis**: Sie können keine Aufgaben löschen, die gerade ausgeführt werden.*

- Wählen Sie zum Anzeigen des Aufgabenverlaufs eine Aufgabe aus, und klicken Sie auf **Aufgabenverlauf**.
- Doppelklicken Sie auf eine Aufgabe, um weitere Details anzuzeigen.

- Sie können eine geplante Aufgabe bearbeiten, indem Sie die Aufgabe auswählen und das Fenster **Aufgabe bearbeiten** über **Bearbeiten** öffnen. Passen Sie die Aufgabenspezifikationen nach Bedarf an, und klicken Sie auf **Aktualisieren**. Eine Beschreibung der Registerkarte finden Sie im Abschnitt **Neue Aufgabe erstellen** in diesem Kapitel.
- Sie können eine neue Aufgabe basierend auf einer bereits konfigurierten Aufgabe erstellen. Wählen Sie die Aufgabe aus, die Sie kopieren möchten, und klicken Sie auf **Speichern unter**, um das Fenster **Speichern unter** anzuzeigen. Die Registerkarten werden mit den Informationen der bereits konfigurierten Aufgabe gefüllt. Passen Sie die Aufgabenspezifikationen nach Bedarf an, und klicken Sie auf **Aktualisieren**. Eine Beschreibung der Registerkarte finden Sie unter **Neue Aufgabe erstellen** in diesem Kapitel.

***Hinweis**: Wird eine Aufgabe geändert oder aktualisiert, wird der Verlauf ungültig und das „Datum letzte Ausführung“ ist leer.*

CommandCenter-NOC

Durch das Hinzufügen eines CommandCenter-NOC (CC-NOC, NOC = Netzwerkbetriebszentrum) zur Konfiguration können Sie Ihre Zielverwaltungsfunktionen um Überwachungs-, Berichterstattungs- und Warndienste für die seriellen und KVM-Zielsysteme erweitern. Weitere Informationen zur Installation und zum Betrieb Ihrer CC-NOC-Appliance finden Sie in der Dokumentation *CommandCenter NOC* von Raritan.

Wichtig: Im folgenden Vorgang werden Aktivierungscodes erzeugt. Sie müssen diese Aktivierungscodes dem CC-NOC-Administrator bereitstellen, der sie innerhalb von fünf Minuten in CC-NOC konfigurieren muss. Vermeiden Sie das Übertragen der Aktivierungscodes per E-Mail oder auf anderen elektronischen Wegen, um mögliches Abfangen von automatisierten Systemen zu vermeiden. Ein Telefongespräch oder der Austausch aufgeschriebener Codes zwischen vertrauten Parteien dient als besserer Schutz gegen automatisiertes Abfangen.

Ein CC-NOC hinzufügen

***Hinweis**: Damit Sie eine gültige Verbindung herstellen können, müssen die Zeiteinstellungen für CC-NOC und CC-SG synchronisiert werden. Die beste Methode zur Synchronisation ist die Verwendung eines gemeinsamen NTP-Servers (Network Time Protocol). Daher ist es erforderlich, dass CC-NOC und CC-SG so konfiguriert werden, dass sie einen NTP-Server verwenden.*

1. Klicken Sie im Menü **Zugriff** auf **CC-NOC-Konfiguration**. Das Fenster **CC-NOC-Konfiguration** wird angezeigt.
2. Klicken Sie auf **Hinzufügen**. Das Fenster **CC-NOC-Konfiguration hinzufügen** wird angezeigt.

3. Wählen Sie die Softwareversion von CC-NOC aus, die Sie hinzufügen möchten, und klicken Sie auf **Weiter**. Version 5.1 bietet weniger Integrationsfeatures als 5.2 und höher und erfordert nur das Hinzufügen eines Namens und einer IP-Adresse. Weitere Informationen zu CC-NOC 5.1 finden Sie unter **www.raritan.com/support**. Klicken Sie auf **Product Documentation** und dann auf **CommandCenter NOC**.

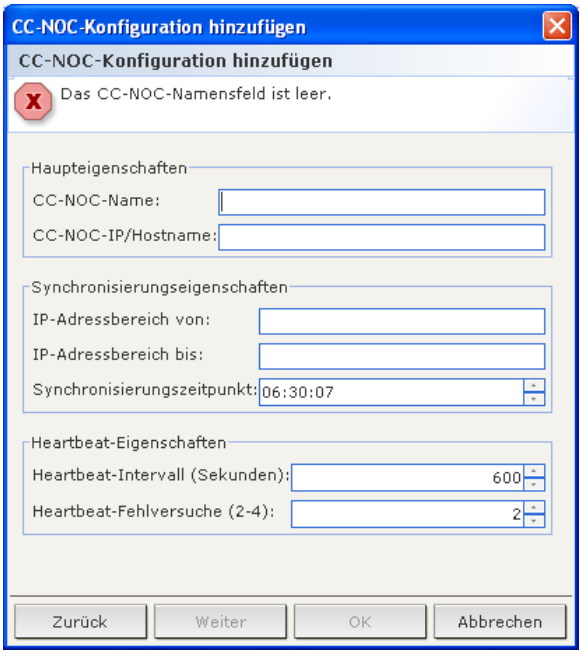


Abbildung 179 Fenster CC-NOC-Konfiguration hinzufügen

4. Geben Sie einen beschreibenden Namen für CC-NOC im Feld **Name** ein. Der Name darf aus maximal 50 alphanumerischen Zeichen bestehen.
5. Geben Sie die IP-Adresse oder den Hostnamen von CC-NOC im Feld **CC-NOC-IP/Hostname** ein. Dieses Feld muss ausgefüllt werden. Die Regeln zur Vergabe von Hostnamen sind unter **Terminologie/Abkürzungen** in **Kapitel 1: Einleitung** beschrieben.
6. Geben Sie zum Abrufen täglicher Informationen über Ziele in der CC-NOC-Datenbank einen Erkennungsbereich in die Felder **IP-Adressbereich von** und **IP-Adressbereich bis** ein. Dieser IP-Bereich stellt den Adressbereich dar, den CC-SG betrachtet, und weist CC-NOC an, Ereignisse für diese Geräte an CC-SG zu senden. Dieser Bereich ist mit dem Erkennungsbereich verknüpft, der in CC-NOC konfiguriert wurde. Weitere Informationen finden Sie im **CommandCenter NOC Handbuch für Administratoren** von Raritan. Beachten Sie beim Eingeben von Bereichen folgende Regeln:

IP-ADRESSBEREICH	BESCHREIBUNG
Wenn der hier eingegebene CC-SG-Bereich nur ein *Subset* des in CC-NOC konfigurierten Bereichs ist, …	… **dann** gibt CC-NOC alle bekannten Zielgeräteinformationen in diesem Bereich zurück.
Wenn der hier eingegebene CC-SG-Bereich eine *Teilliste* (gültige Schnittmenge) des in CC-NOC konfigurierten Bereichs enthält, …	… **dann** gibt CC-NOC alle bekannten Zielgeräteinformationen in diesem Schnittmengenbereich zurück.
Wenn der hier eingegebene CC-SG-Bereich ein *Superset* des in CC-NOC konfigurierten Bereichs ist, …	… **dann** gibt CC-NOC alle bekannten Zielgeräteinformationen in diesem Bereich zurück. Im Wesentlichen gibt CC-NOC Ziele zurück, die im CC-NOC-Bereich definiert sind.
Wenn der hier eingegebene CC-SG-Bereich keine *Übereinstimmung* mit dem in CC-NOC konfigurierten Bereich hat, …	… **dann** gibt CC-NOC keine Zielgeräteinformationen zurück.

Damit CC-NOC ein Gerät nicht mehr verwaltet, kann die *Verwaltung* entfernt werden. Weitere Informationen finden Sie im **CommandCenter NOC Handbuch für Administratoren**.

***Hinweis**: Verwenden Sie den Bericht **CC-NOC-Synchronisation**, um Ziele anzuzeigen, die CC-SG abonniert. In dem Bericht werden auch neue Ziele angezeigt, die von CC-NOC erkannt wurden. Weitere Informationen zum Bericht **CC-NOC-Synchronisation** finden Sie in **Kapitel 10: Erstellen von Berichten**.*

7. Geben Sie eine **Zeit für die Synchronisierung** an, um zu planen, wann die Zielinformationen in der CC-NOC-Datenbank abgerufen werden. Die Datenbanken werden aktualisiert, sobald Ziele erkannt oder nicht mehr verwaltet werden. Der Standardwert ist die aktuelle Uhrzeit auf dem Client-Computer. Sie sollten die Synchronisierung in einen Zeitraum mit geringer Auslastung legen, damit sie die Leistung anderer Prozesse nicht beeinträchtigt.
8. Geben Sie für **Heartbeat-Intervall** ein, wie oft (in Sekunden) CC-SG eine Heartbeat-Nachricht an CC-NOC sendet. Dadurch wird bestätigt, ob CC-NOC noch läuft und verfügbar ist. Der Standardwert ist **60** Sekunden. Der gültige Bereich liegt zwischen **30-120** Sekunden. Normalerweise muss dieser Wert nicht geändert werden.
9. Geben Sie für **Fehlgeschlagene Heartbeat-Versuche** die Anzahl der aufeinander folgenden Heartbeats an, die erfolgen muss, bevor ein Knoten von CC-NOC als nicht verfügbar eingestuft wird. Der Standardwert ist **2** Heartbeats. Der gültige Bereich liegt zwischen **2-4** Heartbeats. Normalerweise muss dieser Wert nicht geändert werden.
10. Klicken Sie auf **Weiter**.
11. Kopieren Sie die Aktivierungscodes entweder in die CC-NOC-Felder, wenn Sie der CC-NOC-Administrator sind, oder übermitteln Sie die zwei Aktivierungscodes an den CC-NOC-Administrator. Wie im **CommandCenter NOC Administrator Guide** beschrieben, gibt der CC-NOC-Administrator die Aktivierungscodes dann in CC-NOC ein. Dadurch wird ein Austausch von Sicherheitszertifikaten gestartet.

Wichtig: Zur Erhöhung der Sicherheit müssen Sie die Aktivierungscodes innerhalb von fünf Minuten in CC-NOC eingeben, nachdem sie in CC-SG erzeugt wurden. Dies minimiert das Zeitfenster für Unbefugte, die mit einem Brute-Force-Angriff in das System einzudringen versuchen. Vermeiden Sie das Übertragen der Aktivierungscodes per E-Mail oder auf anderen elektronischen Wegen, um mögliches Abfangen von automatisierten Systemen zu vermeiden. Ein Telefongespräch oder der Austausch aufgeschriebener Codes zwischen vertrauten Parteien dient als besserer Schutz gegen automatisiertes Abfangen.

12. Nach dem Austausch der Zertifikate ist ein sicherer Kanal zwischen CC-NOC und CC-SG hergestellt. Die CC-NOC-Daten werden in CC-SG kopiert. Klicken Sie zum Abschließen des Vorgangs auf **OK**. Wird der Vorgang nicht innerhalb von **5** Minuten abgeschlossen, werden die Daten nicht in CC-SG gespeichert und gespeicherte Zertifikate werden gelöscht. Versuchen Sie den Vorgang erneut ab Schritt 1 in **Ein CC-NOC hinzufügen** auf Seite 189.

***Hinweis**: CommandCenter-NOC kann nur Standalone- oder Primärknoten-CC-SG-Servern hinzugefügt werden.*

Ein CC-NOC bearbeiten

1. Klicken Sie im Menü **Zugriff** auf **CC-NOC-Konfiguration.** Das Fenster **CC-NOC-Konfiguration** wird angezeigt.
2. Markieren Sie ein CC-NOC in der Liste, und klicken Sie auf **Bearbeiten**. Das Fenster **CC-NOC-Konfiguration bearbeiten** wird angezeigt.
3. Ändern Sie die Konfiguration nach Bedarf. Weitere Informationsfelder finden Sie im vorherigen Abschnitt **Ein CC-NOC hinzufügen**.

CC-NOC starten

So starten Sie CC-NOC in CC-SG:

1. Klicken Sie im Menü **Zugriff** auf **CC-NOC-Konfiguration.**
2. Markieren Sie im Fenster **CC-NOC-Konfiguration** ein verfügbares CC-NOC.
3. Klicken Sie auf **Starten**. Dadurch wird eine Verbindung mit einem konfigurierten CC-NOC hergestellt.

Ein CC-NOC löschen

Führen Sie Folgendes aus, um ein CC-NOC in CC-SG zu entfernen und die Registrierung aufzuheben.

1. Klicken Sie im Menü **Zugriff** auf **CC-NOC-Konfiguration.** Das Fenster **CC-NOC-Konfiguration** wird angezeigt.
2. Wählen Sie in CC-SG ein CC-NOC aus, und klicken Sie auf **Löschen**. Sie werden aufgefordert, den Löschvorgang zu bestätigen.
3. Klicken Sie auf **Ja**, um das CC-NOC zu löschen. Das Löschen des CC-NOC wird durch eine entsprechende Meldung bestätigt.

SSH-Zugriff auf CC-SG

Verwenden Sie SSH-Clients (Secure Shell) wie Putty oder OpenSHH-Client, um auf eine Befehlszeilenschnittstelle auf SSH-Server (v2) auf CC-SG zuzugreifen. Nur ein Teil der CC-SG-Befehle zur Verwaltung von Geräten und CC-SG wird über SSH ausgegeben.

Der Benutzer des SSH-Clients wird von CC-SG authentifiziert, in dem vorhandene Authentifizierungs- und Autorisierungsrichtlinien auf den SSH-Client angewendet werden. Die für den SSH-Client verfügbaren Befehle werden von den Berechtigungen für die Benutzergruppen bestimmt, denen der Benutzer des SSH-Clients angehört.

Administratoren, die über SSH auf CC-SG zugreifen, können einen CC-Superuser SSH-Benutzer nicht abmelden, können jedoch alle anderen Benutzer von SSH-Clients, einschließlich Systemadministratoren, abmelden.

So greifen Sie auf CC-SG über SSH zu:

1. Starten Sie einen SSH-Client wie Putty.
2. Geben Sie die IP-Adresse von CC-SG und den Wert **22** für den Port ein. Öffnen Sie dann die Verbindung. Sie können den Port für den SSH-Zugriff im Sicherheitsmanager konfigurieren. Weitere Informationen finden Sie unter **Sicherheitsmanager** in diesem Kapitel.
3. Melden Sie sich bei Aufforderung mit Ihrem CC-SG-Benutzernamen und -Kennwort an.

4. Eine Shell-Eingabeaufforderung wird angezeigt. Geben Sie **ls** ein, um alle verfügbaren Befehle anzuzeigen. Sie können auch **?** oder **help** eingeben, um Beschreibungen und Formate zur Eingabe aller Befehle anzuzeigen.

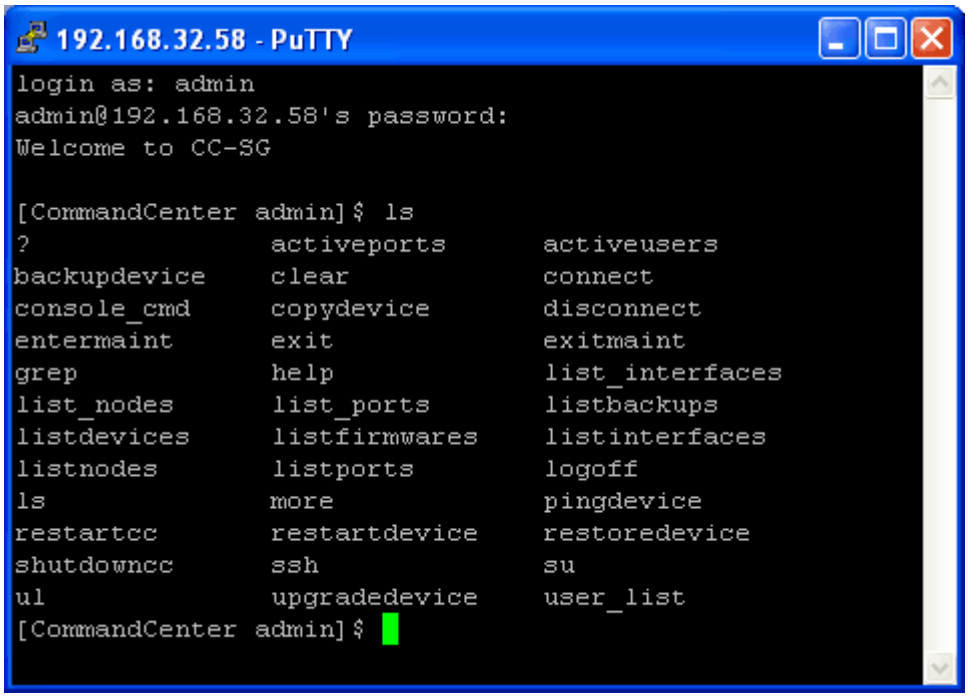


Abbildung 180 CC-SG-Befehle über SSH

SSH-Befehle

In der folgenden Tabelle sind alle verfügbaren SSH-Befehle aufgeführt. Sie müssen über die entsprechenden Berechtigungen in CC-SG verfügen, um auf jeden Befehl zugreifen zu können.

BEFEHL BESCHREIBUNG
activeports Führt aktive Ports auf.
activeusers Führt aktive Benutzer auf.
backup device <[-host <Host>] | [-id <Geräte-ID>]> backup_name [description] Sichert die Gerätekonfiguration.
clear Löscht den Bildschirm.
connect [-d <Gerätename>] [-e <Escape_Zeichen>] <[-i <Schnittstellen-ID>] | [-n <Portname>] | [Port-ID]> Stellt eine Verbindung zu einem seriellen Port her. Wenn <Portname> oder <Gerätename> Leerzeichen enthalten, sollten die Namen in Anführungszeichen eingeschlossen werden.
copydevice <[-b <Sicherungs-ID>] | [source_device_host]> target_device_host Kopiert die Gerätekonfiguration.
disconnect <[-u <Benutzername>] [-p <Port-ID>] [-id <Verbindungs-ID>]> Schließt die Portverbindung.
entermaint minutes [message] Startet den CC-SG-Wartungsmodus.
exitmaint Beendet den Wartungsmodus für CommandCenter.
grep search_term Suchtext des Piped Output Stream.
help Zeigt das Hilfefenster an.
listbackups <[-id <Geräte-ID>] | [host]> Führt verfügbare Sicherungen für Gerätekonfigurationen auf.
listdevices Führt verfügbare Geräte auf.
listfirmwares [[-id <Geräte-ID>] | [host]] Führt Firmwareversionen auf, die zur Aktualisierung verfügbar sind.
listinterfaces [-id <Knoten-ID>] Führt alle Schnittstellen auf.
listnodes Führt alle Knoten auf.
listports [[-id <Geräte-ID>] | [host]] Führt alle Ports auf.
logoff [-u <Benutzername>] message Meldet den Benutzer ab.
ls Führt die Befehle auf.

more [-p <Seitengröße>] Zeigt mehr Daten an.
pingdevice <[-id <Geräte-ID>] | [host]> Pingt Gerät an.
restartcc minutes [message] Startet CC-SG neu.
restartdevice <[-id <Geräte-ID>] | [host]> Startet Gerät neu.
restoredevice <[-host <Host>] | [-id <Geräte-ID>]> [backup_id] Stellt die Gerätekonfiguration wieder her.
shutdowncc minutes [message] Fährt CC-SG herunter.
ssh [-e <Escape_Zeichen>] <[-id <Geräte-ID>] | [host]> Öffnet eine SSH-Verbindung zu einem SX-Gerät.
su [-u <Benutzername>] Ändert einen Benutzer.
upgradedevice <[-id <Geräte-ID>] | [host]> Aktualisiert die Gerätefirmware.
exit Beendet die SSH-Sitzung.

Geben Sie einen Befehl mit dem Switch **-h** ein, wird die Hilfe für den Befehl angezeigt (z. B. **listfirmwares -h**).

Tipps zu Befehlen

Im Folgenden werden einige Unterschiede zwischen SSH-Befehlen beschrieben:

- Bei Befehlen, die eine IP-Adresse weiterleiten (z. B. upgradedevice), können Sie den Hostnamen für eine IP-Adresse einsetzen. Die Regeln zur Vergabe von Hostnamen werden unter Terminologie/Abkürzungen in **Kapitel 1: Einleitung** beschrieben.
- Die Befehle copydevice und restartdevice gelten nur für einige Raritan-Geräte wie Dominion SX. IPMI-Server und generische Geräte unterstützen diese Befehle nicht.

SSH-Verbindung zu einem SX-Gerät herstellen

Sie können eine SSH-Verbindung zu einem SX-Gerät herstellen, um administrative Aufgaben auf dem Gerät durchzuführen. Nach dem Verbindungsaufbau stehen die administrativen Befehle zur Verfügung, die vom SX-Gerät unterstützt werden.

***Hinweis**: Stellen Sie vor der Verbindung sicher, dass das SX-Gerät zu CC-SG hinzugefügt wurde.*

1. Geben Sie **`listdevices`** ein, um sicherzustellen, dass das SX zu CC-SG hinzugefügt wurde.

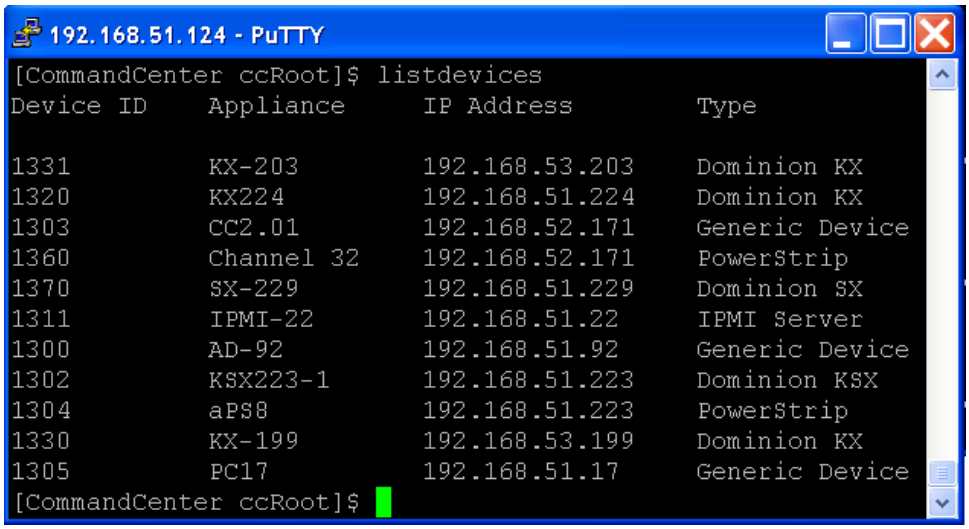


Abbildung 181 Geräte in CC-SG aufführen

2. Stellen Sie eine Verbindung zum SX-Gerät her, indem Sie **`ssh -id <Geräte-ID>`** eingeben. Für das oben gezeigte Beispiel können Sie eine Verbindung zu SX-229 herstellen, indem Sie **`ssh -id 1370`** eingeben.

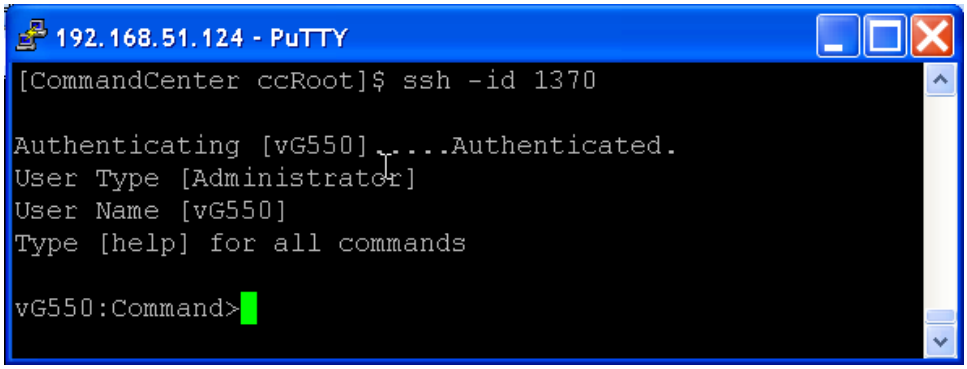


Abbildung 182 Auf das SX-Gerät über SSH zugreifen

Verbindung zum Knoten mit SSH über serielle Out-of-Band-Schnittstelle herstellen

Sie können SSH verwenden, um eine Verbindung zu einem Knoten über die zugewiesene serielle Out-of-Band-Schnittstelle herzustellen. Die SSH-Verbindung ist im Proxymodus.

1. Geben Sie **`listinterfaces`** ein, um die Knoten-IDs und verknüpften Schnittstellen anzuzeigen.

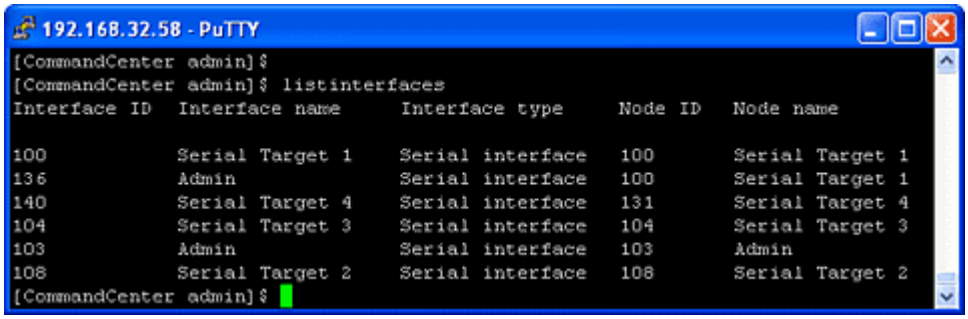


Abbildung 183 Listinterfaces in SSH

2. Geben Sie **`connect -i <Schnittstellen-ID>`** ein, um eine Verbindung zu dem Knoten herzustellen, der mit der Schnittstelle verknüpft ist.

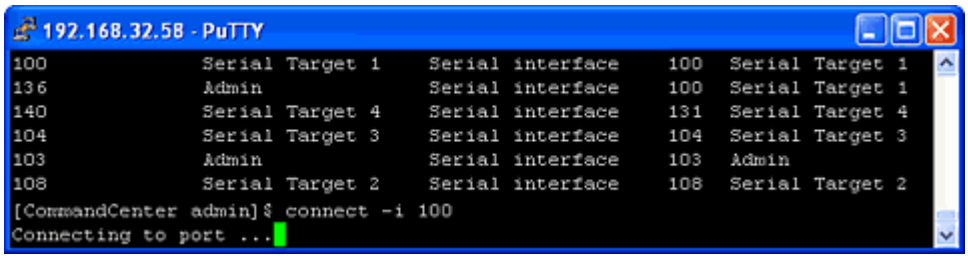


Abbildung 184 Verbindung zum Knoten über serielle Out-of-Band-Schnittstelle herstellen

3. Geben Sie nach dem Verbindungsaufbau zum Knoten die standardmäßigen Escape-Tastenfolge „~“ gefolgt von „.“ ein. Bei der angezeigten Eingabeaufforderung können Sie bestimmte Befehle oder Aliasse wie unten beschrieben eingeben:

BEFEHL	ALIAS	BESCHREIBUNG
quit	**q**	Trennt die Verbindung, und wechselt zur SSH-Eingabeaufforderung.
get_write	**gw**	Richtet den Schreibzugriff ein. SSH-Benutzer können Befehle auf dem Zielserver ausführen, während Browser-Benutzer den Vorgang nur beobachten können.
get_history	**gh**	Ruft die Verlaufsdaten ab. Zeigt die letzten Befehle und Ergebnisse für den Zielserver an.
send_break	**sb**	Sendet einen Pausebefehl. Unterbricht die Schleife auf dem Zielserver, die vom Browser-Benutzer gestartet wurde.
help	**?,h**	Zeigt das Hilfefenster an.

Sitzungen beenden

Sie können die Verbindung zwischen SSH und CC-SG trennen, indem Sie **`exit`** eingeben.

Diagnosekonsole

Die Diagnosekonsole ist eine standardmäßige, nicht grafische Schnittstelle, die lokalen Zugriff auf CC-SG bereitstellt. Der Zugriff erfolgt über einen seriellen oder KVM-Port oder über SSH-Clients (Secure Shell) wie Putty oder OpenSSH-Client.

Zwei gültige Anmeldenamen stehen bereit: **status** für Zugriff auf die Statuskonsole und **admin** für Zugriff auf die Administratorkonsole. Bei allen Benutzernamen und Kennwörtern zur Anmeldung wird die Groß- und Kleinschreibung berücksichtigt.

Die Statuskonsole

Laut Standardkonfiguration ist kein Kennwort für die Statuskonsole erforderlich. Melden Sie sich im Anmeldedialogfeld mit **status** an, um die aktuellen Systeminformationen anzuzeigen. Sie können den Zustand von CC-SG feststellen, die verschiedenen Dienste, die von CC-SG verwendet werden, sowie die verknüpften Netzwerke anzeigen.

Die Administratorkonsole

Der Standardbenutzername und das Kennwort für die Administratorkonsole lauten **admin**/**raritan**. Über das Konto **admin** können Sie Anfangsparameter festlegen, Erstkonfigurationen für das Netzwerk bereitstellen, Protokolldateien debuggen, einige eingeschränkte Diagnosefunktionen ausführen und CC-SG neu starten. Das Konto **admin** der Diagnosekonsole unterscheidet sich von dem Konto **admin** und dem Kennwort, die für den CC-SG-Administrations-Client und den HTML-basierten Zugriffs-Client verwendet werden. Sie können für beide Konten ein Kennwort oder verschiedene Kennwörter einrichten. Wenn Sie ein Kennwort ändern, wird das andere davon nicht betroffen.

***Hinweis**: Wenn Sie über SSH auf die Diagnosekonsole zugreifen, übernehmen die Statuskonsole und Administratorkonsole die, die in Ihrem SSH-Client konfigurierten Anzeigeeinstellungen sowie die Tastaturbindungen. Dies entspricht ggf. nicht in allen Punkten dieser Dokumentation.*

Auf die Diagnosekonsole über VGA-/Tastatur-/Mausport zugreifen

1. Schließen Sie einen VGA-Monitor sowie eine PS2-Tastatur und -Maus auf der Rückseite der CC-SG-Einheit an.
2. Das Videosignal sollte automatisch erkannt werden. Drücken Sie die **Eingabetaste** auf der Tastatur, um den Anmeldebildschirm anzuzeigen:

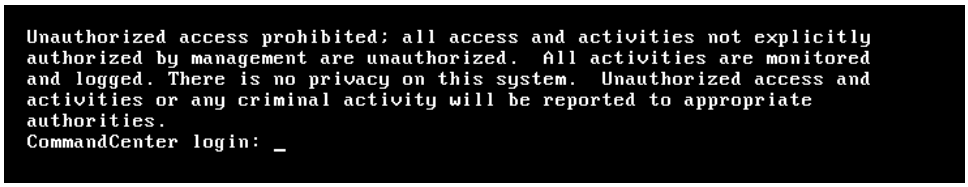


Abbildung 185 Bei der Diagnosekonsole anmelden

Über SSH auf die Diagnosekonsole zugreifen

1. Starten Sie einen SSH-Client wie Putty auf einem Client-PC, der über Netzwerkkonnektivität zu CC-SG verfügt.
2. Geben Sie eine IP-Adresse oder einen IP-Hostnamen von CC-SG ein, wenn CC-SG mit einem DNS-Server registriert wurde, und legen Sie **23** für den Port fest.
3. Klicken Sie auf die Schaltfläche zum Verbinden. Ein Fenster zur Eingabe der Anmeldeinformationen wird angezeigt.

Auf die Statuskonsole zugreifen

Ein Kennwort ist für den Zugriff auf die Statuskonsole nicht erforderlich, die Verwendung von Kennwörtern kann jedoch aktiviert werden.

1. Geben Sie beim Anmeldebildschirm **status** ein. Die Statuskonsole wird mit Lesezugriff angezeigt.

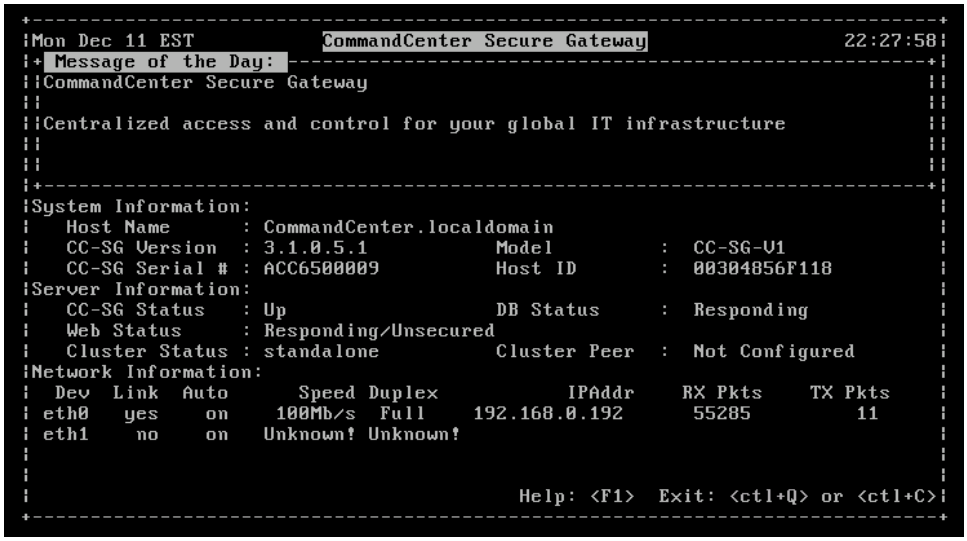


Abbildung 186 Statuskonsole

- In diesem Fenster werden Informationen dynamisch angezeigt, damit Sie den Zustand Ihres Systems bestimmen und prüfen können, ob CC-SG und die Unterkomponenten funktionieren.
- Die Zeitangabe oben rechts im Fenster stellt den Zeitpunkt dar, an dem die CC-SG-Daten das letzte Mal abgerufen wurden.
- Die Informationen auf diesem Bildschirm werden ca. alle 5 Sekunden aktualisiert.
- Drücken Sie **STRG+L**, um den aktuellen Bildschirm zu löschen und aktualisierte Informationen anzuzeigen. Sie können den Bildschirm höchstens einmal pro Sekunde aktualisieren.
- Drücken Sie **STRG+Q** oder **STRG+C**, um den Bildschirm zu schließen.
- Die Statuskonsole akzeptiert keine anderen Eingabewerte oder Navigationsbefehle. Alle anderen Eingabeversuche werden ignoriert.

In der folgenden Tabelle sind die Statuszustände für CC-SG und die CC-SG-Datenbank beschrieben:

STATUS	BESCHREIBUNG
CC-SG Status: Verfügbar	CC-SG ist verfügbar.
CC-SG Status: Nicht verfügbar	CC-SG wird ggf. neu hochgefahren. Hält der Status Nicht verfügbar an, versuchen Sie, CC-SG neu zu starten.
CC-SG Status: Restarting (Neu starten)	CC-SG wird neu gestartet.
DB Status: Responding (Antwortet)	CC-SG-Datenbank ist verfügbar.
DB Status: Nicht verfügbar	CC-SG wird ggf. neu hochgefahren.

Auf die Administratorkonsole zugreifen

***Hinweis**: Die Informationen, die in der Administratorkonsole angezeigt werden, sind statisch. Werden Konfigurationsänderungen über die grafische Benutzeroberfläche von CC-SG oder die Diagnosekonsole vorgenommen, müssen Sie sich bei der Administratorkonsole erneut anmelden, nachdem die Änderungen übernommen wurden, um sie in der Administratorkonsole anzuzeigen.*

1. Geben Sie beim Anmeldebildschirm **admin** ein.
2. Geben Sie Ihr CC-SG-**Kennwort** ein. Das Standardkennwort lautet **raritan**. Nach der ersten Anmeldung läuft dieses Kennwort ab, und Sie müssen ein neues festlegen. Geben Sie dieses Kennwort ein, und geben Sie bei Aufforderung ein neues Kennwort ein. Weitere Informationen zum Einstellen der Sicherheitsstufe des Kennworts finden Sie in diesem Kapitel unter **Kennwörter für die Diagnosekonsole (Admin)**.
3. Der Hauptbildschirm der Administratorkonsole wird angezeigt. Sie können Erstkonfigurationseinstellungen für die Systemnetzwerkschnittstelle vornehmen, den Tipp des Tages im Statusfenster ändern und Protokolldateien anzeigen. Sie können die Administratorkonsole über das Dateimenü verlassen:

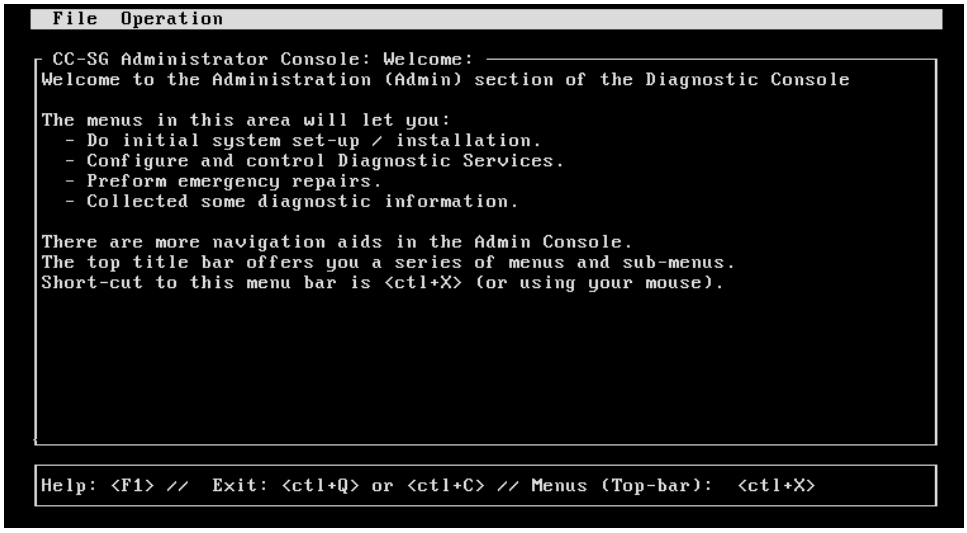


Abbildung 187 Administratorkonsole

Die Administratorkonsole navigieren

In der folgenden Tabelle sind die verschiedenen Navigationsmöglichkeiten für die Menüs der Diagnosekonsole aufgeführt. In einigen Sitzungen (besonders SSH) können Sie auch mit der Maus in den verschiedenen Formularen navigieren. Ggf. funktioniert dies jedoch nicht bei allen SSH-Clients oder bei der KVM-Konsole.

TASTEN	BESCHREIBUNG:
STRG+C oder STRG+Q	Schließen der Diagnosekonsole.
STRG+L	Löschen des Bildschirms und erneutes Anzeigen der Informationen (die Informationen werden jedoch nicht aktualisiert).
TABULATOR	Wechseln zur nächsten verfügbaren Option.
LEERTASTE	Auswählen der aktuellen Option.
Pfeiltasten	Wechseln zu anderen Felder einer Option.
Maus	Zeigen auf und Auswählen von Optionen, falls vorhanden.

Vertragliche Einschränkungen der Serviceleistungen und Tipp des Tages in der Diagnosekonsole bearbeiten

Die Meldung zu vertraglichen Einschränkungen der Serviceleistungen (RSA) wird in der Administratorkonsole nach der Eingabe eines Benutzernamens zur Anmeldung und vor der Eingabe eines Kennworts angezeigt. Der Tipp des Tages (MOTD) wird oben in der Statuskonsole angezeigt.

1. Klicken Sie zum Bearbeiten der RSA- (wird auch als Pre-Login Message in der Diagnostic Console bezeichnet) oder MOTD-Nachricht auf **Operation**, **Diagnostic Console Config** und dann auf **Edit Pre-Login Message** oder **Edit MOTD**.

2. Verwenden Sie die Tasten **Löschen** und **Rücktaste**, und geben Sie in das bereitgestellte Feld eine neue Nachricht ein. Für MOTD können Sie höchstens 76 Zeichen eingeben.

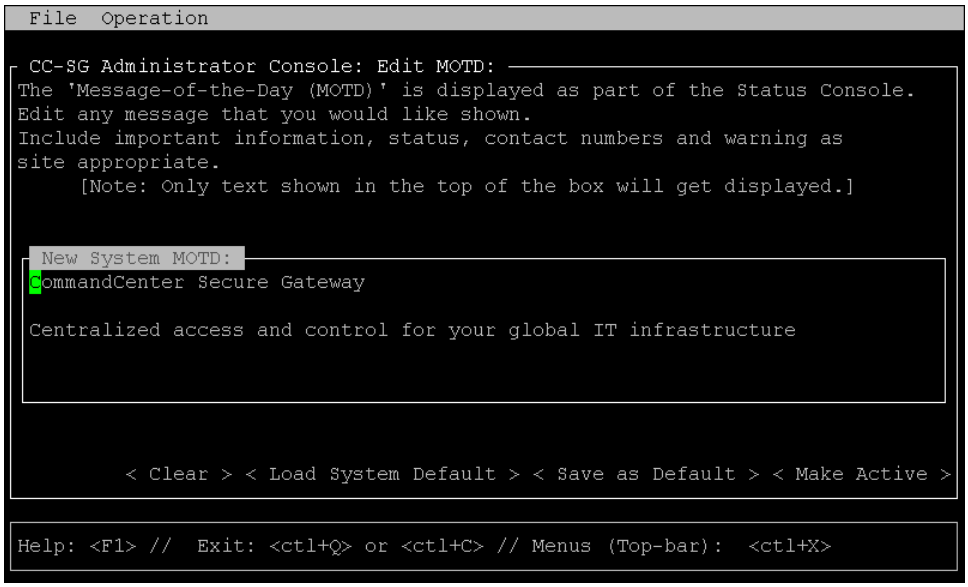


Abbildung 188 MOTD für die Statuskonsole bearbeiten

3. Klicken Sie unten im Bildschirm auf **Make Active**, oder drücken Sie die Tabulatortaste, bis **Make Active** ausgewählt ist, und drücken Sie die **Leertaste**.
4. Die Pre-Login-Nachricht und der Tipp des Tages verfügen über drei getrennte Puffer oder Bereiche:

- Fenster der Administratorkonsole: Beginnt mit einer Kopie des Puffers für Aktive-Nachricht und kann von diesem Benutzer/dieser Sitzung bearbeitet werden.
- Der Systempuffer mit einer Vorlage oder Modellnachricht für das gesamte System wird zurückgesetzt.
- Der Puffer für Aktive-Nachricht (wird dem Benutzer bei der Interaktion mit dem System angezeigt). Die Daten bleiben auch beim erneuten Starten oder Hochfahren des gesamten Systems erhalten.

SCHALTFLÄCHE	BESCHREIBUNG
Löschen	Löscht den Text, der im Fenster der Administratorkonsole angezeigt wird. Hat keinen Einfluss auf den Wert, der vom System verwendet wird.
Load System Default	Ersetzt das Fenster der Administratorkonsole mit dem Inhalt des Systempuffers.
Save as Default	Kopiert das aktuelle Fenster der Administratorkonsole in den Systempuffer. Hat keinen Einfluss auf die Aktive-Nachricht-Anzeige.
Make Active	Ersetzt die aktuelle Aktive-Nachricht mit dem Inhalt des Fensters der Administratorkonsole. Alle neuen Benutzer sehen die neue Nachricht.

Konfiguration der Diagnosekonsole bearbeiten

Die Diagnosekonsole kann über den seriellen Port (COM1), den KVM-Port oder über SSH-Clients (Secure Shell) aufgerufen werden. Sie können für jeden Porttyp konfigurieren, ob Benutzer sich über **status** oder **admin** anmelden können und ob Field Support über den Port auf die Diagnosekonsole zugreifen kann. Bei SSH-Clients können Sie außerdem konfigurieren, welche Portnummer verwendet werden sollte. Dies ist jedoch nur möglich, falls kein anderer CC-SG-Dienst den gewünschten Port verwendet.

So bearbeiten Sie die Konfiguration der Diagnosekonsole:

1. Klicken Sie auf **Operation**, **Diagnostic Console Config** und dann auf **Diagnostic Console Service**.
2. Verwenden Sie die Tabulator-, ↓↑- und Eingabetasten, um zu bestimmen, welche Elemente in der Diagnosekonsole konfiguriert und verfügbar sein sollen. Es stehen drei Zugriffsmethoden für die Diagnosekonsole zur Verfügung: Serieller Port (COM1), KVM-Konsole, SSH (IP-Netzwerk). Die Diagnosekonsole bietet drei Dienste: Status-Anzeige, Administratorkonsole, Raritan Field Support. In diesem Fenster können Sie auswählen, welche Dienste über die verschiedenen Zugriffsmethoden zur Verfügung stehen.
3. Geben Sie die Portnummer für den SSH-Zugriff auf die Diagnosekonsole in das Feld **Port** ein. Der Standardport lautet **23**.

Wichtig: Stellen Sie sicher, dass Sie nicht den Admin- oder Field Support-Zugriff vollständig sperren.

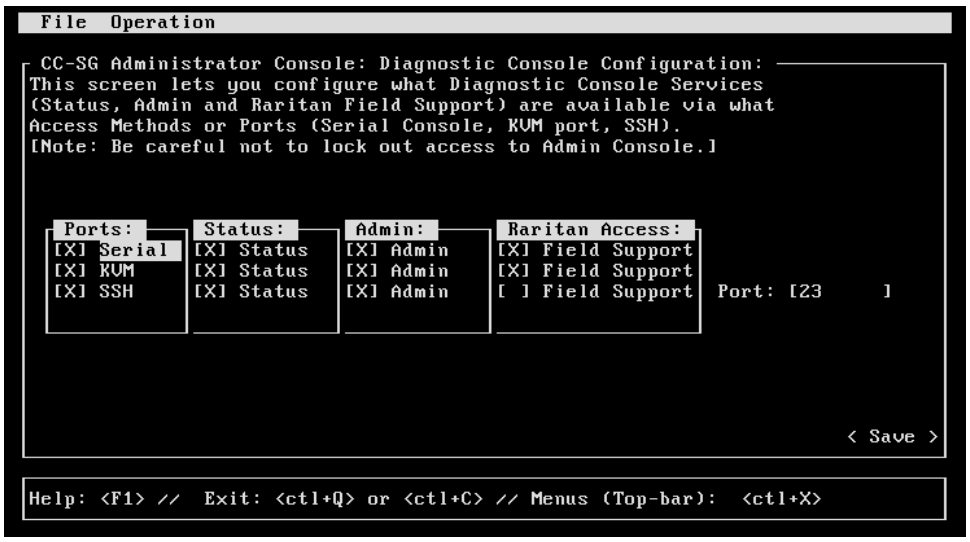


Abbildung 189 Konfiguration der Diagnosekonsole bearbeiten

4. Klicken Sie unten im Bildschirm auf **Save**, oder drücken Sie die **Tabulatortaste**, bis die Option **Save** hervorgehoben ist, und drücken Sie dann die **Eingabetaste**.

Netzwerkschnittstellenkonfiguration bearbeiten (Network Interfaces)

Über die Netzwerkschnittstellenkonfiguration können Sie Erstkonfigurationsaufgaben wie die Einstellung des Hostnamens und der IP-Adresse von CC-SG durchführen. Klicken Sie zum Navigieren mit der Maus, oder verwenden Sie die **Tabulator-** und Pfeiltasten. Drücken Sie die **Eingabetaste**, um einen Wert auszuwählen.

1. Klicken Sie zum Bearbeiten der Informationen der Netzwerkschnittstelle auf **Operation**, **Network Interfaces** und dann auf **Network Interface Config**.

2. Wurden die Netzwerkschnittstellen bereits konfiguriert, wird ein **Warnhinweis** angezeigt, dass Sie die grafische Benutzeroberfläche von CC-SG (Administrations-Client) zur Konfiguration der Schnittstellen verwenden sollten. Klicken Sie zum Fortfahren auf **YES**. Der Standardbildschirm der Netzwerkschnittstellenkonfiguration wird wie folgt angezeigt:

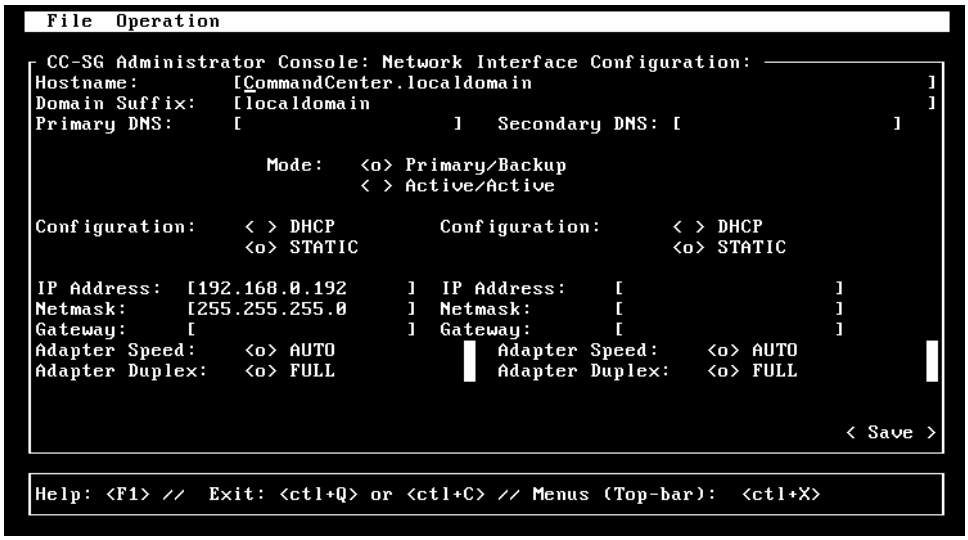


Abbildung 190 Netzwerkschnittstellen bearbeiten

3. Geben Sie Ihren Hostnamen im Feld **Host Name** ein. Nach dem Speichern wird das Feld aktualisiert, um den vollständig qualifizierten Domänennamen (Fully-Qualified Domain Name, FQDN), falls bekannt, anzuzeigen. Die Regeln zur Vergabe von Hostnamen werden unter **Terminologie/Abkürzungen** in **Kapitel 1: Einleitung** beschrieben.
4. Wählen Sie im Modusfeld **Primary/Backup Mode** oder **Active/Active Mode** aus. Weitere Informationen finden Sie in diesem Kapitel unter **Netzwerkkonfiguration.** Wählen Sie das Feld mit der Tabulatortaste aus, und wechseln Sie mithilfe der Pfeiltasten zwischen den beiden Moduseinstellungen. Drücken Sie zur Auswahl des Modus die **Leertaste**.
5. Klicken Sie mit der Maus, oder verwenden Sie die Tabulatortaste, um im Feld **Configuration** die Option **DHCP** oder **Static** in der Liste auszuwählen.
   - Wenn Sie **DHCP** auswählen und Ihr DHCP-Server richtig konfiguriert ist, werden die DNS-Informationen, das Domänensuffix, die IP-Adresse, das Standardgateway und die Subnetzmaske automatisch ausgefüllt, nachdem Sie **Save** ausgewählt und die Administratorkonsole verlassen und erneut aufgerufen haben.
   - Wenn Sie **Static** ausgewählt haben, geben Sie Werte für **IP Address** (erforderlich), **Netmask** (erforderlich), **Default Gateway** (optional), **Primary DNS** (optional) und **Secondary DNS** (optional) sowie den Domänennamen in **Domain Suffix** (optional) ein.
   - Auch wenn die IP-Konfiguration einer Schnittstelle durch DHCP bestimmt wird, müssen die richtig formatierten Werte für **IP address** und **Netmask** bereitgestellt werden.
6. Verwenden Sie die Tabulatortaste oder klicken Sie auf **Adapter Speed**, und verwenden Sie die Tasten ↓↑, um eine Geschwindigkeit in der Liste auszuwählen. Die Werte 10, 100 und 1.000 Mbps werden in einer Liste aufgeführt (in der nur ein Wert gleichzeitig angezeigt wird). Verwenden Sie die Pfeiltasten ↓↑, um die Werte anzuzeigen. Die **Leertaste** dient zur Auswahl eines anderen Wertes (falls erwünscht).
7. Wenn Sie die Option **AUTO** nicht für **Adapter Speed** ausgewählt haben, klicken Sie auf **Adapter Duplex**, und verwenden Sie die Tasten ↓↑, um einen Duplexmodus (**FULL** oder **HALF**) in der Liste auszuwählen (falls vorhanden). Sie können den Duplexmodus jederzeit auswählen. Er gilt jedoch nur, wenn **Adapter Speed** nicht auf **AUTO** festgelegt ist.
8. Wiederholen Sie diese Schritte für die zweite Netzwerkschnittstelle, wenn **Active/Active Mode** aktiviert ist.

9. Klicken Sie auf **Save**, um die Änderungen zu speichern. CC-SG wird erneut gestartet und meldet alle Benutzer der grafischen Benutzeroberfläche von CC-SG ab und beendet ihre Sitzung. Ein Warnhinweis wird angezeigt, der auf die bevorstehende Netzwerkkonfiguration und die damit verbundenen Auswirkungen auf CC-SG-Benutzer hinweist. Wählen Sie zum Fortfahren <**YES**> aus.
10. Der Systemstatus kann über ein Statusfenster der Diagnosekonsole überwacht werden. Am KVM-Port können Sie eine andere Terminalsitzung auswählen, indem Sie <**ALT**>+<**F2**> drücken und sich mit **status** anmelden. Sie können die ursprüngliche Terminalsitzung wieder anzeigen, indem Sie <**ALT**>+<**F1**> drücken. Sechs verfügbare Terminalsitzungen sind über <**F1**> bis <**F6**> verfügbar. Bei SSH-Zugriff können Sie eine andere SSH-Sitzung über den Client starten und sich über das Konto **status** anmelden. Wenn Konnektivität bei der Netzwerkkonfiguration zugelassen ist, sollten keine Probleme auftreten.

IP-Adresse anpingen (Network Interfaces)

Prüfen Sie mit der Ping-Funktion, ob alle Verbindungen zwischen Ihrem CC-SG-Computer und einer bestimmten IP-Adresse richtig funktionieren.

Hinweis: *Einige Sites sperren Ping-Anfragen ausdrücklich. Stellen Sie sicher, dass das Zielnetzwerk und das dazwischenliegende Netzwerk Ping-Anfragen zulassen, bevor Sie davon ausgehen, dass ein Fehler vorliegt.*

1. Klicken Sie auf **Operation**, **Network Interfaces** und dann auf **Ping**.
2. Geben Sie die IP-Adresse oder den Hostnamen (falls DNS richtig auf CC-SG konfiguriert ist) des Ziels in das Feld **Ping Target** ein.
3. Optional können Sie Folgendes auswählen:

OPTION	BESCHREIBUNG
Show other received ICMP packets	Verbose-Ausgabe, die alle empfangenen ICMP-Pakete zusätzlich zu den ECHO_RESPONSE-Paketen aufführt. Tritt selten auf.
No DNS Resolution	Löst Adressen nicht in Hostnamen auf.
Record Route	Zeichnet die Route auf. Legt die Option zur Aufzeichnung der IP-Route fest, durch die die Route des Pakets im IP-Header gespeichert wird.
Use Broadcast Address	Ermöglicht das Anpingen einer Broadcastnachricht.
Adaptive Timing	Anpassbares anpingen. Das Interpacket-Intervall passt sich an die Round-Trip-Zeit an, sodass sich effektiv nicht mehr als eine unbeantwortete Anfrage im Netzwerk befindet. Das Mindestintervall beträgt 200 ms.

4. Sie können optional Werte dafür eingeben, wie viele Sekunden der Ping-Befehl ausgeführt wird, wie viele Ping-Anfragen gesendet werden sowie die Größe der Ping-Pakete (standardmäßig 56, was 64 ICMP-Datenbyte in Verbindung mit 8 Byte ICMP-Headerdaten entspricht). Werden die Felder nicht ausgefüllt, werden die Standardwerte verwendet.
5. Klicken Sie unten rechts im Fenster auf **Ping**. Wird als Ergebnis eine Reihe von Antworten angezeigt, funktioniert die Verbindung. Die Zeitangabe gibt an, wie schnell die Verbindung ist. Wenn statt einer Antwort der Fehler „timed out“ angezeigt wird, ist die Verbindung zwischen Ihrem Computer und der Domäne unterbrochen. In diesem Fall sollten Sie „traceroute“ ausführen. Weitere Informationen finden Sie im nächsten Abschnitt.
6. Drücken Sie **STRG+C**, um die Ping-Sitzung zu beenden. Die Eingabeaufforderung „**Return?“** wird angezeigt, bevor die Diagnosekonsole angezeigt wird (damit angezeigte Daten bei Bedarf geprüft und analysiert werden können).

Hinweis: *Sie können die statistische Zusammenfassung der Sitzung mit **Strg+Q** anzeigen und das Ziel weiterhin anpingen.*

Traceroute verwenden (Network Interfaces)

Traceroute wird häufig zur Problembehandlung in Netzwerken verwendet. Indem Sie die Liste der Router anzeigen, die verwendet wurden, können Sie den Pfad von Ihrem Computer zu einem bestimmten Ziel im Netzwerk bestimmen. Aufgeführt werden alle Router, die das Paket weiterleiten, bis es am Ziel angekommen ist oder nicht am Ziel ankommt und fallen gelassen wird. Außerdem können Sie anzeigen, wie viel Zeit jede Teilstrecke von Router zu Router beansprucht hat. Sie können dadurch Routing-Probleme oder Firewalls kennzeichnen, die den Zugriff auf eine Site sperren.

So führen Sie traceroute für eine IP-Adresse oder einen Hostnamen durch:

1. Klicken Sie auf **Operation**, **Network Interfaces** und dann auf **Traceroute**.
2. Geben Sie die IP-Adresse oder den Hostnamen des Ziels, das Sie prüfen möchten, im Feld **Traceroute Target** ein.
3. Optional können Sie Folgendes auswählen:

OPTION	BESCHREIBUNG
Verbose	Verbose-Ausgabe, die alle empfangenen ICMP-Pakete außer TIME_EXCEEDED und UNREACHABLE aufführt.
No DNS Resolution	Löst Adressen nicht in Hostnamen auf.
Use ICMP (vs. normal UDP)	ICMP ECHO- anstelle von UDP-Datagrammen verwenden.

4. Sie können optional Werte eingeben, wie viele Teilstrecken der Befehl traceroute bei ausgehenden Prüfpaketen verwendet (der Standardwert lautet 30), wie viele Teilstrecken der UDP-Zielport für Prüfpakete verwendet (der Standardwert lautet 33434) und wie groß die traceroute-Pakete sein sollen. Werden die Felder nicht ausgefüllt, werden die Standardwerte verwendet.
5. Klicken Sie unten rechts im Fenster auf **Traceroute**.
6. Drücken Sie **STRG+C** oder **STRG+Q**, um die Traceroute-Sitzung zu beenden. Eine Eingabeaufforderung **Return?** wird angezeigt. Drücken Sie die **Eingabetaste**, um zum Traceroute-Menü zu wechseln. Die Eingabeaufforderung **Return?** wird auch angezeigt, wenn Traceroute beendet wird, sobald die Ereignisse „destination reached“ oder „hop count exceeded“ eintreten.

Static Routes bearbeiten (Network Interfaces)

In Static Routes können Sie die aktuelle IP-Routing-Tabelle anzeigen und Routen bearbeiten, hinzufügen oder löschen. Die sorgfältige Verwendung und Platzierung statischer Routen kann die Leistung Ihres Netzwerks verbessern. Sie sparen Bandbreite für wichtige Geschäftsanwendungen und es kann für die Aktiv/Aktiv-Netzwerkeinstellungen nützlich sein, bei denen jede Schnittstelle mit einer separaten IP-Domäne verbunden ist. Weitere Informationen finden Sie unter Netzwerkkonfiguration in Kapitel 12: Erweiterte Administration. Klicken Sie mit der Maus, oder verwenden Sie die Tabulator- und ↓↑-Tasten zum Navigieren, und drücken Sie zum Auswählen eines Werts die **Eingabetaste**.

So zeigen Sie statische Routen an oder bearbeiten diese:

1. Klicken Sie auf **Operation**, **Network Interfaces** und dann auf **Static Routes**.

2. Die aktuelle IP-Routingtabelle wird angezeigt. Sie können eine Host- oder Netzwerkroute hinzufügen oder eine Route löschen. Mithilfe der Schaltfläche <**Refresh**> werden die Routinginformationen in der Tabelle oben aktualisiert.

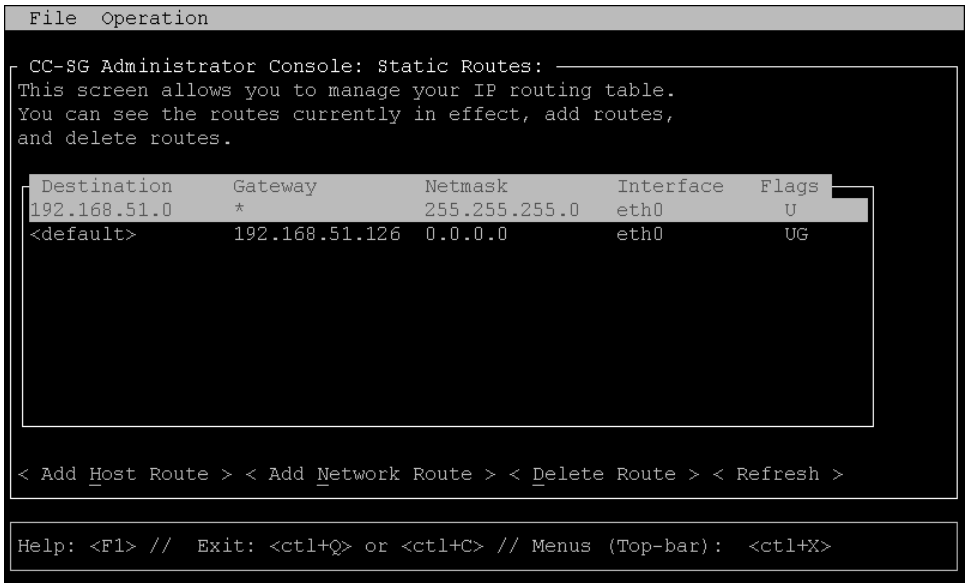


Abbildung 191 Static Routes bearbeiten

Protokolldateien anzeigen (Admin)

Sie können eine oder mehrere Protokolldateien in LogViewer anzeigen sowie mehrere Dateien gleichzeitig durchsuchen, um die Systemaktivität zu untersuchen.

So zeigen Sie Protokolldateien an:

1. Klicken Sie auf **Operation**, **Admin** und dann auf **System Logfile Viewer**.
2. Der Logviewer-Bildschirm ist in 4 Hauptbereiche (siehe unten) aufgeteilt:
   - Liste der Protokolldateien, die zurzeit im System verfügbar sind. Ist die Liste länger als das Anzeigefenster, können Sie mithilfe der Pfeiltasten durch die Liste blättern.
   - Sortierkriterien für Listen mit Protokolldateien. Protokolldateien können nach dem Dateinamen, dem letzten Änderungsdatum oder der Größe der Protokolldatei sortiert werden.
   - Viewer-Anzeigeoptionen (siehe Details unten).
   - Export-/Anzeigeoption.

3. Klicken Sie mit der Maus, oder verwenden Sie die Pfeiltasten zum Navigieren, und drücken Sie zum Auswählen einer Protokolldatei (mit X hervorgehoben) die **Leertaste**. Sie können mehrere Protokolldateien gleichzeitig anzeigen.

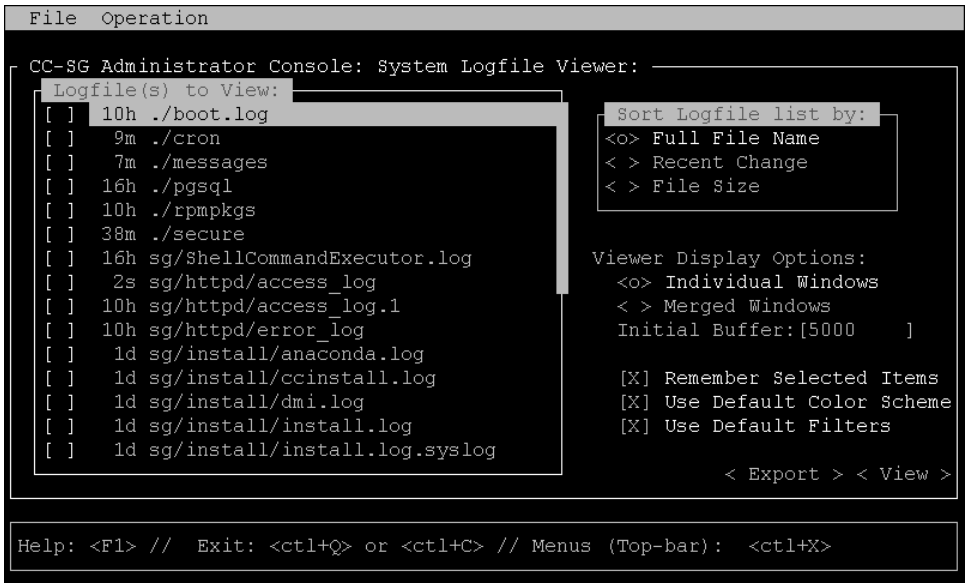


Abbildung 192 Protokolldateien zur Anzeige auswählen

Die Liste der Protokolldateien wird nur aktualisiert, wenn die verknüpfte Liste aktiviert wird (ein Benutzer wechselt beispielsweise in den Listenbereich der Protokolldateien) oder wenn eine neue Sortieroption ausgewählt wird. Entweder wird ein Zeitstempel vor Dateinamen angezeigt, um zu kennzeichnen, wann neue Daten für die Protokolldatei eingegangen sind, oder die Größe der Protokolldatei. Zeitstempel zeigen s → Sekunden, m → Minuten, h → Stunden und d → Tage an. Dateigrößen sind B → Bytes, K → Kilo (1.000) Bytes, M → Megabytes (1.000.000) und G→ Gigabytes. Wenn als Sortieroption weder der Dateiname noch das letzte Änderungsdatum verwendet werden, werden Zeitstempel verwendet. Dateigröße wird für **Dateigröße** verwendet.

Das Fenster „Sort Logfile list by:“ besteht aus Optionsfeldern (jeweils nur eins aktivierbar) und legt fest, wie Protokolldateien im Fenster „Logfile to View“ angezeigt werden.

OPTION	BESCHREIBUNG
Individual Windows	Zeigt die ausgewählten Protokolle in einzelnen Unterfenstern an.
Merged Windows	Zeigt die ausgewählten Protokolle in einem Fenster an.
Initial Buffer	Legt die anfängliche Puffer- oder Verlaufsgröße fest. Der Standardwert beträgt **5000**. Das System ist so konfiguriert, dass alle neuen Informationen zwischengespeichert werden.
Remember Selected Items	Ist dieses Feld markiert, wird die aktuelle Auswahl der Protokolldateien (falls vorhanden) gespeichert. Andernfalls wird die Auswahl zurückgesetzt, sobald eine neue Liste mit Protokolldateien erzeugt wird. Diese Option ist hilfreich, wenn Sie Dateien schrittweise bearbeiten möchten.
Use Default Color Scheme	Ist dieses Feld markiert, werden einige Protokolldateien mit einem standardmäßigen Farbschema angezeigt. Hinweis: Multitail-Befehle können verwendet werden, um das Farbschema zu ändern, nachdem die Protokolldateien angezeigt wurden.
Use Default Filters	Ist dieses Feld markiert, werden auf bestimmte Protokolldateien automatisch Filter angewendet.

Export	Diese Option fasst alle ausgewählten Protokolldateien in einem Paket zusammen und stellt sie über Webzugriff zur Verfügung, damit sie abgerufen und an den technischen Support von Raritan weitergeleitet werden können. Der Zugriff auf den Inhalt dieses Pakets steht Kunden nicht zur Verfügung. Exportierte Protokolldateien stehen bis zu 10 Tage zur Verfügung, bevor sie automatisch vom System gelöscht werden.
View	Anzeigen der ausgewählten Protokolle.

Wird **View** mit der Option **Individual Windows** ausgewählt, zeigt LogViewer Folgendes an:

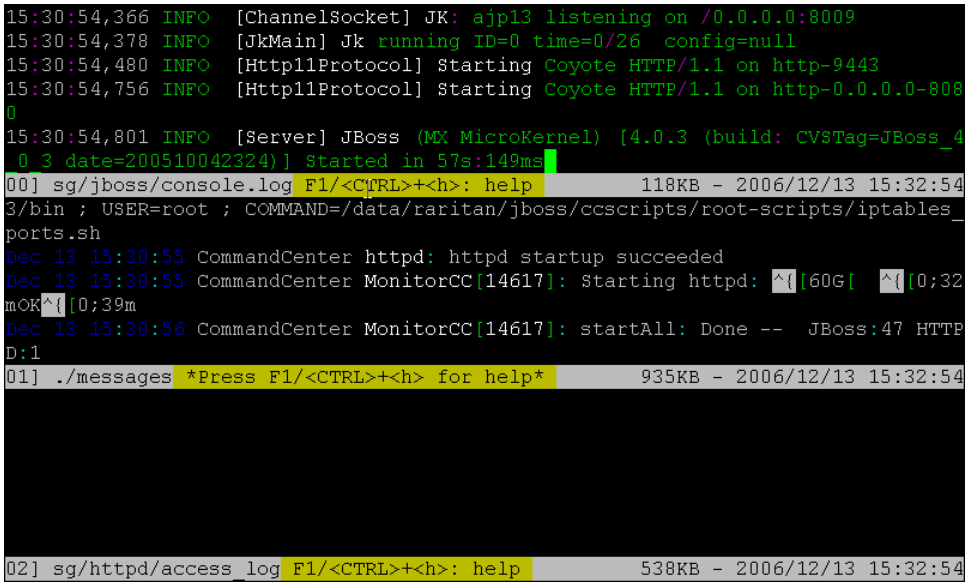


Abbildung 193 Protokolldateien zur Anzeige auswählen

4. Geben Sie beim Anzeigen von Protokolldateien **q, STRG+Q** oder **STRG+C** ein, um zum vorherigen Bildschirm zu wechseln.
5. Sie können die Farben in einer Protokolldatei bei Bedarf ändern, um wichtige Daten hervorzuheben. Geben Sie **c** ein, um die Farben in einer Protokolldatei zu ändern, und wählen Sie eine Protokolldatei in der Liste aus, falls Sie mehrere anzeigen.

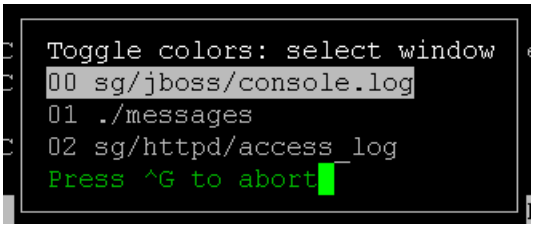


Abbildung 194 Farben in Protokolldateien ändern

6. Geben Sie **i** zur Anzeige von Systeminformationen ein.

***Hinweis**: Die Systemauslastung ist zu Beginn der Administratorkonsole-Sitzung statisch. Verwenden Sie das TOP-Dienstprogramm, um die Systemressourcen dynamisch zu überwachen.*

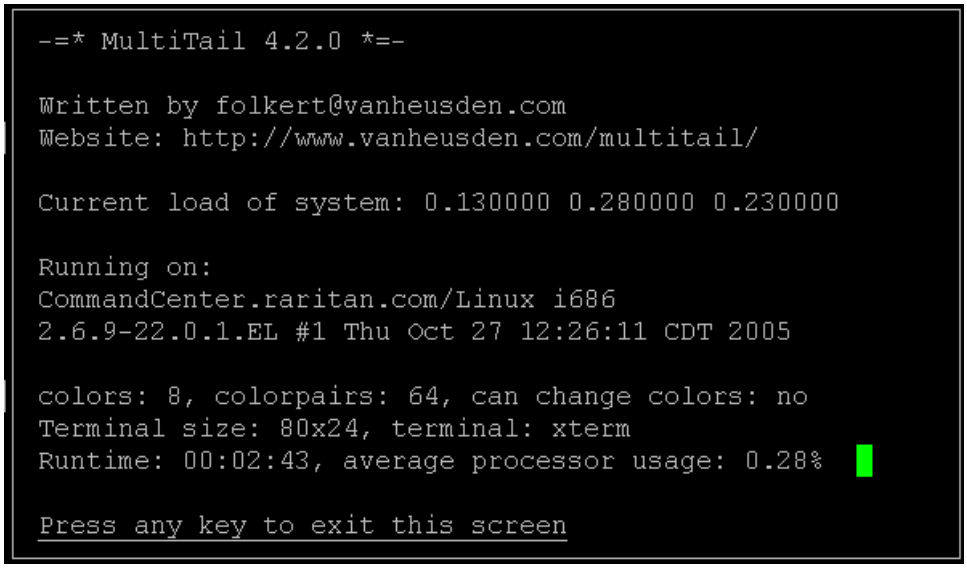


Abbildung 195 Informationen anzeigen

7. Sie können Filter mit regulären Ausdrücken für die Protokolldatei verwenden. Geben Sie **e** ein, um einen regulären Ausdruck hinzuzufügen oder zu bearbeiten, und wählen Sie eine Protokolldatei in der Liste aus, falls Sie mehrere anzeigen.

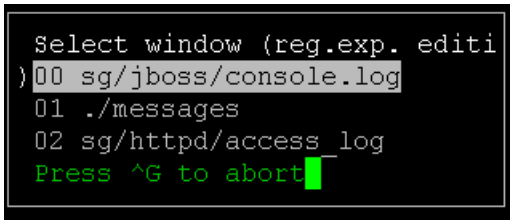


Abbildung 196 Ausdrücke in Protokolldateien hinzufügen

8. Geben Sie **a** ein, um einen regulären Ausdruck hinzuzufügen. Wenn Sie beispielsweise Informationen zur **WARN**-Nachricht in der Protokolldatei **sg/jboss/console.log** anzeigen möchten, geben Sie **WARN** ein, und wählen Sie **match** aus.

***Hinweis**: Dieser Bildschirm zeigt auch das Default Filter Scheme für console.log an, das die meisten Java-Heap-Nachrichten entfernt.*

Abbildung 197 Regulären Ausdruck für Protokolldateien festlegen

9. Mit **F1** können Sie die Hilfe für alle LogViewer-Optionen anzeigen. Beenden Sie die LogViewer-Sitzung mit **STRG+C** und **STRG+Q**.

CC-SG neu starten (Admin)

Sie können CC-SG neu starten, wobei dann alle aktuellen CC-SG-Benutzer abgemeldet und die Sitzungen mit Remotezielservern beendet werden.

Wichtig: Es wird DRINGEND empfohlen, CC-SG über die grafische Benutzeroberfläche von CC-SG neu zu starten, wenn es nicht absolut notwendig ist, den Neustart hier auszuführen. Weitere Informationen finden Sie unter **CC-SG neu starten** in **Kapitel 11: Systemwartung**. Beim Neustarten von CC-SG in der Diagnosekonsole werden die Benutzer der grafischen Benutzeroberfläche von CC-SG über den Neustart NICHT informiert.

So starten Sie CC-SG neu:

1. Klicken Sie auf **Operation**, **Admin** und dann auf **CC-SG Restart**.
2. Klicken Sie auf **Restart CC-SG Application**, oder drücken Sie die **Eingabetaste**. Bestätigen Sie den Neustart im nächsten Bildschirm.

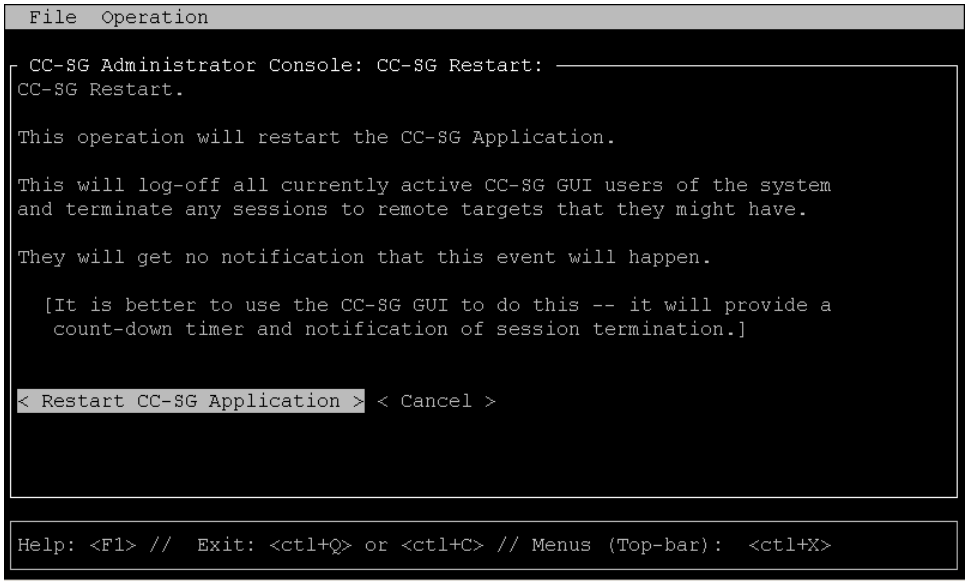


Abbildung 198 CC-SG in der Diagnosekonsole neu starten

CC-SG neu hochfahren (Admin)

Mit dieser Option wird das gesamte CC-SG neu hochgefahren. Dies entspricht dem Aus- und erneutem Einschalten. Benutzer erhalten keine Benachrichtigung. Benutzer von CC-SG, SSH und der Diagnosekonsole (einschließlich dieser Sitzung) werden abgemeldet. Alle Verbindungen zu Remotezielservern werden getrennt.

So fahren Sie CC-SG neu hoch:

1. Klicken Sie auf **Operation**, **Admin** und dann auf **CC-SG System Reboot**.
2. Klicken Sie auf **REBOOT System**, oder drücken Sie die Eingabetaste, um CC-SG neu hochzufahren. Bestätigen Sie das Hochfahren im nächsten Bildschirm.

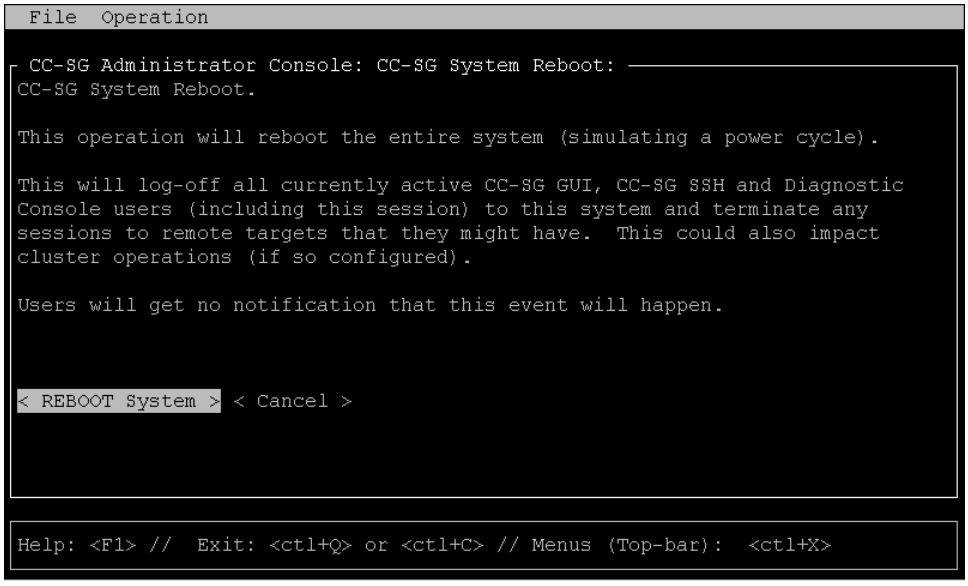


Abbildung 199 CC-SG in der Diagnosekonsole neu hochfahren

CC-SG-System (Admin) ausschalten

Mit dieser Option wird das gesamte CC-SG ausgeschaltet. Benutzer erhalten keine Benachrichtigung. Benutzer von CC-SG, SSH und der Diagnosekonsole (einschließlich dieser Sitzung) werden abgemeldet. Alle Verbindungen zu Remotezielservern werden getrennt. Sie können die CC-SG-Einheit nur wieder einschalten, indem Sie die Power-Taste vorne am Gerät bestätigen.

So schalten Sie CC-SG aus:

1. Klicken Sie auf **Operation**, **Admin** und dann auf **CC-SG System Power OFF**.
2. Klicken Sie entweder auf **Power OFF the CC-SG** oder drücken Sie die **Eingabetaste**, um den Strom an der CC-SG-Einheit abzuschalten. Bestätigen Sie das Ausschalten im nächsten Bildschirm.

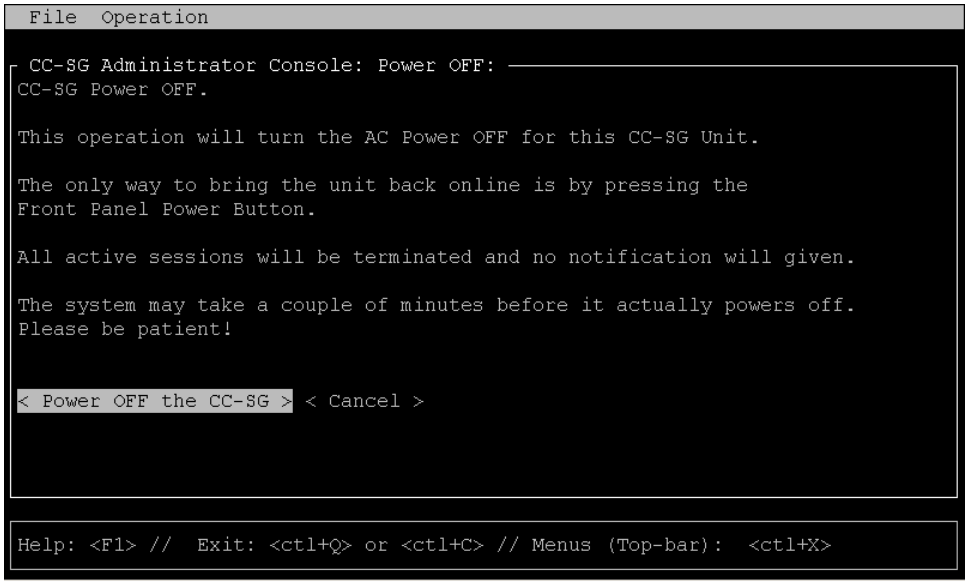


Abbildung 200 CC-SG in der Diagnosekonsole ausschalten

Administratorkennwort (Admin) von CC-SG (Benutzeroberfläche) zurücksetzen

Mit dieser Option wird das Kennwort des Kontos **admin** des CC-SG-Benutzers auf den dokumentierten Standardwert zurückgesetzt.

***Hinweis**: Dies ist nicht das Kennwort für den Benutzer **admin** der Diagnosekonsole. Weitere Informationen zum Ändern dieses Kennworts finden Sie unter **DiagCon Passwords**.*

So setzen Sie das **admin** Kennwort der grafischen Benutzeroberfläche von CC-SG zurück:

1. Klicken Sie auf **Operation**, **Admin** und dann auf **CC-SG ADMIN Password Reset**.
2. Klicken Sie auf **Reset CC-SG GUI Admin Password**, oder drücken Sie die **Eingabetaste**, um das **admin** Kennwort auf die werksseitige Standardeinstellung zurückzusetzen. Bestätigen Sie das Zurücksetzen im nächsten Bildschirm.

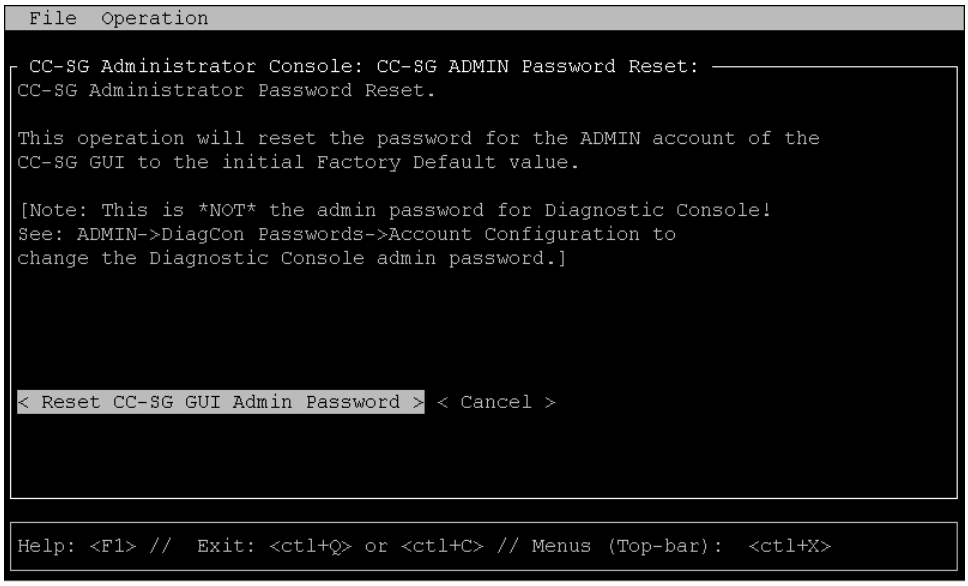


Abbildung 201 Admin-Kennwort für die Benutzeroberfläche von CC-SG in der Diagnosekonsole zurücksetzen

Werksseitig eingestelte Konfiguration von CC-SG (Admin) zurücksetzen

Durch diese Option wird das gesamte CC-SG-System oder Teile davon auf die werksseitig eingestellten Standardwerte zurückgesetzt. Alle aktiven CC-SG-Benutzer werden ohne Benachrichtigung abgemeldet, und die SNMP-Verarbeitung wird unterbrochen. Sie sollten den **Wartungsmodus** für CC-SG starten, bevor Sie diesen Vorgang starten. Falls möglich, sollten Sie CC-SG über den Administrations-Client und nicht über die Diagnosekonsole zurücksetzen. Die Option zum Zurücksetzen des Administrations-Client kann alle hier aufgeführten Funktionen außer des Zurücksetzens der Netzwerkwerte durchführen.

1. Klicken Sie im Menü **Operation** auf **Admin** und dann auf **Factory Reset**. Folgender Bildschirm wird mit sieben Optionen zum Zurücksetzen angezeigt.

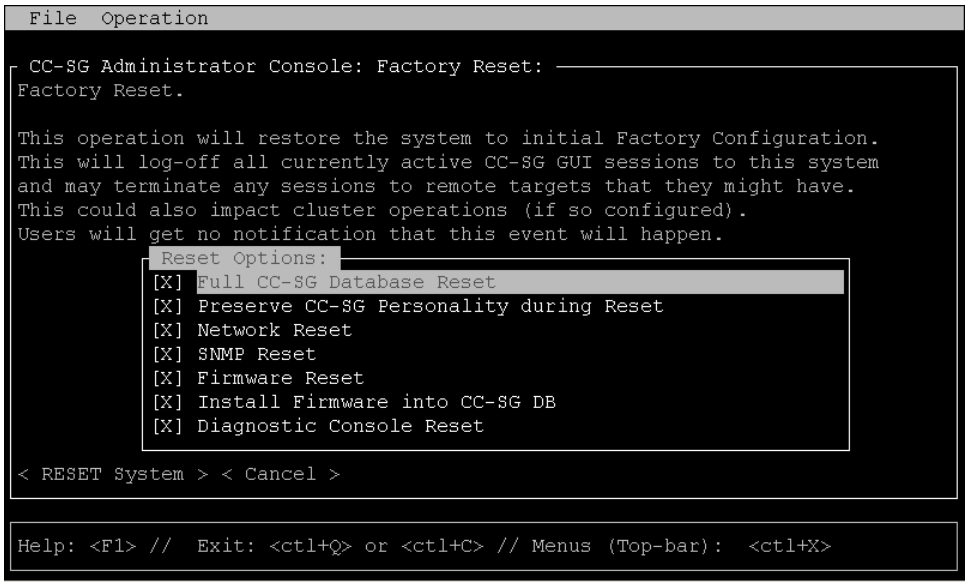


Abbildung 202 Werksseitige CC-SG-Konfiguration zurücksetzen

OPTION	BESCHREIBUNG
Full CC-SG Database Reset	Diese Option entfernt die vorhandene CC-SG-Datenbank vollständig und erstellt eine neue Version, die mit den Standardwerten gefüllt wird.
Preserve CC-SG Personality during Reset	Diese Option funktioniert nur, wenn die vorherige Option auch ausgewählt wurde. Beim Erstellen einer neuen CC-SG-Datenbank (vorherige Option) werden die folgenden Werte in die neue Version der Datenbank migriert (wenn sie gelesen werden können und verfügbar sind, ansonsten werden Standardwerte verwendet). Es wird versucht, folgende Daten zu übernehmen. Standardwerte werden in Klammern dargestellt. ▪ Sichere Kommunikation [nicht sicher] zwischen PC-Clients und CC-SG. ▪ Strenge Kennwortüberprüfung [aus] gibt an, ob die strenge Kennwortüberprüfung erzwungen wird. ▪ Direkte und Proxy-Verbindungen [Direkt] gibt an, ob PC-Clients über direkte oder Proxy-Verbindungen mit Out-of-Band-Knoten verbunden werden. ▪ Leerlaufzeitgeber [1800] zeigt die Zeit an, die verstreicht, bis inaktive Sitzungen abgemeldet werden. ▪ Modemeinstellung [10.0.0.1/10.0.0.2/<keine>] zeigt die Einstellung des Modems für die Server-IP-Adresse, Client-IP-Adresse und Rückrufnummer an.
Network Reset	Diese Option setzt die Netzwerkwerte auf die werksseitigen Standardwerte zurück: ▪ Hostname = CommandCenter ▪ Domänenname = localdomain ▪ Modus = Primary / Backup ▪ Konfiguration = Static ▪ IP-Adresse = 192.168.0.192 ▪ Netzmaske = 255.255.255.0 ▪ Gateway = <keiner> ▪ Primärer DNS-Server = <keiner> ▪ Sekundärer DNS-Server = <keiner> ▪ Adaptergeschwindigkeit = Auto
SNMP Reset	Setzt die SNMP-Konfiguration auf die werksseitigen Standardwerte zurück. ▪ Port: 161 ▪ Community mit Lesezugriff: public ▪ Community mit Lese/Schreibzugriff: private ▪ Systemkontakt, -name, -standort: <leer> ▪ SNMP-Trap-Konfiguration ▪ SNMP-Trap-Ziele
Firmware Reset	Entfernt hochgeladene Firmwaredateien und stellt die Standardversionen im Dateisystemspeicher wieder her, nimmt jedoch keine Änderungen an der CC-SG-Datenbank vor.
Install Firmware into CC-SG DB	Lädt Firmwaredateien aus dem Dateisystem-basierenden Speicher in die CC-SG-Datenbank.
Diagnostic Console Reset	Stellt die Diagnosekonsole mit der werksseitig eingestellten Standardkonfiguration, den Kontoeinstellungen und Standardwerten wieder her.

Kennwörter für die Diagnosekonsole (Admin)

Mit dieser Option können Sie die Sicherheitsstärke von Kennwörtern (status und admin) sowie Kennwortattribute konfigurieren. Dazu gehören die Höchstanzahl von Tagen, die verstreichen müssen, bevor das Kennwort geändert werden muss. Führen Sie diese Aufgaben über das Menü **Account Configuration** durch. Die Optionen dieser Menüs beziehen sich nur auf Konten der Diagnosekonsole (**status** und **admin**) und Kennwörter. Sie haben keine Auswirkungen auf normale CC-SG-Konten oder -Kennwörter der Benutzeroberfläche.

Password Configuration

1. Klicken Sie auf **Operation**, **Admin**, **DiagCon Passwords** und dann auf **Password Configuration**.
2. Geben Sie im Feld **Länge der Kennwortchronik** die Anzahl an Kennwörtern ein, die gespeichert werden sollen. Die Standardeinstellung ist **5**.

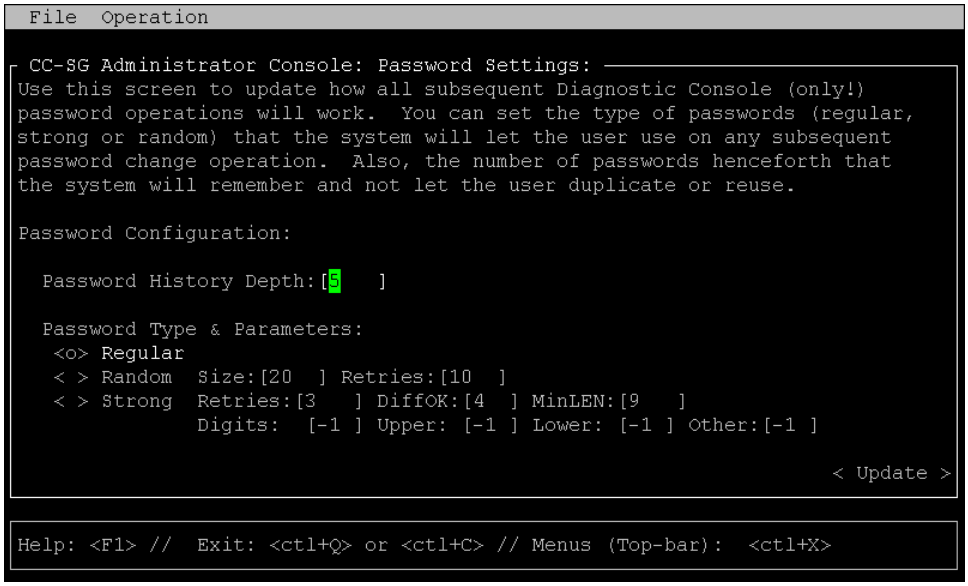


Abbildung 203 Kennworteinstellungen konfigurieren

3. Wählen Sie **Regular**, **Random** oder **Strong** für die Kennwörter für **admin** und **status** (falls aktiviert) aus.

KENNWORTEINSTELLUNG	BESCHREIBUNG
Regular	Dies ist der Standardwert. Kennwörter müssen länger als 4 Zeichen mit wenigen Einschränkungen sein. Dies ist die standardmäßige Kennwortkonfiguration des Systems.
Random	Bietet zufällig erzeugte Kennwörter. Konfigurieren Sie die maximale Kennwortgröße **size** in Bits (Mindestwert 14, Höchstwert 70 und Standardwert 20) und die Anzahl der Wiederholungen **retries** (Standardwert 10), d. h. wie oft Sie gefragt werden, ob Sie das neue Kennwort übernehmen möchten. Sie können entweder annehmen (indem Sie das neue Kennwort zweimal eingeben) oder das zufällige Kennwort ablehnen. Sie können kein eigenes Kennwort auswählen.
Strong	Erzwingt sichere Kennwörter. **Retries** ist die Anzahl an Versuchen, die Sie haben, bis eine Fehlermeldung ausgegeben wird. **DiffOK** ist die Anzahl der Zeichen, die in dem neuen Kennwort im Vergleich zum alten Kennwort gleich sein darf. **MinLEN** ist die Mindestzeichenlänge, die für das Kennwort erforderlich ist. Legen Sie die Werte für **Digits** (Zahlen), **Upper** (Großbuchstaben), **Lower** (Kleinbuchstaben) und **Other** (Sonderzeichen) fest, die für das Kennwort erforderlich sind. Positive Zahlen geben die Höchstanzahl von „credit“ dieser Zeichenklasse an, der für die „simplicity“-Zählung gesammelt werden kann. Negative Zahlen geben an, dass das Kennwort mindestens so viele Zeichen der angegebenen Klasse enthalten **muss**. Der Wert **-1** bedeutet also, dass jedes Kennwort mindestens eine Zahl enthalten muss.

Account Configuration

Standardmäßig erfordert das Konto **status** kein Kennwort, Sie können hier jedoch ein Kennwort konfigurieren. Andere Aspekte des **admin**-Kennworts können konfiguriert werden, und die Field Support-Konten können aktiviert oder deaktiviert werden.

1. Klicken Sie zum Konfigurieren von Konten auf **Operation**, **Admin**, **DiagCon Passwords** und dann auf **Account Configuration**.
2. Auf dem Bildschirm werden die Einstellungen für jedes Konto **Status**, **Admin**, **FS1** und **FS2** angezeigt.

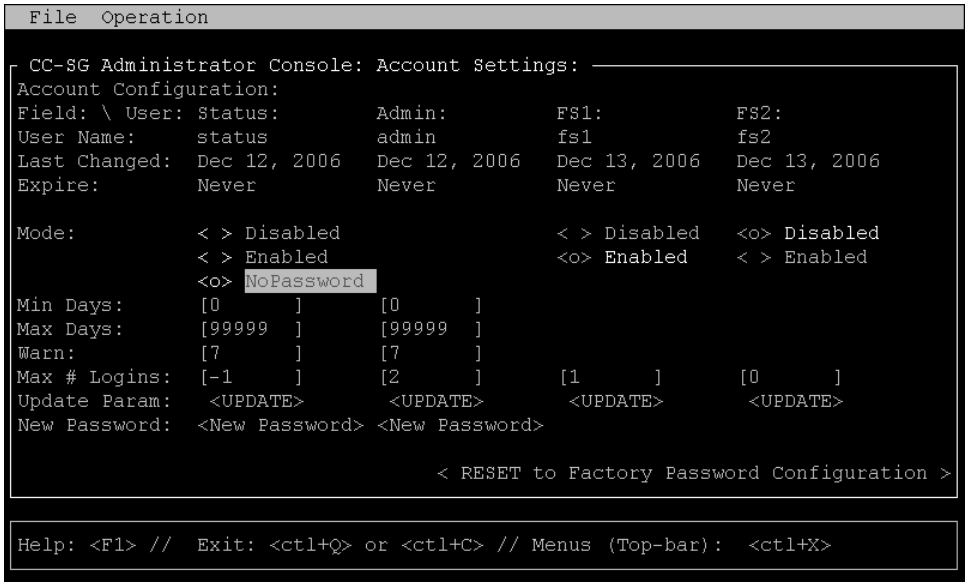


Abbildung 204 Konten konfigurieren

Dieses Fenster ist in drei Hauptbereiche eingeteilt:

- Oben werden die Informationen mit Leseberechtigung zu den Konten im System angezeigt.
- Im mittleren Bereich werden die verschiedenen Parameter angezeigt, die sich auf jede ID beziehen und dafür relevant sind. Außerdem wird eine Reihe an Schaltflächen bereitgestellt, damit die Parameter aktualisiert oder neue Kennwörter für die Konten bereitgestellt werden können.
- Im letzten Bereich wird die Kennwortkonfiguration auf den Auslieferungszustand zurückgesetzt.

3. Wenn ein Kennwort für das **Status**-Konto erforderlich sein soll, wählen Sie darunter die Option **Enabled** aus.
4. Für die Konten **Admin** und **Status** können Sie Folgendes konfigurieren:

EINSTELLUNG	BESCHREIBUNG
User \ User Name	(Lesezugriff) Der aktuelle Benutzername oder die Benutzer-ID für dieses Konto.
Last Changed	(Lesezugriff) Das Datum, an dem das Kennwort für dieses Konto zuletzt geändert wurde.
Expire	(Lesezugriff) Das Datum, an dem das Kennwort für dieses Konto geändert werden muss.
Mode	Eine konfigurierbare Option, wenn das Konto deaktiviert (Anmeldung nicht zulässig) oder aktiviert (Token zur Authentifizierung erforderlich) oder der Zugriff erlaubt und kein Kennwort erforderlich ist. (Sperren Sie nicht beide Admin- und FS1-Konten gleichzeitig, da Sie sonst die Diagnosekonsole nicht verwenden können.)
Min Days	Die Mindestanzahl an Tagen nach einer Kennwortänderung, nach denen das Kennwort erneut geändert werden kann. Der Standardwert ist **0**.
Max Days	Die Höchstanzahl an Tagen, die das Kennwort gültig ist. Der Standardwert ist **99999**.
Warning	Die Anzahl an Tagen, die Warnhinweise ausgegeben werden, bevor das Kennwort ungültig wird.
Max # of Logins	Die Höchstanzahl an gleichzeitigen Anmeldungen, die für das Konto zulässig ist. Negative Zahlen bedeuten keine Einschränkungen (**-1** ist der Standardwert für die Anmeldung mit **status**). **0** bedeutet, dass sich keiner anmelden kann. Eine positive Zahl legt die Anzahl an Benutzern fest, die gleichzeitig angemeldet sein können (**2** ist der Standardwert für die Anmeldung mit **admin**).
UPDATE	Vorgenommene Änderungen für diese ID werden gespeichert.
New Password	Geben Sie ein neues Kennwort für das Konto ein.

Disk Status anzeigen (Utilities)

Diese Option zeigt den Status der CC-SG-Festplatten an: Festplattengröße, ob sie aktiv und betriebsbereit sind, Status von RAID-1 sowie der von verschiedenen Dateisystemen verwendete Festplattenspeicher.

So zeigen Sie den CC-SG-Festplattenstatus an:

1. Klicken Sie auf **Operation**, **Utilities** und dann auf **Disk Status**.

2. Klicken Sie auf **Refresh**, oder drücken Sie die **Eingabetaste**, um das Fenster zu aktualisieren. Es ist besonders hilfreich, die Anzeige beim Aktualisieren oder Installieren zu aktualisieren, um den Fortschritt der RAID-Festplatten anzuzeigen, wenn sie neu erstellt und synchronisiert werden.

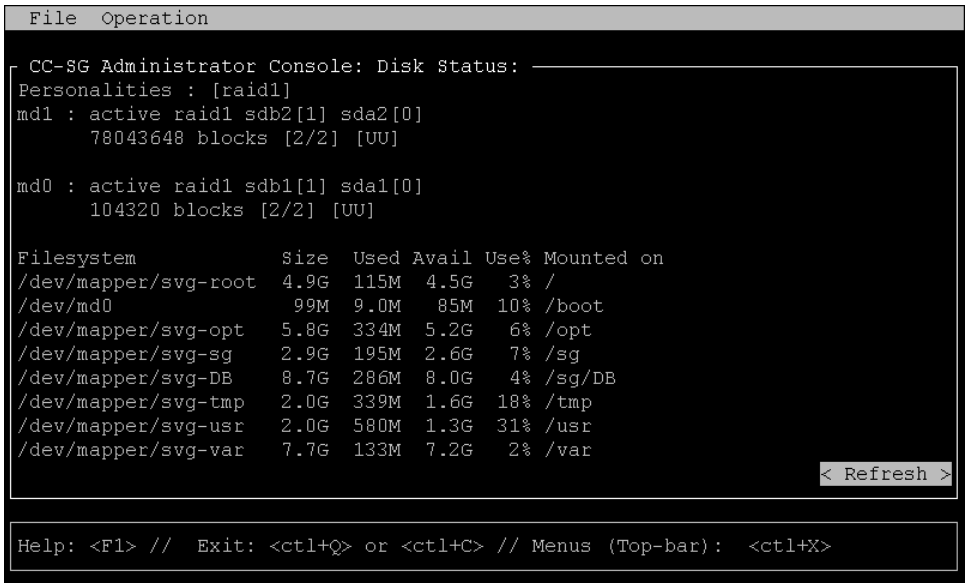


Abbildung 205 Disk Status von CC-SG in der Diagnosekonsole anzeigen

***Hinweis**: Die Festplattenlaufwerke werden vollständig synchronisiert, und der vollständige RAID-1-Schutz steht zur Verfügung, wenn Sie ein Fenster wie oben gezeigt sehen. Beachten Sie, dass der Status der Arrays **md0** und **md1** den Wert [**UU**] aufweist.*

Top Display anzeigen (Utilities)

Mit dieser Option können Sie die Prozessliste und die Attribute, die zurzeit unter CC-SG ausgeführt werden, sowie den allgemeinen Systemzustand anzeigen.

1. Klicken Sie zum Anzeigen der ausgeführten CC-SG-Prozesse auf **Operation**, **Utilities** und dann auf **Top Display**.
2. Zeigen Sie die Gesamtanzahl der Prozesse an, die ausgeführt werden, ruhen oder unterbrochen wurden.

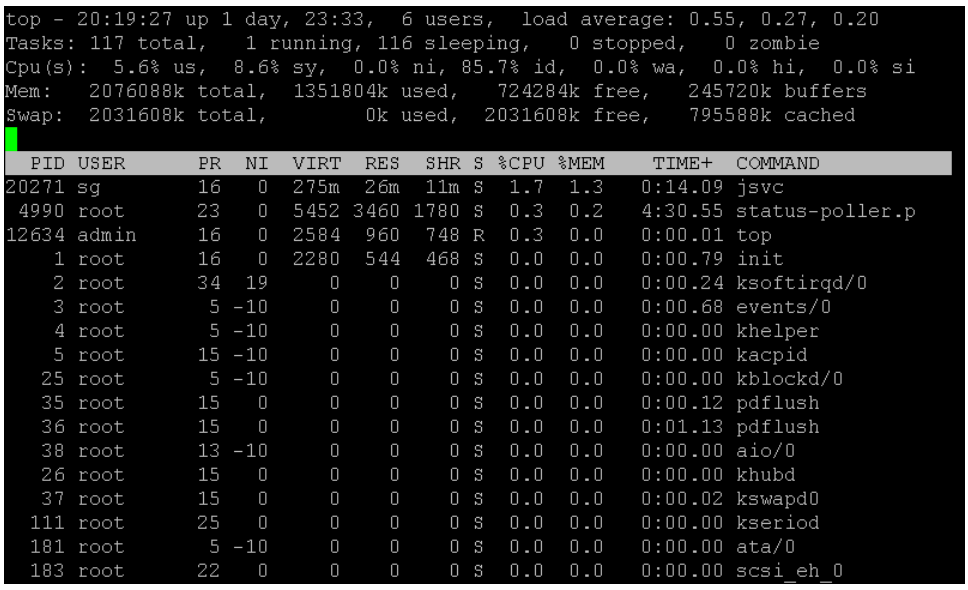


Abbildung 206 CC-SG-Prozesse in der Diagnosekonsole anzeigen

3. Geben Sie **h** ein, um eine umfassende Hilfeseite für den Befehl **top** anzuzeigen. Die Hilfetaste **F1** funktioniert in diesem Fall nicht. Drücken Sie zum Wechseln zur Administratorkonsole auf **Strg+Q** oder **Strg+C**.

NTP (Network Time Protocol) Status (Utilities) anzeigen

Mit dieser Option können Sie den Status des NTP-Zeitdaemons anzeigen, falls dieser konfiguriert und unter CC-SG ausgeführt wird.

So zeigen Sie den Status des NTP-Daemons in CC-SG an:

1. Klicken Sie auf **Operation**, **Utilities** und dann auf **NTP Status Display**.
2. Der NTP-Daemon kann nur im CC-SG-Administrations-Client konfiguriert werden. Ist NTP nicht aktiviert und richtig konfiguriert, wird Folgendes angezeigt:

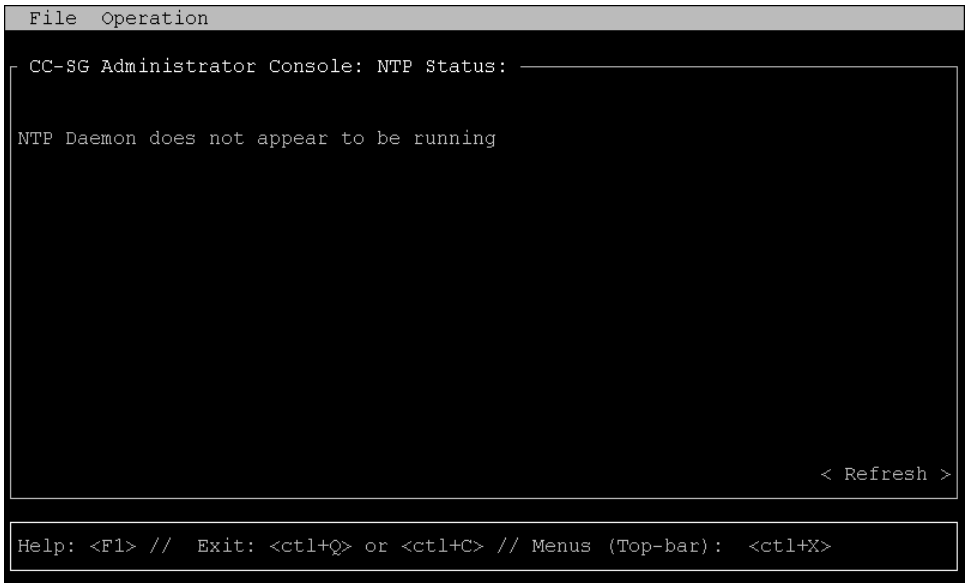


Abbildung 207 NTP nicht in der Benutzeroberfläche von CC-SG konfiguriert

3. Ist NTP richtig konfiguriert und wird unter CC-SG ausgeführt, sollte ein ähnlicher Bildschirm wie folgt angezeigt werden:

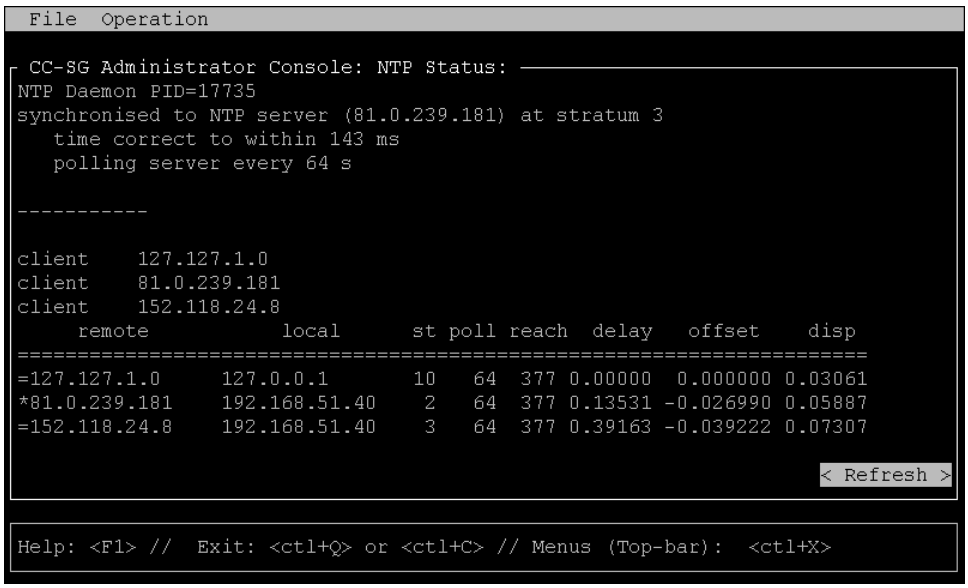


Abbildung 208 NTP läuft auf der Benutzeroberfläche von CC-SG

4. Aktualisieren Sie die Informationen auf dieser Seite über **Refresh**.

Diese Seite wurde absichtlich leer gelassen.

Anhang A: Technische Daten (G1, V1 und E1)

G1-Plattform

Allgemeine technische Daten

Formfaktor	1U
Abmessungen (T x B x H)	563 mm x 440 mm x 44 mm
Gewicht	10,92 kg
Stromversorgung	Redundante, während des Betriebs austauschbare Netzteile mit automatischer Spannungsanpassung 110/220 V - 2,0 A
Mittlerer Reparaturabstand (Mean Time Between Failure, MTBF)	38.269 Stunden
KVM-Administrationsport	(DB15 + PS2 Tastatur/Maus)
Serieller Administrationsport	DB9
Konsolenport	Nicht zutreffend

Technische Daten für die Hardware

Prozessor	Intel® Pentium® III 1 GHz
Arbeitsspeicher	512 MB
Netzwerkschnittstellen	(2) 10/100 Ethernet (RJ45)
Festplatte und Controller	(2) 40-GB IDE mit 7200 U/min, RAID 1
CD-ROM-Laufwerk	CD-ROM 40x Lesezugriff

Umgebungsanforderungen

BETRIEB	
Luftfeuchtigkeit	20 % bis 85 % relative Luftfeuchtigkeit
Höhe über NN	Kann problemlos in Höhen von 0 bis 3.048 m betrieben und bis zu 12.192 m gelagert werden.
Erschütterung	5-55-5 Hz, 0,38 mm, 1 Minute/Zyklus; 30 Minuten für jede Achse (x, y, z)
Stoß	Nicht zutreffend
LAGERUNG	
Temperatur	0-30° C; 32-104° F
Luftfeuchtigkeit	10 % bis 90 % relative Luftfeuchtigkeit
Höhe über NN	Kann problemlos in Höhen von 0 bis 3.048 m betrieben und bis zu 12.192 m gelagert werden.
Erschütterung	5-55-5 Hz, 0,38 mm, 1 Minute/Zyklus; 30 Minuten für jede Achse (x, y, z)
Stoß	Nicht zutreffend

V1-Plattform

Allgemeine technische Daten

Formfaktor	1U
Abmessungen (T x B x H)	615 mm x 485 mm x 44 mm
Gewicht	10,80 kg
Stromversorgung	Ein Netzteil (1 x 300 Watt)
Betriebstemperatur	10° C- 35° C
Mittlerer Reparaturabstand (Mean Time Between Failure, MTBF)	36.354 Stunden
KVM-Administrationsport	(DB15 + PS2 oder USB Tastatur/Maus)
Serieller Administrationsport	DB9
Konsolenport	(2) USB 2.0 Ports

Technische Daten für die Hardware

Prozessor	AMD Opteron 146
Arbeitsspeicher	2 GB
Netzwerkschnittstellen	(2) 10/100/1000 Ethernet (RJ45)
Festplatte und Controller	(2) 80-GB SATA mit 7200 U/min, RAID 1
CD-ROM-Laufwerk	DVD-ROM

Umgebungsanforderungen

BETRIEB	
Luftfeuchtigkeit	8% bis 90 % relative Luftfeuchtigkeit
Höhe über NN	Kann problemlos in Höhen von 0 bis 3.048 m betrieben und bis zu 12.192 m gelagert werden
Erschütterung	5-55-5 Hz, 0,38 mm, 1 Minute/Zyklus; 30 Minuten für jede Achse (X,Y,Z)
Stoß	Nicht zutreffend
LAGERUNG	
Temperatur	-40° C - +60° C
Luftfeuchtigkeit	5 % bis 95 % relative Luftfeuchtigkeit
Höhe über NN	Kann problemlos in Höhen von 0 bis 3.048 m betrieben und bis zu 12.192 m gelagert werden
Erschütterung	5-55-5 Hz, 0,38 mm, 1 Minute/Zyklus; 30 Minuten für jede Achse (X,Y,Z)
Stoß	Nicht zutreffend

E1-Plattform

Allgemeine technische Daten

Formfaktor	2U
Abmessungen (T x B x H)	687 mm x 475 mm x 88 mm
Gewicht	20 kg
Stromversorgung	SP502-2S während des Betriebs austauschbare Netzteile 500 W 2U
Betriebstemperatur	0~50° C
Mittlerer Reparaturabstand (Mean Time Between Failure, MTBF)	53.564 Stunden
KVM-Administrationsport	PS/2-Tastatur- und -Mausports, 1 VGA-Port
Serieller Administrationsport	Serieller Fast UART 16550 Port
Konsolenport	(2) USB 2.0 Ports

Technische Daten für die Hardware

Prozessor	(2) AMD Opteron 250 2,4 G 1 MB Prozessoren
Arbeitsspeicher	4 GB
Netzwerkschnittstellen	Intel PRO/1000 PT Dual Port Server Adapter
Festplatte und Controller	(2) WD740ADFD SATA 74 GB 10 K RPM 16 MB Cache
CD-ROM-Laufwerk	DVD-ROM

Umgebungsanforderungen

BETRIEB	
Luftfeuchtigkeit	5-90 %, nicht-kondensierend
Höhe über NN	Meeresspiegel bis 2.130 m
Erschütterung	10 Hz bis 500 Hz Durchlauf bei 0,5 g konstanter Beschleunigung über eine Stunde auf jeder der senkrechten Achsen X, Y und Z
Stoß	5 g für 11 ms mit ½ Sinuskurve für jede senkrechte Achse X, Y und Z
LAGERUNG	
Temperatur	-40-70° C
Luftfeuchtigkeit	5-90 %, nicht-kondensierend
Höhe über NN	Meeresspiegel bis 12.192 m
Erschütterung	10 Hz bis 300 Hz Durchlauf bei 2 g konstanter Beschleunigung über eine Stunde auf jeder der senkrechten Achsen X, Y und Z
Stoß	30 g für 11 ms mit ½ Sinuskurve für jede senkrechte Achse X, Y und Z

Diese Seite wurde absichtlich leer gelassen.

Anhang B: CC-SG und Netzwerkkonfiguration

Einleitung

Dieser Anhang enthält die Netzwerkanforderungen (Adressen, Protokolle und Ports) für eine typische CC-SG-Bereitstellung. Sie finden Informationen, wie Sie Ihr Netzwerk für beide externen Zugriffe (bei Bedarf) und zur Einhaltung der internen Sicherheits- und Routingrichtlinien (falls verwendet) konfigurieren können. Details werden für TCP/IP-Netzwerkadministratoren bereitgestellt, deren Rolle und Verantwortungsbereich über den eines CC-SG-Administrators hinausgeht und die CC-SG und die Komponenten in den Sicherheitszugriff und die Routingrichtlinien einer Site integrieren möchten.

Wie im Diagramm unten dargestellt, kann eine CC-SG-Bereitstellung keine, einige oder alle Features wie eine Firewall oder ein VPN (Virtual Private Network) aufweisen. Die folgende Tabelle enthält die Protokolle und Ports, die von CC-SG und den verknüpften Komponenten benötigt werden. Sie müssen mit diesen vertraut sein, insbesondere wenn Ihr Netzwerk Firewalls oder VPNs aufweist und Zugriffs- und Sicherheitsrichtlinien in Ihrem Netzwerk verwendet werden.

Übersicht

Die folgenden Abschnitte enthalten eine sehr umfassende und genaue Analyse der Kommunikation und Portverwendung von CC-SG und der verknüpften Komponenten. Falls Sie lediglich wissen möchten, welche Ports bei einer Firewall offen sein müssen, damit Zugriff auf CC-SG und die verwalteten Ziele gewährleistet werden kann, lesen Sie die folgende Tabelle:

Portnummer	Protokoll	Zweck
80	TCP	HTTP-Zugriff auf CC-SG
443	TCP	HTTP-(SSL-)Zugriff auf CC-SG
8080	TCP	CC-SG <-> PC Client
2400	TCP	Knotenzugriff (Proxymodus & In-Band-Zugriff)
5000[1]	TCP	Knotenzugriff (Direktmodus)
51000[1]	TCP	SX-Zielzugriff (Direktmodus)

Diese Liste kann weiter gekürzt werden:

- Port 80 kann ausgeschlossen werden, falls der Zugriff auf CC-SG vollständig über HTTPS-Adressen läuft.
- Ports 5000 bis 51000 können ausgeschlossen werden, wenn der CC-SG-Proxymodus für alle Verbindungen der Firewalls verwendet wird.

Die Mindestkonfiguration erfordert daher nur drei (3) Ports [443, 8080 und 2400], die offen sein müssen, um externen Zugriff auf CC-SG zu ermöglichen.

In den Abschnitten unten finden Sie Informationen zu diesen Zugriffsmethoden und Ports sowie Konfigurationssteuerungen und -optionen.

[1] Diese Ports müssen pro Raritan-Gerät geöffnet werden, auf das extern zugegriffen wird. Die anderen Ports in der Tabelle müssen nur für den Zugriff auf CC-SG geöffnet werden.

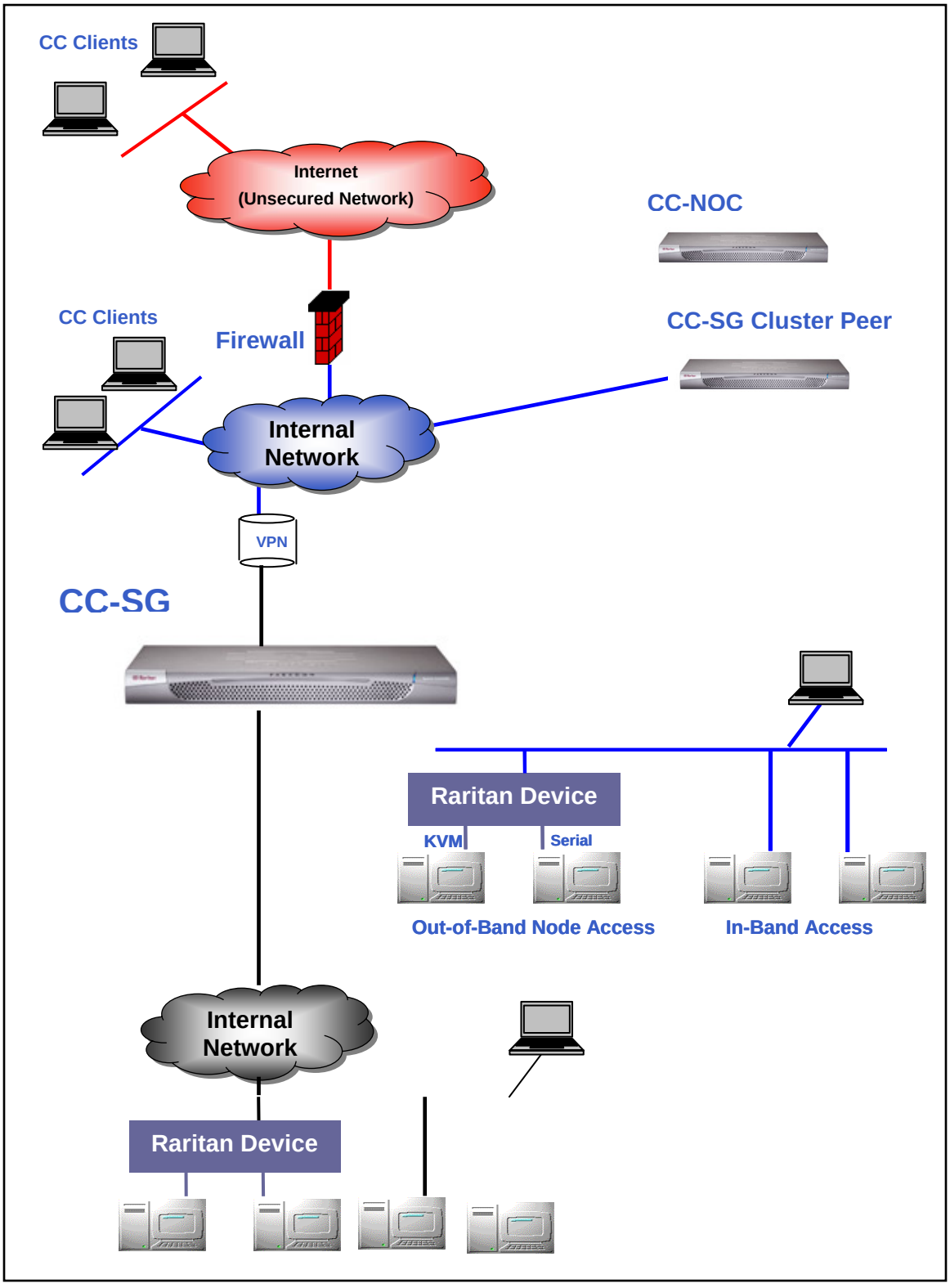


Abbildung 209 CC-SG-Bereitstellungselemente

CC-SG-Kommunikationskanäle

Die Kommunikationskanäle sind wie folgt aufgeteilt:

- CC-SG ↔ Raritan-Geräte
- CC-SG ↔ CC-SG Clustering (optional)
- CC-SG ↔ Infrastrukturdienste
- Clients ↔ CC-SG
- Clients ↔ Ziele (Direktmodus)
- Clients ↔ Ziele (Proxymodus)
- Clients ↔ Ziele (In-Band)
- CC-SG ↔ CC-NOC

Für jeden Kommunikationskanal enthalten die Tabellen in den folgenden Abschnitten:

- die symbolischen **IP-Adressen**, die von den Kommunikationsteilnehmern verwendet werden. Diese Adressen müssen für jeden Kommunikationspfad zwischen den Entitäten erlaubt sein.
- die **Richtung**, in die die Kommunikation hergestellt wird. Dies kann für Ihre besonderen Site-Richtlinien wichtig sein. Für eine bestimmte CC-SG-Rolle muss der Pfad zwischen den kommunizierenden Parteien verfügbar sein. Dies gilt auch für alternative Routenpfade, die ggf. bei einem Netzwerkausfall verwendet werden.
- die **Portnummer** und das **Protokoll**, die von CC-SG verwendet werden.
- Zeigt an, ob der Port **Konfigurierbar** ist, d. h. die Benutzeroberfläche oder Diagnosekonsole stellen ein Feld bereit, in dem Sie einen anderen Wert für die Portnummer als den Standardwert angeben können. Dies kann aufgrund von Konflikten mit anderen Anwendungen im Netzwerk oder aus Sicherheitsgründen nötig sein.

CC-SG und Raritan-Geräte

Eine Hauptrolle von CC-SG ist die Verwaltung und Steuerung von Raritan-Geräten (z. B. Dominion KX, KSX usw.). Normalerweise kommuniziert CC-SG mit diesen Geräten über ein TCP/IP-Netzwerk (lokal, WAN oder VPN), und die Protokolle TCP und UDP werden wie folgt verwendet:

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?
CC-SG → Lokale Broadcast	5000	UDP	ja
CC-SG → Remote LAN IP	5000	UDP	ja
CC-SG → Raritan-Gerät	5000	TCP	ja
Raritan-Gerät → CC-SG	5001	UDP	nein

CC-SG Clustering

Wenn das optionale CC-SG Clustering-Feature verwendet wird (d. h. zwei CC-SG-Einheiten sind miteinander verbunden und funktionieren als eine Einheit), müssen die folgenden Ports für die miteinander verbundenen Subnetzwerke verfügbar sein. {Wird das optionale Clustering-Feature nicht verwendet, müssen diese Ports im Netzwerk nicht zur Verfügung stehen.}

Jede CC-SG im Cluster kann ein anderes LAN aufweisen. Die Verbindung zwischen den Einheiten sollte jedoch sehr zuverlässig und nicht anfällig für Zeiten mit hoher Belastung sein.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?
CC-SG → Lokale Broadcast	10000	UDP	nein
CC-SG → Remote LAN IP	10000	UDP	nein
CC-SG ↔ CC-SG	5432	TCP	nein
CC-SG ↔ CC-SG	8732	TCP	nein
CC-SG ↔ CC-SG	3232	TCP	nein

Zugriff auf Infrastrukturdienste

CC-SG kann zur Verwendung verschiedener Dienste nach Industriestandard wie DHCP, DNS und NTP konfiguriert werden. Damit CC-SG mit diesen optionalen Servern kommunizieren kann, werden die folgenden Ports und Protokolle verwendet:

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?
DHCP-Server → CC-SG	68	UDP	nein
CC-SG → DHCP-Server	67	UDP	nein
NTP-Zeitserver ↔ CC-SG	123	UDP	nein
CC-SG → DNS	53	UDP	nein

Verbindung von PC-Clients mit CC-SG

PC-Clients verwenden für die Verbindung zu CC-SG einen dieser drei Modi:

- Web / Java-Applet CC-SG-Schnittstelle der Benutzeroberfläche
- CC-SG Befehlszeilenschnittstelle über SSH
- CC-SG Diagnosekonsole

Der erste Modus stellt die Hauptmethode für Benutzer und Administratoren dar, eine Verbindung zu CC-SG aufzubauen. Die anderen beiden Modi werden weniger häufig verwendet. Diese Modi erfordern folgende Netzwerkkonfiguration:

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?
Client → CC-SG Benutzeroberfläche	443	TCP	nein
Client → CC-SG Benutzeroberfläche	80	TCP	nein
Client → CC-SG Benutzeroberfläche	8080	TCP	nein
Client → CC-CLI SSH	22	TCP	ja
Client → CC-Diagnosekonsole	23	TCP	ja

Verbindung von PC-Clients mit Knoten

Eine weitere wichtige Rolle von CC-SG ist die Verbindung von PC-Clients mit verschiedenen Zielen (oder Knoten). Diese Ziele können serielle oder KVM-Konsolenverbindungen zu Raritan-Geräten (auch Out-of-Band-Verbindungen) darstellen. Ein weiterer Modus ist die IBA-Methode (In-Band Access) wie Virtual Network Computer (VNC), Windows Remote Desktop (RDP) oder Secure Shell (SSH).

Ein weiterer Aspekt der Kommunikation zwischen dem PC-Client und dem Ziel ist, ob:

- der PC-Client direkt mit dem Ziel verbunden ist (entweder über ein Raritan-Gerät oder In-Band Access). Dies wird als **Direktmodus** bezeichnet.
- der PC-Client mit dem Ziel über CC-SG verbunden ist, wobei CC-SG als Anwendungsfirewall dient. Dies wird als **Proxymodus** bezeichnet.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?
Client → CC-SG über Proxy → Ziel	2400 (an CC-SG)	TCP	nein
Client → Raritan-Ziel (Direktmodus)	5000 (am Gerät)	TCP	ja
Client → Dominion SX → (Direktmodus)	51000	TCP	ja

CC-SG und Client für IPMI, iLO/RILOE, DRAC, RSA

Eine weitere wichtige Rolle von CC-SG ist die Verwaltung von Drittanbietergeräten wie iLO/RILOE, Integrated Lights Out/Remote Insight Lights Out Server von Hewlett Packard. Ziele eines iLO/RILOE-Geräts werden ein-/ausgeschaltet und direkt aktiviert und deaktiviert. IPMI-Server **(**Intelligent Platform Management Interface) können ebenfalls von CC-SG gesteuert werden. Das gleiche gilt für Dell DRAC- und RSA-Ziele.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar
CC-SG → IPMI	623	UDP	nein
CC-SG → iLO/RILOE (verwendet HTTP-Ports)	80 oder 443	UDP	nein
CC-SG → DRAC	80 oder 443	UDP	nein
CC-SG → RSA	80 oder 443	UDP	nein

CC-SG und SNMP

Mit Simple Network Management Protocol (SNMP) sendet CC-SG SNMP-Traps (Ereignisbenachrichtigungen) an einen SNMP-Manager im Netzwerk. CC-SG unterstützt außerdem SNMP-Get/Set-Anfragen mit Unternehmensverwaltungslösungen von Drittanbietern wie HP OpenView.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?
SNMP Manager → CC-SG	161	UDP	ja
CC-SG → SNMP Manager	162	UDP	ja

CC-SG und CC-NOC

CC-NOC ist eine optionale Appliance, die in Verbindung mit CC-SG bereitgestellt werden kann. CommandCenter-NOC (CC-NOC) ist eine Netzwerküberwachungsappliance zur Überwachung des Status von Servern, Geräten und Raritan-Geräten, die von CC-SG verwaltet werden.

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?
CC-SG ↔ CC-NOC	9443	TCP	nein

Interne CC-SG-Ports

CC-SG verwendet mehrere Ports für interne Funktionen und die lokale Firewall sperrt den Zugriff auf diese Ports. Einige externe Scanner erkennen diese ggf. als „gesperrt“ oder „gefiltert“. Der externe Zugriff auf diese Ports ist nicht erforderlich und kann weiterhin gesperrt werden. Diese Ports werden zurzeit verwendet:

1088, 1098, 2222, 4444, 4445, 8009, 8083 und 8093

Außer diesen Ports hat CC-SG ggf. noch einige TCP- und UDP-Ports im Bereich 32xxx (oder höher) geöffnet. Der externe Zugriff auf diese Ports ist nicht erforderlich und kann gesperrt werden.

CC-SG-Zugriff über NAT-fähige Firewall

Verwendet die Firewall NAT (Network Address Translation) mit PAT (Port Address Translation), sollte der Proxymodus für alle Verbindungen, die diese Firewall verwenden, konfiguriert werden. Außerdem muss die Firewall für externe Verbindungen zu den Ports 80 (kein-SSL)/443 (SSL)[2], 8080 und 2400 so konfiguriert sein, dass an CC-SG weitergeleitet wird (da der PC-Client die Sitzungen an diesen Ports startet).

Alle IBA-Verbindungen (In-Band Access) verwenden CC-SG als Proxy-Verbindung, sodass keine weitere Konfiguration nötig ist. OBA-Verbindungen (Out-of-Band Access), die die Firewall verwenden, müssen im Menü **Setup ➔ Konfigurationsmanager ➔ Verbindungsmodus** so konfiguriert werden, dass sie den Proxymodus verwenden. CC-SG stellt dann eine Verbindung zu den verschiedenen Zielen (entweder IBA oder OBA) im Namen der PC-Client-Anfragen her. CC-SG beendet die PC-Client- und Ziel-TCP/IP-Verbindung jedoch, die über eine Firewall geleitet wird.

[2] Nicht-SSL-Verkehr sollte nicht über eine Firewall abgewickelt werden.

Sicherheit und Scannen nach offenen Ports

Als Bestandteil der CC-SG-Qualitätssicherung werden mehrere Scanner für offene Ports auf das Produkt angewendet, und Raritan stellt sicher, dass die Produkte nicht für diese bekannten Angriffe anfällig sind. Alle offenen oder gefilterten/gesperrten Ports werden in den Abschnitten oben aufgeführt. Einige der häufigen Schwachstellen sind:

Problem-ID[3]	Zusammenfassung	Hinweis
CVE-1999-0517 CVE-1999-0186 CVE-1999-0254 CVE-1999-0516	snmp (161/UDP) - der Community-Name des SNMP-Remoteserver kann erraten werden.	Der Standardname für die CC-SG SNMP-Community lautet „public“. Benutzer sollten diesen Wert auf den standortspezifischen Wert ändern (Menü **Setup ➔ Konfigurationsmanager ➔ SNMP**). Weitere Informationen finden Sie im **CC-SG-Handbuch für Administratoren**.
CVE-2000-0843	Der Remote-Telnet-Server hat die Verbindung plötzlich bei Eingabe eines langen Benutzernamens und eines Kennworts getrennt.	Standardmäßig wird Port 23 für Telnet-Dienste verwendet. CC-SG verwendet diesen Port jedoch für SSH V2-Sitzungen der Diagnosekonsole. Benutzer können den Port ändern und/oder verhindern, dass die Diagnosekonsole die SSH-Zugriffsmethode verwendet. Weitere Informationen finden Sie im **CC-SG-Handbuch für Administratoren**.
CVE-2004-0230	Der Remotehost ist ggf. anfällig für einen „ Sequence Number Approximation“ Fehler, der einem Angreifer ermöglicht, gefälschte RST-Pakete an den Remotehost zu senden und bestehende Verbindungen zu trennen.	Das zugrunde liegende TCP/IP-Protokollstack, das von CC-SG verwendet wird, ist hierfür nicht anfällig.
CVE-2004-0079 CVE-2004-0081 CVE-2004-0112	Der Remotehost verwendet eine OpenSSL-Version, die älter als 0.9.6m oder 0.9.7d ist.	Die folgenden Patches wurden für OpenSSL verwendet, um dies zu vermeiden: • RHSA-2004:120 • RHSA-2005:830. • RHSA-2003:101-01

[3] CVEs finden Sie unter **http://cve.mitre.org**.

Diese Seite wurde absichtlich leer gelassen.

Anhang C: Benutzergruppenberechtigungen

MENÜ > UNTERMENÜ	MENÜELEMENT	ERFORDERLICHE BERECHTIGUNG	BESCHREIBUNG
Secure Gateway	**Dieses Menü steht allen Benutzern zur Verfügung.**		
	Mein Profil	Keine*	
	Tipp des Tages	Keine*	
	Drucken	Keine*	
	Abmelden	Keine*	
	Beenden	Keine*	
Benutzer	**Dieses Menü und die Benutzerstrukturansicht stehen nur Benutzern mit der Berechtigung „User Management“ (Benutzerverwaltung) zur Verfügung.**		
> Benutzermanager	> Benutzer hinzufügen	User Management	
	(Benutzer bearbeiten)	User Management	Über Benutzerprofil
	> Benutzer löschen	User Management	
	> Benutzer aus Gruppe löschen	User Management	
	> Benutzer abmelden	User Management	
	> Massenkopieren	User Management	
> Benutzergruppen-manager	> Benutzergruppe hinzufügen	User Management	
	(Benutzergruppen bearbeiten)	User Management	Über Benutzergruppenprofil
	> Benutzergruppe löschen	User Management	
	> Benutzer der Gruppe zuweisen	User Management	
	> Benutzer abmelden	User Management	
Geräte	**Dieses Menü und die Benutzerstrukturansicht stehen nur Benutzern mit folgenden Berechtigungen zur Verfügung:** **Device-, Port- and Node Management (Geräte-, Port-, und Knotenverwaltung)** **Device Configuration and Upgrade Management (Gerätekonfiguration und Aktualisierungsverwaltung)**		
	Geräte erkennen	Device-, Port- and Node Management	
> Gerätemanager	> Gerät hinzufügen	Device-, Port- and Node Management	
	(Geräte bearbeiten)	Device-, Port- and Node Management	Über das Geräteprofil

MENÜ > UNTERMENÜ	MENÜELEMENT	ERFORDERLICHE BERECHTIGUNG	BESCHREIBUNG
	> Gerät löschen	Device-, Port- and Node Management	
	> Massenkopieren	Device-, Port- and Node Management	
	> Gerät aktualisieren	Device Configuration and Upgrade Management	
>> Konfiguration	>> Sicherungsknoten	Device Configuration and Upgrade Management	
	>> Wiederherstellen	Device Configuration and Upgrade Management	
	>> Konfiguration kopieren	Device Configuration and Upgrade Management	
	>> Gerät neu starten	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
	> Gerät anpingen	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
	> Verwaltung unterbrechen	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
	> Gerätestrommanager	Device-, Port- and Node Management	

MENÜ > UNTERMENÜ	MENÜELEMENT	ERFORDERLICHE BERECHTIGUNG	BESCHREIBUNG
	> Administration starten	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
	> Benutzerstation-Administration starten		
	> Benutzerverbindung trennen	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
	> Topologieansicht	Device-, Port- and Node Management	
> Ansicht ändern	> Benutzerdefinierte Ansicht erstellen	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
	> Strukturansicht	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
> Portmanager	> Verbinden	Device-, Port- and Node Management	
	> Ports konfigurieren	Device-, Port- and Node Management	
	> Lesezeichen für Port	Device-, Port- and Node Management	
	> Port trennen	Device-, Port- and Node Management	
	> Massenkopieren	Device-, Port- and Node Management	

MENÜ > UNTERMENÜ	MENÜELEMENT	ERFORDERLICHE BERECHTIGUNG	BESCHREIBUNG
	> Ports löschen	Device-, Port- and Node Management	
> Portsortieroptionen	> Nach Portname	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
	> Nach Portstatus	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
Knoten	**Dieses Menü und die Knotenstrukturansicht stehen nur Benutzern mit folgenden Berechtigungen zur Verfügung:** **Device-, Port- and Node Management (Geräte-, Port- und Knotenverwaltung)** **Node In-Band Access (In-Band Knotenzugriff)** **Node Out-of-Band Access (Out-of-Band Knotenzugriff)** **Node Power Control (Knoten-Stromversorgungssteuerung)**		
	Knoten hinzufügen	Device-, Port- and Node Management	
	(Knoten bearbeiten)	Device-, Port- and Node Management	Über das Knotenprofil
	Knoten löschen	Device-, Port- and Node Management	
	<Schnittstellenname>	In-Band-Zugriff oder Out-of-Band-Zugriff	
	Trennen	In-Band-Zugriff oder Out-of-Band-Zugriff	
	Stromversorgungssteuerung	Node Power Control	
	Gruppenstromversorgungssteuerung	Node Power Control	

MENÜ > UNTERMENÜ	MENÜELEMENT	ERFORDERLICHE BERECHTIGUNG	BESCHREIBUNG
> Knotensortier-optionen	> Nach Knotenname	Eine der Folgenden: Device-, Port- and Node Management In-Band-Zugriff oder Out-of-Band-Zugriff oder Node Power Control	
	> Nach Knotenstatus	Eine der Folgenden: Device-, Port- and Node Management Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	
> Chat	> Chatsitzung starten	Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	
	> Chatsitzung anzeigen	Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	
	> Chatsitzung beenden	Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	

MENÜ > UNTERMENÜ	MENÜELEMENT	ERFORDERLICHE BERECHTIGUNG	BESCHREIBUNG
> Ansicht ändern	> Benutzerdefinierte Ansicht erstellen	Eine der Folgenden: Device-, Port- and Node Management Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	
	> Strukturansicht	Eine der Folgenden: Device-, Port- and Node Management Node In-Band Access oder Node Out-of-Band Access oder Node Power Control	
Zuordnungen	**Dieses Menü steht nur Benutzern zur Verfügung, die die Berechtigung „User Security Management“ (Benutzersicherheitsverwaltung) aufweisen.**		
	> Zuordnungen	User Security Management	Umfasst Funktionen zum Hinzufügen, Bearbeiten und Löschen.
	> Gerätegruppe	User Security Management	Umfasst Funktionen zum Hinzufügen, Bearbeiten und Löschen.
	> Knotengruppe	User Security Management	Umfasst Funktionen zum Hinzufügen, Bearbeiten und Löschen.
	> Richtlinien	User Security Management	Umfasst Funktionen zum Hinzufügen, Bearbeiten und Löschen.
Berichte	**Dieses Menü steht allen Benutzern zur Verfügung.**		
	Überwachungsliste	CC Setup And Control	
	Fehlerprotokoll	CC Setup And Control	
	Zugriffsbericht	Nur Verfügbar für Benutzer in der Gruppe „System Administrators“	

MENÜ > UNTERMENÜ	MENÜELEMENT	ERFORDERLICHE BERECHTIGUNG	BESCHREIBUNG
	Verfügbarkeitsbericht	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
> Benutzer	> Aktive Benutzer	User Management	
	> Gesperrte Benutzer	CC Setup And Control	
	> Benutzerdaten	Zum Anzeigen aller Benutzerdaten: User Management Zum Anzeigen Ihrer eigenen Benutzerdaten: Keine	
	> Benutzer in Gruppen	User Management	
	> Gruppendaten	User Security Management	
	> AD-Benutzer-gruppenbericht	CC Setup and Control oder User Management	
> Geräte	Anlagenverwaltung	Device-, Port- and Node Management	
> Knoten	> Knotenanlagebericht	Device-, Port- and Node Management	
	> Aktive Knoten	Device-, Port- and Node Management	
	> Knotenerstellung	Device-, Port- and Node Management	
> Ports	> Port abfragen	Device-, Port- and Node Management	
	> Aktive Ports	Device-, Port- and Node Management	
	Geplante Berichte	CC Setup And Control	
	CC-NOC-Synchronisation	CC Setup And Control	
Zugang			

MENÜ > UNTERMENÜ	MENÜELEMENT	ERFORDERLICHE BERECHTIGUNG	BESCHREIBUNG
	CC-NOC-Konfiguration	CC Setup And Control	
Administration	**Dieses Menü steht nur Benutzern mit einer der folgenden Berechtigung zur Verfügung:** **CC Setup And Control (CC Setup und Steuerung)** **Kombination aus Device-, Port- and Node Management (Geräte-, Port- und Knotenverwaltung), User Management (Benutzerverwaltung) und User Security Management (Benutzersicherheitsverwaltung)**		
	Setup-Assistent	Alle der Folgenden: Device-, Port- and Node Management, User Management und User Security Management	
	Tipp des Tages einrichten	CC Setup And Control	
	Anwendungen	CC Setup And Control	
	Firmware	CC Setup And Control	
	Konfiguration	CC Setup And Control	
	Sicherheit	CC Setup And Control	
	Benachrichtigungen	CC Setup And Control	
	Aufgaben	CC Setup And Control	
	Kompatibilitätsmatrix	Device Configuration and Upgrade Management	
Systemwartung			
	Sicherungsknoten	CC Setup And Control	
	Wiederherstellen	CC Setup And Control	
	Zurücksetzen	CC Setup And Control	
	Neu starten	CC Setup And Control	
	Aktualisieren	CC Setup And Control	
	Herunterfahren	CC Setup And Control	
> Wartungsmodus	> Wartungsmodus starten	CC Setup And Control	
	> Wartungsmodus beenden	CC Setup And Control	

MENÜ > UNTERMENÜ	MENÜELEMENT	ERFORDERLICHE BERECHTIGUNG	BESCHREIBUNG
Ansicht		Keine*	
Fenster		Keine*	
Hilfe		Keine*	

*Keine bedeutet, dass keine bestimmte Berechtigung erforderlich ist. Benutzer mit Zugriff auf CC-SG können diese Menüs und Befehle anzeigen und darauf zugreifen.

Diese Seite wurde absichtlich leer gelassen.

Anhang D: SNMP-Traps

CC-SG stellt die folgenden Traps bereit:

SNMP-TRAP	BESCHREIBUNG
ccUnavailable	Die CC-SG-Anwendung ist nicht verfügbar.
ccAvailable	Die CC-SG-Anwendung ist verfügbar.
ccUserLogin	Ein Benutzer hat sich bei CC-SG angemeldet.
ccUserLogout	Ein Benutzer hat sich bei CC-SG abgemeldet.
ccPortConnectionStarted	CC-SG-Sitzung wurde gestartet.
ccPortConnectionStopped	CC-SG-Sitzung wurde angehalten.
ccPortConnectionTerminated	CC-SG-Sitzung wurde beendet.
ccImageUpgradeStarted	CC-SG-Abbildaktualisierung wurde gestartet.
ccImageUpgradeResults	Ergebnisse der CC-SG-Abbildaktualisierung.
ccUserAdded	Neuer Benutzer wurde zu CC-SG hinzugefügt.
ccUserDeleted	Benutzer wurde aus CC-SG gelöscht.
ccUserModified	Ein CC-SG-Benutzer wurde bearbeitet.
ccUserAuthenticationFailure	CC-SG-Fehler bei der Benutzerauthentifizierung.
ccLanCardFailure	CC-SG hat einen LAN-Kartenfehler erkannt.
ccHardDiskFailure	CC-SG hat einen Festplattenfehler erkannt.
ccLeafNodeUnavailable	CC-SG hat einen Verbindungsfehler zu einem Endknoten erkannt.
ccLeafNodeAvailable	CC-SG hat einen verfügbaren Endknoten erkannt.
ccIncompatibleDeviceFirmware	CC-SG hat ein Gerät mit inkompatibler Firmware erkannt.
ccDeviceUpgrade	CC-SG hat die Firmware auf einem Gerät aktualisiert.
ccEnterMaintenanceMode	CC-SG befindet sich im Wartungsmodus.
ccExitMaintenanceMode	CC-SG hat den Wartungsmodus verlassen.
ccUserLockedOut	CC-SG-Benutzer wurde gesperrt.
ccDeviceAddedAfterCCNOCNotification	CC-SG hat ein Gerät nach einer Benachrichtigung von CC-NOC hinzugefügt.
ccScheduledTaskExecutionFailure	Der Grund, warum eine geplante Aufgabe nicht durchgeführt werden konnte.
ccDiagnosticConsoleLogin	Benutzer hat sich in der CC-SG-Diagnosekonsole angemeldet.
ccDiagnosticConsoleLogout	Benutzer hat sich von der CC-SG-Diagnosekonsole abgemeldet.
ccNOCAvailable	CC-SG hat festgestellt, dass CC-NOC verfügbar ist.
ccNOCUnavailable	CC-SG hat festgestellt, dass CC-NOC nicht verfügbar ist.
ccUserGroupAdded	Eine neue Benutzergruppe wurde CC-SG hinzugefügt.
ccUserGroupDeleted	CC-SG-Benutzergruppe wurde gelöscht.
ccUserGroupModified	CC-SG-Benutzergruppe wurde bearbeitet.
ccSuperuserNameChanged	CC-SG-Superuser-Kennwort wurde geändert.
ccSuperuserPasswordChanged	CC-SG-Superuser-Kennwort wurde geändert.
ccLoginBannerChanged	CC-SG-Anmeldebanner wurde geändert.
ccMOTDChanged	CC-SG Tipp des Tages wurde geändert.

Diese Seite wurde absichtlich leer gelassen.

Anhang E: Problembehandlung

- Wenn Sie CC-SG über Ihren Webbrowser starten möchten, benötigen Sie ein Java-Plug-in. Verfügt Ihr Computer nicht über die richtige Version, führt CC-SG Sie durch die Installationsschritte. Verfügt Ihr Computer nicht über ein Java-Plug-in, kann CC-SG nicht automatisch gestartet werden. In dem Fall müssen Sie Ihre alte Java-Version deinstallieren oder deaktivieren und für einwandfreien Betrieb die Konnektivität über einen seriellen Port zu CC-SG herstellen.
- Wird das CC-SG-Applet nicht geladen, überprüfen Sie die Webbrowsereinstellungen.
  - In Internet Explorer: Vergewissern Sie sich, dass die Java-Option aktiviert ist.
  - Öffnen Sie das Java-Plug-in über die Systemsteuerung, und passen Sie die Einstellungen für Ihren Browser an.
- Treten beim Hinzufügen von Geräten Probleme auf, überprüfen Sie, ob diese Geräte mit den korrekten Firmwareversionen ausgestattet sind.
- Wird das Netzwerkschnittstellenkabel zwischen dem Gerät und CC-SG getrennt, warten Sie den Zeitraum der konfigurierten Heartbeat-Minuten ab, bevor Sie das Netzwerkschnittstellenkabel erneut anschließen. Während des konfigurierten Heartbeat-Zeitraums wird das Gerät im eigenständigen Modus betrieben, und der Zugriff ist über RRC, MPC oder RC möglich.
- Wenn Sie eine Fehlermeldung erhalten, dass Ihre Clientversion von der Serverversion abweicht und das Verhalten ggf. unvorhersehbar ist, sollten Sie einen Neustart durchführen und den Zwischenspeicher Ihres Browsers löschen.

Clientbrowser-Anforderungen

(Eine vollständige Liste der unterstützen Browser und Plattformen finden Sie in der **Kompatibilitätsmatrix** unter **http://www.raritan.com/support**. Klicken Sie auf der Seite **Support** auf **Firmwareaktualisierungen** und dann auf **CommandCenter Secure Gateway**.)

Diese Seite wurde absichtlich leer gelassen.

Anhang F: Zwei-Faktoren-Authentifizierung

Als Teil der CC-SG RADIUS-basierten Remoteauthentifizierung kann CC-SG so konfiguriert werden, dass es auf einen RSA RADIUS-Server zeigt, der die Zwei-Faktoren-Authentifizierung über einen verknüpften RSA-Authentifizierungsmanager unterstützt. CC-SG funktioniert wie ein RADIUS-Client und sendet die Benutzerauthentifizierungsanfragen an den RSA RADIUS-Server. Die Authentifizierungsanfrage umfasst die Benutzer-ID, ein festgelegtes Kennwort und einen Code für den dynamischen Token.

Unterstützte Umgebungen

Die folgenden Komponenten der RSA Zwei-Faktoren-Authentifizierung funktionieren mit CC-SG.

- RSA RADIUS Server 6.1 unter Windows Server 2003
- RSA Authentication Manager 6.1 unter Windows Server 2003
- RSA Secure ID SID700 Hardware Token.

Frühere RSA-Produktversionen sollten auch mit CC-SG funktionieren, dies wurde jedoch noch nicht getestet.

Setupanforderungen

Die richtige Konfiguration eines RSA RADIUS-Servers und RSA-Authentifizierungsmanagers würde den Rahmen dieses Handbuchs sprengen. Weitere Informationen finden Sie in der RSA-Dokumentation.

Beachten Sie jedoch, dass folgende Schritte durchgeführt werden müssen:

1. Token importieren.
2. CC-SG-Benutzer erstellen und Token dem Benutzer zuweisen.
3. Benutzerkennwort erstellen.
4. Agent Host für den RADIUS-Server erstellen.
5. Agent Host (Typ: Kommunikationsserver) für CC-SG erstellen.
6. RADIUS CC-SG-Client erstellen.

Bekannte Probleme

Der Modus RSA RADIUS „New PIN“, der ein Herausforderungskennwort/PIN erfordert, funktioniert nicht. Benutzern in diesem Schema müssen stattdessen festgelegte Kennwörter zugewiesen werden.

Diese Seite wurde absichtlich leer gelassen.

Anhang G: Häufig gestellte Fragen (FAQs)

FRAGE	ANTWORT
Allgemein	
Was ist CC-SG?	CC-SG ist ein Netzwerkverwaltungsgerät zum Aggregieren und Integrieren mehrerer in einem Rechenzentrum bereitgestellter Server und Netzwerkgeräte, die an einem IT-fähigen Raritan-Gerät angeschlossen sind.
Wozu kann ich CC-SG einsetzen?	Mit zunehmender Anzahl von Servern und Geräten im Rechenzentrum wird deren Verwaltung immer komplexer. CC-SG ermöglicht dem Systemadministrator über nur ein Gerät auf alle Server, Geräte und Benutzer zuzugreifen und diese zu verwalten und anzuzeigen.
Was ist CommandCenter-NOC?	CommandCenter-NOC ist ein Netzwerküberwachungsgerät zur Überprüfung und Überwachung des Status von Servern, Geräten und Raritan-Geräten, auf die CC-SG Zugriff bietet.
Welche Raritan-Produkte unterstützt CC-SG?	CC-SG unterstützt alle Dominion-Produkte: - Raritan KVM-über-IP-Produkte – Dominion KX - Raritan Secure Console Server-Produkte – Dominion SX - Raritan-Produkte zur Verwaltung von Remoteniederlassungen – Dominion KSX. CC-SG unterstützt in Verbindung mit optionalen IP-Benutzerstationen auch Paragon II.
Wie wird CC-SG in andere Raritan-Produkte integriert?	CC-SG verwendet eine einmalige und proprietäre Such- und Erkennungstechnologie zum Herstellen einer Verbindung mit ausgewählten Raritan-Geräten mit einer bekannten Netzwerkadresse. Nach der Verbindungsherstellung und Konfiguration von CC-SG erhalten Sie eine transparente Übersicht über alle an CC-SG angeschlossenen Geräte, die leicht betrieben und verwaltet werden können.
Ist der PDA-Zugriff möglich?	Im Allgemeinen ja, solange der PDA über einen Java-fähigen Browser verfügt und die 128-Bit SSL-Verschlüsselung (oder geringer in einigen Regionen) unterstützt. Wenden Sie sich an den technischen Support von Raritan, wenn Sie weitere Informationen benötigen. Diesbezüglich wurden keine Tests durchgeführt.
Wird der Status von CC-SG durch den Status der Geräte beschränkt, für die es als Proxy eingesetzt wird?	Nein. Da die CC-SG-Software auf einem dedizierten Server ausgeführt wird, haben Sie auch dann Zugriff auf CC-SG, wenn ein Gerät ausgeschaltet ist, für das CC-SG als Proxy fungiert.
Kann ich auf neuere Versionen der CC-SG-Software aktualisieren, wenn sie erhältlich sind?	Ja. Wenden Sie sich hierzu an einen Raritan-Vertriebsmitarbeiter oder direkt an Raritan, Inc.
Wie viele Knoten und/oder Dominion- und/oder IP-Reach-Geräte können an CC-SG angeschlossen werden?	Für die Anzahl von Knoten und/oder Dominion- und/oder IP-Reach-Geräten, die an CC-SG angeschlossen werden können, gibt es keinen festgelegten Höchstwert. Allerdings können auch nicht unendlich viele Ports/Geräte angeschlossen werden. Die Leistung des Prozessors und der Arbeitsspeicher des Hostservers bestimmen, wie viele Ports tatsächlich angeschlossen werden können.

FRAGE	ANTWORT
Kann ich die Leistung von Microsoft Internet Explorer optimieren, wenn ich diesen als bevorzugten Webbrowser verwende?	Zum Verbessern der Leistung von Microsoft Internet Explorer beim Zugriff auf die Konsole deaktivieren Sie die Optionen **Java JIT-Compiler aktiviert**, **Java-Protokollierung aktiviert** und **Java-Konsole aktiviert**. Wählen Sie in der Hauptmenüleiste **Extras > Internetoptionen > Erweitert**. Vergewissern Sie sich, dass diese Optionen **nicht** aktiviert sind.
Wie gehe ich vor, wenn ich CC-SG keinen Konsolenport/seriellen Port hinzufügen kann?	Wenn das Konsolengerät/serielle Gerät ein Dominion-Produkt ist, stellen Sie Folgendes sicher: - Die Dominion-Einheit ist aktiviert. - Die maximale Anzahl konfigurierter Benutzerkonten für die Dominion-Einheit wurde noch nicht erreicht.
Welche Java-Version unterstützt Raritan CC-SG?	Weitere Informationen zu den server-und clientseitigen Java-Anforderungen erhalten Sie in der Kompatibilitätsmatrix unter **http://www.raritan.com/support**. Klicken Sie auf **Firmwareaktualisierungen** und dann auf **CommandCenter Secure Gateway**.
Ein Administrator hat der CC-SG-Datenbank einen neuen Knoten hinzugefügt und mir diesen Knoten zugewiesen. Wie kann ich den Knoten in meiner Knotenstruktur anzeigen?	Klicken Sie auf der Symbolleiste auf die Schaltfläche **Aktualisieren**, um die Struktur zu aktualisieren und den neu zugewiesenen Knoten anzuzeigen. Vergessen Sie nicht, dass beim Aktualisieren von CC-SG alle derzeitigen Konsolensitzungen geschlossen werden.
Inwiefern wird der Windows-Desktop in Zukunft unterstützt?	Der Zugriff auf CC-SG von außerhalb der Firewall wird durch Konfigurieren der richtigen Ports an der Firewall ermöglicht. Die folgenden Ports sind Standardports: 80: für HTTP-Zugriff über einen Webbrowser 443: für HTTPS-Zugriff über einen Webbrowser 8080: für den CC-SG-Serverbetrieb 2400: für Verbindungen im Proxymodus 5001: für IPR-/DKSX-/DKX-/P2-SC-Ereignisbenachrichtigung Wenn sich zwischen zwei Clusterknoten eine Firewall befindet, sollten die folgenden Ports für den problemlosen Betrieb des Clusters geöffnet werden: 8732: für den Clusterknotenheartbeat 5432: für Clusterknoten-DB-Replikation
Welche Richtlinien gelten für den Entwurf umfangreicher Systeme – sind Beschränkungen oder Voraussetzungen vorhanden?	Raritan bietet zwei Modelle für die Serverskalierbarkeit: das Rechenzentrummodell und das Netzwerkmodell. Das Rechenzentrummodell verwendet Paragon zum Skalieren auf Tausende von Systemen in einem Rechenzentrum. Dies ist die effektivste und kostengünstigste Methode zum Skalieren eines einzelnen Standorts. Diese Methode unterstützt auch das Netzwerkmodell mit IP-Reach und der IP-Benutzerstation (UST-IP). Das Netzwerkmodell skaliert mittels TCP/IP-Netzwerk und aggregiert den Zugriff über CC-SG, weshalb die Benutzer weder IP-Adressen noch die Topologie von Zugriffsgeräten kennen müssen. Außerdem ist nur eine Anmeldung erforderlich.

FRAGE	ANTWORT
Authentifizierung	
Wie viele Benutzerkonten können für CC-SG erstellt werden?	Überprüfen Sie die Bestimmungen in Ihrer Lizenz. Für die Anzahl von Benutzerkonten, die für CC-SG erstellt werden können, liegt keine festgelegte Beschränkung vor. Es kann jedoch auch keine unbegrenzte Anzahl von Konten erstellt werden. Die Größe der Datenbank, die Leistung des Prozessors und der Arbeitsspeicher des Hostservers beeinflussen die Anzahl der Benutzerkonten, die erstellt werden können.
Kann ich einem bestimmten Benutzer einen spezifischen Knotenzugriff zuweisen?	Ja, wenn Sie Administratorberechtigungen besitzen. Administratoren haben die Möglichkeit, jedem Benutzer bestimmte Knoten zuzuweisen.
Wie erfolgt die Verwaltung bei mehr als 1000 Benutzern? Wird Active Directory unterstützt?	CC-SG ist mit Microsoft Active Directory, Sun iPlanet oder Novell eDirectory kompatibel. Ist ein Benutzerkonto bereits auf einem Authentifizierungsserver vorhanden, unterstützt CC-SG die Remoteauthentifizierung mittels **AD/TACACS+/RADIUS/LDAP**.
Welche Optionen sind für die Authentifizierung mit Verzeichnisdiensten und Sicherheitstools verfügbar (z. B. LDAP, AD, Radius usw.)	CC-SG lässt sowohl die lokale Authentifizierung als auch die Remoteauthentifizierung zu. Zu den unterstützten Remoteauthentifizierungsservern zählen: AD, TACACS+, RADIUS und LDAP.
Sicherheit	
Beim Anmelden wird manchmal eine Meldung mit dem Hinweis angezeigt, dass die falschen Anmeldeinformationen verwendet wurden, obwohl ich sicher bin, dass ich den korrekten Benutzernamen und das richtige Kennwort eingebe. Woran liegt das?	Bei jeder Anmeldung in CC-SG wird eine sitzungsspezifische ID gesendet. Diese ID verfügt über eine Timeoutfunktion. Wenn Sie sich nach diesem Timeout bei der Einheit anmelden, ist die Sitzungs-ID ungültig. Wenn Sie bei gedrückter Umschalttaste auf den Befehl zum erneuten Laden klicken, wird die Seite von CC-SG aktualisiert. Sie können auch das aktuelle Browserfenster schließen, ein neues Browserfenster öffnen und sich dann erneut anmelden. Dieses Verfahren verbessert die Sicherheit, da die im Webcache gespeicherten Informationen nicht für den Zugriff auf die Einheit verwendet werden können.
Wie werden Kennwörter gesichert?	Kennwörter werden mittels MD5-Verschlüsselung, einem unidirektionalen Hash, verschlüsselt. Hierdurch erhalten Sie zusätzliche Sicherheit, um den Zugriff nicht autorisierter Benutzer auf die Kennwortliste zu verhindern.
Manchmal wird beim Klicken auf ein beliebiges Menü in CC-SG der Hinweis angezeigt, dass ich nicht mehr angemeldet bin, nachdem ich meine Arbeitsstation eine Zeit lang nicht verwendet habe. Woran liegt das?	CC-SG misst die Zeit jeder Benutzersitzung. Findet während eines vordefinierten Zeitraums keine Aktivität statt, meldet CC-SG den Benutzer ab. Die konfigurierbare Länge dieses Zeitraums ist auf 60 Minuten voreingestellt. Es wird empfohlen, dass die Benutzer CC-SG nach Abschluss einer Sitzung beenden.

FRAGE	ANTWORT
Da Raritan Stammzugriff auf den Server erhält, kann dies zu Schwierigkeiten mit Regierungsbehörden führen. Können Kunden ebenfalls Zugriff auf Stammebene erhalten, oder bietet Raritan eine Methode diesen Zugriff zu überprüfen oder für diesen Zugriff Verantwortung zu übernehmen?	Nachdem ein Gerät von Raritan, Inc. ausgeliefert wurde, hat niemand mehr Zugriff auf den Server.
Erfolgt die SSL-Verschlüsselung sowohl intern als auch extern (nicht nur WAN, sondern auch LAN)?	Sowohl intern als auch extern. Die Sitzung wird unabhängig von der Quelle (LAN/WAN) verschlüsselt.
Unterstützt CC-SG die CRL-Liste, d. h., die LDAP-Liste ungültiger Zertifikate?	Nein.
Unterstützt CC-SG Client Certificate Request?	Nein.
Kontoführung	
Die Ereigniszeiten im Überwachungslistenbericht scheinen nicht zu stimmen. Woran liegt das?	Die Protokollereigniszeiten werden gemäß den Zeiteinstellungen des Client-Computers protokolliert. Sie können die Zeit- und Datumseinstellungen des Computers anpassen.
Besteht die Möglichkeit festzustellen, wer einen Netzschalter ein- oder ausgeschaltet hat?	Das direkte Ausschalten des Netzschalters wird nicht protokolliert. Allerdings wird das Ein-/Ausschalten über CC-SG protokolliert.
Leistung	
Als CC-SG-Administrator habe ich über 500 Knoten hinzugefügt, die ich alle mir zugewiesen habe. Das Anmelden in CC-SG nimmt jetzt sehr viel Zeit in Anspruch.	Wenn Sie sich als Administrator viele Knoten zugewiesen haben, lädt CC-SG beim Anmelden alle Knoteninformationen. Der Anmeldvorgang wird dadurch beträchtlich verlangsamt. Administratorkonten sollten in erster Linie zum Verwalten der Konfiguration und Einstellungen von CC-SG verwendet werden. Diesen Konten sollte keine hohe Anzahl von Knoten zugewiesen werden.
Wie ist die Bandbreitennutzung pro Client?	Der Remotezugriff auf eine serielle Konsole über TCP/IP verursacht die gleiche Netzwerkaktivität wie eine telnet-Sitzung. Allerdings ist der Durchsatz auf die RS232-Bandbreite des Konsolenports plus SSL/TCP/IP-Overhead beschränkt. Der Raritan Remote Client (RRC) steuert den Remotezugriff auf eine KVM-Konsole. Diese Anwendung bietet eine konfigurierbare Bandbreite, von der LAN-Bandbreite bis zu einer für einen Remotebenutzer geeigneten Bandbreite.

FRAGE	ANTWORT
Gruppierung	
Kann ein bestimmter Server mehreren Gruppen hinzugefügt werden?	Ja. Genau so, wie ein Benutzer mehreren Gruppen angehören kann, kann auch ein Gerät mehreren Gruppen angehören. Beispiel: Eine Sun-Station in New York City kann den Gruppen Sun: „Betriebssystemtyp = Solaris“ und der Gruppe New York City: „Standort = NYC“ angehören.
Welche andere Verwendung würde durch die aktive Verwendung des Konsolenports blockiert werden (z. B. einige UNIX-Varianten, die über Netzwerkschnittstellen keine Verwaltung zulassen)?	Eine Konsole gilt allgemein als sicherer und zuverlässiger Zugriffspfad. Einige UNIX-Systeme erlauben den Zugriff auf Stammebene nur an der Konsole. Aus Sicherheitsgründen verhindern andere Systeme u. U. mehrere Anmeldungen, weshalb Benutzern der Zugriff verweigert wird, wenn der Administrator angemeldet ist. Der Administrator kann außerdem, falls notwendig, die Netzwerkschnittstellen von der Konsole aus deaktivieren, um den gesamten anderen Zugriff zu blockieren. Die normale Eingabe von Befehlen an der Konsole hat keine andere Auswirkung als die Eingabe gleicher Befehle an jeder anderen Schnittstelle. Da die Konsolenanmeldung nicht vom Netzwerk abhängig ist, unterstützt ein überlastetes System, das auf eine Netzwerkanmeldung nicht mehr reagiert, trotzdem die Konsolenanmeldung. Ein weiterer Vorteil des Konsolenzugriffs sind die Problembehandlung und Diagnose bei System- und Netzwerkproblemen.
Wie wird der Tausch von CIMS auf physischer Ebene mit Änderungen in der logischen Datenbank vereinbart?	Jedes CIM besitzt eine Seriennummer und einen Zielsystemnamen. Raritan-Systeme gehen davon aus, dass ein CIM am benannten Ziel angeschlossen bleibt, wenn seine Verbindung zwischen Switches verschoben wird. Dieses Verschieben wird automatisch in der Systemkonfiguration berücksichtigt und von CC-SG registriert. Wird ein CIM jedoch auf einen anderen Server verschoben, muss es vom Administrator umbenannt werden.
Interoperabilität	
Wie wird CC-SG in andere Blade Chassis-Produkte integriert?	CC-SG unterstützt jedes Gerät mit einer KVM-Schnittstelle oder seriellen Schnittstelle als transparentes Durchgangsgerät.
Bis zu welchem Grad ist CC-SG in KVM-Tools anderer Anbieter bis zur KVM-Port-Ebene oder Standardkonfigurationsebene integrierbar?	Die Integration in KVM-Switches von Drittanbietern erfolgt normalerweise über Tastaturmakros, wenn KVM-Drittanbieter die Kommunikationsprotolle für diese Switches nicht veröffentlichen. Je nach Fähigkeiten der KVM-Switches von Drittanbietern variiert der Grad der Integration.
Wie kann ich die Beschränkung von vier gleichzeitigen Pfaden über ein IP-Reach-Gerät umgehen und eine 8-Pfad-Lösung realisieren?	Die beste derzeitige Implementierung ist das Aggregieren von IP-Reach-Geräten mit CC-SG. Raritan beabsichtigt, die gleichzeitigen Zugriffspfade pro Gerät in Zukunft zu erhöhen. Dieses Vorhaben befindet sich noch in der Entwicklungsphase, da andere Projekte Vorrang haben. Wir freuen uns jedoch über Anregungen zu Nachfrage und Verwendungsbeispielen einer 8-Pfad-Lösung.

FRAGE	ANTWORT
Autorisierung	
Ist die Autorisierung über RADIUS/TACACS+/LDAP möglich?	LDAP und TACACS werden nur zur Remoteauthentifizierung und nicht zur Autorisierung verwendet.
Benutzerfreundlichkeit	
Bei der Konsolenverwaltung über Netzwerkport oder lokalen seriellen Port (z. B. COM2): Was geschieht mit der Protokollierung; erfasst CC-SG lokale Verwaltung oder geht diese verloren?	Das Anmelden in CC-SG über die CC-SG-Konsole gleicht dem Zuweisen der Stammberechtigung für das Betriebssystem (Linux), das im CC-SG ausgeführt wird. Syslog zeichnet diese Art von Ereignis auf. Die Benutzereingabe an der CC-SG-Konsole geht jedoch verloren.

Anhang H: Tastenkombinationen

Die folgenden Tastenkombinationen können im Administrations-Client verwendet werden.

VORGANG	TASTENKOMBINATIONEN
Aktualisieren	F5
Fenster drucken	Strg + P
Hilfe	F1
Zeile in Verknüpfungstabelle einfügen	Strg + I

Firmenhauptsitz in Nordamerika

Raritan

400 Cottontail Lane
Somerset, NJ 08873
USA
Tel. (1) (732) 764-8886
oder (1) (800) 724-8090
Fax (1) (732) 764-8887
E-Mail: **sales@raritan.com**
Website: Raritan.com

Raritan NC

4901 Waters Edge Dr.
Suite 101
Raleigh, NC 27606
Tel. (919) 277-0642
E-Mail: **sales.nc@raritan.com**
Website: Raritan.com

Raritan Canada

4 Robert Speck Pkwy, Suite 1500
Mississauga, ON L4Z 1S1 Kanada
Tel. (1) (905) 949-3650
Fax (1) (905) 949-3651
E-Mail: **sales.canada@raritan.com**
Website: Raritan.ca

Firmenhauptsitz in Europa

Raritan Netherlands

Eglantierbaan 16
2908 LV Capelle aan den IJssel
Niederlande
Tel. (31) 10-284-4040
Fax (31) 10-284-4049
E-Mail: **sales.europe@raritan.com**
Website: Raritan.info

Raritan Germany

Lichtstraße 2
D-45127 Essen, Deutschland
Tel. (49) 201-747-98-0
Fax (49) 201-747-98-50
Email: **sales.germany@raritan.com**
Website: Raritan.de

Raritan France

120 Rue Jean Jaurés
92300 Levallois-Perret, Frankreich
Tel. (33) 14-756-2039
Fax (33) 14-756-2061
E-Mail: **sales.france@raritan.com**
Website: Raritan.fr

Raritan U.K.

36 Great St. Helen's
London EC3A 6AP, United Kingdom
Tel. (44) 20-7614-7700
Fax (44) 20-7614-7701
E-Mail: **sales.uk@raritan.com**
Website: Raritan.co.uk

Raritan Italy

Via dei Piatti 4
20123 Milan, Italien
Tel. (39) 02-454-76813
Fax (39) 02-861-749
E-Mail: **sales.italy@raritan.com**
Website: Raritan.it

Firmenhauptsitz in Japan

Raritan Japan

4th Floor, Shinkawa NS Building
1-26-2 Shinkawa, Chuo-Ku
Tokio 104-0033, Japan
Tel. (81) 03-3523-5991
Fax (81) 03-3523-5992
E-Mail: **sales@raritan.co.jp**
Website: Raritan.co.jp

Raritan Osaka

1-15-8 Nishihonmachi, Nishi-ku
Osaka 550-0005, Japan
Tel. (81) (6) 4391-7752
Fax (81) (6) 4391-7761
E-Mail: **sales@raritan.co.jp**
Website: Raritan.co.jp

Firmenhauptsitz Asien-Pazifik

Raritan Taiwan

5F, 121, Lane 235, Pao-Chiao Road
Hsin Tien City
Taipei Hsien, Taiwan, Republik China
Tel. (886) 28919-1333
Fax (886) 28919-1338
E-Mail: **sales.taiwan@raritan.com**
Chinesische Website: Raritan.com.tw
Englische Website: Raritan-ap.com

Raritan Shanghai

Rm 17E Cross Region Plaza
No. 899 Lingling Road
Schanghai, China 200030
Tel. (86) 215425-2499
Fax (86) 215425-3992
E-Mail: **sales.china@raritan.com**
Website: Raritan.com.cn

Raritan Beijing

Unit 1310, Air China Plaza
No.36 XiaoYun Road
Chaoyang District
Peking 100027, China
Tel. (86) 108447-5706
Fax (86) 108447-5700
E-Mail: **sales.china@raritan.com**
Website: Raritan.com.cn

Raritan Guangzhou

Room 1205/F, Metro Plaza
183 Tian He Bei Road
Guangzhou 510075, China
Tel. (86-20) 8755 5581
Fax (86-20) 8755 5571
E-Mail: **sales.china@raritan.com**
Website: Raritan.com.cn

Raritan Korea

#3602, Trade Tower,
World Trade Center
Samsung-dong, Kangnam-gu
Seoul, Korea
Tel: (82) 2 557-8730
Fax (82) 2 557-8733
E-Mail: **sales.korea@raritan.com**
Website: Raritan.co.kr

Raritan Australia

Level 2, 448 St Kilda Road,
Melbourne, VIC 3004, Australien
Tel. (61) 39866-6887
Fax (61) 39866-7706
E-Mail: **sales.au@raritan.com**
Website: Raritan.co.au

Raritan India

210 2nd Floor Orchid Square Sushant Lok 1,
Block B, Gurgaon 122 002 Haryana Indien
Tel. (1) (91) 124 5107881
Fax (1) (91) 124 5107880
E-Mail: **sales.india@raritan.com**
Website: Raritan.co.in

Raritan OEM Division

Peppercon AG, Raritan OEM Division
Scheringerstrasse 1
08056 Zwickau, Deutschland
Tel: (49) 375-27-13-49-0
E-Mail: **info@peppercon.com**
Website: www.peppercon.de