CC-SG

CommandCenter Secure Gateway

Handbuch für Administratoren

Version 3.2

CCA-0F-G
Oktober 2007
255-80-5140-00

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.

VCCI-Informationen (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.

Inhalt

Kapitel 15 Erweiterte Administration 173

Anhang B CC-SG und Netzwerkkonfiguration 272

CC-SG – Voraussetzungen

Dieses Kapitel enthält einige der am häufigsten vorkommenden Anwendungsfälle, damit sich Benutzer schnell mit der praktischen Anwendung von CC-SG vertraut machen können. Bitte beachten Sie, dass dieser Abschnitt allgemeine Beispiele bietet, die entsprechend der tatsächlich vorhandenen Konfiguration und Vorgänge variieren können.

In diesem Kapitel

So konfigurieren und erzwingen Sie sichere Kennwörter

1. Wählen Sie **Administration** > **Sicherheit**.
2. Öffnen Sie die Registerkarte **Anmeldeeinstellungen**.
3. Markieren Sie das Kontrollkästchen **Sichere Kennwörter für alle Benutzer erforderlich**.
4. Wählen Sie eine **Maximale Kennwortlänge**. Kennwörter müssen weniger als die maximale Anzahl an Zeichen enthalten.
5. Wählen Sie eine **Länge der Kennwortchronik**. Diese Zahl legt fest, wie viele vorherige Kennwörter in der Chronik gespeichert werden und nicht erneut verwendet werden können. Ist **Länge der Kennwortchronik** beispielsweise auf 5 festgelegt, können Benutzer keines ihrer vorherigen 5 Kennwörter verwenden.

6. Wählen Sie einen **Kennwort-Ablaufintervall**. Alle Kennwörter laufen nach einer festgelegten Anzahl an Tagen ab. Nachdem ein Kennwort abgelaufen ist, müssen Benutzer beim nächsten Anmelden ein neues Kennwort eingeben.
7. Wählen Sie **Anforderungen für sichere Kennwörter**:
   - 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.
8. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Weitere Informationen zur Anmeldesicherheit finden Sie unter *Anmeldeeinstellungen* (auf Seite 202).

CC-SG auf eine neue Firmware-Version aktualisieren

Sie können die Firmware von CC-SG aktualisieren, wenn eine neuere Version veröffentlicht wird. Sie finden die Firmware-Dateien auf der Raritan-Website im Support-Bereich.

Laden Sie die Firmware-Datei auf Ihren Client-PC herunter, bevor Sie mit der Aktualisierung beginnen.

Sie sollten vor dem Aktualisieren eine Sicherheitskopie von CC-SG erstellen. Wenn Sie mit einem CC-SG-Cluster arbeiten, müssen Sie zuerst das Cluster entfernen und jeden Knoten einzeln aktualisieren.

Hinweis: Wenn Sie von 3.0.2 auf 3.1 aktualisieren und Active Directory verwenden, lesen Sie bitte in der Readme-Datei der Version 3.1 die besonderen Anleitungen.

Wichtig!

Wenn Sie sowohl CC-SG als auch ein Gerät oder eine Gerätegruppe aktualisieren müssen, aktualisieren Sie zuerst CC-SG und dann die Geräte.

CC-SG wird während des Aktualisierungsvorgangs von 3.1.1 auf 3.2 neu gestartet. Während der Aktualisierung dürfen Sie Folgendes NICHT: den Vorgang anhalten, die Einheit manuell neu starten, die Einheit ausschalten oder die Einheit aus- und einschalten.

➢ *So aktualisieren Sie CC-SG:*

1. Laden Sie die Datei mit der Firmware auf Ihren Client PC herunter.
2. ***Wartungsmodus starten*** (auf Seite 163)
3. Sobald sich CC-SG im Wartungsmodus befindet, wählen Sie **Systemwartung** > **Aktualisieren**.
4. Klicken Sie auf **Durchsuchen**. Wechseln Sie zur CC-SG-Firmwaredatei, wählen Sie diese aus, und klicken Sie auf **Öffnen**.
5. Klicken Sie auf **OK**, um die Firmwaredatei an CC-SG zu senden.

   Nachdem die Firmwaredatei an CC-SG gesandt wurde, wird eine Erfolgsmeldung angezeigt. In dieser Meldung wird Ihnen mitgeteilt, dass CC-SG mit dem Aktualisierungsvorgang begonnen hat. Dazu werden alle Benutzer bei CC-SG abgemeldet.
6. Klicken Sie auf **OK**, um CC-SG zu verlassen und den Neustart durchzuführen. Sie müssen ca. 8 Minuten warten, während CC-SG neu startet.
7. Schließen Sie Ihr Browserfenster, und löschen Sie den Browser-Cache.
8. Öffnen Sie nach 8 Minuten ein neues Browserfenster, und starten Sie CC-SG.
9. Wählen Sie **Hilfe** > **Info zu Raritan Secure Gateway**. Überprüfen Sie die Versionsnummer, um zu bestätigen, 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.

Wartungsmodus beenden (auf Seite 163)

Stromversorgung zu einer Knotengruppe steuern und den Stromversorgungs-Steuervorgang überwachen

Stromversorgung für Knotengruppe steuern

Sie können alle Knoten in einer Gruppe einschalten, ausschalten, aus- und einschalten und normal herunterfahren, wenn diese mit einer Stromversorgungs-Schnittstelle verknüpft sind.

Dies ist nützlich, wenn Sie alle Knoten in einer Knotengruppe ausschalten müssen, damit Sie am Gestell und der Verkabelung der Knoten arbeiten können, oder wenn Sie andere Wartungsarbeiten an einer Knotengruppe durchführen müssen.

Weitere Informationen zum Einrichten von Stromversorgungs-Steuerungsvorgängen für Knoten mit mehreren Stromversorgungs-Steuerungsschnittstellen finden Sie unter Tipps zur Stromversorgungssteuerung von Knoten mit mehreren Schnittstellen.

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Klicken Sie im Menü **Knoten** auf **Gruppenstromversorgungssteuerung**. Das Fenster **Gruppenstromversorgungssteuerung** wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Knotengruppe**, und wählen Sie in der Liste die Knotengruppe aus, deren Stromversorgung gesteuert werden soll.
4. Wählen Sie in der Liste **Verfügbar** die Schnittstelle für den Stromversorgungs-Steuerungsvorgang aus, und klicken Sie dann auf **Hinzufügen**, um die Schnittstelle in die Liste **Ausgewählt** zu verschieben. Wiederholen Sie diesen Schritt, bis alle erforderlichen Schnittstellen in der Liste **Ausgewählt** aufgeführt werden. Wenn Sie eine Schnittstelle entfernen möchten, wählen Sie diese in der Liste **Ausgewählt** aus, und klicken Sie auf **Entfernen**.
5. Sie müssen die Schnittstellen der Liste **Ausgewählt** in der Reihenfolge anordnen, in der CC-SG den Stromversorgungs-Steuerungsvorgang ausführen soll. Wählen Sie in der Liste **Ausgewählt** eine Schnittstelle aus, und verschieben Sie die Schnittstellen mit den Pfeilschaltflächen nach unten bzw. oben, um die Schnittstellen in die gewünschte Reihenfolge zu bringen.
6. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Vorgang**, und wählen Sie in der Liste **Einschalten**, **Ausschalten**, **Aus- und einschalten** oder **Normal herunterfahren** aus.

7. Wenn Sie im Feld **Vorgang** die Option **Einschalten**, **Ausschalten** oder **Normal herunterfahren** ausgewählt haben, geben Sie die Zeitdauer in Sekunden (0 bis 120) in das Feld **Vorgangsintervall (Sekunden)** ein, die zwischen den Schnittstellen liegen soll.
8. Klicken Sie auf **OK**, um die Anfrage für den Stromversorgungs-Steuervorgang über die ausgewählten Schnittstellen zu senden. Auf dem Bildschirm wird eine Bestätigungsmeldung angezeigt.
9. Das Fenster **Meldungen zum Stromversorgungsstatus für** wird geöffnet, in dem der Status des Stromversorgungs-Steuerungsvorgangs angezeigt wird. In diesem Fenster werden Meldungen eingeblendet, wenn neue Informationen zum Stromversorgungs-Steuerungsvorgang vorliegen. Lassen Sie dieses Fenster geöffnet, bis alle Stromversorgungs-Steuerungsvorgänge abgeschlossen sind, um den Fortschritt zu überwachen.

   Weitere Informationen zu den CC-SG-Meldungen zu erfolgreichen und fehlgeschlagenen Stromversorgungs-Steuerungsvorgängen finden Sie unter ***Meldungen zum Stromversorgungsstatus*** (auf Seite 19).

Meldungen zum Stromversorgungsstatus

Das Fenster **Meldungen zum Stromversorgungsstatus für** wird angezeigt, wenn Sie einen Stromversorgungs-Steuerungsvorgang starten. Sie sollten dieses Fenster geöffnet lassen, bis alle Stromversorgungs-Steuerungsvorgänge abgeschlossen sind.

Sie können das Fenster vergrößern/verkleinern, minimieren oder maximieren und den Text im Fenster kopieren und an einer anderen Stelle einfügen.

Das Fenster **Meldungen zum Stromversorgungsstatus für** wird aktualisiert, wenn neue Informationen zum Status des Stromversorgungs-Steuerungsvorgangs vorliegen.

In folgenden Situationen wird eine neue Meldung im Fenster **Meldungen zum Stromversorgungsstatus für** angezeigt:

- Die Anforderung des Stromversorgungs-Steuerungsvorgangs wurde gesendet.
- Der Stromversorgungs-Steuerungsvorgang ist fehlgeschlagen.
- Der Stromversorgungs-Steuerungsvorgang wurde erfolgreich abgeschlossen.

- Alle angeforderten Stromversorgungs-Steuerungsvorgänge wurden erfolgreich abgeschlossen.

➢ *So werden die Statusinformationen beim Schließen des Fensters "Meldungen zum Stromversorgungsstatus für" aktualisiert:*

Wenn Sie das Statusfenster schließen, bevor der Stromversorgungs-Steuerungsvorgang abgeschlossen wurde, geschieht Folgendes:

- Wenn ein Stromversorgungs-Steuerungsvorgang fehlschlägt, wird eine Popup-Warnmeldung mit Informationen zum fehlgeschlagenen Vorgang eingeblendet.
- In der Statusleiste am unteren Rand des Browserfensters wird eine Meldung eingeblendet, wenn der gesamte Vorgang erfolgreich abgeschlossen wurde.
- Popup-Warnmeldungen werden nur bei fehlgeschlagenen Vorgängen eingeblendet. Bei erfolgreichen Vorgängen werden keine solchen Meldungen angezeigt.

Mehrere Geräte innerhalb eines beschränkten Zeitraums aktualisieren

Sie können eine Aufgabe planen, um mehrere Geräte des gleichen Typs, z. B. KX oder SX, innerhalb einer Gerätegruppe zu aktualisieren. Sobald die Aufgabe beginnt, ist im Menü Berichte > Geplante Berichte der Bericht „Gerätefirmware aktualisieren“ verfügbar. In diesem Bericht können Sie den Aktualisierungsstatus in Echtzeit verfolgen. Dieser Bericht wird auch per E-Mail gesandt, wenn Sie die Option auf der Registerkarte Benachrichtigung festlegen.

Im Raritan-Benutzerhandbuch des jeweiligen Geräts finden Sie Informationen über die geschätzten Aktualisierungszeiten.

➢ *So planen Sie eine Firmwareaktualisierung für Geräte:*

1. Wählen Sie Administration > Aufgaben.
2. Klicken Sie auf Neu.
3. Geben Sie auf der Registerkarte Hauptfenster einen Namen und eine Beschreibung für die Aufgabe ein. Mit dem von Ihnen gewählten Namen werden die Aufgabe und der Bericht, der der Aufgabe zugewiesen ist, gekennzeichnet.
4. Öffnen Sie die Registerkarte Aufgabendaten.

5. Legen Sie die Details für die Geräteaktualisierung fest:
   a. Aufgabenvorgang: Wählen Sie Gerätefirmware aktualisieren.
   b. Gerätegruppe: Wählen Sie die Gerätegruppe, die die Geräte enthält, die Sie aktualisieren möchten.
   c. Gerätetyp: Wählen Sie den Gerätetyp, den Sie aktualisieren möchten. Wenn Sie mehr als einen Gerätetyp aktualisieren müssen, müssen Sie für jeden Typ eine Aufgabe planen.
   d. Gleichzeitige Aktualisierungen: Legen Sie die Anzahl der Geräte fest, die mit der Dateiübertragungsaufgabe der Aktualisierung gleichzeitig beginnen sollen. Die Höchstanzahl beträgt 10. Nach jeder Dateiübertragung wird eine neue Dateiübertragung begonnen. Auf diese Weise wird sichergestellt, dass nur die maximale Anzahl an gleichzeitigen Aktualisierungen zur selben Zeit durchgeführt wird.
   e. Aktualisierungsdatei: Wählen Sie die Firmwareversion, auf die Sie aktualisieren möchten. Es werden nur die verfügbaren Aktualisierungsdateien, die für den ausgewählten Gerätetyp geeignet sind, als Optionen angezeigt.
6. Legen Sie den Zeitraum für die Aktualisierung fest:
   a. Startdatum/Startzeit: Wählen Sie das Datum und die Uhrzeit, zu der die Aufgabe beginnen soll. Das Startdatum und die Startzeit müssen in der Zukunft liegen.
   b. Aktualisierungszeitfenster beschränken und Spätester Startzeitpunkt (Datum/Uhrzeit) für Aktualisierung: Wenn Sie alle Aktualisierungen innerhalb eines festgelegten Zeitfensters beenden müssen, verwenden Sie diese Felder, um das Datum und die Uhrzeit festzulegen, nach der keine neuen Aktualisierungen beginnen können. Wählen Sie Aktualisierungszeitfenster beschränken, um das Feld Spätester Startzeitpunkt (Datum/Uhrzeit) für Aktualisierung zu aktivieren.
7. Legen Sie fest, welche Geräte in welcher Reihenfolge aktualisiert werden. Platzieren Sie Geräte mit einer höheren Priorität an den Anfang der Liste:
   a. Wählen Sie in der Liste Verfügbar alle Geräte aus, die Sie aktualisieren möchten. Klicken Sie auf Hinzufügen, um das jeweilige Gerät in die Liste Ausgewählt zu verschieben.
   b. Wählen Sie in der Liste Ausgewählt ein Gerät aus, und verschieben Sie es mit den Pfeiltasten an die Position in der Reihenfolge, an der es aktualisiert werden soll.

8. Öffnen Sie die Registerkarte Wiederholen. Legen Sie fest, ob fehlgeschlagene Aktualisierungen wiederholt werden sollen.
   a. Wiederholungsanzahl: Geben Sie an, wie oft CC-SG eine fehlgeschlagene Aktualisierung wiederholen soll.
   b. Wiederholungsintervall: Geben Sie die Zeitdauer an, die zwischen den Versuchen verstreichen soll. Standardmäßig können 30, 60 und 90 Minuten ausgewählt werden. Dies sind die optimalen Wiederholungsintervalle.
9. Öffnen Sie die Registerkarte Benachrichtigung. Legen Sie E-Mail-Adressen fest, die Benachrichtigungen über eine erfolgreiche und fehlgeschlagene Ausführung empfangen sollen. Standardmäßig wird die E-Mail-Adresse des Benutzers verwendet, der zurzeit angemeldet ist. Die E-Mail-Adressen der Benutzer werden im Benutzerprofil konfiguriert.
   a. Klicken Sie auf Hinzufügen, geben Sie die E-Mail-Adresse in das eingeblendete Fenster ein, und klicken Sie dann auf OK.
   b. Wählen Sie Bei Fehler, wenn eine E-Mail gesendet werden soll, falls eine Aktualisierung fehlschlägt.
   c. Wählen Sie Bei Erfolg, wenn eine E-Mail gesendet werden soll, falls alle Aktualisierungen erfolgreich abgeschlossen werden.
10. Klicken Sie zum Speichern der Änderungen auf OK.

Nach dem Beginn der Aufgabenausführung können Sie den Bericht „ Gerätefirmware aktualisieren “ jederzeit während des geplanten Zeitraums öffnen, um den Status der Aktualisierungen anzuzeigen. Weitere Informationen finden Sie unter ***Gerätefirmware aktualisieren – Bericht*** (siehe "Bericht „ Gerätefirmware aktualisieren “" auf Seite 160).

Benutzerdefinierte Ansicht als Standard für Knoten und alle Benutzer festlegen

Wenn Sie über die Berechtigung **CC-Setup und -Steuerung** verfügen, können Sie eine benutzerdefinierte Ansicht als Standardansicht für alle Benutzer festlegen.

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Wählen Sie **Knoten > Ansicht ändern > Benutzerdefinierte Ansicht erstellen**.
3. Klicken Sie auf den Pfeil der Dropdown-Liste **Name**, und wählen Sie in der Liste die benutzerdefinierte Ansicht aus, die Sie als systemweite Standardansicht festlegen möchten.

4. Aktivieren Sie das Kontrollkästchen **Systemweit**, und klicken Sie auf **Speichern**.

Für alle Benutzer, die sich in CC-SG anmelden, wird die Registerkarte **Knoten** anhand der ausgewählten benutzerdefinierten Ansicht sortiert. Die Benutzer können die benutzerdefinierte Ansicht jedoch ändern.

Weitere Informationen zu den Arten benutzerdefinierter Ansichten und Anleitungen zu deren Erstellung finden Sie unter ***Benutzerdefinierte Ansichten*** (siehe "Benutzerdefinierte Ansichten für Geräte und Knoten" auf Seite 113).

Kapitel 1 Einleitung

Das CommandCenter Secure Gateway (CC-SG) Handbuch für Administratoren bietet Anleitungen für die Verwaltung und Wartung von CC-SG.

Dieses Handbuch richtet sich an Administratoren, die über alle verfügbaren Berechtigungen verfügen.

Benutzer, die keine Administratoren sind, finden weitere Informationen im **CommandCenter Secure Gateway-Benutzerhandbuch** von Raritan.

In diesem Kapitel

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.

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.

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.

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 zugewiesen. Es ist einfacher, zuerst die Zuordnungen richtig einzurichten und dann Geräte und Ports hinzuzufügen. „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 Dominion KX, Dominion KX II, 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 Zielserver und -systeme oder „Knoten". Bitte überprüfen Sie die CC-SG-Kompatibilitätsmatrix auf der Support-Website von Raritan auf eine Liste der unterstützten Geräte.

Elemente: Werte einer Kategorie. Das Element „New York City" gehört beispielsweise zur Kategorie „Standort" und das Element „Windows" zur Kategorie „Betriebssystemtyp".

Verwaiste Ports: Bei der Verwaltung von Paragon-Geräten kann ein verwaister Port entstehen, wenn ein CIM- oder Zielserver aus dem System entfernt oder abgeschaltet (manuell oder unbeabsichtigt) wird. Weitere Informationen hierzu finden Sie im Benutzerhandbuch für Paragon II-Geräte von Raritan.

Hostname: Ein Hostname kann verwendet werden, wenn die DNS-Serverunterstützung aktiviert ist. Weitere Informationen finden Sie im Abschnitt über Netzwerke unter ***Erweiterte Administration*** (auf Seite 173). Der Hostname und der vollständig qualifizierte Domänenname (Hostname + Suffix) dürfen nicht mehr als 257 Zeichen umfassen. Er kann aus einer beliebigen Anzahl an 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 Datum und Uhrzeit des Zugriffs.

Knoten: Zielsysteme wie Server, Desktop-PCs und andere Netzwerkgeräte, auf die CC-SG-Benutzer 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 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.

Benutzergruppen: Mehrere Benutzer mit der gleichen Zugriffsebene und den gleichen Berechtigungen.

Kapitel 2 Zugreifen auf CC-SG

Sie haben mehrere Möglichkeiten für den Zugriff auf CC-SG:

- **Browser**: CC-SG unterstützt verschiedene Webbrowser. (Eine vollständige Liste der unterstützten Browser finden Sie in der Kompatibilitätsmatrix auf der Support-Website von Raritan.)
- **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 unter ***Erweiterte Administration*** (auf Seite 173).
- **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 unter ***Erweiterte Administration*** (auf Seite 173).

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

In diesem Kapitel

Browserbasierter Zugriff

1. Verwenden Sie einen unterstützten Internetbrowser, und geben Sie folgenden URL ein: http://<IP-Adresse>/admin wobei <IP-Adresse> für die IP-Adresse von CC-SG steht. Beispiel: **https://10.20.3.30/admin**.
2. Klicken Sie im angezeigten Fenster mit dem Sicherheitshinweis auf **Ja**, um fortzufahren.

3. 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.
4. Sind die vertraglichen Einschränkungen der Serviceleistungen aktiviert, lesen Sie den Text, und markieren Sie das Kontrollkästchen **Ich stimme den Vertragsbedingungen zu**.
5. 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

➢ *So laden Sie den Thick-Client von CC-SG herunter:*

1. Starten Sie einen Webbrowser, und geben Sie diesen URL ein: **http(s)://<IP-Adresse>/install** wobei <IP-Adresse> für die IP-Adresse von CC-SG steht.
   - Wenn eine Sicherheitswarnung angezeigt wird, klicken Sie auf **Start**, um das Herunterladen fortzusetzen.
   - 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).
2. Nach dem Herunterladen wird ein neues Fenster angezeigt, in dem Sie die IP-Adresse von CC-SG angeben können.

3. Geben Sie in das Feld **Zu verbindende IP-Adresse** die IP-Adresse der CC-SG-Einheit ein, auf die Sie zugreifen möchten. Nachdem die Verbindung hergestellt 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.
4. Wenn CC-SG für sichere Browserverbindungen konfiguriert ist, müssen Sie das Kontrollkästchen **Secure Socket Layer (SSL)** aktivieren. 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.
5. **So überprüfen Sie die Einstellung in CC-SG:** Wählen Sie **Administration** > **Sicherheit**. Sehen Sie sich auf der Registerkarte **Verschlüsselung** die Option **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.
6. 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.
7. Das Anmeldefenster wird angezeigt.
8. 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*

Wenn auf Ihrem Client-Computer **Java Version 1.4.x** ausgeführt wird und Sie bei der Installation des Thick-Clients im Fenster **Desktop Integration** (Desktop-Integration) auf **Yes** (Ja) geklickt haben, 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.

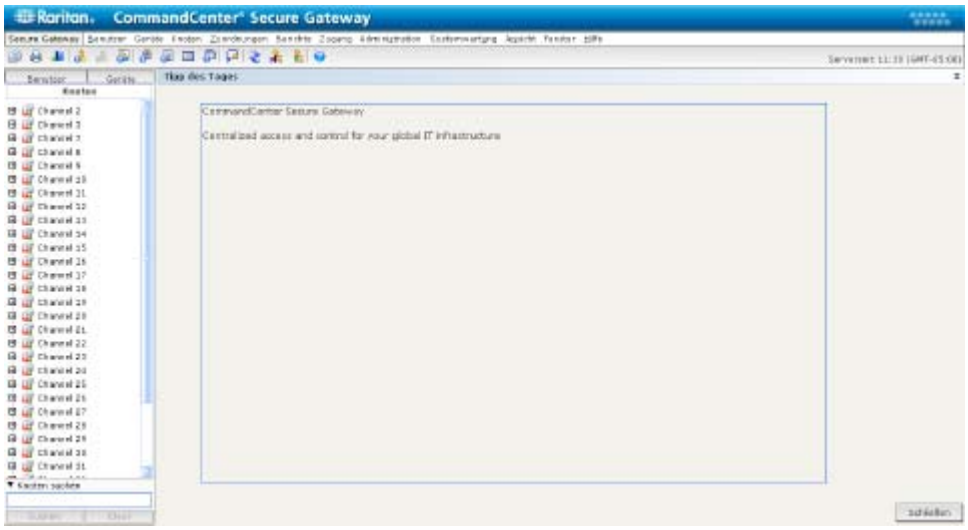
➢ *Java 1.5*

Wenn auf Ihrem Client-Computer **Java Version 1.5** ausgeführt wird, können Sie:

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

CC-SG-Administrations-Client

Nach der Anmeldung wird der CC-SG-Administrations-Client angezeigt.



- **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 im Kontextmenü **Verbinden**, um eine Verbindung zu dieser Schnittstelle herzustellen. Sie können die Knoten nach Knotennamen (alphabetisch) oder Knotenstatus (Verfügbar, Beschäftigt, Nicht verfügbar) sortieren. Klicken Sie mit der rechten Maustaste in die Strukturansicht, wählen Sie im Kontextmenü **Knotensortieroptionen** und dann **Nach Knotenname** oder **Nach Knotenstatus**.
- **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.
- **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**, 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 in die Strukturansicht, wählen Sie im Kontextmenü **Portsortieroptionen** und dann **Nach Knotenname** oder **Nach Knotenstatus**.
- **Symbolleiste mit Kurzbefehlen**: Diese Symbolleiste enthält Schaltflächen zum Ausführen der am häufigsten benötigten Befehle.
- **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.

- **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 finden Sie unter ***Aufgabenmanager*** (auf Seite 214). Diese Uhrzeit unterscheidet sich eventuell von der auf Ihrem Client-PC verwendeten Uhrzeit.

Kapitel 3 Erste Schritte

Nach der ersten Anmeldung bei CC-SG sollten Sie die IP-Adresse bestätigen, die CC-SG-Serverzeit einstellen und die Version der installierten Firmware und Anwendung überprüfen. Sie müssen die Firmware und Anwendungen ggf. aktualisieren.

Nach dem Abschluss der Erstkonfigurationen können Sie mit ***Konfigurieren von CC-SG mit dem Setup-Assistenten*** (auf Seite 16) fortfahren.

In diesem Kapitel

IP-Adresse bestätigen

1. Wählen Sie **Administration** > **Konfiguration**.
2. Klicken Sie auf die Registerkarte **Netzwerksetup**.
3. (Optional) Überprüfen Sie, dass die Netzwerkeinstellungen richtig sind, und nehmen Sie Änderungen vor, falls erforderlich. Weitere Informationen finden Sie unter ***Netzwerkeinrichtung*** (auf Seite 178).
4. Klicken Sie auf **Konfiguration aktualisieren**, um die Änderungen zu übernehmen.
5. Klicken Sie auf **Jetzt neu starten**, um Ihre Einstellungen zu bestätigen und CC-SG neu zu starten.

CC-SG-Serverzeit festlegen

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 unter *Aufgabenmanager* **(auf Seite 214). Die Uhrzeit, die auf Ihrem Client-PC eingestellt ist, unterscheidet sich eventuell von der auf CC-SG eingestellten Uhrzeit.**

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

In einer Clusterkonfiguration kann die Zeitzone nicht geändert werden.

➢ *So konfigurieren Sie die Serveruhrzeit und das Datum von CC-SG:*

1. Wählen Sie Administration >Konfiguration.
2. Klicken Sie auf die Registerkarte **Uhrzeit/Datum**.
   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 den Pfeil neben der 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.

Wählen Sie **Systemwartung** > **Neu starten**, um CC-SG neu zu starten.

Kompatibilitätsmatrix überprüfen

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. Sie können die Kompatibilitätsmatrix auch auf der Support-Website von Raritan ansehen.

➢ *So überprüfen Sie die Kompatibilitätsmatrix:*

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

Anwendungsversionen prüfen und aktualisieren

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

➢ *So überprüfen Sie eine Anwendungsversion:*

1. Wählen Sie **Administration** > **Anwendungen**.
2. Wählen Sie in der Liste einen **Anwendungsnamen** aus. Beachten Sie die Zahl im Feld **Version**. Für einige Anwendungen wird nicht automatisch eine Versionszahl angezeigt.

➢ *So aktualisieren Sie eine Anwendung:*

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. (Eine vollständige Liste der unterstützten Anwendungsversionen finden Sie in der **Kompatibilitätsmatrix** auf der Support-Website von Raritan.)

1. Speichern Sie die Datei mit der Anwendung auf Ihrem Client-PC.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Anwendungsname**, und wählen Sie die zu aktualisierende Anwendung in der Liste aus. Wenn Sie die Anwendung nicht sehen, müssen Sie die Anwendung zuerst hinzufügen. ***Anwendungen hinzufügen*** (auf Seite 175)

3. Klicken Sie auf **Durchsuchen**, und wählen Sie die Datei zur Anwendungsaktualisierung im angezeigten Dialogfeld zum Öffnen aus. Klicken Sie auf **Öffnen**.
4. Der Anwendungsname wird im **Anwendungsmanager** im Feld **Neue Anwendungsdatei** angezeigt.
5. Klicken Sie auf **Senden**. Eine Statusanzeige informiert über den Ladevorgang der neuen Anwendung. Nach dem Laden wird in einem neuen Fenster angezeigt, dass die Anwendung der CC-SG-Datenbank hinzugefügt wurde und nun verwendet werden kann.
6. Wenn das Feld **Version** nicht automatisch aktualisiert wird, geben Sie die neue Versionszahl in das Feld **Version** ein. Das Feld **Version** wird bei einigen Anwendungen automatisch aktualisiert.
7. Klicken Sie auf **Aktualisieren**.

Kapitel 4 Konfigurieren von CC-SG mit dem Setup-Assistenten

Der Setup-Assistent dient als einfache Möglichkeit, Erstkonfigurationsaufgaben für CC-SG auszuführen, nachdem die Netzwerkkonfiguration 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 Zuordnen von Richtlinien und Rechten für Benutzergruppen und das Hinzufügen von Benutzern. Nachdem Sie den Setup-Assistenten abgeschlossen haben, können Sie Ihre Konfigurationseinstellungen einzeln ändern.

Der Setup-Assistent ist in 4 Aufgaben unterteilt:

- ***Zuordnungen*** (siehe "Zuordnungen im Setup-Assistenten" auf Seite 17): Definieren der Kategorien und Elemente, die Sie zum Verwalten Ihrer Geräte verwenden.
- ***Geräte-Setup*** (auf Seite 18): Erkennen von Geräten in Ihrem Netzwerk und Hinzufügen dieser Geräte zu CC-SG. Konfigurieren von Geräteports.
- ***Gruppen erstellen*** (auf Seite 20): Kategorisieren der Geräte und Knoten, die CC-SG in Gruppen verwaltet, und Erstellen von Richtlinien mit unbeschränktem Zugriff für jede Gruppe.
- ***Benutzerverwaltung*** (auf Seite 23): 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.

Informationen über die Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).

In diesem Kapitel

Vor der Verwendung des 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). Ordnen Sie dabei auch eine IP-Adresse zu.

Zuordnungen im Setup-Assistenten

Kategorien und Elemente erstellen

1. Klicken Sie im Fenster Setup-Assistent auf **Zuordnungen**. Klicken Sie dann im linken Fensterbereich auf **Kategorien erstellen**, um den Fensterbereich **Kategorien erstellen** zu öffnen.
2. Geben Sie zum Verwalten der Geräte in das Feld **Kategoriename** den entsprechenden Namen der Kategorie wie „Standort“ ein.
3. Im Feld **Gültig für** können Sie angeben, ob die Kategorie für Geräte, Knoten oder beides verfügbar sein soll. Klicken Sie auf das Dropdown-Menü **Gültig für**, und wählen Sie einen Wert in 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 zum Einfügen einer neuen Zeile  , um bei Bedarf neue Zeilen in die Tabelle **Elemente** einzufügen.
   - Sie können Elemente löschen, indem Sie eine Zeile auswählen und auf das Symbol zum Löschen von Zeilen  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. (Optional) 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 zugewiesen werden soll.

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

Geräte erkennen und hinzufügen

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.

1. Geben Sie in die Felder für den Adressbereichsanfang und das Adressbereichsende den Bereich der IP-Adressen ein, den Sie nach den Geräten durchsuchen möchten.
2. Geben Sie in das Feld **Maske** die Subnetzmaske ein, die Sie nach Geräten durchsuchen möchten.
3. 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.
4. 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.
5. Klicken Sie auf **Erkennen**.
6. Nach Abschluss des Erkennungsvorgangs wird eine Bestätigungsnachricht angezeigt. Klicken Sie in der Bestätigungsmeldung auf **OK**.

7. 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.
8. 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. Der Fensterbereich **Gerät hinzufügen** hängt vom Gerätetyp ab, den Sie hinzufügen.
9. Sie können neuen Text in die entsprechenden Felder **Gerätename** und **Beschreibung** eingeben.
10. Vergewissern Sie sich, dass die IP-Adresse, die Sie beim Hinzufügen des Geräts zu CC-SG angegebenen haben, im Feld **Geräte-IP-Adresse oder Hostname** angezeigt wird. Geben Sie andernfalls die richtige Adresse in das Feld ein.
11. Die TCP-Portnummer wird abhängig vom Gerätetyp automatisch eingefügt.
12. Geben Sie in die entsprechenden Felder **Benutzername** und **Kennwort** ein, die Sie beim Hinzufügen des Geräts zu CC-SG erstellt haben.
13. Geben Sie in das Feld **Heartbeat-Zeitlimit** die Dauer in Sekunden ein, die vor Überschreitung des Zeitlimits zwischen Gerät und CC-SG verstreichen sollte.
14. Wenn Sie ein Dominion SX-Gerät hinzufügen, markieren Sie das Kontrollkästchen **Lokaler Zugriff: Zulässig**, wenn der lokale Zugriff auf das Gerät zugelassen werden soll. Deaktivieren Sie das Kontrollkästchen **Lokaler Zugriff: Zulässig**, wenn kein lokaler Zugriff auf das Gerät zugelassen werden soll.
15. Wenn Sie ein PowerStrip-Gerät manuell hinzufügen, klicken Sie auf den Pfeil neben der Dropdown-Liste **Anzahl der Ports**, und wählen Sie die Anzahl der PowerStrip-Ausgänge aus.
16. Wenn Sie einen IPMI-Server hinzufügen, geben Sie in die entsprechenden Felder ein **Intervall** für die Verfügbarkeitsprüfung und eine **Authentifizierungsmethode** ein, die der im IPMI-Server konfigurierten Methode entsprechen muss.
17. 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.

18. Klicken Sie unten im Fensterbereich unter **Gerätezuordnungen** auf den Pfeil neben der Dropdown-Spalte Element, die mit jeder Kategorie übereinstimmt, die Sie dem Gerät zuordnen möchten. Wählen Sie dann das gewünschte Element für die Zuweisung zum Gerät in der Liste aus.
19. Soll das Element auf das Gerät und die mit dem Gerät verbundenen Knoten angewendet werden, markieren Sie das Kontrollkästchen **Auf Knoten anwenden**.
20. (Optional) 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.
21. Klicken Sie auf **OK**, nachdem Sie alle gewünschten Geräte hinzugefügt haben. Im Fensterbereich **Geräteübersicht** wird eine Liste der Geräte angezeigt, die Sie hinzugefügt haben.
22. 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.

   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 Entfernen eines Geräts aus der Gruppe den Gerätenamen in der Liste **Ausgewählt** aus, und klicken Sie auf **Entfernen**.
   - 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 zuordnen möchten.

   b. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile  , 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.

1. 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.

2. (Optional) 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.
3. 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.
4. Geben Sie in das Feld **Gruppenname** einen Namen für die Knotengruppe ein, die Sie erstellen möchten.
5. Sie haben zwei Möglichkeiten, Knoten einer Gruppe 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**.

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 Entfernen eines Knotens aus der Gruppe den Knotennamen in der Liste **Ausgewählt** aus, und klicken Sie auf **Entfernen**.

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 zuordnen möchten.

b. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile  , 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. ***Richtlinien für die Zugriffssteuerung*** (auf Seite 106).

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. (Optional) 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.

1. Klicken Sie auf **OK**, nachdem Sie alle gewünschten Knotengruppen hinzugefügt haben. Im Fensterbereich **Gruppenübersicht** wird eine Liste der Gruppen angezeigt, die Sie hinzugefügt haben.
2. 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

Der Fensterbereich **Benutzergruppe hinzufügen** wird angezeigt, wenn Sie nach der Aufgabe zum Erstellen von Gruppen auf **Weiter** klicken. Sie können auch auf **Benutzerverwaltung** und dann im linken Fensterbereich in der Strukturansicht **Aufgabenassistent** auf **Benutzergruppe hinzufügen** klicken, um den gleichnamigen Fensterbereich zu öffnen.

1. Geben Sie in das Feld **Benutzergruppenname** einen Namen für die Benutzergruppe ein, die Sie erstellen möchten. Benutzergruppennamen können aus bis zu 32 Zeichen bestehen.
2. Geben Sie in das Feld **Beschreibung** eine Beschreibung für die Benutzergruppe ein.
3. 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.
4. 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 zuordnen möchten.
5. Klicken Sie auf die Registerkarte **Richtlinien**.
6. Wählen Sie in der Liste **Alle Richtlinien** die Richtlinie aus, die Sie der Benutzergruppe zuordnen 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 zugeordnet. Wiederholen Sie diesen Schritt, um der Benutzergruppe weitere Richtlinien zuzuweisen.
7. Wählen Sie zum Entfernen einer Richtlinie aus der Benutzergruppe den Namen der Richtlinie in der Liste **Ausgewählte Richtlinien** aus, und klicken Sie auf **Entfernen**.
8. Wenn Sie Benutzer, für die Remoteauthentifizierung verwendet wird, mit Active Directory-Modulen verknüpfen möchten, klicken Sie auf die Registerkarte **Active Directory-Zuordnungen**. Markieren Sie das Kontrollkästchen, das jedem Active Directory-Modul entspricht, das Sie mit dieser Benutzergruppe verknüpfen möchten.
9. (Optional) 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.

10. Klicken Sie auf **OK**, nachdem Sie alle gewünschten Benutzergruppen hinzugefügt haben. Der Fensterbereich **Benutzer hinzufügen** wird angezeigt. Sie können auch auf **Benutzerverwaltung** und dann im linken Fensterbereich in der Strukturansicht **Aufgabenassistent** auf **Benutzer hinzufügen** klicken, um den gleichnamigen Fensterbereich zu öffnen.
11. Geben Sie in das Feld **Benutzername** den Namen für den Benutzer zur Anmeldung bei CC-SG ein.
12. Markieren Sie das Kontrollkästchen **Anmeldung aktiviert**, wenn der Benutzer über die Anmeldeberechtigung für CC-SG verfügen soll.
13. 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.
14. 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.
15. Markieren Sie das Kontrollkästchen **Änderung des Kennworts bei der nächsten Anmeldung erzwingen**, wenn der Benutzer gezwungen werden soll, das zugeordnete Kennwort bei der nächsten Anmeldung zu ändern.
16. Markieren Sie das Kontrollkästchen **Änderung des Kennworts periodisch erzwingen**, wenn Sie festlegen möchten, wie oft der Benutzer zur Kennwortänderung gezwungen werden soll.
17. Geben Sie in das Feld **Gültigkeitsdauer (in Tagen)** die Anzahl an Tagen ein, die der Benutzer dasselbe Kennwort verwenden kann, bevor eine Änderung erzwungen wird.
18. Geben Sie die E-Mail-Adresse des Benutzers in das Feld **E-Mail-Adresse** ein.
19. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Benutzergruppe**, und wählen Sie in der Liste die Benutzergruppe aus, der Sie den Benutzer zuordnen möchten.
20. (Optional) 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.

21. 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.

Kapitel 5 Zuordnungen, Kategorien und Elemente

In diesem Kapitel

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 Amerika, Asien-Pazifik und Europa 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 zugewiesenen Elementen (Amerika, Asien-Pazifik und Europa) über die CC-SG-Schnittstelle angezeigt werden. Sie können die Organisation und Anzeige Ihrer Server in CC-SG beliebig nach Ihren Wünschen anpassen.

Zuordnungsterminologie

- **Zuordnungen**: Beziehungen zwischen Kategorien und Kategorieelementen zu Knoten und Geräten.
- **Kategorie**: Eine Variable, die bestimmte Werte (genannt Elemente) enthält. „Standort“ ist beispielsweise eine Kategorie, die Elemente wie „Amerika“ und „Asien-Pazifik“ enthält. „Betriebssystemtyp“ ist eine weitere Kategorie, die Elemente wie „Windows“, „Unix“ oder „Linux“ enthalten kann.
- **Elemente**: Werte einer Kategorie. Das Element „Amerika“ gehört beispielsweise zur Kategorie „Standort“.

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 zugeordnet 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 zuirdnen, 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. ***Konfigurieren von CC-SG mit dem Setup-Assistenten*** (auf Seite 16)
- Mit dem **Zuordnungsmanager** können Sie nur mit Zuordnungen arbeiten. Konfigurationsaufgaben werden nicht automatisiert. Mit dem Zuordnungsmanager können Sie auch Ihre Zuordnungen bearbeiten, nachdem Sie den Setup-Assistenten verwendet haben. ***Zuordnungsmanager*** (auf Seite 29)

Zuordnungsmanager

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

Kategorien hinzufügen

1. Wählen Sie **Zuordnungen** > **Zuordnung**.
2. Klicken Sie auf **Hinzufügen**. Das Fenster **Kategorie hinzufügen** wird angezeigt.
3. Geben Sie in das Feld **Kategoriename** einen Kategorienamen ein. Informationen über die Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
4. Wählen Sie den Datentyp für Elemente.
   - Wählen Sie **Zeichenfolge**, wenn der Wert als Text gelesen wird.
   - Wählen Sie **Ganze Zahl**, wenn der Wert eine Zahl ist.
5. Wählen Sie im Feld Gültig für aus, ob diese Kategorie für **Geräte oder Knoten** oder **Geräte und Knoten** gilt.

6. Klicken Sie zum Erstellen der neuen Kategorie auf **OK**. Der neue Kategoriename wird im Feld **Kategoriename** angezeigt.

Kategorien bearbeiten

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.

1. Wählen Sie **Zuordnungen** > **Zuordnung**.
2. Klicken Sie auf den Pfeil neben der 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.
4. Geben Sie den neuen Kategorienamen in das Feld **Kategoriename** ein.
5. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Gültig für**, um diese Kategorie auf **Geräte, Knoten** oder **Beides** anzuwenden.
6. Klicken Sie zum Speichern der Änderungen auf **OK**. Der aktualisierte Kategoriename wird im Feld **Kategoriename** angezeigt.

Kategorien 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. Wählen Sie **Zuordnungen** > **Zuordnung**.
2. Klicken Sie auf den Pfeil neben der 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.
4. Klicken Sie auf **Ja**, um die Kategorie zu löschen.

Elemente hinzufügen

1. Wählen Sie **Zuordnungen** > **Zuordnung**.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Kategoriename**, und wählen Sie die Kategorie aus, der Sie ein neues Element hinzufügen möchten.

3. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile.
4. Geben Sie den Namen des neuen Elements in die leere Zeile ein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303). Bei Elementnamen wird die Groß- und Kleinschreibung berücksichtigt.
5. Klicken Sie zum Speichern der Änderungen auf **OK**.

Elemente bearbeiten

1. Klicken Sie im Menü **Zuordnungen** auf **Zuordnungsmanager**.
2. Klicken Sie auf den Pfeil neben der 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.
4. Geben Sie den neuen Namen des Elements in das Feld **Neuen Elementwert eingeben** ein. Bei Elementnamen wird die Groß- und Kleinschreibung berücksichtigt.
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.

Elemente löschen

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

1. Wählen Sie **Zuordnungen** > **Zuordnung**.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Kategoriename**, und wählen Sie die Kategorie zum Löschen des Elements aus.
3. Wählen Sie in der Liste **Elemente** das zu löschende Element aus, und klicken Sie auf das Symbol zum Entfernen einer Zeile.
4. Klicken Sie zum Speichern der Änderungen auf OK.

Kapitel 6 Geräte, Gerätegruppen und Ports

Wenn Sie Raritan-PowerStrip-Geräte, die mit anderen Raritan-Geräten verbunden sind, zu CC-SG hinzufügen möchten, finden Sie weitere Informationen unter ***Verwaltete PowerStrips*** (auf Seite 59).

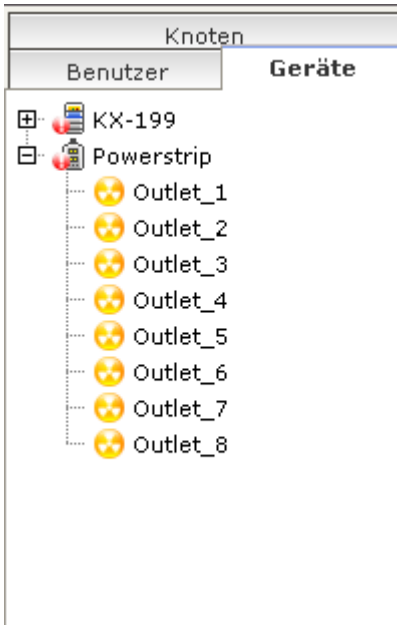
Hinweis: *Verwenden Sie zur Konfiguration von iLO/RILOE-Geräten, IPMI-Geräten, Dell DRAC-Geräten, IBM RSA-Geräten oder anderen Geräten, die nicht von Raritan hergestellt wurden, das Menü* ***Knoten hinzufügen****, und fügen Sie diese Elemente als Schnittstelle hinzu. Weitere Informationen finden Sie unter* **Knoten, Knotengruppen und Schnittstellen** *(auf Seite 68).*

In diesem Kapitel

Geräte anzeigen

Die Registerkarte Geräte

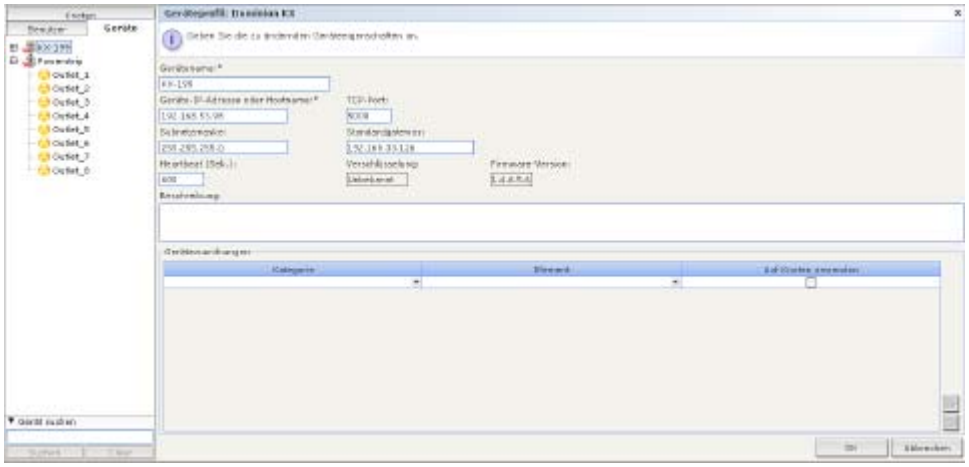
Klicken Sie auf die Registerkarte **Geräte**, um alle Geräte anzuzeigen, die in CC-SG verwaltet werden.



Die konfigurierten Ports der einzelnen Geräte werden unter den Geräten, zu denen sie gehören, verschachtelt angezeigt. Geräte mit konfigurierten Ports werden in der Liste mit einem Pluszeichen (+) angezeigt. Klicken Sie auf das Pluszeichen (+), um die Portliste ein- oder auszublenden.

Fenster Geräteprofil

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



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
	Verwaister Port (Weitere Informationen zum Ghosting-Modus finden Sie im Benutzerhandbuch für Paragon II-Geräte von Raritan.)
	Gerät wurde angehalten
	Gerät nicht verfügbar
	Powerstrip

Symbol	Bedeutung
	Ausgangsport

Portsortieroptionen

Auf der Registerkarte Geräte werden konfigurierte Ports unter ihren übergeordneten Geräten verschachtelt angezeigt. Sie können die Sortierung der Ports ändern. Nach Status aufgelistete Ports werden innerhalb ihrer Verbindungsstatusgruppe alphabetisch sortiert. Geräte werden ebenfalls entsprechend sortiert angezeigt.

1. Wählen Sie **Geräte** > **Portsortieroptionen**.
2. Wählen Sie **Nach Portname** oder **Nach Portstatus** aus, um die Ports im Gerät alphabetisch nach Namen oder Verfügbarkeitsstatus zu sortieren.

Kontextmenüoptionen auf der Registerkarte Geräte

Sie können auf der Registerkarte Geräte mit der rechten Maustaste auf ein Gerät oder einen Port klicken, um ein Menü mit Befehlen anzuzeigen, die für das ausgewählte Gerät oder den ausgewählten Port verfügbar sind.

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 Suchmethode kann unter **Mein Profil** (siehe "Eigene Standardsucheinstellungen ändern" auf Seite 102) konfiguriert werden.

➢ *So suchen Sie ein Gerät:*

- Geben Sie unten auf der Registerkarte Geräte in das Feld **Gerät suchen** eine Suchzeichenfolge ein, und drücken Sie dann die **Eingabetaste**.
- Die Suchfunktion unterstützt ***Platzhalter*** (siehe "Platzhalter für die Suche" auf Seite 35) in der Suchzeichenfolge.

Platzhalter für die Suche

Platzhalter	Beschreibung
?	Beliebiges Zeichen

[-]	Zeichen in einem Bereich
*	Kein oder mehrere Zeichen

Beispiele mit Platzhaltern

Beispiel	Beschreibung
KX?	Findet **KX1** und **KXZ**, aber nicht **KX1Z**.
KX*	Findet **KX1**, **KX**, **KX1** und **KX1Z**.
KX[0-9][0-9]T	Findet **KX95T**, **KX66T**, aber nicht **KXZ** und **KX5PT**.

Geräte erkennen

Mit Geräte erkennen wird eine Suche nach allen Raritan-Geräten in Ihrem Netzwerk gestartet. Nach dem Erkennen der Geräte können Sie diese zu CC-SG hinzufügen, falls sie nicht bereits verwaltet werden.

➢ *So erkennen Sie Geräte:*

1. Wählen Sie **Geräte** > **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 **Strg**-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.
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.
8. Geben Sie den Benutzernamen und das Kennwort in die Felder **Benutzername** und **Kennwort** ein, um eine Authentifizierung des Geräts durch CC-SG für die zukünftige Kommunikation zu ermöglichen.
9. Wählen Sie die **Kategorien** und **Elemente** aus, die Sie auf das Gerät anwenden möchten.
10. 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**.
11. (Optional) Sie können die folgenden Felder bei Bedarf anpassen: **Gerätename**, **Heartbeat-Zeitlimit**, **Lokaler Zugriff** (falls für Gerätetyp verfügbar), **Beschreibung, Alle Ports konfigurieren** und **Gerätezuordnungen**.
12. 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.

    Wenn die Firmwareversion eines Geräts mit CC-SG nicht kompatibel ist, wird eine Meldung angezeigt. 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 **Gerät aktualisieren**.

Geräte hinzufügen

Sie müssen CC-SG Geräte hinzufügen, bevor Sie Ports konfigurieren oder Schnittstellen, die Zugriff auf die mit den Ports verbundenen Knoten bieten, hinzufügen können. **Gerät hinzufügen** wird verwendet, um ein Gerät hinzuzufügen, dessen Eigenschaften Sie kennen und für CC-SG bereitstellen können.

Wenn Sie Raritan-PowerStrip-Geräte, die mit anderen Raritan-Geräten verbunden sind, zu CC-SG hinzufügen möchten, finden Sie Informationen unter ***Stromversorgungssteuerung konfigurieren*** (siehe "Verwaltete PowerStrips" auf Seite 59).

➢ *So fügen Sie CC-SG ein Gerät hinzu:*

1. Wählen Sie **Geräte** > **Gerätemanager** > **Gerät hinzufügen**.
2. Klicken Sie auf den Pfeil neben der 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

1. Geben Sie den Namen des neuen Geräts in das Feld **Gerätename** ein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
2. Geben Sie die IP-Adresse oder den Hostnamen des Geräts in das Feld **Geräte-IP-Adresse oder Hostname** ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
3. Geben Sie in das Feld **TCP-Portnummer** die Nummer des TCP-Kommunikationsports ein, der zur Kommunikation mit dem Gerät verwendet wird. Es können höchstens 5 numerische Zeichen eingegeben werden. Die Standardportnummer der meisten Raritan-Geräte lautet 5000.
4. Geben Sie den für die Anmeldung verwendeten Benutzernamen in das Feld **Benutzername** ein. Der Benutzer muss für den Zugriff Administratorberechtigungen besitzen.
5. Geben Sie das für den Zugriff auf dieses Gerät erforderliche Kennwort in das Feld **Kennwort** ein. Der Benutzer muss für den Zugriff Administratorberechtigungen besitzen.

6. Geben Sie in das Feld **Heartbeat-Zeitlimit (Sek.)** die Zeit (in Sekunden) ein, die verstreichen soll, bevor zwischen dem neuen Gerät und CC-SG ein Zeitüberschreitungsfehler auftritt.
7. Beim Hinzufügen eines Dominion SX-Geräts ermöglicht Ihnen das Kontrollkästchen Lokalen Port-Zugriff zulassen, den lokalen Port-Zugriff auf das Gerät zuzulassen oder zu verweigern. Markieren Sie das Kontrollkästchen, wenn Sie Benutzern direkten Zugriff auf dieses Gerät geben möchten, während es von CC-SG verwaltet wird.
8. (Optional) Sie können auch eine kurze Beschreibung für das Gerät in das Feld **Beschreibung** eingeben.
9. 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.
   - Ein neuer Knoten wird für jeden Port und eine Out-of-Band-Schnittstelle wird für diesen Knoten erstellt.
10. 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 unter ***Zuordnungen*** (siehe "Zuordnungen, Kategorien und Elemente" auf Seite 27).
    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.

       Wenn Sie das Element verknüpften Knoten und Geräten zuordnen 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 unter ***Zuordnungen*** (siehe "Zuordnungen, Kategorien und Elemente" auf Seite 27).

11. 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. Oder klicken Sie auf **OK**, um dieses Gerät hinzuzufügen und den Bildschirm Gerät hinzufügen nicht anzuzeigen.
12. Wenn die Firmwareversion des Geräts mit CC-SG nicht kompatibel ist, wird eine Meldung angezeigt. 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 ***Gerät aktualisieren*** (auf Seite 45).

PowerStrip-Geräte hinzufügen

Das Hinzufügen eines PowerStrip-Geräts zu CC-SG hängt davon ab, mit welchem Raritan-Gerät der PowerStrip physisch verbunden ist. Weitere Informationen finden Sie unter ***Verwaltete PowerStrips*** (auf Seite 59).

Geräte bearbeiten

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

➢ *So bearbeiten Sie ein Gerät:*

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät zum Bearbeiten aus.
2. Ändern Sie auf dem Bildschirm Geräteprofil bei Bedarf die Parameter.
3. Klicken Sie zum Speichern der Änderungen auf **OK**.

PowerStrip-Geräte 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.
2. Geben Sie die neuen Geräteeigenschaften in die entsprechenden Felder ein. Bearbeiten Sie bei Bedarf die Kategorien und Elemente, die dem Gerät zugewiesen sind.
3. Klicken Sie auf die Registerkarte **Ausgang**, um alle Ausgänge des PowerStrip anzuzeigen.

4. Ist ein Ausgang mit einem Knoten verknüpft, können Sie auf den Hyperlink **Knoten** klicken, um das Knotenprofil anzuzeigen.
5. 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.
6. Klicken Sie zum Speichern der Änderungen auf **OK**. Eine Meldung wird eingeblendet, wenn das Gerät geändert wurde.

Geräte 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 diesen Ports zugewiesen sind, werden von den Knoten entfernt. Besteht keine weitere Schnittstelle für diese Knoten, werden die Knoten auch aus CC-SG entfernt.

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.*

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät zum Löschen aus.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Gerät löschen**.
3. Klicken Sie zum Löschen des Geräts auf **OK**. Eine Meldung wird eingeblendet, wenn das Gerät gelöscht wurde.

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 wurden, 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 zu Knoten hinzugefügt werden können.

Seriellen Port konfigurieren

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie ein serielles Gerät.
2. Wählen Sie **Geräte** > **Portmanager** > **Ports konfigurieren**.
3. 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.
4. Klicken Sie neben dem zu konfigurierenden seriellen Port auf die entsprechende Schaltfläche **Konfigurieren**.
5. Geben Sie in das Feld **Portname** einen Portnamen ein. Der Einfachheit halber sollten Sie den Port nach dem mit dem Port verbundenen Ziel benennen. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
6. 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.
7. 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.
8. Klicken Sie zum Hinzufügen des Ports auf **OK**.

KVM-Port konfigurieren

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie ein KVM-Gerät.
2. Wählen Sie **Geräte** > **Portmanager** > **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**.

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. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
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.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie den Port zum Bearbeiten aus.
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 zum Speichern der Änderungen auf **OK**.

Ports löschen

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

Wichtig: Wenn Sie einen Port löschen, der einem Knoten zugewiesen 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. Wählen Sie **Geräte** > **Portmanager** > **Ports löschen**.
3. Markieren Sie jeweils die Ports, die Sie aus dem Gerät löschen möchten.
4. Klicken Sie zum Löschen des ausgewählten Ports auf **OK**. Eine Meldung wird eingeblendet, wenn der Port gelöscht wurde.

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. Wählen Sie **Geräte** > **Gerätemanager** > **Massenkopieren**.
3. Wählen Sie in der Liste **Alle Geräte** die Geräte aus, auf die Sie die Kategorien und Elemente des im 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**. Eine Meldung wird eingeblendet, wenn die Gerätekategorien und -elemente kopiert wurden.

Gerät aktualisieren

Sie können Geräte aktualisieren, wenn eine neue Version der Gerätefirmware verfügbar ist.

Wichtig! Bitte überprüfen Sie die Kompatibilitätsmatrix, um sicherzustellen, dass die neue Gerätefirmwareversion mit Ihrer CC-SG-Firmwareversion kompatibel ist. Wenn Sie sowohl CC-SG als auch ein Gerät oder eine Gerätegruppe aktualisieren müssen, aktualisieren Sie zuerst CC-SG und dann die Geräte.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie in der Gerätestrukturansicht ein Gerät aus.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Gerät aktualisieren**.
3. **Firmwarename:** 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.
   - Wenn die Firmwareversion des Geräts mit CC-SG nicht kompatibel ist, wird eine Meldung angezeigt. Klicken Sie zum Aktualisieren des Geräts auf **Ja**. Klicken Sie zum Abbrechen der Aktualisierung auf **Nein**.
5. Eine Meldung wird angezeigt. Klicken Sie zum Neustarten des Geräts auf **Ja**. Eine Meldung wird eingeblendet, wenn das Gerät aktualisiert wurde.
6. Schließen Sie Ihr Browserfenster, um sicherzustellen, dass Ihr Browser alle aktualisierten Dateien lädt. Melden Sie sich dann bei CC-SG in einem neuen Browserfenster an.

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. Jedes Gerät sichert eventuell unterschiedliche Komponenten der Konfiguration. Lesen Sie das Benutzerhandbuch des Geräts, das Sie sichern möchten, um weitere Informationen zu erhalten.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät zum Sichern aus.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Konfiguration** > **Sicherung**.
3. Geben Sie einen Namen für diese Sicherung in das Feld **Sicherungsname** ein.
4. (Optional) Sie können auch eine kurze Beschreibung für die Sicherung in das Feld **Beschreibung** eingeben.
5. Klicken Sie auf **OK**, um die Gerätekonfiguration zu sichern. Eine Meldung wird eingeblendet, wenn die Gerätekonfiguration gesichert wurde.

Hinweis: *Beim Sichern eines SX 3.0.1-Geräts werden die angefügten PowerStrip-Konfigurationen nicht gesichert. Wenn Sie das SX 3.0.1-Gerät mit der Sicherung wiederherstellen, müssen Sie die PowerStrips neu konfigurieren.*

Gerätekonfiguration wiederherstellen

Gerätekonfiguration wiederherstellen

Die folgenden Gerätetypen ermöglichen Ihnen die Wiederherstellung einer vollständigen Sicherung der Gerätekonfiguration.

- KX
- KSX
- KX101
- SX
- IP-Reach

Bei KX2-Geräten können Sie auswählen, welche Komponenten einer Sicherung Sie auf dem Gerät wiederherstellen möchten.

- **Geschützt**: Der gesamte Inhalt der ausgewählten Sicherungsdatei mit Ausnahme der Netzwerkeinstellungen (Personality Package) wird auf dem Gerät wiederhergestellt.
- **Vollständig**: Der gesamte Inhalt der ausgewählten Sicherungsdatei wird auf dem Gerät wiederhergestellt.
- **Benutzerdefiniert**: Mit dieser Option können Sie die Geräteeinstellung, die Benutzer- und Benutzergruppeneinstellungen oder beides wiederherstellen.

Gerätekonfiguration wiederherstellen (KX, KSX, KX101, SX, IP-Reach)

Sie können eine vollständige Sicherungskonfiguration auf KX, KSX, KX101, SX- und IP-Reach-Geräten wiederherstellen.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät aus, auf dem Sie eine Sicherungskonfiguration wiederherstellen möchten.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Konfiguration** > **Wiederherstellen**.
3. Wählen Sie in der Tabelle **Verfügbare Sicherungen** die Sicherungskonfiguration aus, die Sie auf dem Gerät wiederherstellen möchten.
4. Klicken Sie auf **OK**.
5. Klicken Sie zum Neustarten des Geräts auf **Ja**. Eine Meldung wird eingeblendet, wenn alle Daten wiederhergestellt wurden.

Alle Konfigurationsdaten mit Ausnahme der Netzwerkeinstellungen auf einem KX2-Gerät wiederherstellen

Mit der Wiederherstellungsoption Geschützt können Sie alle Konfigurationsdaten einer Sicherungsdatei mit Ausnahme der Netzwerkeinstellungen auf einem KX2-Gerät wiederherstellen.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät aus, auf dem Sie eine Sicherungskonfiguration wiederherstellen möchten.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Konfiguration** > **Sicherung**.
3. Wählen Sie in der Tabelle **Verfügbare Sicherungen** die Sicherungskonfiguration aus, die Sie auf dem Gerät wiederherstellen möchten.
4. **Wiederherstellungstyp**: Wählen Sie **Geschützt**.
5. Klicken Sie auf **OK**.
6. Klicken Sie zum Neustarten des Geräts auf **Ja**. Eine Meldung wird eingeblendet, wenn alle Benutzer- und Systemkonfigurationsdaten wiederhergestellt wurden.

Nur Geräteeinstellungen oder Benutzer- und Benutzergruppendaten auf einem KX2-Gerät wiederherstellen

Mit der Wiederherstellungsoption Benutzerdefiniert können Sie Geräteeinstellungen, Benutzer- und Benutzergruppendaten oder beides wiederherstellen.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät aus, auf dem Sie eine Sicherungskonfiguration wiederherstellen möchten.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Konfiguration** > **Wiederherstellen**.
3. Wählen Sie in der Tabelle **Verfügbare Sicherungen** die Sicherungskonfiguration aus, die Sie auf dem Gerät wiederherstellen möchten.
4. **Wiederherstellungstyp**: Wählen Sie **Benutzerdefiniert**.
5. **Wiederherstellungsoptionen**: Wählen Sie die Komponenten, die Sie auf dem Gerät wiederherstellen möchten: Geräteeinstellungen und Benutzer- und Benutzergruppendaten.

6. Klicken Sie auf **OK**.
7. Klicken Sie zum Neustarten des Geräts auf **Ja**. Eine Meldung wird eingeblendet, wenn die Daten wiederhergestellt wurden.

Alle Konfigurationsdaten auf einem KX2-Gerät wiederherstellen

Mit der Wiederherstellungsoption Vollständig können Sie alle Konfigurationsdaten einer Sicherungsdatei auf einem KX2-Gerät wiederherstellen.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät aus, auf dem Sie eine Sicherungskonfiguration wiederherstellen möchten.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Konfiguration** > **Wiederherstellen**.
3. Wählen Sie in der Tabelle **Verfügbare Sicherungen** die Sicherungskonfiguration aus, die Sie auf dem Gerät wiederherstellen möchten.
4. **Wiederherstellungstyp**: Wählen Sie **Vollständig**.
5. Klicken Sie auf **OK**.
6. Klicken Sie zum Neustarten des Geräts auf **Ja**. Eine Meldung wird eingeblendet, wenn alle Benutzer- und Systemkonfigurationsdaten wiederhergestellt wurden.

Gerätekonfiguration kopieren

Sie können Konfigurationen von einem Gerät auf ein anderes Gerät oder mehrere 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. Wählen Sie Geräte > Gerätemanager > Konfiguration > Konfiguration kopieren.
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. Eine Meldung wird eingeblendet, wenn die Gerätekonfiguration kopiert wurde.

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 Neustarten aus.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Gerät neu starten**.
3. Klicken Sie zum Neustarten des Geräts auf **OK**.
4. Klicken Sie auf Ja, um zu bestätigen, dass alle Benutzer, die auf das Gerät zugreifen, abgemeldet werden.

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 Pingen aus.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Gerät anpingen**. Das Fenster **Gerät anpingen** wird mit dem Ergebnis des Ping-Befehls angezeigt.

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. Wählen Sie **Geräte** > **Gerätemanager** > **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. Wählen Sie **Geräte** > **Gerätemanager** > **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. Der Gerätestrommanager bietet eine auf PowerStrips zentrierte Ansicht der Ausgänge.

Bevor Sie den Gerätestrommanager verwenden können, muss eine physische 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 Stromversorgungsport verknüpft, der dem Dominion KSX-Gerät zugeordnet ist und der die Verwaltung des PowerStrip bereitstellt.

1. Wählen Sie auf der Registerkarte **Geräte** ein PowerStrip-Gerät aus.
2. Wählen Sie **Geräte** > **Gerätestrommanager**.
3. Die Ausgänge werden im Fensterbereich **Status der Ausgänge** aufgeführt. Möglicherweise müssen Sie nach unten blättern, um alle Ausgänge anzuzeigen.
   - Verwenden Sie für jeden Ausgang die Optionsschaltflächen **Ein** oder **Aus**, um den Ausgang ein- oder auszuschalten.
   - Klicken Sie auf **Aus- und einschalten**, um das mit dem Ausgang verbundene Gerät neu zu starten.

Administration starten

Falls für das ausgewählte Gerät verfügbar, bietet der Befehl **Administration starten** Zugriff auf die Verwaltungsschnittstelle des Geräts.

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

Topologieansicht

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

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

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät aus, dessen Topologieansicht Sie anzeigen möchten.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Topologieansicht.** Die **Topologieansicht** für das ausgewählte Gerät wird angezeigt.
   - Klicken Sie auf + oder -, um die Ansicht ein- oder auszublenden.

Benutzerverbindung trennen

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

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

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.

1. Klicken Sie auf die Registerkarte **Geräte**, und wählen Sie das Gerät aus, von dem Sie einen oder mehrere Benutzer trennen möchten.

2. Wählen Sie Geräte > Gerätemanager > 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.

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.

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 den **Paragon II-Systemcontroller** aus.

2. Klicken Sie mit der rechten Maustaste auf **Paragon II-Systemcontroller**, und wählen Sie dann **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 **Verwaltung starten**, um Raritan Remote Console zu aktivieren und die blaue Gerätekonfigurationsanzeige in einem neuen Fenster zu öffnen.

Gerätegruppenmanager

Mit dem Gerätegruppenmanager 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 unter ***Richtlinien für die Zugriffssteuerung*** (auf Seite 106).

Gerätegruppen hinzufügen

1. Wählen Sie **Zuordnungen** > **Gerätegruppen**. Das Fenster Gerätegruppenmanager wird angezeigt. Vorhandene Gerätegruppen werden im linken Fensterbereich angezeigt.
2. Klicken Sie auf der Symbolleiste auf das Symbol Neue Gruppe  . Der Fensterbereich **Gerätegruppe: Neu** wird angezeigt.
3. Geben Sie in das Feld **Gruppenname** einen Namen für die Gerätegruppe ein, die Sie erstellen möchten. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
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 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 Entfernen eines Geräts aus der Gruppe den Gerätenamen in der Liste **Ausgewählt** aus, und klicken Sie auf **Entfernen**.
- 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 zuordnen möchten.

b. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile  , 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.

1. **Präfix**: Feld leer lassen oder **NOT** auswählen. Wenn **NOT** ausgewählt ist, sucht diese Regel nach Werten, die dem Ausdruck nicht entsprechen.
2. **Kategorie**: Wählen Sie ein Attribut aus, das in der Regel bewertet wird. Es sind alle Kategorien verfügbar, die Sie im **Zuordnungsmanager** erstellt haben.
3. **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).
4. **Element**: Wählen Sie einen Wert für das Kategorieattribut zum Vergleich aus. Hier werden nur Elemente dargestellt, die der ausgewählten Kategorie zugewiesen sind. (Beispiel: wenn eine Kategorie „Abteilung“ bewertet wird, werden Elemente mit der Bezeichnung „Standort“ nicht angezeigt).
5. **Regelname**: Der Name, der der Regel in dieser Zeile zugeordnet wurde. Dieser Name kann nicht bearbeitet werden. Er wird zur Beschreibung im Feld **Kurzer Ausdruck** verwendet.

6. Wenn Sie eine weitere Regel hinzufügen möchten, klicken Sie auf **Neue Zeile einfügen**, 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.
7. Die Tabelle mit Regeln 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 1: 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.

Beispiel 2: 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 sowohl 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 entfernen möchten, wählen Sie die Zeile aus, und klicken Sie auf das Symbol zum Entfernen der ausgewählten Zeile  .
- Wenn Sie eine Liste der Geräte anzeigen möchten, deren Parameter den von Ihnen definierten Regeln entsprechen, klicken Sie auf **Geräte anzeigen**.

  a. 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.

  b. 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.

  c. 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.

d. (Optional) 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. Klicken Sie auf **OK**, nachdem Sie alle gewünschten Gerätegruppen hinzugefügt haben, um Ihre Änderungen zu speichern.

Gerätegruppen bearbeiten

1. Wählen Sie **Zuordnungen** > **Gerätegruppen**. Das Fenster Gerätegruppenmanager wird angezeigt.
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. (Optional) Geben Sie einen neuen Namen für die Gerätegruppe 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 finden Sie unter **Gerätegruppen hinzufügen** (auf Seite 54).
5. Klicken Sie zum Speichern der Änderungen auf **OK**.

Gerätegruppen löschen

1. Wählen Sie **Zuordnungen** > **Gerätegruppen**. Das Fenster Gerätegruppenmanager wird angezeigt.
2. Vorhandene Gerätegruppen werden im linken Fensterbereich angezeigt. Wählen Sie die Gerätegruppe aus, die gelöscht werden soll. Der Fensterbereich für Gerätegruppendetails wird angezeigt.
3. Wählen Sie **Gruppen** > **Löschen**.
4. Der Fensterbereich zum Löschen von Gerätegruppen wird angezeigt. Klicken Sie auf **Löschen**.
5. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Kapitel 7 Verwaltete PowerStrips

In CC-SG müssen PowerStrips mit einem der folgenden Geräte verbunden sein:

- Dominion KX
- Dominion KX2
- Dominion SX 3.0
- Dominion SX 3.1
- Dominion KSX
- Paragon II-Systemcontroller (P2SC)

Für die Konfiguration von PowerStrips in CC-SG müssen Sie wissen, an welches Raritan-Gerät der PowerStrip physisch angeschlossen ist.

In diesem Kapitel

Vorgang zum Konfigurieren der Stromversorgungssteuerung in CC-SG

1. Schließen Sie alle physischen Verbindungen zwischen dem Gerät, dem PowerStrip und den Knoten, die vom PowerStrip mit Strom versorgt werden, ab. Weitere Informationen zu den physischen Verbindungen zwischen PowerStrips, Geräten und Knoten finden Sie in den Handbüchern für den Schnellstart für RPC und Dominion PX sowie im CC-SG Implementierungshandbuch.
2. Fügen Sie das Verwaltungsgerät zu CC-SG hinzu. Der Vorgang unterscheidet sich für die unterschiedlichen Raritan-Geräte. Lesen Sie bitte den Abschnitt, der für das Gerät geschrieben wurde, an das der PowerStrip angeschlossen ist:
   - ***PowerStrips, die an KX-, KX2- und P2SC-Geräte angeschlossen sind, konfigurieren;*** (siehe "PowerStrips, die an KX-, KX2- und P2SC-Geräte angeschlossen sind, konfigurieren" auf Seite 60)

- ***PowerStrips, die an SX 3.0- und KSX-Geräte angeschlossen sind, konfigurieren;*** (siehe "PowerStrips, die an SX 3.0- und KSX-Geräte angeschlossen sind, konfigurieren" auf Seite 61)
- ***PowerStrips, die an SX 3.1-Geräte angeschlossen sind, konfigurieren*** (auf Seite 64).

3. ***Ausgänge konfigurieren*** (siehe "Ausgänge auf einem PowerStrip konfigurieren" auf Seite 66).
4. Weisen Sie jedem Ausgang den Knoten zu, der ihn mit Strom versorgt: ***Verwaltete PowerStrip-Schnittstelle einem Knoten hinzufügen*** (siehe "Schnittstellen für verwaltete Powerstrip-Verbindungen" auf Seite 76)

PowerStrips, die an KX-, KX2- und P2SC-Geräte angeschlossen sind, konfigurieren

CC-SG erkennt automatisch PowerStrips, die an KX- und KX2-Geräte angeschlossen sind. Sie können in CC-SG die folgenden Aufgaben durchführen, um PowerStrips zu konfigurieren und zu verwalten, die an KX- und KX2-Geräte angeschlossen sind.

- PowerStrip-Gerät, das an ein KX- oder KX2-Gerät angeschlossen ist, hinzufügen
- PowerStrip eines KX- oder KX2-Geräts an einen anderen Port bewegen
- PowerStrip, der an ein KX- oder KX2-Gerät angeschlossen ist, löschen

PowerStrip-Gerät, das an ein KX-, KX2- oder P2SP-Gerät angeschlossen ist, hinzufügen

Wenn Sie CC-SG ein KX- oder KX2-Gerät, das an einen PowerStrip angeschlossen ist, hinzufügen, wird der PowerStrip automatisch hinzugefügt. Der PowerStrip wird auf der Registerkarte Geräte unter dem KX- oder KX2-Gerät, an das er angeschlossen ist, angezeigt.

Nächste Schritte:

1. ***Ausgänge konfigurieren*** (siehe "Ausgänge auf einem PowerStrip konfigurieren" auf Seite 66).
2. Weisen Sie jedem Ausgang den Knoten zu, der ihn mit Strom versorgt: ***Verwaltete PowerStrip-Schnittstelle einem Knoten hinzufügen*** (siehe "Schnittstellen für verwaltete Powerstrip-Verbindungen" auf Seite 76)

PowerStrip eines KX-, KX2- oder P2SC-Geräts an einen anderen Port bewegen

Wenn Sie einen PowerStrip physisch von einem KX-, KX2- oder P2SC-Gerät oder Port zu einem anderen KX-, KX2- oder P2SC-Gerät oder Port bewegen, erkennt CC-SG automatisch den PowerStrip und aktualisiert seine Zuordnungen auf das richtige Gerät. Sie brauchen CC-SG den PowerStrip nicht separat hinzuzufügen.

Hinweis: *Wenn Sie einen PowerStrip von einem P2SC-Port physisch entfernen aber diesen PowerStrip nicht an einen anderen Port anschließen, entfernt CC-SG den PowerStrip nicht vom alten Port. Sie müssen eine teilweise oder vollständige Datenbankzurücksetzung der UMT-Einheit, an die der PowerStrip angeschlossen ist, durchführen, um den PowerStrip von der Registerkarte Geräte zu entfernen. Lesen Sie die entsprechende Dokumentation von Raritan.*

PowerStrip, der an ein KX-, KX2- oder P2SC-Gerät angeschlossen ist, löschen

Sie können einen PowerStrip, der an ein KX- oder KX2-Gerät angeschlossen ist, nicht aus CC-SG löschen. Sie müssen den PowerStrip vom KX- oder KX2-Gerät physisch trennen, um den PowerStrip aus CC-SG zu löschen. Nachdem Sie den PowerStrip von einem KX- oder KX2-Gerät physisch getrennt haben, werden der PowerStrip und alle konfigurierten Ausgänge nicht mehr auf der Registerkarte Geräte angezeigt.

PowerStrips, die an SX 3.0- und KSX-Geräte angeschlossen sind, konfigurieren

Sie können in CC-SG die folgenden Aufgaben durchführen, um PowerStrips zu konfigurieren und zu verwalten, die an SX 3.0- und KSX-Geräte angeschlossen sind.

Hinweis: *PowerStrips müssen physisch an den Stromversorgungsport eines KSX-Geräts angeschlossen sein.*

- PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, hinzufügen
- PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, löschen
- Geräte- oder Portzuordnung eines PowerStrips ändern (SX 3.0, KSX)

PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, hinzufügen

1. ***SX 3.0- oder KSX-Gerät zu CC-SG hinzufügen*** (siehe "KVM- oder serielle Geräte hinzufügen" auf Seite 38).
2. Wählen Sie **Geräte** > **Gerätemanager** > **Gerät hinzufügen**.
3. Wählen Sie im Dropdown-Menü **Gerätetyp** die Option **PowerStrip**.
4. Geben Sie einen Namen in das Feld **Powerstrip-Name** ein. Halten Sie Ihren Mauszeiger über das Feld, um die für den Namen zulässige Anzahl an Zeichen zu sehen. Leerstellen sind nicht zulässig.
5. Klicken Sie auf das Dropdown-Menü **Anzahl der Ausgänge**, und wählen Sie die Anzahl der Ausgänge für den PowerStrip aus.
6. Klicken Sie auf das Dropdown-Menü **Verwaltungsgerät**, und wählen Sie dann das SX 3.0- oder KSX-Gerät aus, das an diesen Powerstrip angeschlossen ist.
7. Klicken Sie auf das Dropdown-Menü **Verwaltungsport**, und wählen Sie den Port am SX 3.0- oder KSX-Gerät aus, an den dieser Powerstrip angeschlossen ist.
8. (Optional) Sie können auch eine kurze Beschreibung für den PowerStrip in das Feld **Beschreibung** eingeben.
9. (Optional) Markieren Sie das Kontrollkästchen **Alle Ausgänge konfigurieren**, wenn jeder Ausgang dieses PowerStrip-Geräts automatisch zur Registerkarte **Geräte** hinzugefügt werden soll. Wenn Sie jetzt nicht alle Ausgänge konfigurieren, können Sie ***die Ausgänge später konfigurieren*** (siehe "Ausgänge auf einem PowerStrip konfigurieren" auf Seite 66).
10. (Optional) 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. Weitere Informationen finden Sie unter ***Zuordnungen*** (siehe "Zuordnungen, Kategorien und Elemente" auf Seite 27).
11. Wenn Sie diesen PowerStrip 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. Sie können auch auf **OK** klicken, um diesen Powerstrip hinzuzufügen und den Bildschirm Gerät hinzufügen nicht anzuzeigen.

Nächste Schritte:

1. ***Ausgänge konfigurieren*** (siehe "Ausgänge auf einem PowerStrip konfigurieren" auf Seite 66).
2. Weisen Sie jedem Ausgang den Knoten zu, der ihn mit Strom versorgt: ***Verwaltete PowerStrip-Schnittstelle einem Knoten hinzufügen*** (siehe "Schnittstellen für verwaltete Powerstrip-Verbindungen" auf Seite 76)

PowerStrip, der an ein SX 3.0- oder KSX-Gerät angeschlossen ist, löschen

Sie können einen PowerStrip, der an ein SX 3.0-, KSX- oder P2SC-Gerät angeschlossen ist, sogar dann löschen, wenn der PowerStrip noch immer physisch angeschlossen ist. Wenn Sie den PowerStrip vom SX 3.0-, KSX- oder P2SC-Gerät, dem er zugeordnet ist, trennen, wird er auf der Registerkarte Geräte weiterhin unter diesem Gerät angezeigt. Wenn Sie den PowerStrip aus der Anzeige entfernen möchten, müssen Sie ihn löschen.

1. Wählen Sie auf der Registerkarte Geräte den PowerStrip zum Löschen aus.
2. Wählen Sie Geräte > Gerätemanager > Gerät löschen.
3. Klicken Sie zum Löschen des PowerStrips auf OK. Eine Meldung wird eingeblendet, wenn der PowerStrip gelöscht wurde. Das PowerStrip-Symbol wird von der Registerkarte Geräte entfernt.

Geräte- oder Portzuordnung eines PowerStrips ändern (SX 3.0, KSX)

Wenn ein PowerStrip physisch von einem SX 3.0- oder KSX-Gerät oder Port zu einem anderen SX 3.0- oder KSX-Gerät oder Port bewegt wird, müssen Sie in CC-SG im PowerStrip-Profil die Zuordnung ändern.

1. Wählen Sie auf der Registerkarte Geräte den PowerStrip aus, der von einem SX 3.0- oder KSX-Gerät oder Port zu einem anderen Gerät oder Port bewegt wurde.
2. Klicken Sie auf das Dropdown-Menü **Verwaltungsgerät**, und wählen Sie dann das SX 3.0- oder KSX-Gerät aus, das an diesen PowerStrip angeschlossen ist.
3. Klicken Sie auf das Dropdown-Menü **Verwaltungsport**, und wählen Sie den Port am SX 3.0- oder KSX-Gerät aus, an den dieser PowerStrip angeschlossen ist.
4. Klicken Sie auf **OK**.

PowerStrips, die an SX 3.1-Geräte angeschlossen sind, konfigurieren

Sie können in CC-SG die folgenden Aufgaben durchführen, um PowerStrips zu konfigurieren und zu verwalten, die an SX 3.1-Geräte angeschlossen sind.

- PowerStrip-Gerät, das an ein SX 3.1-Gerät angeschlossen ist, hinzufügen
- PowerStrip eines SX 3.1-Geräts an einen anderen Port bewegen
- PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, löschen

PowerStrip-Gerät, das an ein SX 3.1-Gerät angeschlossen ist, hinzufügen

Der Vorgang zum Hinzufügen eines PowerStrips, der an ein SX 3.1-Gerät angeschlossen ist, hängt davon ab, ob das SX 3.1-Gerät zu CC-SG hinzugefügt wurde.

Wenn der PowerStrip an das SX 3.1-Gerät angeschlossen ist und das Gerät noch nicht zu CC-SG hinzugefügt wurde:

1. ***SX 3.1-Gerät zu CC-SG hinzufügen*** (siehe "KVM- oder serielle Geräte hinzufügen" auf Seite 38).
2. CC-SG erkennt den PowerStrip und fügt ihn automatisch hinzu. Der PowerStrip wird auf der Registerkarte Geräte unter dem SX 3.1-Gerät, an das er angeschlossen ist, angezeigt.

Wenn das SX 3.1-Gerät bereits zu CC-SG hinzugefügt wurde und der PowerStrip später an das Gerät angeschlossen wird:

1. ***SX 3.1-Gerät zu CC-SG hinzufügen*** (siehe "KVM- oder serielle Geräte hinzufügen" auf Seite 38).
2. ***Ports des SX 3.1-Geräts konfigurieren.*** (siehe "Ports konfigurieren" auf Seite 41)
3. Wählen Sie auf der Registerkarte **Geräte** das SX 3.1-Gerät aus, an das der PowerStrip angeschlossen ist.
4. Klicken Sie auf das Pluszeichen (+) neben dem Gerätesymbol, um die Portliste einzublenden.
5. Klicken Sie mit der rechten Maustaste auf den SX 3.1-Port, an den der PowerStrip angeschlossen ist, und wählen Sie im Popup-Menü die Option Powerstrip hinzufügen.

6. Geben Sie die Anzahl der Ausgänge ein, die der PowerStrip enthält, und klicken Sie dann auf **OK**.

Nächste Schritte:

1. ***Ausgänge konfigurieren*** (siehe "Ausgänge auf einem PowerStrip konfigurieren" auf Seite 66).
2. Weisen Sie jedem Ausgang den Knoten zu, der ihn mit Strom versorgt: ***Verwaltete PowerStrip-Schnittstelle einem Knoten hinzufügen*** (siehe "Schnittstellen für verwaltete Powerstrip-Verbindungen" auf Seite 76)

PowerStrip eines SX 3.1-Geräts an einen anderen Port bewegen

Wenn Sie einen PowerStrip physisch von einem SX 3.1-Gerät oder Port zu einem anderen SX 3.1-Gerät oder Port bewegen, müssen Sie ***den PowerStrip vom alten SX 3.1-Port löschen*** (siehe "PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, löschen" auf Seite 65) und ***den PowerStrip dem neuen SX 3.1-Port hinzufügen*** (siehe "PowerStrip-Gerät, das an ein SX 3.1-Gerät angeschlossen ist, hinzufügen" auf Seite 64).

PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, löschen

Sie können einen PowerStrip, der an ein SX 3.1-Gerät angeschlossen ist, sogar dann löschen, wenn der PowerStrip noch immer physisch angeschlossen ist. Wenn Sie den PowerStrip vom SX 3.1-Gerät, dem er zugeordnet ist, trennen, wird er auf der Registerkarte Geräte weiterhin unter diesem Gerät angezeigt. Wenn Sie den PowerStrip aus der Anzeige entfernen möchten, müssen Sie ihn löschen.

1. Wählen Sie auf der Registerkarte **Geräte** den PowerStrip zum Löschen aus.
2. Wählen Sie **Geräte** > **Gerätemanager** > **Gerät löschen**.
3. Klicken Sie zum Löschen des PowerStrips auf **OK**. Eine Meldung wird eingeblendet, wenn der PowerStrip gelöscht wurde. Das PowerStrip-Symbol wird von der Registerkarte Geräte entfernt.

Ausgänge auf einem PowerStrip konfigurieren

Sie müssen die Ausgänge auf einem PowerStrip durch das ***Hinzufügen der verwalteten PowerStrip-Schnittstelle zum Knoten*** (siehe "Schnittstellen für verwaltete Powerstrip-Verbindungen" auf Seite 76) konfigurieren, bevor Sie jeden Ausgang einem Knoten zuordnen können.

➢ *So konfigurieren Sie Ausgänge im PowerStrip-Profil:*

1. Klicken Sie auf der Registerkarte **Geräte** auf das Pluszeichen (+) neben dem Gerät, das an den PowerStrip angeschlossen ist, um alle Ports einzublenden.
2. Wählen Sie den PowerStrip aus, dessen Ausgänge Sie konfigurieren möchten.
3. Wählen Sie im Bildschirm Geräteprofil: PowerStrip die Registerkarte **Ausgänge**.
4. Markieren Sie das Kontrollkästchen für jeden Ausgang, den Sie konfigurieren möchten, und klicken Sie dann auf **OK**.

Die Ausgänge werden auf der Registerkarte **Geräte** unter dem PowerStrip-Symbol angezeigt.

➢ *So konfigurieren Sie Ausgänge im Bildschirm Ports konfigurieren:*

1. Klicken Sie auf der Registerkarte **Geräte** auf das Pluszeichen (+) neben dem Gerät, das an den PowerStrip angeschlossen ist, um alle Ports einzublenden.
2. Wählen Sie den PowerStrip aus, dessen Ausgänge Sie konfigurieren möchten.
3. Wählen Sie **Geräte** > **Portmanager** > **Ports konfigurieren**.
   - Wenn Sie mehrere Ausgänge mit den im Bildschirm angezeigten Standardnamen konfigurieren möchten, markieren Sie das Kontrollkästchen für jeden Ausgang, den Sie konfigurieren möchten. Klicken Sie dann auf **OK**, um jeden Ausgang mit dem Standardnamen zu konfigurieren.
   - Wenn Sie jeden Ausgang individuell konfigurieren möchten, klicken Sie neben dem Ausgang auf die Schaltfläche **Konfigurieren**, und geben Sie dann den Namen für den Ausgang in das Feld **Portname** ein. Klicken Sie zum Konfigurieren des Ports auf **OK**.

➢ *So löschen Sie einen Ausgang:*

1. Klicken Sie auf der Registerkarte **Geräte** auf das Pluszeichen (+) neben dem Gerät, das an den PowerStrip angeschlossen ist, um alle Ports einzublenden.
2. Klicken Sie auf das Pluszeichen (+) neben dem PowerStrip, um alle Ausgänge einzublenden.
3. Wählen Sie **Geräte** > **Portmanager** > **Ports löschen**.
4. Markieren Sie das Kontrollkästchen für jeden Ausgang, den Sie löschen möchten, und klicken Sie dann auf **OK**, um den Ausgang zu löschen.

Kapitel 8 Knoten, Knotengruppen und Schnittstellen

In diesem Abschnitt wird beschrieben, wie Knoten und die zugewiesenen Schnittstellen angezeigt, konfiguriert und bearbeitet werden. Außerdem wird beschrieben, wie Knotengruppen erstellt werden. Der Verbindungsaufbau zu Knoten wird kurz erläutert. Weitere Informationen zum Verbindungsaufbau zu Knoten finden Sie im **CommandCenter Secure Gateway-Benutzerhandbuch** von Raritan.

In diesem Kapitel

Knoten anzeigen

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

Registerkarte "Knoten"

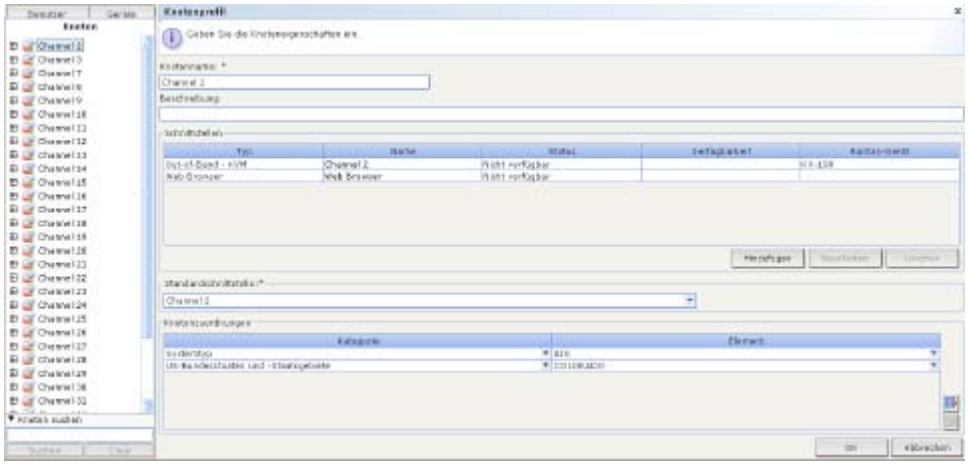
Wenn Sie auf die Registerkarte Knoten klicken, werden alle Knoten, auf die Sie zugreifen können, in einer Baumstruktur angezeigt.

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.

Weitere Informationen zum Anzeigen der Registerkarte Knoten auf verschiedene Weisen finden Sie unter ***Benutzerdefinierte Ansichten*** (siehe "Benutzerdefinierte Ansichten für Geräte und Knoten" auf Seite 113).

Knotenprofil

Klicken Sie auf der Registerkarte Knoten 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 zugeordnet wurden. Knoten, die virtuelle Medien unterstützen, umfassen eine weitere Spalte, in der angezeigt wird, ob die virtuellen Medien aktiviert oder deaktiviert sind.



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 Netzwerkinfrastruktureinheit 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, Ports und Schnittstellen später jederzeit bearbeiten.

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.

Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).

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

Knoten hinzufügen

➢ *So fügen Sie CC-SG einen Knoten hinzu:*

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Wählen Sie Knoten > **Knoten hinzufügen**.
3. Geben Sie den Namen des neuen Knotens in das Feld **Knotenname** ein. Alle Knotennamen in CC-SG müssen eindeutig sein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
4. (Optional) 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 **Schnittstellen** des Bildschirms Knoten hinzufügen auf **Hinzufügen**, um eine Schnittstelle hinzuzufügen. Weitere Informationen finden Sie unter ***Schnittstellen hinzufügen*** (auf Seite 73).
6. (Optional) Sie können eine Liste mit **Kategorien** und **Elementen** konfigurieren, um diesen Knoten besser beschreiben und verwalten zu können. Weitere Informationen finden Sie unter ***Zuordnungen*** (siehe "Zuordnungen, Kategorien und Elemente" auf Seite 27).
   - 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 unter ***Zuordnungen*** (siehe "Zuordnungen, Kategorien und Elemente" auf Seite 27).
7. Klicken Sie zum Speichern der Änderungen auf **OK**. Der Knoten wird der Knotenliste hinzugefügt.

Durch das Konfigurieren von Ports erstellte Knoten

Beim Konfigurieren der Ports eines Geräts wird automatisch ein Knoten für jeden Port erstellt. Für jeden Knoten wird auch eine Schnittstelle erstellt.

Wird ein Knoten automatisch erstellt, wird ihm der gleiche Name wie dem Port gegeben, dem er zugewiesen ist. Wenn dieser Knotenname bereits vorhanden ist, wird dem Knotennamen eine Erweiterung hinzugefügt. Ein Beispiel ist Kanal1(1). Die Erweiterung ist die Zahl in Klammern. Diese Erweiterung ist bei der Zeichenanzahl des Knotennamens nicht eingeschlossen. Wenn Sie den Knotennamen bearbeiten, ist der neue Name auf die maximale Anzahl an Zeichen beschränkt. Weitere Informationen finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).

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 (siehe "Schnittstellen für In-Band-Verbindungen" auf Seite 74)

   - **In-Band - DRAC KVM**: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem Dell DRAC-Server über eine DRAC-Schnittstelle herzustellen. Sie müssen auch eine DRAC-Stromversorgungs-Schnittstelle konfigurieren.
   - **In-Band - iLO Processor KVM**: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem HP-Server über eine iLO- oder RILOE-Schnittstelle herzustellen.
   - **In-Band - 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.
   - **In-Band - RSA KVM**: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem IBM RSA-Server über eine RSA-Schnittstelle herzustellen. Sie müssen auch eine RSA-Stromversorgungs-Schnittstelle konfigurieren.
   - **In-Band - SSH**: Wählen Sie diese Option aus, um eine SSH-Verbindung zu einem Knoten herzustellen.
   - **In-Band - VNC**: Wählen Sie diese Option aus, um eine KVM-Verbindung zu einem Knoten über eine VNC-Serversoftware herzustellen.

   Out-of-Band-Verbindungen (siehe "Schnittstellen für Out-of-Band KVM-, Out-of-Band serielle Verbindungen" auf Seite 75)

   - **Out-of-Band - 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.

- **Out-of-Band - Seriell**: Wählen Sie diese Option aus, um eine serielle Verbindung zu einem Knoten über ein serielles Raritan-Gerät (SX, KSX) herzustellen.

Stromversorgungsverbindungen (siehe "Schnittstellen für DRAC-, RSA- und iLO Processor-Stromversorgungsverbindungen" auf Seite 75)

- **Stromversorgungssteuerung - DRAC**: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem Dell DRAC-Server zu erstellen.
- **Stromversorgungssteuerung - iLO Processor**: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem HP iLO/RILOE-Server zu erstellen.
- **Stromversorgungssteuerung - IPMI** (siehe "Schnittstellen für IPMI-Stromversorgungsverbindungen" auf Seite 76): Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem Knoten mit einer IPMI-Verbindung herzustellen.
- **Stromversorgungssteuerung - RSA**: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem RSA-Server zu erstellen.

Verwaltete PowerStrip-Verbindungen (siehe "Schnittstellen für verwaltete Powerstrip-Verbindungen" auf Seite 76)

- **Verwalteter PowerStrip**: Wählen Sie diese Option aus, um eine Stromversorgungsverbindung zu einem Knoten herzustellen, der über einen Raritan-PowerStrip wie Dominion PX versorgt wird.

Webbrowserverbindungen (siehe "Webbrowser-Schnittstelle" auf Seite 77)

- **Webbrowser**: Wählen Sie diese Option aus, um eine Verbindung zu einem Gerät mit einem eingebetteten Webserver herzustellen.

3. Im Feld **Name** wird ein Standardname angezeigt. Dies ist davon abhängig, welchen Schnittstellentyp Sie auswählen. Sie können den Namen ändern. Dieser Name wird neben der Schnittstelle in der Knotenliste angezeigt. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).

Schnittstellen für In-Band-Verbindungen

1. Geben Sie die IP-Adresse oder den Hostnamen dieser Schnittstelle in das Feld **IP-Adresse/Hostname** ein.

2. (Optional) Geben Sie einen TCP-Port für diese Verbindung in das Feld **TCP-Port** ein.
3. Geben Sie einen Benutzernamen für diese Verbindung in das Feld **Benutzername** ein.
4. (Optional) Geben Sie ein Kennwort für diese Verbindung in das Feld **Kennwort** ein.
5. (Optional) Sie können auch eine Beschreibung für diese Schnittstelle in das Feld **Beschreibung** eingeben.
6. Klicken Sie zum Speichern der Änderungen auf **OK**.

Schnittstellen für Out-of-Band KVM-, Out-of-Band serielle Verbindungen

1. **Anwendungsname**: Wählen Sie in der Liste die Anwendung aus, mit der Sie über die Schnittstelle eine Verbindung zum Konten herstellen möchten. CC-SG wählt die Anwendung basierend auf Ihrem Browser automatisch aus, wenn Sie **Automatisch erkennen** markieren.
2. **Raritan-Gerätename**: Wählen Sie das Raritan-Gerät aus, das den Zugriff auf diesen Knoten bereitstellt. Hinweis: Sie müssen zunächst ein Gerät zu CC-SG hinzufügen, bevor dies in der Liste angezeigt werden kann.
3. **Raritan-Portname**: Wählen Sie den Port auf dem Raritan-Gerät aus, das den 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.
4. (Optional) Sie können auch eine Beschreibung für diese Schnittstelle in das Feld **Beschreibung** eingeben.
5. Klicken Sie zum Speichern der Änderungen auf **OK**.

Schnittstellen für DRAC-, RSA- und iLO Processor-Stromversorgungsverbindungen

1. Geben Sie die IP-Adresse oder den Hostnamen dieser Schnittstelle in das Feld **IP-Adresse/Hostname** ein.
2. (Optional) Geben Sie einen TCP-Port für diese Verbindung in das Feld **TCP-Port** ein.
3. Geben Sie einen Benutzernamen für diese Verbindung in das Feld **Benutzername** ein.

4. (Optional) Geben Sie ein Kennwort für diese Verbindung in das Feld **Kennwort** ein.
5. (Optional) Sie können auch eine Beschreibung für diese Schnittstelle in das Feld **Beschreibung** eingeben.
6. Klicken Sie zum Speichern der Änderungen auf **OK**.

Schnittstellen für verwaltete Powerstrip-Verbindungen

Wenn Sie eine verwaltete Powerstrip-Schnittstelle erstellen, die ein KX-Gerät als Verwaltungsgerät festlegt, wird der von Ihnen festgelegte Ausgang in den Namen des zugewiesenen Knotens umbenannt.

1. **Verwaltungsgerät:** Wählen Sie das Raritan-Gerät aus, an das der Powerstrip angeschlossen ist. Das Gerät muss zu CC-SG hinzugefügt werden.
2. **Verwaltungsgerät:** Wählen Sie den Port auf dem Raritan-Gerät aus, an das der Powerstrip angeschlossen ist.
3. **Powerstrip-Name**: 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.
4. **Ausgangsname**: Wählen Sie den Namen des Ausgangs aus, an den der Knoten angeschlossen ist.
5. (Optional) Sie können auch eine Beschreibung für diese Schnittstelle in das Feld **Beschreibung** eingeben.
6. Klicken Sie zum Speichern der Änderungen auf **OK**.

Schnittstellen für IPMI-Stromversorgungsverbindungen

1. Geben Sie die IP-Adresse oder den Hostnamen dieser Schnittstelle in das Feld **IP-Adresse/Hostname** ein.
2. Geben Sie eine UDP-Portnummer für diese Schnittstelle in das Feld **UDP-Port** ein.
3. **Authentifizierung:** Wählen Sie ein Authentifizierungsschema für die Verbindung zu dieser Schnittstelle aus.
4. Geben Sie für diese Schnittstelle ein Überprüfungsintervall in das Feld **Überprüfungsintervall (Sekunden)** ein.
5. Geben Sie einen Benutzernamen für diese Schnittstelle in das Feld **Benutzername** ein.
6. (Optional) Geben Sie ein Kennwort für diese Schnittstelle in das Feld **Kennwort** ein.

7. (Optional) Sie können auch eine Beschreibung für diese Schnittstelle in das Feld **Beschreibung** eingeben.
8. Klicken Sie zum Speichern der Änderungen auf **OK**.

Webbrowser-Schnittstelle

Sie können eine Webbrowser-Schnittstelle hinzufügen, um eine Verbindung zu einem Gerät mit einem eingebetteten Webserver, z. B. Dominion PX, zu erstellen. ***Beispiel: Webbrowser-Schnittstelle zu einem PX-Knoten hinzufügen*** (auf Seite 79) Mit einer Webbrowser-Schnittstelle kann auch eine Verbindung zu einer Webanwendung, z. B. der Webanwendung, die einer RSA-, DRAC- oder iLO Processor-Karte zugewiesen ist, hergestellt werden.

Eine Webbrowser-Schnittstelle lässt eventuell keine automatische Anmeldung zu, wenn die Webanwendung weitere Informationen als den Benutzernamen und das Kennwort benötigt, z. B. eine Sitzungs-ID.

Benutzer müssen über die ***Node In-Band Access (In-Band Knotenzugriff)-Berechtigung*** (siehe "Benutzergruppen hinzufügen" auf Seite 94) verfügen, um auf eine Webbrowser-Schnittstelle zugreifen zu können.

Nur wenn DNS konfiguriert wurde, werden URLs aufgelöst. DNS muss nicht für IP-Adressen konfiguriert sein.

1. Der Standardname für eine Webbrowser-Schnittstelle ist Webbrowser. Sie können den Namen im Feld Name ändern. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
2. Geben Sie den URL oder Domänennamen der Webanwendung in das Feld URL ein. Beachten Sie, dass Sie den URL eingeben müssen, bei dem die Webanwendung erwartet, den Benutzernamen und das Kennwort zu lesen. Die Höchstanzahl sind 120 Zeichen. Beachten Sie diese Beispiele für die richtigen Formate:
   - http(s)://192.168.1.1/login.asp
   - http(s)://www.Beispiel.com/cgi/login
   - http(s)://Beispiel.com/home.html
3. (Optional) Geben Sie die Kombination von Benutzername und Kennwort ein, die den Zugriff auf diese Schnittstelle zulässt.

Hinweis: Lassen Sie die Felder für den Benutzernamen und das Kennwort bei DRAC-, iLO- und RSA-Webanwendungen leer, da sonst die Verbindung fehlschlägt.

4. Geben Sie die Feldnamen der Felder für den Benutzernamen und das Kennwort, die im Anmeldebildschirm für die Webanwendung verwendet werden, in das Feld für Benutzername und im Feld für Kennwort ein. Sie müssen den HTML-Quelltext des Anmeldebildschirms anzeigen, um die Feldnamen zu suchen. Verwechseln Sie die Feldnamen nicht mit den Feldbeschriftungen. ***Tipps für das Hinzufügen einer Webbrowser-Schnittstelle*** (auf Seite 78)
5. (Optional) Sie können auch eine Beschreibung für diese Schnittstelle in das Feld **Beschreibung** eingeben.
6. Klicken Sie zum Speichern der Änderungen auf **OK**.

Tipps für das Hinzufügen einer Webbrowser-Schnittstelle

Zum Konfigurieren der Webbrowser-Schnittstelle müssen Sie einige Informationen aus dem HTML-Quelltext zusammentragen, um die tatsächlichen Feldnamen der Felder Benutzername und Kennwort zu identifizieren. Alle Anbieter implementieren diese Authentifizierungsfelder unterschiedlich. Außerdem variieren die Namen dieser Felder von Gerät zu Gerät sowie zwischen den Firmwareversionen einzelner Geräte. Aus diesem Grund gibt es nicht nur eine Methode zum Suchen dieser Feldnamen. Im Vorgang unten wird eine mögliche Methode beschrieben.

Ein Softwaretechniker oder Systemadministrator kann Ihnen bei der Suche und Identifizierung der entsprechenden Feldnamen helfen.

➢ *Tipp zum Suchen der Feldnamen:*

1. Suchen Sie im HTML-Quelltext der Anmeldeseite für die Webanwendung nach der Beschriftung des Felds, z. B. Benutzername und Kennwort.
2. Wenn Sie die Feldbeschriftung gefunden haben, suchen Sie im angrenzenden Code nach einem Tag, der so ähnlich aussieht wie `name="user"`.

   Das Wort in Anführungszeichen ist der Feldname.

Beispiel: Webbrowser-Schnittstelle zu einem PX-Knoten hinzufügen

Ein PowerStrip, der von einem Dominion PX verwaltet wird, kann als Knoten zu CC-SG hinzugefügt werden. Sie können dem Knoten dann eine Webbrowser-Schnittstelle hinzufügen, über die Benutzer auf die webbasierte Verwaltungsanwendung des Dominion PX-Geräts zugreifen können.

- *Verwenden Sie die folgenden Werte, um eine Webbrowser-Schnittstelle für einen Dominion PX-Knoten hinzuzufügen:*

URL: `<DOMINION PX-IP-ADRESSE>/auth.asp`

Benutzername: Der Benutzername des Dominion PX-Administrators.

Kennwort: Das Kennwort des Dominion PX-Administrators.

Feld für Benutzername = `login`

Feld für Kennwort = `password`

Ergebnisse nach dem Hinzufügen von Schnittstellen

Wenn Sie einem Knoten eine Schnittstelle hinzufügen, wird die Schnittstelle in der Tabelle **Schnittstellen** und dem Dropdown-Menü **Standardschnittstelle** des Bildschirms **Knoten hinzufügen** oder **Knotenprofil** 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.

Wenn Sie eine verwaltete Powerstrip-Schnittstelle hinzufügen, die ein KX-Gerät als Verwaltungsgerät festlegt, wird der von Ihnen festgelegte Ausgang in den Namen des zugewiesenen Knotens umbenannt.

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.
3. Wählen Sie in der Tabelle **Schnittstellen** die Schnittstellenzeile aus, die Sie bearbeiten möchten.
4. Klicken Sie auf **Bearbeiten**.
5. Bearbeiten Sie bei Bedarf die Felder. Weitere Informationen zu den Feldern finden Sie unter ***Schnittstellen hinzufügen*** (auf Seite 73).
6. Klicken Sie zum Speichern der Änderungen auf **OK**.

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.
3. Wählen Sie in der Tabelle **Schnittstellen** die Schnittstellenzeile aus, die Sie löschen möchten.
4. Klicken Sie auf **Löschen**. Eine Bestätigungsmeldung wird angezeigt.
5. Klicken Sie auf **Ja**, um die Schnittstelle zu löschen.

Lesezeichen für Schnittstelle

Wenn Sie häufig auf einen Knoten über eine bestimmte Schnittstelle zugreifen, können Sie ein Lesezeichen für diese Schnittstelle in Ihrem Browser erstellen, d. h. die Schnittstelle Ihren Favoriten hinzufügen.

➢ *So erstellen Sie ein Lesezeichen für eine Schnittstelle in Ihrem Browser:*

1. Wählen Sie auf der Registerkarte **Knoten** die Schnittstelle aus, für die ein Lesezeichen erstellt werden soll. Sie müssen den Knoten erweitern, um die Schnittstellen anzuzeigen.
2. Wählen Sie **Knoten > Lesezeichen für Knotenschnittstelle**.

3. Wählen Sie **URL in Zwischenablage kopieren**.
4. Klicken Sie auf **OK**. Der URL wird in die Zwischenablage kopiert.
5. Öffnen Sie ein neues Browserfenster, und fügen Sie den URL in die Adresszeile ein.
6. Drücken Sie die **Eingabetaste**, um eine Verbindung zum URL herzustellen.
7. Fügen Sie den URL als Lesezeichen (Favorit) in Ihrem Browser hinzu.

➢ *So erstellen Sie ein Lesezeichen für eine Schnittstelle in Internet Explorer bzw. so fügen Sie eine Schnittstelle den Favoriten hinzu:*

1. Wählen Sie auf der Registerkarte **Knoten** die Schnittstelle aus, für die ein Lesezeichen erstellt werden soll. Sie müssen den Knoten erweitern, um die Schnittstellen anzuzeigen.
2. Wählen Sie **Knoten > Lesezeichen für Knotenschnittstelle**.
3. Wählen Sie **Lesezeichen hinzufügen (nur IE)**.
4. Im Feld **Lesezeichenname** wird ein Standardname für das Lesezeichen angezeigt. Sie können den Namen ändern. Dieser Name wird in Internet Explorer in der Liste **Favoriten** angezeigt.
5. Klicken Sie auf **OK**. Das Fenster **Zu Favoriten hinzufügen** wird eingeblendet.
6. Klicken Sie auf **OK**, um das Lesezeichen der Liste **Favoriten** hinzuzufügen.

➢ *So greifen Sie auf eine mit einem Lesezeichen versehene Schnittstelle zu:*

1. Öffnen Sie ein Browserfenster.
2. Wählen Sie die Schnittstelle in der Liste der Lesezeichen (Favoriten) im Browser aus.
3. Wenn der CC-SG-Zugriffs-Client angezeigt wird, melden Sie sich als ein Benutzer an, der Zugriff auf die Schnittstelle hat. Die Verbindung zur Schnittstelle wird hergestellt.

Knoten bearbeiten

Sie können einen Knoten bearbeiten, um den Namen, die Beschreibung, die Schnittstellen, die Standardschnittstelle oder die Zuordnungen zu ändern.

➢ *So bearbeiten Sie einen Knoten:*

1. Klicken Sie auf die Registerkarte **Knoten**, und wählen Sie den Knoten zum Bearbeiten aus. Das Knotenprofil wird angezeigt.
2. Bearbeiten Sie bei Bedarf die Felder.
   - **Knotenname**: Der Knotenname, der im Bildschirm Knotenprofil und auf der Registerkarte Knoten angezeigt wird. Alle Knotennamen in CC-SG müssen eindeutig sein.
   - **Beschreibung**: Eine Beschreibung des Knotens, damit Benutzer ihn leichter identifizieren können.
   - **Schnittstellen**: Sie können eine Schnittstelle hinzufügen, bearbeiten oder löschen.
   - **Standardschnittstelle**: Die Schnittstelle, über die standardmäßig eine Verbindung zu einem Knoten hergestellt wird.
   - **Knotenzuordnungen**: Eine Liste mit konfigurierten **Kategorien** und **Elementen**, um diesen Knoten besser beschreiben und verwalten zu können.
3. Klicken Sie zum Speichern der Änderungen auf **OK**.

Knoten löschen

Wenn Sie einen Knoten löschen, wird dieser von der Registerkarte Knoten entfernt. Benutzer können nicht mehr auf den Knoten zugreifen. Wenn Sie einen Knoten löschen, werden alle Schnittstellen, Zuordnungen und zugeordneten Ports gelöscht.

➢ *So löschen Sie einen Knoten:*

1. Wählen Sie auf der Registerkarte **Knoten** den Knoten zum Löschen aus.
2. Wählen Sie **Knoten** > **Knoten löschen**. Das Fenster **Knoten löschen** wird angezeigt.
3. Klicken Sie zum Löschen des Knotens auf **OK**.

4. Klicken Sie auf **Ja**, um zu bestätigen, dass durch das Löschen des Knotens auch alle Schnittstellen und zugewiesenen Ports gelöscht werden. Nach dem Löschvorgang wird eine Liste aller gelöschten Elemente angezeigt.

Massenkopieren für Knotenkategorien und -elemente

Mit dem Befehl Massenkopieren können Sie die einem Knoten zugeordneten Kategorien und Elemente auf mehrere andere Knoten mittels Kopieren übertragen. Kategorien und Elemente sind die einzigen Eigenschaften, die bei diesem Vorgang kopiert werden.

1. Klicken Sie auf die Registerkarte **Knoten**, und wählen Sie einen Knoten aus.
2. Wählen Sie **Knoten** > **Massenkopieren**.
3. Wählen Sie in der Liste **Alle Knoten** die Knoten aus, auf die Sie die Kategorien und Elemente des im Feld **Knotenname** angezeigten Knotens kopieren möchten.
   - Klicken Sie auf den Pfeil nach rechts, um der Liste **Ausgewählte Knoten** einen Knoten hinzuzufügen.
   - Zum Entfernen eines Knotens aus der Liste **Ausgewählte Knoten** wählen Sie den Knoten, und klicken Sie dann auf den Pfeil nach links.
4. Klicken Sie zum Massenkopieren auf **OK**. Eine Meldung wird eingeblendet, wenn die Knotenkategorien und -elemente kopiert wurden.

Verbindung zu 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 finden Sie im **CommandCenter Secure Gateway-Benutzerhandbuch** von Raritan.

➢ *So stellen Sie eine Verbindung mit einem Knoten her:*

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Wählen Sie den Knoten aus, zu dem Sie eine Verbindung herstellen möchten. Führen Sie außerdem Folgendes durch:
   - Klicken Sie in der Tabelle **Schnittstellen** auf den Namen der Schnittstelle, über die Sie die Verbindung herstellen möchten.

- Erweitern Sie auf der Registerkarte **Knoten** die Liste der Schnittstellen unter dem Knoten, mit dem Sie eine Verbindung herstellen möchten. Doppelklicken Sie auf den Namen der Schnittstelle, über die Sie eine Verbindung herstellen möchten.

Knoten anpingen

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

➢ *So pingen Sie einen Knoten an:*

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

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 an demselben Knoten können miteinander chatten.

➢ *So starten Sie eine Chatsitzung:*

1. Wählen Sie **Knoten** > **Chat** > **Chatsitzung starten**.
2. Geben Sie im unteren linken Feld eine Nachricht ein, und klicken Sie auf **Senden**. Die Nachricht wird im oberen linken Feld für alle Benutzer angezeigt.

➢ *So treten Sie einer verfügbaren Chatsitzung bei:*

- Wählen Sie **Knoten** > **Chat** > **Chatsitzung anzeigen**.

➢ *So beenden Sie eine Chatsitzung:*

1. Klicken Sie in der Chatsitzung auf **Schließen**. Eine Bestätigungsmeldung wird angezeigt.
   - Klicken Sie auf **Ja**, um die Chatsitzung für alle Teilnehmer zu schließen.
   - Klicken Sie auf **Nein**, um die Chatsitzung zu verlassen jedoch für andere Teilnehmer nicht zu schließen.

Knotengruppen

Knotengruppen werden zur Verwaltung von mehreren Knoten verwendet. Die Knotengruppe dient als Basis für eine Richtlinie, die den Zugriff auf diese Knotengruppe zulässt oder verweigert. Weitere Informationen finden Sie unter ***Richtlinien hinzufügen*** (auf Seite 108). Knoten können manuell oder durch Erstellen eines booleschen Ausdrucks, der einen Satz gemeinsamer Attribute beschreibt, gruppiert werden.

Wenn Sie den Setup-Assistenten 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 unter ***Zuordnungen*** (siehe "Zuordnungen, Kategorien und Elemente" auf Seite 27).

➢ *So zeigen Sie Knotengruppen an:*

- Wählen Sie **Zuordnungen** > **Knotengruppen**. Das Fenster **Knotengruppenmanager** wird angezeigt. Die Liste der vorhandenen Knotengruppen wird links angezeigt, und Details der ausgewählten Knotengruppe werden im Hauptfenster angezeigt.
  - 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.
  - 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 unter ***Benutzer und Benutzergruppen konfigurieren*** (siehe "Benutzer und Benutzergruppen" auf Seite 91).

- Wenn Sie eine Gruppe anzeigen, die 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.

Knotengruppen hinzufügen

➢ *So fügen Sie eine Knotengruppe hinzu:*

1. Wählen Sie **Zuordnungen** > **Knotengruppe**. Das Fenster **Knotengruppenmanager** wird angezeigt.
2. Wählen Sie **Gruppen** > **Hinzufügen**. Eine Vorlage einer Knotengruppe wird angezeigt.
3. Geben Sie in das Feld **Gruppenname** einen Namen für die Knotengruppe ein, die Sie erstellen möchten. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
4. 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

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** die Knoten aus, die 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 Entfernen eines Knotens aus der Gruppe den Knotennamen in der Liste **Ausgewählt** aus, und klicken Sie auf **Entfernen**.

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 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

1. Klicken Sie auf die Registerkarte **Knoten auswählen**.
2. Klicken Sie auf **Neue Zeile einfügen**, 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 der ausgewählten Kategorie zugewiesen 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 zugeordnet wurde. Sie können diese Werte nicht bearbeiten. Verwenden Sie diese Werte, um Beschreibungen in das 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 **Neue Zeile einfügen**, 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.
   - Markieren Sie in der Tabelle die Regeln, die gelöscht werden sollen, und klicken Sie auf **Zeile entfernen**.
5. Die Tabelle mit Regeln stellt 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 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 1: Wenn Sie Knoten 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.

Beispiel 2: 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. Lassen Sie diesen Vergleich zuerst durchführen, indem Sie ihn in Klammern einschließen: (Regel0|Regel1). Da die Knoten sowohl diesen Vergleich erfüllen als auch 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.

6. 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.
7. 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.
8. 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**.
9. 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.

Knotengruppen bearbeiten

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

➢ *So bearbeiten Sie eine Knotengruppe:*

1. Wählen Sie **Zuordnungen** > **Knotengruppe**. Das Fenster **Knotengruppenmanager** wird angezeigt.
2. Klicken Sie in der Knotengruppenliste 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**.
4. Klicken Sie zum Speichern der Änderungen auf **OK**.

Knotengruppen löschen

1. Wählen Sie **Zuordnungen** > **Knotengruppe**. Das Fenster **Knotengruppenmanager** wird angezeigt.
2. Wählen Sie in der Knotengruppenliste links den Knoten aus, den Sie löschen möchten.
3. Wählen Sie **Gruppen** > **Löschen**.

Kapitel 9 Benutzer und Benutzergruppen

Benutzerkonten werden erstellt, damit Benutzern ein Benutzername und Kennwort für den Zugriff auf CC-SG zugeordnet werden kann.

Eine **Benutzergruppe** definiert mehrere Berechtigungen für ihre Mitglieder. Sie können nur den Benutzergruppen und nicht den eigentlichen Benutzern Berechtigungen zuordnen. Alle Benutzer müssen mindestens einer Benutzergruppe angehören.

CC-SG verwaltet eine zentralisierte Benutzerliste und Benutzergruppenliste zur Authentifizierung und Autorisierung.

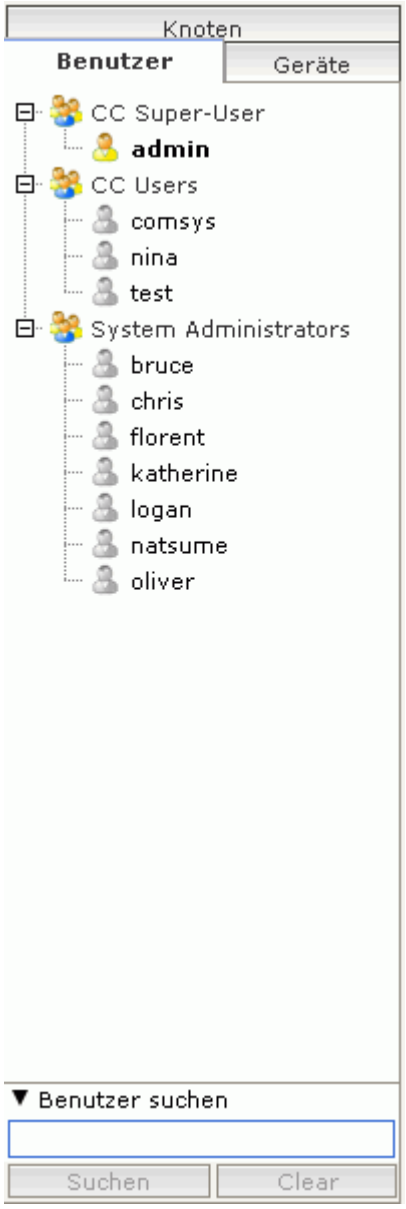
Die Konfiguration von CC-SG zur Verwendung externer Authentifizierung wird in ***Remoteauthentifizierung*** (auf Seite 123) beschrieben.

Das Erstellen von Zugriffsrichtlinien, die Sie den Benutzergruppen zuordnen können, wird in ***Richtlinien für die Zugriffssteuerung*** (auf Seite 106) beschrieben.

In diesem Kapitel

Registerkarte Benutzer

Klicken Sie auf die Registerkarte **Benutzer**, um alle Benutzergruppen und Benutzer in CC-SG anzuzeigen.



Benutzer sind unter den Benutzergruppen angeordnet, denen sie zugewiesen sind. Benutzergruppen mit zugeordneten Benutzern werden in der Liste mit dem Symbol + angezeigt. Klicken Sie auf das Pluszeichen (+), um die Liste der Benutzer in einer Gruppe ein- oder auszublenden. Aktive Benutzer, die zurzeit bei CC-SG angemeldet sind, werden in Fettdruck dargestellt.

Mithilfe der Registerkarte Benutzer können Sie in der Struktur nach Benutzern suchen.

Standardbenutzergruppen

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

Die CC-Superuser-Gruppe

Die **CC Super-User** -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 zugeordneten 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. Die Anforderungen für sichere Kennwörter sind:

- 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.

Systemadministratorgruppe

Die **Systemadministrator** gruppe 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.

Wichtig! Viele Menüelemente können nur ausgewählt werden, wenn zuvor die entsprechende Benutzergruppe oder der Benutzer ausgewählt wurde.

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 zugeordnet. Benutzer, die der Gruppe zugeordnet werden, erben diese Berechtigungen. Wenn Sie beispielsweise eine Gruppe erstellen und dieser die Berechtigung **Benutzerverwaltung** zuordnen, können alle Benutzer dieser Gruppe die Befehle im Menü **Benutzermanager** anzeigen und ausführen. Weitere Informationen finden Sie in ***Anhang C: Benutzergruppenberechtigungen*** (siehe "Benutzergruppenberechtigungen" auf Seite 280).

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 festlegen, auf welche Knoten die Benutzergruppe zugreifen kann

➢ *So fügen Sie eine Benutzergruppe hinzu:*

1. Wählen Sie **Benutzer** > **Benutzergruppenmanager** > **Benutzergruppe hinzufügen**. Das Fenster **Benutzergruppe hinzufügen** wird angezeigt
2. Geben Sie einen neuen Benutzergruppennamen in das Feld **Benutzergruppenname** ein. Benutzergruppennamen müssen eindeutig sein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
3. (Optional) Sie können auch eine kurze Beschreibung für diese 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 zuordnen möchten.
6. Unter der Berechtigungstabelle wird der Bereich **Knotenzugriff** mit Berechtigungen für drei Arten des Knotenzugriffs angezeigt: **Out-of-Band-Zugriff für Knoten**, **In-Band-Zugriff für für Knoten**, und **Stromversorgungssteuerung für Knoten**. Markieren Sie das Kontrollkästchen für die Art des Knotenzugriffs, die Sie der Benutzergruppe zuordnen möchten.
7. Klicken Sie auf die Registerkarte **Geräte- /Knotenrichtlinien** . Eine Tabelle mit Richtlinien wird angezeigt.

   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 deren Erstellung finden Sie unter ***Richtlinien und Knotengruppen konfigurieren*** (siehe "Richtlinien für die Zugriffssteuerung" auf Seite 106).
8. Wählen Sie in der Liste **Alle Richtlinien** die Richtlinie aus, die Sie der Benutzergruppe zuordnen möchten, und klicken Sie auf **Hinzufügen** , um die Richtlinie in die Liste **Ausgewählte Richtlinien** zu verschieben. Richtlinien in der Liste **Ausgewählte Richtlinien** gewähren oder verweigern den Zugriff auf die Knoten oder Geräte, die durch die Richtlinie gesteuert werden.

   Wiederholen Sie diesen Schritt, um der Benutzergruppe weitere Richtlinien zuzuweisen.

   - Wenn Sie dieser Gruppe den Zugriff auf alle verfügbaren Knoten gewähren möchten, wählen Sie in der Liste **Richtlinie hinzufügen** die Option **Richtlinie mit unbeschränkten Zugriff** us, und klicken Sie auf **Hinzufügen**.
   - Wählen Sie zum Entfernen einer Richtlinie von der Benutzergruppe den Namen der Richtlinie in der Liste **Ausgewählte Richtlinien** aus, und klicken Sie auf **Entfernen**.
9. (Optional) Wenn Sie die Konfiguration der Richtlinien für diese Gruppe abgeschlossen haben, klicken Sie zum Speichern dieser Gruppe und Erstellen einer weiteren auf **Übernehmen**. Wiederholen Sie die Schritte in diesem Abschnitt, um Benutzergruppen hinzuzufügen.
10. Klicken Sie zum Speichern der Änderungen auf **OK**.

Benutzergruppen bearbeiten

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

Hinweis: *Sie können die Berechtigungen oder Richtlinien der* ***CC-Super User*** *-Gruppe nicht bearbeiten.*

➢ *So bearbeiten Sie eine Gruppe:*

1. Klicken Sie links auf die Registerkarte **Benutzer**.
2. Klicken Sie auf der Registerkarte **Benutzer** auf eine Benutzergruppe. Das **Benutzergruppenprofil** wird angezeigt.
3. (Optional) Geben Sie einen neuen Namen für die Benutzergruppe in das Feld **Benutzergruppenname** ein.
4. (Optional) Sie können auch eine neue Beschreibung für diese 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 zuordnen 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 für jede Richtlinie, die Sie von der Benutzergruppe entfernen möchten, den Namen der Richtlinie in der Liste **Ausgewählte Richtlinien** aus, und klicken Sie auf **Entfernen**.
12. Klicken Sie zum Speichern der Änderungen auf **OK**.

Benutzergruppen löschen

Sie können eine Benutzergruppe löschen, wenn sie keine Mitglieder enthält.

➢ *So löschen Sie eine Benutzergruppe:*

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 **Benutzer** > **Benutzergruppenmanager** > **Benutzergruppe löschen**.
4. Klicken Sie zum Löschen der Benutzergruppe auf **OK**.

Benutzer hinzufügen

Wenn Sie zu CC-SG einen Benutzer hinzufügen, müssen Sie eine Benutzergruppe festlegen, um dem Benutzer die Zugriffsberechtigungen zu geben, die der Benutzergruppe zugeordnet sind.

➢ *So fügen Sie einen Benutzer hinzu:*

1. Wählen Sie auf der Registerkarte **Benutzer** die Gruppe aus, zu der Sie einen Benutzer hinzufügen möchten.
2. Wählen Sie **Benutzer** > **Benutzermanager** > **Benutzer hinzufügen**.
3. Geben Sie im Feld **Benutzername** den Benutzernamen des Benutzer ein, der hinzugefügt werden soll. Dieser Name wird für die Anmeldung bei CC-SG verwendet. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
4. Markieren Sie das Kontrollkästchen **Anmeldung aktiviert** wenn der Benutzer über die Anmeldeberechtigung für CC-SG verfügen soll.
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** das Kennwort ein, das der Benutzer zur Anmeldung in CC-SG verwenden soll.

   Hinweis: Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Kennwörtern verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).

   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 unter ***Erweiterte Administration*** (auf Seite 173).

7. Markieren Sie das Kontrollkästchen **Änderung des Kennworts bei der nächsten Anmeldung erzwingen**, wenn der Benutzer gezwungen werden soll, das zugeordnete Kennwort bei der nächsten Anmeldung zu ändern.
8. Markieren Sie das Kontrollkästchen **Änderung des Kennworts periodisch erzwingen**, wenn Sie angeben möchten, wie oft der Benutzer zur Kennwortänderung gezwungen werden soll.
9. Falls das Feld **Gültigkeitsdauer (in Tagen)** markiert ist, geben Sie die Anzahl an 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. Klicken Sie auf das Dropdown-Menü **Benutzergruppen**, und wählen Sie die Gruppe aus, zu der der Benutzer hinzugefügt wird.
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

Durch das Bearbeiten eines Benutzers können Sie die Gruppe, der dieser Benutzer angehört, nicht ändern. Weitere Informationen finden Sie unter ***Benutzer einer Gruppe zuordnen*** (auf Seite 100).

➢ *So bearbeiten Sie einen Benutzer:*

1. Klicken Sie auf der Registerkarte **Benutzer** auf das Pluszeichen (+), um die Benutzergruppe einzublenden, die einen Benutzer enthält, den Sie bearbeiten möchten. Wählen Sie dann den Benutzer aus. Das **Benutzerprofil** wird angezeigt.
2. 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.
3. 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 Feldere **Neues Kennwort** und **Neues Kennwort erneut eingeben** sind deaktiviert.
4. 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 unter ***Erweiterte Administration*** (auf Seite 173).
5. Markieren Sie das Kontrollkästchen **Änderung des Kennworts bei der nächsten Anmeldung erzwingen**, wenn der Benutzer gezwungen werden soll, das zugeordnete Kennwort bei der nächsten Anmeldung zu ändern.
6. 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.
7. Klicken Sie zum Speichern der Änderungen auf **OK**.

Benutzer löschen

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

Dieser Vorgang löscht alle Instanzen des Benutzers. Dies gilt auch, wenn der Benutzer mehreren Benutzergruppen angehört. Lesen Sie ***Benutzer aus einer Gruppe löschen*** (auf Seite 101), wenn Sie den Benutzer aus einer Gruppe entfernen möchten, ohne ihn aus CC-SG zu löschen..

➢ *So löschen Sie einen Benutzer:*

1. Klicken Sie auf der Registerkarte **Benutzer** auf das Pluszeichen (+), um die Benutzergruppe einzublenden, die einen Benutzer enthält, den Sie löschen möchten. Wählen Sie dann den Benutzer aus. Das **Benutzerprofil** wird angezeigt.
2. Wählen Sie **Benutzer** > **Benutzermanager**, **Benutzer löschen**.
3. Klicken Sie auf **OK**, um den Benutzer dauerhaft aus CC-SG zu löschen.

Benutzer einer Gruppe zuordnen

Verwenden Sie diesen Befehl, um vorhandene Benutzer einer Gruppe zuzuordnen, der sie nicht angehören. Benutzer, die auf diese Art und Weise zugeordnet 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**verschieben.

➢ *So ordnen Sie einen Benutzer einer Gruppe zu:*

1. Wählen Sie auf der Registerkarte **Benutzer** die Benutzergruppe aus, zu der Sie Benutzer zuordnen möchten.
2. Wählen Sie **Benutzer** > **Benutzergruppenmanager** > **Benutzer der Gruppe zuweisen**.
3. Die ausgewählte Benutzergruppe wird im Feld **Benutzergruppenname**angezeigt.
4. Benutzer, die der Zielgruppe nicht zugewiesen werden, werden in der Liste **Benutzer nicht in Gruppe** angezeigt.

- Wählen Sie die Benutzer aus, die Sie von dieser Liste hinzufügen möchten, und klicken Sie dann auf > , um die Benutzer in die Liste **Benutzer in Gruppe** zu verschieben.
- Klicken Sie auf die Schaltfläche >> , um alle Benutzer, die sich nicht in der Gruppe befinden, in die Liste **Benutzer in Gruppe** zu verschieben.
- Sie können Mitglieder aus der Zielgruppe entfernen, indem Sie die entsprechenden Benutzer in der Liste **Benutzer in Gruppe** auswählen und auf die Schaltfläche < klicken.
- Klicken Sie auf die Schaltfläche << , um alle Benutzer aus der Liste **Benutzer in Gruppe** zu entfernen.

5. Wenn Sie alle Benutzer in die entsprechenden Spalten verschoben haben, klicken Sie auf **OK**. Die Benutzer in der Liste **Benutzer in Gruppe** werden zur ausgewählten Benutzergruppe hinzugefügt.

Benutzer aus einer Gruppe löschen

Wenn Sie einen Benutzer aus einer Gruppe löschen, wird der Benutzer nur aus der festgelegten Gruppe entfernt. Der Benutzer bleibt in allen anderen zugeordneten Gruppen. Durch das Löschen eines Benutzers aus einer Gruppe wird der Benutzer nicht aus CC-SG gelöscht.

Wenn ein Benutzer nur zu einer Gruppe gehört, können Sie den Benutzer nicht aus der Gruppe löschen. Sie können den Benutzer nur aus CC-SG löschen.

➢ *So löschen Sie einen Benutzer in einer Gruppe:*

1. Klicken Sie auf der Registerkarte **Benutzer** auf das Pluszeichen (+), um die Benutzergruppe einzublenden, die einen Benutzer enthält, den Sie aus einer Gruppe löschen möchten. Wählen Sie dann den Benutzer aus. Das **Benutzerprofil** wird angezeigt.
2. Wählen Sie **Benutzer** > **Benutzermanager** > **Benutzer aus Gruppe löschen**. Das Fenster **Benutzer löschen** wird angezeigt.
3. Klicken Sie zum Löschen des Benutzers aus der Gruppe auf **OK**.

Ihr Benutzerprofil

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 zeigen Sie Ihr Profil an:*

- Wählen Sie **Secure Gateway** > **Mein Profil**. Der Bildschirm **Mein Profil ändern** wird mit Informationen zu Ihrem Konto angezeigt.

Eigenes Kennwort ändern

1. Wählen Sie **Secure Gateway** > **Mein Profil**.
2. Markieren Sie **Kennwort ändern**.
3. Geben Sie das aktuelle Kennwort in das Feld **Altes Kennwort** ein.
4. Geben Sie das neue Kennwort in das Feld **Neues Kennwort** ein. Eine Nachricht wird angezeigt, wenn sichere Kennwörter erforderlich sind.
5. Bestätigen Sie das neue Kennwort im Feld **Neues Kennwort erneut eingeben**.
6. Klicken Sie zum Speichern der Änderungen auf **OK**.

Eigene Standardsucheinstellungen ändern

1. Wählen Sie **Secure Gateway** > **Mein Profil**.
2. 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.
3. Klicken Sie zum Speichern der Änderungen auf **OK**.

Standardschriftgrad für CC-SG ändern

1. Wählen Sie **Secure Gateway** > **Mein Profil**.
2. Klicken Sie auf das Dropdown-Menü **Schriftgrad**, um den Schriftgrad anzupassen, den der Standard-CC-SG-Client verwendet.
3. Klicken Sie zum Speichern der Änderungen auf **OK**.

Eigene E-Mail-Adresse ändern

1. Wählen Sie **Secure Gateway** > **Mein Profil**.
2. 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.
3. Klicken Sie zum Speichern der Änderungen auf **OK**.

Benutzernamen des CC-SG-Superusers ändern

Sie müssen sich bei CC-SG über das CC-SG-Superuser-Konto angemeldet haben, um den Benutzernamen des CC-Superusers zu ändern. Der Standardbenutzername des CC-Superusers ist **admin**.

1. Wählen Sie **Secure Gateway** > **Mein Profil**.
2. Geben Sie einen neuen Namen in das Feld **Benutzername** ein.
3. Klicken Sie zum Speichern der Änderungen auf **OK**.

Benutzer abmelden

Sie können aktive Benutzer individuell oder nach Benutzergruppe von CC-SG abmelden.

➢ *So melden Sie einen Benutzer ab:*

1. Klicken Sie auf der Registerkarte **Benutzer** auf das Pluszeichen (+), um die Benutzergruppe einzublenden, die einen Benutzer enthält, den Sie bei CC-SG abmelden möchten. Wählen Sie dann den Benutzer aus.
   - Halten Sie zum Auswählen mehrerer Benutzer die **Umschalttaste** gedrückt, während Sie auf weitere Benutzer klicken.
2. Wählen Sie **Benutzer** > **Benutzermanager** > **Benutzer abmelden**. Der Bildschirm **Benutzer abmelden** wird mit den ausgewählten Benutzern angezeigt.
3. Klicken Sie auf **OK**, um die Benutzer bei CC-SG abzumelden.

➢ *So melden Sie alle Benutzer einer Benutzergruppe ab:*

1. Wählen Sie auf der Registerkarte **Benutzer** die Benutzergruppe aus, die Sie bei CC-SG abmelden möchten.
   - Halten Sie zum Abmelden mehrerer Benutzergruppen die **Umschalttaste** gedrückt, während Sie auf weitere Benutzergruppen klicken.
2. Wählen Sie **Benutzer** > **Benutzergruppenmanager** > **Benutzer abmelden**. Der Bildschirm **Benutzer abmelden** wird mit den aktiven Benutzern der ausgewählten Gruppen angezeigt.
3. Klicken Sie auf **OK**, um die Benutzer bei CC-SG abzumelden.

Massenkopieren für Benutzer

Sie können Massenkopieren für Benutzer verwenden, um die Benutzergruppenzugehörigkeiten eines Benutzers in einen anderen Benutzer oder in eine Benutzerliste zu kopieren. Wenn die kopierten Benutzer bereits Gruppenzugehörigkeiten besitzen, werden die Zugehörigkeiten entfernt.

➢ *So verwenden Sie Massenkopieren für Benutzer:*

1. Klicken Sie auf der Registerkarte **Benutzer** auf das Pluszeichen (+), um die Benutzergruppe einzublenden, die einen Benutzer enthält, dessen Richtlinien und Berechtigungen Sie kopieren möchten. Wählen Sie dann den Benutzer aus.
2. Wählen Sie **Benutzer** > **Benutzermanager** > **Massenkopieren**. Im Feld **Benutzername** wird der Benutzer angezeigt, dessen Richtlinien und Berechtigungen Sie kopieren.
3. Wählen Sie in der Liste **Alle Benutzer** die Benutzer aus, die die Richtlinien und Berechtigungen des im Feld **Benutzername** angezeigten Benutzers übernehmen sollen.
   - Klicken Sie auf **>** , um einen Benutzernamen in die Liste **Ausgewählte Benutzer** zu verschieben.
   - Klicken Sie auf **>>** , um alle Benutzer in die Liste **Ausgewählte Benutzer** zu verschieben.
   - Wählen Sie zum Entfernen eines Benutzers aus der Liste **Ausgewählte Benutzer** den Benutzer aus, und klicken Sie auf **<** (Pfeil nach links).
   - Klicken Sie auf **<<** , um alle Benutzer aus der Liste **Benutzer in Gruppe** zu entfernen.

4. Klicken Sie zum Kopieren auf **OK**.

Kapitel 10 Richtlinien für die Zugriffssteuerung

In diesem Kapitel

Zugriff anhand von Richtlinien steuern

Richtlinien sind Regeln, die definieren, auf welche Knoten und Geräte Benutzer zugreifen können, wann sie darauf zugreifen können und ob Berechtigungen für virtuelle Medien aktiviert sind, falls zutreffend. Richtlinien erstellen Sie am einfachsten durch Kategorisieren Ihrer Knoten und Geräte in Knoten- und Gerätegruppen. Anschließend erstellen Sie Richtlinien, die Zugriff auf die Knoten und Geräte in jeder Gruppe zulassen oder verweigern. Nachdem Sie eine Richtlinie erstellt haben, ordnen Sie die Richtlinie einer Benutzergruppe zu. Weitere Informationen finden Sie unter ***Richtlinien Benutzergruppen zuordnen*** (auf Seite 112).

CC-SG enthält auch eine **Richtlinie mit unbeschränktem Zugriff**. Wenn Sie allen Benutzern jederzeit Zugriff auf alle Knoten und Geräte gewähren möchten, können Sie allen Benutzergruppen die **Richtlinie mit unbeschränktem Zugriff** zuordnen.

Wenn Sie den **Setup-Assistenten** abgeschlossen haben, wurden eventuell schon einige allgemeine Richtlinien erstellt. Weitere Informationen finden Sie unter ***Konfigurieren von CC-SG mit dem Setup-Assistenten*** (auf Seite 16).

➢ *So steuern Sie den Zugriff mit Richtlinien:*

- Erstellen Sie Knotengruppen, um die Knoten zu verwalten, für die Sie Zugriffsregeln erstellen möchten. Weitere Informationen finden Sie unter ***Knotengruppen hinzufügen*** (auf Seite 86).
- Erstellen Sie Gerätegruppen, um die Geräte zu verwalten, für die Sie Zugriffsregeln erstellen möchten. Weitere Informationen finden Sie unter ***Gerätegruppen hinzufügen*** (auf Seite 54).
- Erstellen Sie eine Richtlinie für eine Knoten- oder Gerätegruppe, die angibt, wann der Zugriff auf die Knoten- oder Gerätegruppe erfolgen darf. Weitere Informationen finden Sie unter ***Richtlinien hinzufügen*** (auf Seite 108).
- Wenden Sie die Richtlinie auf eine Benutzergruppe an. Weitere Informationen finden Sie unter ***Richtlinien Benutzergruppen zuordnen*** (auf Seite 112).

Richtlinien hinzufügen

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 ausgewählte Knoten- oder Gerätegruppe zulässt (**Steuerung**). Benutzer erhalten nicht automatisch die Rechte **Steuerung**, wenn die Richtlinie **Ablehnen** nicht verwendet wird.

Hinweis: Wenn CC-SG im Proxymodus oder im Modus Beides ist, können Sie Benutzern keinen Zugriff auf virtuelle Medien geben. **Verbindungsmodi: Direkt und Proxy** *(auf Seite 192)*

➢ *So fügen Sie eine Richtlinie hinzu:*

1. Wählen Sie **Zuordnungen** > **Richtlinien**. Das Fenster **Richtlinienmanager** wird angezeigt.
2. Klicken Sie auf **Hinzufügen**. Geben Sie den Namen der Richtlinie in das Dialogfeld ein.
3. Geben Sie den Namen der neuen Richtlinie in das Feld **Richtlinienname** ein. Weitere Informationen zu den Regeln, die von CC-SG für die Länge von Namen verwendet werden, finden Sie unter ***Benennungskonventionen*** (siehe "Benennungsregeln" auf Seite 303).
4. Klicken Sie auf **OK**. Die neue Richtlinie wird im Bildschirm **Richtlinienmanager** zur Liste **Richtlinienname** hinzugefügt.
5. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Gerätegruppe**, und wählen Sie die Gerätegruppe aus, für die diese Richtlinie den Zugriff steuern soll.
6. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Knotengruppe**, und wählen Sie die Knotengruppe aus, für die diese Richtlinie den Zugriff steuern soll.
7. Bezieht sich die Richtlinie nur auf eine Gruppenart, müssen Sie nur einen Wert für die Gruppe auswählen.
8. Klicken Sie auf den Pfeil neben 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).

9. Wählen Sie **Benutzerdefiniert** aus, um die gewünschten Tage auszuwählen. Die Kontrollkästchen für die einzelnen Tage werden wählbar.
10. Markieren Sie die Kontrollkästchen für die Tage, an denen die Richtlinie gelten soll.
11. 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.
12. 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.
13. Wählen Sie im Feld **Geräte-/Knotenzugriffsberechtigung** die Option **Steuerung** aus, um diese Richtlinie so zu definieren, dass sie den Zugriff auf die ausgewählten 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 die ausgewählten Knoten- oder Gerätegruppen zu den angegebenen Uhrzeiten und Tagen verweigert.
14. Wenn Sie im Feld **Geräte-/Knotenzugriffsberechtigung** die Option **Steuerung** ausgewählt haben, wird der Bereich **Berechtigung für virtuelle Medien** wählbar. Wählen Sie im Feld **Berechtigung für virtuelle Medien** eine Option aus, um den Zugriff auf virtuelle Medien, die in den ausgewählten Knoten- oder Gerätegruppen verfügbar sind, zu den angegebenen Uhrzeiten und Tagen zuzulassen oder zu verweigern.
    - **Lese-/Schreibzugriff** ermöglicht sowohl Lese- als auch Schreibberechtigung auf virtuelle Medien.
    - **Lesezugriff** ermöglicht nur Leseberechtigungen auf virtuelle Medien.
    - **Ablehnen** verweigert den Zugriff auf virtuelle Medien.
15. Klicken Sie auf **Aktualisieren**, um die neue Richtlinie zu CC-SG hinzuzufügen. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

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 unter ***Wartungsmodus*** (auf Seite 162).

➢ *So bearbeiten Sie eine Richtlinie:*

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. (Optional) 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 neben der Dropdown-Liste **Gerätegruppe**, und wählen Sie die Gerätegruppe aus, für die diese Richtlinie den Zugriff steuern soll.
5. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Knotengruppe**, und wählen Sie die Knotengruppe aus, für die diese Richtlinie den Zugriff steuern soll.
6. Bezieht sich die Richtlinie nur auf eine Gruppenart, müssen Sie nur einen Wert für diese Art auswählen.
7. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Tage**, und wählen Sie aus, an welchen Wochentagen diese Richtlinie gelten soll: **Alle** (jeden Tag), **Wochentag** (nur Montag bis Freitag) und **Wochenende** (nur Samstag und Sonntag) oder **Benutzerdefiniert** (wählen Sie bestimmte Tage aus).
8. Wählen Sie **Benutzerdefiniert** aus, um die gewünschten Tage auszuwählen. Die Kontrollkästchen für die einzelnen Tage werden wählbar.

9. Markieren Sie die Kontrollkästchen für die Tage, an denen die Richtlinie gelten soll.
10. 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.
11. 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.
    - Führen Sie im Feld **Geräte-/Knotenzugriffsberechtigung** folgende Schritte durch:
    - Wählen Sie **Steuerung** aus, um diese Richtlinie so zu definieren, dass sie den Zugriff auf die ausgewählten 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 die ausgewählten Knoten- oder Gerätegruppen zu den angegebenen Uhrzeiten und Tagen verweigert.
12. Wenn Sie im Feld **Geräte-/Knotenzugriffsberechtigung** die Option **Steuerung** ausgewählt haben, wird der Bereich **Berechtigung für virtuelle Medien** wählbar. Wählen Sie im Feld **Berechtigung für virtuelle Medien** eine Option aus, um den Zugriff auf virtuelle Medien, die in den ausgewählten Knoten- oder Gerätegruppen verfügbar sind, zu den angegebenen Uhrzeiten und Tagen zuzulassen oder zu verweigern.
    - **Lese-/Schreibzugriff** ermöglicht sowohl Lese- als auch Schreibberechtigung auf virtuelle Medien.
    - **Lesezugriff** ermöglicht nur Leseberechtigungen auf virtuelle Medien.
    - **Ablehnen** verweigert den Zugriff auf virtuelle Medien.
13. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.
14. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Richtlinien löschen

➢ *So löschen Sie eine Richtlinie:*

1. Wählen Sie **Zuordnungen** > **Richtlinien**. Das Fenster **Richtlinienmanager** wird angezeigt.

2. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Richtlinienname**, und wählen Sie die Richtlinien, die Sie löschen möchten, in der Liste aus.
3. Klicken Sie auf **Löschen**.
4. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Unterstützung für virtuelle Medien

CC-SG bietet Remoteunterstützung von virtuellen Medien für Knoten, die an virtuelle Medien-fähige KX II-Geräte angeschlossen sind. Detaillierte Anleitungen für den Zugriff auf virtuelle Medien finden Sie im Benutzerhandbuch zu Dominion KX II. Weitere Informationen zum Erstellen von Richtlinien zum Zuordnen der Berechtigung für virtuelle Medien zu Benutzergruppen in CC-SG finden Sie unter ***Richtlinien hinzufügen*** (auf Seite 108).

Richtlinien Benutzergruppen zuordnen

Richtlinien müssen Benutzergruppen zugeordnet werden, bevor sie wirksam werden. Nachdem eine Richtlinie einer Benutzergruppe zugeordnet wurde, wird der Zugriff der Gruppenmitglieder durch diese Richtlinie bestimmt. Weitere Informationen zum Zuordnen von Richtlinien zu einer Benutzergruppe finden Sie unter ***Benutzer und Benutzergruppen konfigurieren*** (siehe "Benutzer und Benutzergruppen" auf Seite 91).

Kapitel 11 Benutzerdefinierte Ansichten für Geräte und Knoten

Mit benutzerdefinierten Ansichten können Sie die Anzeige der Knoten und Geräte im linken Fensterbereich mit Kategorien, Knotengruppen und Gerätegruppen unterschiedlich festlegen.

In diesem Kapitel

Typen von benutzerdefinierten Ansichten

Es gibt drei Typen von benutzerdefinierten Ansichten: Ansicht nach Kategorie, Filter nach Knotengruppe und Filter nach Gerätegruppe.

Ansicht nach Kategorie

Bei einer benutzerdefinierten Ansicht des Typs Ansicht nach Kategorie werden in der Liste der Knoten oder Geräte alle Knoten und Geräte angezeigt, die durch die von Ihnen festgelegten Kategorien definiert sind. Knoten oder Geräte, die keiner Kategorie zugeordnet sind, werden ebenfalls angezeigt und sind als „nicht zugewiesen“ gekennzeichnet.

Filter nach Knotengruppe

Bei einer benutzerdefinierten Ansicht des Typs **Filter nach Knotengruppe** werden in der Liste der Knoten nur die von Ihnen festgelegten Knotengruppen angezeigt. Die Gliederung erfolgt auf erster Ebene nach Knotengruppenname. Ein Knoten kann mehrere Male in der Liste angezeigt werden, wenn der Knoten zu mehreren in der benutzerdefinierten Ansicht definierten Knotengruppen gehört. Knoten, die zu keiner der in der benutzerdefinierten Ansicht definierten Knotengruppen gehören, werden in der Liste nicht angezeigt.

Filter nach Gerätegruppe

Bei einer benutzerdefinierten Ansicht des Typs Filter nach Gerätegruppe werden in der Liste der Geräte nur die von Ihnen festgelegten Gerätegruppen angezeigt. Die Gliederung erfolgt auf erster Ebene nach Gerätegruppenname. Ein Gerät kann mehrere Male in der Liste angezeigt werden, wenn das Gerät zu mehreren in der benutzerdefinierten Ansicht definierten Gerätegruppen gehört. Geräte, die zu keiner der in der benutzerdefinierten Ansicht definierten Gerätegruppen gehören, werden in der Liste nicht angezeigt.

Verwenden von benutzerdefinierten Ansichten im Administrations-Client

Benutzerdefinierte Ansichten für Knoten

Benutzerdefinierte Ansicht für Knoten hinzufügen

➢ *Benutzerdefinierte Ansicht für Knoten hinzufügen*

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Klicken Sie im Menü **Knoten** auf **Ansicht ändern** und anschließend 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 im Feld **Name der benutzerdefinierten Ansicht** einen Namen für die neue benutzerdefinierte Ansicht ein.
5. Führen Sie im Bereich **Typ der benutzerdefinierten Ansicht** folgende Schritte aus:
   - Aktivieren Sie die Option **Filter nach Knotengruppe**, um eine benutzerdefinierte Ansicht zu erstellen, in der nur die von Ihnen festgelegten Knotengruppen angezeigt werden.
   - Aktivieren Sie die Option **Ansicht nach Kategorie**, um eine benutzerdefinierte Ansicht zu erstellen, in der die Knoten nach den von Ihnen festgelegten Kategorien angezeigt werden.
6. Klicken Sie auf **OK**.

7. Führen Sie im Bereich **Details der benutzerdefinierten Ansicht** folgende Schritte aus:
   a. Wählen Sie in der Liste **Verfügbar** ein Element aus, das der benutzerdefinierten Ansicht hinzugefügt werden soll, und klicken Sie dann auf **Hinzufügen**, um das Element in die Liste **Ausgewählt** zu verschieben. Wiederholen Sie diesen Schritt für beliebig viele Elemente.
   b. Ordnen Sie die Elemente in der Liste **Ausgewählt** in der Reihenfolge an, in der die einzelnen Gruppen auf der Registerkarte **Knoten** angezeigt werden sollen. Wählen Sie ein Element aus, und klicken Sie auf die Pfeilschaltflächen, um die Elemente in die gewünschte Reihenfolge zu bringen.
   c. Wenn Sie ein Element aus der Liste löschen müssen, wählen Sie das Element aus, und klicken Sie auf **Entfernen**.
8. Klicken Sie auf **Speichern**, um die benutzerdefinierte Ansicht zu speichern. In einer Meldung wird bestätigt, dass die benutzerdefinierte Ansicht hinzugefügt wurde.
9. Wenn Sie die neue benutzerdefinierte Ansicht anwenden möchten, klicken Sie auf **Ansicht anwenden**.

Benutzerdefinierte Ansicht für Knoten anwenden

➢ *Benutzerdefinierte Ansicht auf die Knotenliste anwenden*

1. Klicken Sie im Menü **Knoten** auf **Ansicht ändern** und anschließend auf **Benutzerdefinierte Ansicht**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Name**, und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus.
3. Klicken Sie auf **Ansicht anwenden**, um die benutzerdefinierte Ansicht anzuwenden.

ODER

- Wählen Sie **Knoten > Ansicht ändern**. Alle benutzerdefinierten Ansichten sind als Optionen im Popup-Menü verfügbar. Wählen Sie die benutzerdefinierte Ansicht aus, die angewendet werden soll.

Benutzerdefinierte Ansicht für Knoten ändern

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

2. Klicken Sie im Menü **Knoten** auf **Ansicht ändern** und anschließend auf **Benutzerdefinierte Ansicht erstellen**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Name**, und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus. Im Fensterbereich **Details der benutzerdefinierten Ansicht** werden Details zu den enthaltenen Elementen und die Reihenfolge angezeigt.

➢ *So ändern Sie den Namen einer benutzerdefinierten Ansicht:*

1. Klicken Sie im Fensterbereich **Benutzerdefinierte Ansicht** auf **Bearbeiten**. Das Fenster **Benutzerdefinierte Ansicht bearbeiten** wird angezeigt.
2. Geben Sie im Feld **Neuen Namen für benutzerdefinierte Ansicht eingeben** einen neuen Namen für die benutzerdefinierte Ansicht ein, und klicken Sie auf **OK**. Der neue Name der Ansicht wird im Feld **Name** des Fensters **Benutzerdefinierte Ansicht** angezeigt.

➢ *So ändern Sie den Inhalt der benutzerdefinierten Ansicht:*

1. Führen Sie im Bereich **Details der benutzerdefinierten Ansicht** folgende Schritte aus:
   a. Wählen Sie in der Liste **Verfügbar** ein Element aus, das der benutzerdefinierten Ansicht hinzugefügt werden soll, und klicken Sie dann auf **Hinzufügen**, um das Element in die Liste **Ausgewählt** zu verschieben. Wiederholen Sie diesen Schritt für beliebig viele Elemente.
   b. Ordnen Sie die Elemente in der Liste **Ausgewählt** in der Reihenfolge an, in der die einzelnen Gruppen auf der Registerkarte **Knoten** angezeigt werden sollen. Wählen Sie ein Element aus, und klicken Sie auf die Pfeilschaltflächen, um die Elemente in die gewünschte Reihenfolge zu bringen.
   c. Wenn Sie ein Element aus der Liste löschen müssen, wählen Sie das Element aus, und klicken Sie auf **Entfernen**.
2. Klicken Sie auf **Speichern**, um die benutzerdefinierte Ansicht zu speichern. In einer Meldung wird bestätigt, dass die benutzerdefinierte Ansicht hinzugefügt wurde.
3. Wenn Sie die neue benutzerdefinierte Ansicht anwenden möchten, klicken Sie auf **Ansicht anwenden**.

Benutzerdefinierte Ansicht für Knoten löschen

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Klicken Sie im Menü **Knoten** auf **Ansicht ändern** und anschließend auf **Benutzerdefinierte Ansicht erstellen**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Name**, und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus. Im Fensterbereich **Details der benutzerdefinierten Ansicht** werden Details zu den enthaltenen Elementen und die Reihenfolge angezeigt.
4. Klicken Sie im Fensterbereich **Benutzerdefinierte Ansicht** auf **Löschen**. Die Bestätigungsmeldung **Benutzerdefinierte Ansicht löschen** wird angezeigt.
5. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Benutzerdefinierte Ansicht als Standard für Knoten festlegen

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Klicken Sie im Menü **Knoten** auf **Ansicht ändern** und anschließend auf **Benutzerdefinierte Ansicht erstellen**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Name**, und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus.
4. Klicken Sie im Fensterbereich **Benutzerdefinierte Ansicht** auf **Als Standard festlegen**. Bei der nächsten Anmeldung wird standardmäßig die ausgewählte benutzerdefinierte Ansicht verwendet.

Benutzerdefinierte Ansicht als Standard für Knoten und alle Benutzer festlegen

Wenn Sie über die Berechtigung **CC-Setup und -Steuerung** verfügen, können Sie eine benutzerdefinierte Ansicht als Standardansicht für alle Benutzer festlegen.

1. Klicken Sie auf die Registerkarte **Knoten**.
2. Wählen Sie **Knoten > Ansicht ändern > Benutzerdefinierte Ansicht erstellen**.
3. Klicken Sie auf den Pfeil der Dropdown-Liste **Name**, und wählen Sie in der Liste die benutzerdefinierte Ansicht aus, die Sie als systemweite Standardansicht festlegen möchten.

4. Aktivieren Sie das Kontrollkästchen **Systemweit**, und klicken Sie auf **Speichern**.

Für alle Benutzer, die sich in CC-SG anmelden, wird die Registerkarte **Knoten** anhand der ausgewählten benutzerdefinierten Ansicht sortiert. Die Benutzer können die benutzerdefinierte Ansicht jedoch ändern.

Benutzerdefinierte Ansichten für Geräte

Benutzerdefinierte Ansichten für Geräte hinzufügen

➢ *Benutzerdefinierte Ansichten für Geräte 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 in das Feld **Name der benutzerdefinierten Ansicht** einen Namen für die neue benutzerdefinierte Ansicht ein.
5. Führen Sie im Bereich Typ der benutzerdefinierten Ansicht folgende Schritte aus:
   - Markieren Sie die Option **Filter nach Gerätegruppe**, um eine benutzerdefinierte Ansicht zu erstellen, in der nur die von Ihnen festgelegten Gerätegruppen angezeigt werden.
   - Markieren Sie die Option **Ansicht nach Kategorie**, um eine benutzerdefinierte Ansicht zu erstellen, in der die Geräte nach den von Ihnen festgelegten Kategorien angezeigt werden.
6. Klicken Sie auf **OK**.
7. Führen Sie im Bereich **Details der benutzerdefinierten Ansicht** folgende Schritte aus:
   a. Wählen Sie in der Liste **Verfügbar** ein Element aus, das der benutzerdefinierten Ansicht hinzugefügt werden soll, und klicken Sie dann auf **Hinzufügen**, um das Element in die Liste **Ausgewählt** zu verschieben. Wiederholen Sie diesen Schritt für beliebig viele Elemente.

b. Ordnen Sie die Elemente in der Liste **Ausgewählt** in der Reihenfolge an, in der die einzelnen Gruppen auf der Registerkarte **Knoten** angezeigt werden sollen. Wählen Sie ein Element aus, und klicken Sie auf die Pfeilschaltflächen, um die Elemente in die gewünschte Reihenfolge zu bringen.

c. Wenn Sie ein Element aus der Liste löschen müssen, wählen Sie das Element aus, und klicken Sie auf **Entfernen**.

8. Klicken Sie auf **Speichern**, um die benutzerdefinierte Ansicht zu speichern. In einer Meldung wird bestätigt, dass die benutzerdefinierte Ansicht hinzugefügt wurde.
9. Wenn Sie die neue benutzerdefinierte Ansicht anwenden möchten, klicken Sie auf **Ansicht anwenden**.

Benutzerdefinierte Ansichten für Geräte anwenden

➢ *Benutzerdefinierte Ansichten auf die Geräteliste anwenden*

1. Klicken Sie im Menü Geräte auf **Ansicht ändern**, und klicken Sie dann auf **Benutzerdefinierte Ansicht**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Name**, und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus.
3. Klicken Sie auf **Als aktuell festlegen**, um die benutzerdefinierte Ansicht anzuwenden.

ODER

Wählen Sie Geräte > Ansicht ändern. Alle benutzerdefinierten Ansichten sind als Optionen im Popup-Menü verfügbar. Wählen Sie die benutzerdefinierte Ansicht aus, die angewendet werden soll.

Benutzerdefinierte Ansichten für Geräte ändern

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 auf den Pfeil neben der Dropdown-Liste **Name**, und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus. Im Fensterbereich **Details der benutzerdefinierten Ansicht** werden Details zu den enthaltenen Elementen und die Reihenfolge angezeigt.

➢ *So ändern Sie den Namen einer benutzerdefinierten Ansicht:*

1. Klicken Sie im Fensterbereich **Benutzerdefinierte Ansicht** auf **Bearbeiten**. Das Fenster **Benutzerdefinierte Ansicht bearbeiten** wird angezeigt.
2. Geben Sie in das Feld **Neuen Namen für benutzerdefinierte Ansicht eingeben** einen neuen Namen für die benutzerdefinierte Ansicht ein, und klicken Sie auf **OK**. Der neue Name der Ansicht wird im Feld **Name** des Fensters **Benutzerdefinierte Ansicht** angezeigt.

➢ *So ändern Sie den Inhalt der benutzerdefinierten Ansicht:*

1. Führen Sie im Bereich **Details der benutzerdefinierten Ansicht** folgende Schritte aus:
   a. Wählen Sie in der Liste **Verfügbar** ein Element aus, das der benutzerdefinierten Ansicht hinzugefügt werden soll, und klicken Sie dann auf **Hinzufügen**, um das Element in die Liste **Ausgewählt** zu verschieben. Wiederholen Sie diesen Schritt für beliebig viele Elemente.
   b. Ordnen Sie die Elemente in der Liste **Ausgewählt** in der Reihenfolge an, in der die einzelnen Gruppen auf der Registerkarte **Knoten** angezeigt werden sollen. Wählen Sie ein Element aus, und klicken Sie auf die Pfeilschaltflächen, um die Elemente in die gewünschte Reihenfolge zu bringen.
   c. Wenn Sie ein Element aus der Liste löschen müssen, wählen Sie das Element aus, und klicken Sie auf **Entfernen**.
2. Klicken Sie auf **Speichern**, um die benutzerdefinierte Ansicht zu speichern. In einer Meldung wird bestätigt, dass die benutzerdefinierte Ansicht hinzugefügt wurde.
3. Wenn Sie die neue benutzerdefinierte Ansicht anwenden möchten, klicken Sie auf **Ansicht anwenden**.

Benutzerdefinierte Ansichten für Geräte löschen

1. Klicken Sie auf die Registerkarte Geräte.
2. Wählen Sie Geräte > **Ansicht ändern** > **Benutzerdefinierte Ansicht erstellen**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Name**, und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus. Im Fensterbereich **Details der benutzerdefinierten Ansicht** werden Details zu den enthaltenen Elementen und die Reihenfolge angezeigt.
4. Klicken Sie im Fensterbereich **Benutzerdefinierte Ansicht** auf **Löschen**. Die Bestätigungsmeldung **Benutzerdefinierte Ansicht löschen** wird angezeigt.
5. Klicken Sie in der Bestätigungsmeldung auf **Ja**.

Benutzerdefinierte Ansicht für Geräte als Standard zuordnen

1. Klicken Sie auf die Registerkarte Geräte.
2. Wählen Sie Geräte > **Ansicht ändern** > **Benutzerdefinierte Ansicht erstellen**. Das Fenster **Benutzerdefinierte Ansicht** wird angezeigt.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Name**, und wählen Sie eine benutzerdefinierte Ansicht in der Liste aus.
4. Klicken Sie im Fensterbereich **Benutzerdefinierte Ansicht** auf **Als Standard festlegen**. Bei der nächsten Anmeldung wird standardmäßig die ausgewählte benutzerdefinierte Ansicht verwendet.

Benutzerdefinierte Ansicht von Geräten als Standard für alle Benutzer zuordnen

Wenn Sie über die Berechtigung Geräte-, Port- und Knotenverwaltung verfügen, können Sie eine benutzerdefinierte Ansicht als Standardansicht für alle Benutzer zuordnen.

1. Klicken Sie auf die Registerkarte Geräte.
2. Wählen Sie Geräte >Ansicht ändern > Benutzerdefinierte Ansicht erstellen.
3. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Name**, und wählen Sie in der Liste die benutzerdefinierte Ansicht aus, die Sie als systemweite Standardansicht festlegen möchten.

4. Markieren Sie das Kontrollkästchen **Systemweit**, und klicken Sie auf **Speichern**.

Für alle Benutzer, die sich in CC-SG anmelden, wird die Registerkarte Geräte anhand der ausgewählten benutzerdefinierten Ansicht sortiert. Die Benutzer können die benutzerdefinierte Ansicht jedoch ändern.

Kapitel 12 Remoteauthentifizierung

In diesem Kapitel

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

Jede Anzahl an Remoteservern kann für die externe Authentifizierung verwendet werden. Sie können beispielsweise drei Active Directory-Server, zwei iPlanet- (LDAP) Server und drei RADIUS-Server konfigurieren.

Nur Active Directory kann für die Remoteautorisierung von Benutzern verwendet werden.

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 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 zugeordnete 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 Remoteauthentifizierung verwendet wird, finden Sie unter ***Benutzer und Benutzergruppen konfigurieren*** (siehe "Benutzer und Benutzergruppen" auf Seite 91).

***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 Format eines definierten Namens wird in **RFC2253** (http://www.rfc-editor.org/rfc/rfc2253.txt) beschrieben.

Zur Konfiguration von CC-SG müssen Sie wissen, wie definierte Namen eingegeben werden sowie die Reihenfolge, in der jede Komponente des Namens aufgelistet werden soll.

Definierte Namen für Active Directory festlegen

Definierte Namen für Active Directory sollten dieser Struktur folgen. Sie müssen nicht beides, **Allgemeiner Name** und **Organisationseinheit**, festlegen.

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

Definierte Namen für LDAP festlegen

Definierte Namen für Netscape LDAP und eDirectory LDAP sollten dieser Struktur folgen:

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

Benutzernamen für Active Directory festlegen

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-Benutzer einer importierten AD-Gruppe zugewiesen ist. Beachten Sie, dass Sie mehrere allgemeine Namen, Organisationseinheiten und Domänenkomponenten festlegen können.

Basis-DNs festlegen

Sie können auch einen definierten Namen eingeben, um festzulegen, wo die Suche für Benutzer beginnt. Geben Sie einen definierten Namen in das 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**.

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.

➢ *So legen Sie Module für die Authentifizierung und Autorisierung fest:*

1. Wählen Sie Administration > Sicherheit.
2. Wählen Sie die Registerkarte Authentifizierung. Alle konfigurierten externen Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Führen Sie für jeden aufgelisteten Server folgende Schritte durch:
   a. Markieren Sie das Kontrollkästchen **Authentifizierung**, wenn CC-SG die Benutzer mit dem Server authentifizieren soll.
   b. Markieren Sie das Kontrollkästchen **Autorisierung**, wenn CC-SG die Benutzer mit dem Server autorisieren soll. Nur AD-Server können zur Autorisierung verwendet werden.
4. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Reihenfolge für externe AA-Server festlegen

CC-SG fragt die konfigurierten externen Autorisierungs- und Authentifizierungsserver in der festgelegten Reihenfolge ab. Wenn die erste aktivierte Option nicht verfügbar ist, probiert CC-SG die zweite Option aus, dann die dritte usw., bis der Vorgang erfolgreich ist.

➢ *So legen Sie die Reihenfolge fest, in der CC-SG externe Authentifizierungs- und Autorisierungsserver verwendet:*

1. Wählen Sie Administration > Sicherheit.
2. Wählen Sie die Registerkarte Authentifizierung. Alle konfigurierten externen Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Wählen Sie in der Liste einen Server aus, und klicken Sie auf die Pfeile nach oben und nach unten, um die Reihenfolge der Verwendung festzulegen.
4. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Active Directory und CC-SG

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.

AD-Module zu CC-SG hinzufügen

Wichtig: Erstellen Sie entsprechende AD-Benutzergruppen, und ordnen 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 unter *CC-SG-Netzwerk konfigurieren* **(auf Seite 178).**

➢ *So fügen Sie ein AD-Modul zu CC-SG hinzu:*

1. Wählen Sie Administration > Sicherheit.
2. Wählen Sie die Registerkarte Authentifizierung.
3. Klicken Sie auf **Hinzufügen**, um das Fenster Modul hinzufügen zu öffnen.
4. Klicken Sie auf das Dropdown-Menü **Modultyp**, und wählen Sie **AD** in der Liste aus.
5. Geben Sie den Namen des AD-Servers in das Feld **Modulname** ein.
   - Die Höchstanzahl an Zeichen ist 31.
   - Alle druckbaren Zeichen können verwendet werden.
   - 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.
6. Klicken Sie zum Fortfahren 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.

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 **CC-SG-Standard-DNS verwenden** markieren, um den DNS zu verwenden, der im Abschnitt des Konfigurationsmanagers in CC-SG konfiguriert ist. Weitere Informationen finden Sie unter ***Erweiterte Administration*** (auf Seite 173).

3. Markieren Sie **Anonyme Bindung**, 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 Bindung verwenden, geben Sie den Benutzernamen des Benutzerkontos, den Sie für die Abfrage des AD-Servers verwenden möchten, in das Feld **Benutzername** ein. Das erforderliche Format ist von der AD-Version und -Konfiguration abhängig. Verwenden Sie eines der folgenden Formate.

   Ein Benutzer namens Benutzername und mit dem Anmeldenamen Benutzern in der Domäne raritan.com könnte folgendermaßen eingegeben werden:

   - cn=Benutzername,cn=users,dc=Raritan,dc=com
   - **Benutzername@raritan.com**
   - Raritan/Benutzername

   Hinweis: 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 **Gruppenumfang** auf **Global** und **Gruppentyp** auf **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 zum Fortfahren auf **Weiter**. Die Registerkarte **Erweitert** wird angezeigt.

Erweiterte AD-Einstellungen

➢ *So konfigurieren Sie die erweiterten AD-Einstellungen:*

1. Klicken Sie auf die Registerkarte Erweitert.
2. Geben Sie die Portnummer ein, die der AD-Server überwacht. Der Standardport lautet **389**. Wenn Sie sichere Verbindungen für LDAP verwenden, müssen Sie diesen Port ggf. ändern. Der Standardport für sichere LDAP-Verbindungen lautet **636**.
3. Markieren 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.

1. Geben Sie die Attribute eines Benutzers in das 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.
2. Geben Sie die Art und Weise für die Durchführung der Abfrage für den Benutzereintrag an.
   - Markieren Sie die Option **Bindung verwenden**, wenn der Benutzer, der sich über das Applet anmeldet, über die Berechtigungen verfügt, Abfragen an den AD-Server zu senden. Ist das Muster des Benutzernamens jedoch unter **Bindungsmuster für Benutzernamen** 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: Wird **cn={0},cn=Users,dc=raritan,dc=com** und **TestUser** im Applet festgelegt, verwendet CC-SG **cn=TestUser,cn-Users,dc=raritan,dc=com** für die Verbindung zum AD-Server.

- Markieren Sie **Bindung nach Suche verwenden**, um mit dem Benutzernamen und 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 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.

3. Klicken Sie zum Fortfahren 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**.
2. Legen Sie einen **Basis-DN** (Verzeichnisebene/Eintrag) fest, unter dem die Gruppen, die den zu autorisierenden 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.

1. Geben Sie die Attribute eines Benutzers in das 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.

2. Klicken Sie zum Fortfahren auf **Weiter**. Die Registerkarte **Vertrauensstellungen** wird angezeigt.

AD-Vertrauenseinstellungen

Auf der Registerkarte Vertrauensstellungen 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. Die von Ihnen in CC-SG konfigurierten Vertrauensstellungen sollten mit den in Active Directory konfigurierten Vertrauensstellungen übereinstimmen.

1. Klicken Sie auf die Registerkarte **Vertrauensstellungen**. Wenn Sie mehrere AD-Domänen konfiguriert haben, werden alle anderen Domänen auf der Registerkarte **Vertrauensstellungen** aufgeführt.
2. Klicken Sie für jede Domäne in der Spalte **Vertrauenspartner** auf das Dropdown-Menü **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.
   - **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.
   - **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.
   - **Bidirektional**: Informationen aus beiden Richtungen jeder Domäne sind vertrauenswürdig.
   - **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.

   Das neue AD-Modul wird im Fenster Sicherheitsmanager unter Externe AA-Server angezeigt.

4. Markieren Sie das Kontrollkästchen **Authentifizierung**, wenn CC-SG die Benutzer mit dem AD-Modul authentifizieren soll. Markieren Sie das Kontrollkästchen **Autorisierung**, wenn CC-SG die Benutzer mit dem AD-Modul autorisieren soll.

5. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

AD-Module bearbeiten

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

➢ *So bearbeiten Sie ein AD-Modul:*

1. Wählen Sie Administration > Sicherheit.
2. Wählen Sie die Registerkarte Authentifizierung. Alle konfigurierten externen Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Wählen Sie das AD-Modul aus, das Sie bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
4. 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*** (auf Seite 128), ***Erweiterte AD-Einstellungen*** (auf Seite 130), ***AD-Gruppeneinstellungen*** (auf Seite 131) und ***AD-Vertrauenseinstellungen*** (auf Seite 132).
5. 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.
6. Klicken Sie zum Speichern der Änderungen auf **OK**.

7. 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*** (siehe "Alle Benutzergruppen mit Active Directory synchronisieren" auf Seite 137) und ***Alle AD-Module synchronisieren*** (auf Seite 138).

AD-Benutzergruppen importieren

Sie müssen Gruppeneinstellungen im AD-Modul angeben, bevor Sie Gruppen vom AD-Server importieren können. Weitere Informationen finden Sie unter ***AD-Gruppeneinstellungen*** (auf Seite 131).

Nach dem Ändern von importierten Gruppen oder Benutzern müssen Sie die geänderten AD-Benutzergruppen synchronisieren, damit die importierten Gruppen den entsprechenden Gruppen in Active Directory zugeordnet werden. Außerdem müssen Sie alle AD-Module synchronisieren, um alle Gruppen und Benutzer in allen Modulen zu synchronisieren. Weitere Informationen finden Sie unter ***AD-Benutzergruppen synchronisieren*** (siehe "Alle Benutzergruppen mit Active Directory synchronisieren" auf Seite 137) und ***Alle AD-Module synchronisieren*** (auf Seite 138).

Sie können verschachtelte Gruppen aus Active Directory importieren.

Hinweis: *Vergewissern Sie sich, dass Sie das CC-SG DNS und Domänensuffix im Konfigurationsmanager konfiguriert haben, bevor Sie AD-Benutzergruppen importieren.* **Erweiterte Administration** *(auf Seite 173)*

➢ *So importieren Sie eine AD-Benutzergruppe:*

1. Wählen Sie Administration > Sicherheit.
2. Wählen Sie die Registerkarte Authentifizierung. Alle konfigurierten Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Wählen Sie den AD-Server aus, dessen AD-Benutzergruppe Sie importieren möchten.
4. Klicken Sie auf **AD-Benutzergruppen 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 zuordnen.

5. Wählen Sie die Gruppen aus, die Sie nach CC-SG importieren möchten.
   - Die Namen von importierten Benutzergruppen dürfen bis zu 64 Zeichen enthalten.
   - Geben Sie zur Suche nach Benutzergruppen einen Suchbegriff in das Feld **Benutzergruppe suchen** ein, und klicken Sie auf **Los**.
   - Klicken Sie auf eine Spaltenüberschrift, um die Liste der Benutzergruppen nach den Daten in der Spalte zu sortieren.
   - Klicken Sie auf **Alles auswählen**, um alle Benutzergruppen zum Importieren auszuwählen.
   - Klicken Sie auf **Gesamte Auswahl aufheben**, um die Auswahl aller Benutzergruppen aufzuheben.
6. Wählen Sie in der Spalte **Richtlinien** eine CC-SG-Zugriffsrichtlinie in der Liste aus, um die Richtlinie der ausgewählten Gruppe zuzuordnen.
7. Klicken Sie auf **Importieren**, um die ausgewählten Benutzergruppen zu importieren.

---

*Tipp: 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-Zuordnungen**, um die Daten für das AD-Modul anzuzeigen, das mit der Benutzergruppe verknüpft ist.*

Active Directory mit CC-SG synchronisieren

Die in CC-SG gespeicherten Daten können mit mehreren Methoden mit Ihrem AD-Server synchronisiert werden.

- Tägliche Synchronisierung aller Module: Sie können die geplante Synchronisierung aktivieren, damit CC-SG alle AD-Module täglich zu der ausgewählten Uhrzeit synchronisieren kann. Weitere Informationen finden Sie unter ***Alle AD-Module synchronisieren*** (auf Seite 138). Diese Synchronisierung ist nur erforderlich, wenn Sie Active Directory für die Autorisierung verwenden.
- Manuelle Synchronisierung: Bei dieser Methode können Sie zwei Typen von Synchronisierungen durchführen.
    1. ***Alle Active Directory-Module*** (siehe "Alle AD-Module synchronisieren" auf Seite 138): Bei dieser Option wird der gleiche Vorgang wie bei der täglichen Synchronisierung aller Module durchgeführt. Sie können diese Synchronisierung jedoch jederzeit manuell durchführen. Diese Synchronisierung ist nur erforderlich, wenn Sie Active Directory für die Autorisierung verwenden.
    2. ***Alle Benutzergruppen*** (siehe "Alle Benutzergruppen mit Active Directory synchronisieren" auf Seite 137): Verwenden Sie diese Option, wenn Sie eine Benutzergruppe geändert haben. Die Synchronisierung aller Benutzergruppen ermöglicht Ihnen, importierte und lokale Benutzergruppen den Benutzergruppen zuzuordnen, die als Teil eines AD-Moduls identifiziert wurden. Bei der Synchronisierung von Benutzergruppen werden die Zugriffsinformationen in CC-SG nicht aktualisiert. Zur Aktualisierung der Zugriffsinformationen müssen Sie alle AD-Module synchronisieren. Warten Sie hierzu entweder auf die Ausführung der täglichen Synchronisierung oder führen Sie die Synchronisierung aller Module manuell aus.

Alle Benutzergruppen mit Active Directory synchronisieren

Sie sollten alle Benutzergruppen synchronisieren, wenn Sie eine Benutzergruppe geändert haben. Wenn Sie beispielsweise wissen, dass eine Benutzergruppe von einem AD-Modul in ein anderes verschoben wurde. (Sie können auch die AD-Zuordnung einer Benutzergruppe manuell ändern. Dies führen Sie auf der Registerkarte Active Directory-Zuordnungen im Benutzergruppenprofil durch.)

Wenn Sie die Benutzer oder Domänencontroller geändert haben, sollten Sie ***alle AD-Module synchronisieren*** (auf Seite 138).

Beim Synchronisieren von AD-Benutzergruppen ruft CC-SG die Gruppen für das ausgewählte AD-Modul ab, vergleicht die Namen mit den Benutzergruppen, die von Active Directory bereits importiert wurden, und ermittelt die Übereinstimmungen. Die Ergebnisse werden in CC-SG angezeigt, und Sie können auswählen, welche Gruppen in Active Directory Sie CC-SG zuweisen möchten. Hierbei werden die Benutzerzugriffsinformationen in CC-SG nicht aktualisiert. Bei der Synchronisierung von AD-Benutzergruppen werden nur die Gruppennamen aus Active Directory zu CC-SG zugeordnet.

➢ *So synchronisieren Sie alle Benutzergruppen mit Active Directory:*

1. ***Starten Sie den Wartungsmodus.*** (siehe "Wartungsmodus starten" auf Seite 163)
2. Wählen Sie Administration > Sicherheit.
3. Wählen Sie die Registerkarte Authentifizierung. Alle konfigurierten Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
4. Wählen Sie den AD-Server aus, dessen Benutzergruppen Sie mit den Benutzergruppen in CC-SG synchronisieren möchten.
5. Wählen Sie in der Liste Manuelle Synchronisierung die Option Alle Benutzergruppen aus, und klicken Sie dann auf die Pfeilschaltfläche.
6. Eine Liste aller im AD-Modul gefundenen Benutzergruppen, deren Namen mit Benutzergruppen in CC-SG übereinstimmen, wird angezeigt. Wählen Sie die Benutzergruppen aus, die Sie synchronisieren möchten, und klicken Sie dann auf OK.
7. Eine Bestätigung wird angezeigt, sobald alle importieren Benutzergruppen des ausgewählten Moduls erfolgreich synchronisiert wurden.

8. ***Beenden Sie den Wartungsmodus.*** (siehe "Wartungsmodus beenden" auf Seite 163)

Alle AD-Module synchronisieren

Sie sollten alle AD-Module immer dann synchronisieren, wenn Sie einen Benutzer in Active Directory ändern oder löschen, Benutzerberechtigungen in AD ändern oder einen Domänencontroller ändern.

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 oder dem AD-Modul in CC-SG zugewiesen wurden, und aktualisiert den lokalen CC-SG-Cache. Der lokale CC-SG-Cache enthält alle Domänencontroller für jede Domäne, alle Benutzergruppen, die Modulen in CC-SG zugewiesen sind, sowie die Benutzerdaten für alle bekannten AD-Benutzer. Wurden Benutzergruppen aus den AD-Modulen gelöscht, entfernt CC-SG alle Zuordnungen zu der gelöschten Gruppe aus dem lokalen Cache. Dadurch wird sichergestellt, dass CC-SG über die aktuellen AD-Benutzergruppendaten verfügt.

➢ *So synchronisieren Sie alle AD-Module:*

1. ***Starten Sie den Wartungsmodus.*** (siehe "Wartungsmodus starten" auf Seite 163)
2. Wählen Sie **Administration** > **Sicherheit**.
3. Wählen Sie die Registerkarte Authentifizierung. Alle konfigurierten Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
4. Wählen Sie in der Liste Manuelle Synchronisierung die Option Alle Active Directory-Module aus, und klicken Sie dann auf die Pfeilschaltfläche. Nachdem alle AD-Module erfolgreich synchronisiert wurden, wird eine Bestätigungsmeldung angezeigt.
5. ***Beenden Sie den Wartungsmodus.*** (siehe "Wartungsmodus beenden" auf Seite 163)

Tägliche Synchronisierung aller AD-Module aktivieren oder deaktivieren

➢ *So aktivieren Sie die tägliche Synchronisierung aller AD-Module:*

1. Wählen Sie **Administration** > **Sicherheit**.

2. Wählen Sie die Registerkarte Authentifizierung. Alle konfigurierten Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Markieren Sie das Kontrollkästchen Tägliche Synchronisierung aller Module.
4. Klicken Sie im Feld **Synchronisierungszeitpunkt** auf die Pfeile nach oben oder unten, um die Uhrzeit auszuwählen, zu der CC-SG die tägliche Synchronisierung der AD-Module ausführen soll.
5. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

➢ *So deaktivieren Sie die tägliche Synchronisierung aller AD-Module:*

1. Wählen Sie **Administration** > **Sicherheit**.
2. Wählen Sie die Registerkarte Authentifizierung. Alle konfigurierten Autorisierungs- und Authentifizierungsserver werden in einer Tabelle angezeigt.
3. Heben Sie die Markierung des Kontrollkästchens Tägliche Synchronisierung aller Module auf.
4. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Täglichen AD-Synchronisierungszeitpunkt ändern

Wenn die tägliche Synchronisierung aktiviert ist, können Sie den Zeitpunkt festlegen, zu dem die automatische Synchronisierung durchgeführt wird. Die tägliche Synchronisierung wird standardmäßig um 23:30 Uhr durchgeführt.

➢ *So ändern Sie den täglichen AD-Synchronisierungszeitpunkt:*

1. Wählen Sie **Administration** > **Sicherheit**.
2. Wählen Sie die Registerkarte Authentifizierung. Stellen Sie sicher, dass das Kontrollkästchen Tägliche Synchronisierung aller Module markiert ist.
3. Klicken Sie im Fenster unten im Feld **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.
4. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

LDAP und CC-SG

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.

LDAP-Module (Netscape) zu CC-SG hinzufügen

➢ *So fügen Sie ein LDAP-Modul (Netscape) zu CC-SG hinzu:*

1. Wählen Sie **Administration** > **Sicherheit**.
2. Klicken Sie auf die Registerkarte Authentifizierung.
3. Klicken Sie auf **Hinzufügen...**, um das Fenster Modul hinzufügen zu öffnen.
4. Klicken Sie auf das Dropdown-Menü **Modultyp**, und wählen Sie LDAP in der Liste aus.
5. Geben Sie den Namen des LDAP-Servers in das Feld **Modulname** ein.
6. Klicken Sie zum Fortfahren auf **Weiter**. Die Registerkarte **Allgemein** wird angezeigt.

Allgemeine LDAP-Einstellungen

1. Klicken Sie auf die Registerkarte **Allgemein**.
2. Geben Sie die IP-Adresse oder den Hostnamen des LDAP-Servers in das Feld **IP-Adresse/Hostname** ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
3. Geben Sie den Portwert in das 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 Bindung**, 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) in das 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 in das 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**.
2. Wählen Sie **Base 64**, wenn Sie das Kennwort mit Verschlüsselung zum LDAP-Server senden möchten. Wählen Sie **Unformatierter Text**, wenn Sie das Kennwort als unformatierten Text zum LDAP-Server senden möchten.

3. **Standarddigest**: Wählen Sie die Standardverschlüsselung für Benutzerkennwörter aus.
4. Geben Sie die Parameter für die Benutzer- und Gruppenmitgliedschaftsattribute in die Felder **Benutzerattribut** und **Gruppenmitgliedschaftsattribut** ein. Diese Werte sollten Sie aus Ihrem LDAP-Verzeichnisschema abrufen.
5. Geben Sie das Bindungsmuster in das Feld **Bindungsmuster für Benutzernamen** ein.
   - Markieren 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 markiert, sucht CC-SG auf dem LDAP-Server nach dem Benutzernamen. Wird der Name gefunden, ruft CC-SG das LDAP-Objekt ab und vergleicht das zugewiesene Kennwort lokal mit dem eingegebenen Kennwort.
   - Auf einigen LDAP-Servern kann das Kennwort nicht als Teil des LDAP-Objekts abgerufen werden. Markieren Sie **Bindung nach Suche verwenden**, damit CC-SG das Kennwort wieder an das LDAP-Objekt bindet und es zur Authentifizierung an den Server zurücksendet.
6. Klicken Sie zum Speichern der Änderungen auf **OK**. Das neue LDAP-Modul wird im Fenster Sicherheitsmanager unter Externe AA-Server angezeigt.
7. Markieren Sie das Kontrollkästchen **Authentifizierung**, wenn CC-SG die Benutzer mit dem LDAP-Modul authentifizieren soll.
8. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

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 DNS-Servers>**
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 DNS-Servers>
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

TACACS+ und CC-SG

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 finden Sie unter ***Benutzer und Benutzergruppen*** (auf Seite 91).

TACACS+-Module hinzufügen

1. Wählen Sie **Administration** > **Sicherheit**.
2. Klicken Sie auf die Registerkarte Authentifizierung.
3. Klicken Sie auf **Hinzufügen**, um das Fenster Modul hinzufügen zu öffnen.
4. Wählen Sie **Modultyp** > TACACS+.
5. Geben Sie den Namen des TACACS+-Servers in das Feld **Modulname** ein.
6. Klicken Sie auf **Weiter**. Die Registerkarte **Allgemein** wird angezeigt.

Allgemeine TACACS+-Einstellungen

1. Geben Sie die IP-Adresse oder den Hostnamen des TACACS+-Servers in das Feld **IP-Adresse/Hostname** ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
2. Geben Sie die Portnummer in das Feld **Portnummer** ein, die der TACACS+-Server überwacht. Die Standardportnummer ist **49**.
3. Geben Sie den Authentifizierungsport in das 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**. Das neue TACACS+-Modul wird im Fenster Sicherheitsmanager unter Externe AA-Server angezeigt.

6. Markieren Sie das Kontrollkästchen **Authentifizierung**, wenn CC-SG die Benutzer mit dem TACACS+-Modul authentifizieren soll.
7. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

RADIUS und CC-SG

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 Remoteauthentifizierung verwendet wird, finden Sie unter ***Benutzer und Benutzergruppen*** (auf Seite 91).

RADIUS-Module hinzufügen

1. Wählen Sie **Administration** > **Sicherheit**.
2. Klicken Sie auf die Registerkarte Authentifizierung.
3. Klicken Sie auf **Hinzufügen**, um das Fenster Modul hinzufügen zu öffnen.
4. Klicken Sie auf das Dropdown-Menü **Modultyp**, und wählen Sie RADIUS in der Liste aus.
5. Geben Sie den Namen des RADIUS-Servers in das Feld **Modulname** ein.
6. Klicken Sie zum Fortfahren auf **Weiter**. Die Registerkarte **Allgemein** wird angezeigt.

Allgemeine RADIUS-Einstellungen

1. Klicken Sie auf die Registerkarte **Allgemein**.
2. Geben Sie die IP-Adresse oder den Hostnamen des RADIUS-Servers in das Feld **IP-Adresse/Hostname** ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
3. Geben Sie die Portnummer in das Feld **Portnummer** ein. Der Standardport lautet 1812.
4. Geben Sie den Authentifizierungsport in das 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**.
7. Das neue RADIUS-Modul wird im Fenster Sicherheitsmanager unter Externe AA-Server angezeigt. Markieren Sie das Kontrollkästchen **Authentifizierung**, wenn CC-SG die Benutzer mit dem RADIUS-Modul authentifizieren soll.
8. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

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.

CC-SG wird wie bei der standardmäßigen RADIUS-Remoteauthentifizierung (wie oben beschrieben) konfiguriert. Weitere Informationen finden Sie unter ***Zwei-Faktor-Authentifizierung*** (siehe "Zwei-Faktoren-Authentifizierung" auf Seite 292).

Kapitel 13 Berichte

In diesem Kapitel

Berichte verwenden

Berichtsdaten sortieren

- 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.

Spaltenbreite in Berichten vergrößern/verkleinern

Die ausgewählten Spaltenbreiten werden bei der nächsten Anmeldung und Ausführung von Berichten als Standardberichtsansicht verwendet.

1. Positionieren Sie Ihren Mauszeiger auf der Spaltentrennung in der obersten Zeile, bis der Mauszeiger als Pfeil mit zwei Spitzen angezeigt wird.

2. Klicken Sie und ziehen Sie den Pfeil nach links oder rechts, um die Spaltenbreite anzupassen.

Berichtsdetails anzeigen

- Doppelklicken Sie auf eine Zeile, um die Berichtsdetails anzuzeigen.
- Ist die Zeile hervorgehoben, drücken Sie die Eingabetaste, um Details anzuzeigen.

In mehrseitigen Berichten navigieren

- Klicken Sie auf die Pfeile unten im Bericht, um in mehrseitigen Berichten zu navigieren.

Berichtsanzeigen drucken

Sie können den Bericht so drucken, wie er auf Ihrem Bildschirm angezeigt wird. Wenn Sie alle Berichtsdetails drucken möchten, ***speichern Sie zuerst den Bericht in einer Datei*** (siehe "Berichte in Dateien speichern" auf Seite 148), und drucken Sie dann die Datei.

1. Erstellen Sie den Bericht, den Sie drucken möchten.
2. Wählen Sie Secure Gateway > Drucken.

Berichte in Dateien speichern

Sie können einen Bericht in einer CSV-Datei speichern, die in Excel geöffnet werden kann. Beim Speichern eines Berichts in einer Datei werden alle Berichtsdetails gespeichert; nicht nur die Details, die Sie im Berichtsfenster anzeigen können.

1. Erstellen Sie den Bericht, den Sie in einer Datei speichern möchten.
2. Klicken Sie auf In Datei speichern. (Oder klicken Sie auf Berichtsdaten verwalten, und klicken Sie dann auf Speichern.)
3. Geben Sie einen Namen für die Datei ein, und wählen Sie den Speicherort aus.
4. Klicken Sie auf Speichern.

Berichtsdaten aus CC-SG leeren

Sie können die Datensätze, die im Überwachungslistenbericht und Fehlerprotokollbericht enthalten sind, leeren. Durch das Leeren dieser Berichte werden alle Daten, die gegenwärtig im Überwachungslistenprotokoll oder Fehlerprotokoll enthalten sind, dauerhaft gelöscht.

1. Erstellen Sie den Bericht, dessen Daten Sie aus CC-SG löschen möchten.
2. Klicken Sie auf Leeren.
3. Klicken Sie zum Bestätigen auf Ja.

Berichtsfilter einblenden oder ausblenden

In einigen Berichten sind oben im Berichtsfenster Filterkriterien enthalten. Sie können den Filterbereich ausblenden, wodurch der Berichtsbereich erweitert wird.

➢ *So blenden Sie die Berichtfilter ein oder aus:*

- Klicken Sie oben im Fenster auf die Filtersymbolleiste, um den Filterbereich auszublenden.
- Klicken Sie erneut auf die Filtersymbolleiste, um den Filterbereich einzublenden.

Überwachungslistenbericht

Der **Überwachungslistenbericht** enthält Überwachungsprotokolle und Informationen über den Zugriff auf CC-SG. Sie finden darin Informationen zum 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

➢ *So erstellen Sie den Überwachungslistenbericht:*

1. Wählen Sie Berichte > 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, die der Bericht enthalten wird, beschränken, indem Sie zusätzliche Parameter in die Felder **Meldung**, **Benutzername** und **Benutzer-IP-Adresse** eingeben. In diese Felder können Platzhalter eingegeben werden.
   - Wenn Sie den Bericht auf Meldungstexte beschränken möchten, die einer Aktivität zugewiesen sind, geben Sie den Text in das Feld **Meldung** ein.
   - Wenn Sie den Bericht auf bestimmte Benutzeraktivitäten beschränken möchten, geben Sie den Benutzernamen in das Feld **Benutzername** ein.
   - Wenn Sie den Bericht auf bestimmte IP-Adressen-Aktivitäten beschränken möchten, geben Sie die IP-Adresse des Benutzers in das Feld **Benutzer-IP-Adresse** ein.
4. Klicken Sie zum Erstellen des Berichts auf Übernehmen.
   - Klicken Sie auf **Leeren** (siehe "Berichtsdaten aus CC-SG leeren" auf Seite 149), um die Überwachungsliste zu löschen.

Fehlerprotokollbericht

CC-SG speichert Fehlermeldungen in verschiedenen Fehlerprotokolldateien, die aufgerufen und zum Beheben von Problemen verwendet werden können. Das Fehlerprotokoll enthält einen Teil der Überwachungslisteneinträge, die einer Fehlerbedingung zugewiesen sind.

➢ *So erstellen Sie den Fehlerprotokollbericht:*

1. Wählen Sie Berichte > 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, die der Bericht enthalten wird, beschränken, indem Sie zusätzliche Parameter in die Felder **Meldung**, **Benutzername** und **Benutzer-IP-Adresse** eingeben. In diese Felder können Platzhalter eingegeben werden.
   - Wenn Sie den Bericht auf Meldungstexte beschränken möchten, die mit einer Aktivität verknüpft sind, geben Sie den Text in das Feld **Meldung** ein.
   - Wenn Sie den Bericht auf bestimmte Benutzeraktivitäten beschränken möchten, geben Sie den Benutzernamen in das Feld **Benutzername** ein.
   - Wenn Sie den Bericht auf bestimmte IP-Adressen-Aktivitäten beschränken möchten, geben Sie die IP-Adresse des Benutzers in das Feld **Benutzer-IP-Adresse** ein.
4. Klicken Sie zum Erstellen des Berichts auf Übernehmen.
   - Klicken Sie auf ***Leeren*** (siehe "Berichtsdaten aus CC-SG leeren" auf Seite 149), um das Fehlerprotokoll zu löschen.

Zugriffsbericht

Erstellen Sie den Zugriffsbericht, um folgende Informationen anzuzeigen: alle Geräte und Knoten, auf die zugegriffen wurde, den Zeitpunkt des Zugriffs und den Benutzer, der zugegriffen hat.

➢ *So erstellen Sie den Zugriffsbericht:*

1. Wählen Sie Berichte > Zugriffsbericht.
2. Wählen Sie Knoten oder Geräte.
3. 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.
4. Sie können die Daten, die der Bericht enthalten wird, beschränken, indem Sie zusätzliche Parameter in die Felder **Gerätename**, **Knotenname**, **Benutzername** und **Benutzer-IP-Adresse** eingeben.
   - 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 Knoten beschränken möchten, geben Sie den Portnamen in das Feld **Knotenname** ein.

- Wenn Sie den Bericht auf bestimmte Benutzeraktivitäten beschränken möchten, geben Sie den Benutzernamen in das Feld **Benutzername** ein.
- Wenn Sie den Bericht auf bestimmte IP-Adressen-Aktivitäten beschränken möchten, geben Sie die IP-Adresse des Benutzers in das Feld **Benutzer-IP-Adresse** ein.

5. Wählen Sie im Feld Anzuzeigende Einträge die Anzahl an Einträgen aus, die im Berichtsfenster angezeigt werden sollen.
6. Klicken Sie zum Erstellen des Berichts auf Übernehmen.

Verfügbarkeitsbericht

Der Verfügbarkeitsbericht zeigt den Status aller Verbindungen zu Geräten und Knoten an. Dieser Bericht vermittelt einen vollständigen Überblick über die Verfügbarkeit aller Geräte oder Knoten in Ihrem von CC-SG verwalteten Netzwerk. Berichtsinformationen umfassen:

➢ *So erstellen Sie den Verfügbarkeitsbericht:*

1. Wählen Sie Berichte > Verfügbarkeitsbericht.
2. Wählen Sie die Option Knoten oder Geräte.
3. Klicken Sie auf Übernehmen.

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.

➢ *So erstellen Sie den Bericht „Aktive Benutzer“:*

- Wählen Sie Berichte > Benutzer > Aktive Benutzer.

➢ *So melden Sie einen Benutzer während einer aktiven Sitzung in CC-SG ab:*

1. Wählen Sie im Bericht „Aktive Benutzer“ den Benutzernamen aus, den Sie abmelden möchten.
2. Klicken Sie auf **Abmelden**.

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. ***Sperreinstellungen*** (auf Seite 203)

➢ *So erstellen Sie den Bericht „Gesperrte Benutzer“:*

- Wählen Sie Berichte > Benutzer > Gesperrte Benutzer.

➢ *So heben Sie die Sperre für einen Benutzer, der für CC-SG gesperrt war, wieder auf:*

- Wählen Sie den Benutzernamen aus, für den Sie die Sperre aufheben möchten, und klicken Sie dann auf **Benutzersperre aufheben**.

Benutzerdatenbericht

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

➢ *So erstellen Sie den Benutzerdatenbericht:*

- Wählen Sie Berichte > Benutzer > Benutzerdaten.
  - Im Feld **Benutzername** werden die Benutzernamen aller CC-SG-Benutzer angezeigt.
  - Im Feld **Telefon** wird die Rückrufnummer für Benutzer angezeigt. Diese Nummer ist nur bei Benutzern von CC-SG G1-Systemen verfügbar, 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 unter ***Benutzer hinzufügen*** (auf Seite 97).
  - Im Feld **Gültigkeitsdauer des Kennworts** wird die Anzahl an Tagen angezeigt, die der Benutzer dasselbe Kennwort verwenden kann, bevor es geändert werden muss. Weitere Informationen finden Sie unter ***Benutzer hinzufügen*** (auf Seite 97).
  - Im Feld **Gruppen** werden die Benutzergruppen angezeigt, denen der Benutzer angehört.

- Im Feld **Berechtigungen** werden die CC-SG-Berechtigungen angezeigt, die dem Benutzer zugeordnet wurden. Weitere Informationen finden Sie in ***Anhang C: Benutzergruppenberechtigungen*** (siehe "Benutzergruppenberechtigungen" auf Seite 280).
- 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.

Bericht „ Benutzer in Gruppen “

Der Bericht „Benutzer in Gruppen“ enthält Informationen über die Benutzer und Gruppen, denen sie zugewiesen sind.

➢ *So erstellen Sie den Bericht „Benutzer in Gruppen“:*

- Wählen Sie Berichte > Benutzer > Benutzer in Gruppen.
- Doppelklicken Sie auf die Benutzergruppe, um die zugeordneten Richtlinien anzuzeigen.

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.

➢ *So erstellen Sie den Gruppendatenbericht:*

- Wählen Sie Berichte > Benutzer > Gruppendaten.
  - 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.

➢ *So erstellen Sie den AD-Benutzergruppenbericht:*

1. Wählen Sie Berichte > Active Directory > AD-Benutzergruppenbericht.
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 zum Erstellen des Berichts auf **Übernehmen**.

Anlagenverwaltungsbericht

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

➢ *So erstellen Sie den Anlagenverwaltungsbericht:*

1. Wählen Sie Berichte > Geräte > Anlagenverwaltungsbericht. Der Anlagenverwaltungsbericht wird für alle Geräte erstellt.
   - Wenn Sie die Berichtsdaten nach Gerätetyp filtern möchten, klicken Sie auf den Pfeil neben 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.
   - Bei Geräten, deren Versionen nicht der Kompatibilitätsmatrix entsprechen, wird der Text im Feld **Gerätename** rot angezeigt.

- Klicken Sie auf **Aktualisieren**, um einen neuen Bericht zu erstellen. Dies kann abhängig von der Systemkonfiguration einige Minuten dauern.

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.

➢ *So erstellen Sie den Knotenanlagebericht:*

1. Wählen Sie Berichte > Knoten > Knotenanlagebericht.
2. Wählen Sie die Filterkriterien aus, die Sie auf den Bericht anwenden möchten. Die folgenden Kriterien sind verfügbar: Alle Knoten, Knotengruppe, Gerätegruppe und Geräte.
   - Wenn Sie Knotengruppe, Schnittstellentyp oder Gerätegruppe auswählen, klicken Sie auf den entsprechenden Pfeil neben der Dropdown-Liste, und wählen Sie in der Liste einen Parameter aus.
   - Wenn Sie Geräte auswählen, 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.

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.

➢ *So erstellen Sie den Bericht „Aktive Knoten“:*

1. Wählen Sie Berichte > Knoten > Aktive Knoten. Der Bericht „Aktive Knoten“ wird erstellt, falls aktive Knoten vorhanden sind.

- Sie können einen Knoten von einer aktuellen Sitzung trennen. Wählen Sie dazu den entsprechenden Knoten aus, und klicken Sie auf **Trennen**.

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.

➢ *So erstellen Sie den Knotenerstellungsbericht:*

1. Wählen Sie Berichte > Knoten > Knotenerstellung.
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. Wählen Sie Alle Knoten oder Potentielle Duplikate aus, um festzulegen, ob Sie den Bericht auf nur die Knoten beschränken möchten, die als potentielle Duplikate gekennzeichnet wurden.
4. Klicken Sie auf Übernehmen. Der Knotenerstellungsbericht wird erstellt.
   - Im Ergebnisfeld wird Erfolg, Fehlgeschlagen oder Potenzielle Duplikate angezeigt, um den Status nach dem Knotenerstellungs-Versuch zu beschreiben.

Portabfragebericht

Im Portabfragebericht werden alle Ports nach Portstatus aufgelistet.

➢ *So erstellen Sie den Portabfragebericht:*

1. Wählen Sie Berichte > Ports > Port abfragen.
2. Wählen Sie im Bereich **Portstatus/Verfügbarkeit** den Portstatus aus, den der Bericht enthalten soll. Durch das Markieren mehrerer Kontrollkästchen werden Ports mit allen ausgewählten Statuszuständen eingeschlossen. Sie müssen mindestens eine Verfügbarkeitsoption auswählen, wenn eine Statusoption festgelegt ist.

Statustyp	Portstatus	Definition
	Alle	Alle Ports.
Status:		
	Verfügbar	
	Nicht verfügbar	Die Verbindung zum Port ist nicht möglich, da das Gerät ausgeschaltet und nicht verfügbar ist.
Verfügbarkeit:		
	Leerlauf	Der Port ist konfiguriert, und eine Verbindung zum Port ist möglich.
	Verbunden	
	Beschäftigt	Ein Benutzer ist mit diesem Port verbunden.
	Eingeschaltet	
	Ausgeschaltet	
Nicht konfiguriert:		
	Neu	Dem Port wurde ein neuer Zielserver angefügt, doch der Port wurde noch nicht konfiguriert.
	Nicht verwendet	An den Port ist kein Zielserver angeschlossen, und der Port wurde nicht konfiguriert.

3. (Optional) Markieren Sie **Verwaiste Ports**, um verwaiste Ports einzuschließen. 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. (Optional) Markieren Sie Angehaltene Ports oder Gesperrte Ports, um angehaltene oder gesperrte Ports einzuschließen. Angehaltene Ports entstehen, wenn ein Gerät angehalten wurde. Gesperrte Ports entstehen, wenn ein Gerät aktualisiert wird.
5. Wählen Sie die Anzahl an Datenzeilen aus, die im Berichtsfenster im Feld Anzuzeigende Einträge angezeigt werden sollen.

Hinweis: Diese Einstellung gilt nicht, wenn der Bericht als Aufgabe erstellt wird.

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

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.

➢ *So erstellen Sie den Bericht „Aktive Ports“:*

- Wählen Sie Berichte > Ports > Aktive Ports.

➢ *So trennen Sie einen Port von einer aktuellen Sitzung:*

- Wählen Sie im Bericht „Aktive Ports“ den Port aus, den Sie trennen möchten, und klicken Sie dann auf **Trennen**.

Geplante Berichte

Geplante Berichte sind Berichte, die im Aufgabenmanager geplant wurden. Sie finden die Berichte „ Gerätefirmware aktualisieren “ und „ Gerät neu starten “ im Fenster Geplante Berichte. Geplante Berichte können im HTML-Format angezeigt werden. Weitere Informationen finden Sie unter ***Aufgabenmanager*** (auf Seite 214).

➢ *So greifen Sie auf einen geplanten Bericht zu:*

1. Wählen Sie Berichte > 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.
   - Zum Anzeigen eines Berichts markieren Sie den Bericht in der Liste, und klicken Sie auf **Bericht anzeigen**.
   - (Optional) Filtern Sie die angezeigten Berichte:
   a. Geben Sie Parameter ein.

- Wählen Sie einen **Berichtstyp** aus.
- Wählen Sie einen **Berichtseigentümer** aus.
- Ändern Sie die Start- und Enddaten in den Feldern **Berichte erstellt zwischen**.
- Geben Sie einen Berichtsnamen ein, um nach dem Namen zu filtern. Sie können den vollständigen Namen oder einen Teil des Namens eingeben. Bei den Übereinstimmungen wird die Groß- und Kleinschreibung nicht berücksichtigt. Platzhalter sind nicht zulässig.

b. Klicken Sie auf **Berichte abrufen**, um die gefilterte Liste anzuzeigen.

Bericht „ Gerätefirmware aktualisieren “

Sie finden den Bericht „Gerätefirmware aktualisieren“ in der Liste Geplante Berichte. Dieser Bericht wird erstellt, wenn die Aufgabe Gerätefirmware aktualisieren ausgeführt wird. Zeigen Sie den Bericht an, um Statusinformationen über die Aufgabe in Echtzeit zu erhalten. Nachdem die Aufgabe abschlossen wurde, sind die Berichtsinformationen statisch.

Weitere Informationen zum Anzeigen von Berichten finden Sie unter ***Geplante Berichte*** (auf Seite 159).

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*** (auf Seite 222). Sie können in diesem Bericht auch Ziele aus der CC-SG-Datenbank löschen.

➢ *So erstellen Sie den CC-NOC-Synchronisation-Bericht:*

1. Wählen Sie Berichte > CC-NOC-Synchronisation.
2. Wählen Sie einen Wert für **Datum zuletzt erkannt** aus, und klicken Sie dann 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**.

Kapitel 14 Systemwartung

In diesem Kapitel

Wartungsmodus

Der Wartungsmodus schränkt den Zugriff auf CC-SG ein, damit Administratoren bestimmte Aufgaben ohne Unterbrechung durchführen können, z. B. CC-SG aktualisieren.

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 unter ***Aufgabenmanager*** (auf Seite 214). Beendet CC-SG den Wartungsmodus, werden geplante Aufgaben so schnell wie möglich ausgeführt.

Wartungsmodus starten

1. So starten Sie den Wartungsmodus:
   a. Wählen Sie Systemwartung > Wartungsmodus > Wartungsmodus starten.
   b. Kennwort: Geben Sie Ihr Kennwort ein. Nur Benutzer mit der Berechtigung CC-Setup- und -Steuerung können den Wartungsmodus starten.
   c. Broadcastnachricht: Geben Sie die Nachricht für Benutzer ein, die bei CC-SG abgemeldet werden.
   d. Wartungsmodus starten nach (Min.): Geben Sie die Dauer in Minuten von 0 bis 30 ein, die verstreichen sollen, bis CC-SG den Wartungsmodus startet. Durch die Eingabe von 0 Minuten wird der Wartungsmodus sofort gestartet.
   e. Klicken Sie auf **OK**.
   f. Klicken Sie im Bestätigungsfeld auf OK.

Wartungsmodus beenden

1. So beenden Sie den Wartungsmodus:
   a. Wählen Sie Systemwartung > Wartungsmodus > Wartungsmodus beenden.
   b. Klicken Sie auf **OK**, um den Wartungsmodus zu beenden.

   Eine Nachricht wird angezeigt, wenn CC-SG den Wartungsmodus beendet 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. Durch das Starten des Wartungsmodus wird sichergestellt, dass die Datenbank während der Sicherung nicht geändert wird.

1. Wählen Sie **Systemwartung** > **Sicherung**.
2. Geben Sie einen Namen für diese Sicherung in das Feld **Sicherungsname** ein.
3. (Optional) 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. (Optional) Wenn Sie eine Kopie dieser Sicherungsdatei auf einem externen Server speichern möchten, markieren Sie **Sicherung an Remotestandort**.
6. Wählen Sie ein **Protokoll**, das für die Verbindung zum Remoteserver verwendet wird (entweder **FTP** oder **SFTP**).
7. Geben Sie die IP-Adresse oder den Hostnamen des Servers in das Feld **Hostname** ein.
8. Wenn Sie für das ausgewählte Protokoll nicht den Standardport (FTP: 21, SFTP: 22) verwenden, geben Sie den verwendeten Kommunikationsport in das Feld **Portnummer** ein.
9. Geben Sie einen Benutzernamen für den Remoteserver in das Feld **Benutzername** ein.

10. Geben Sie ein Kennwort für den Remoteserver in das Feld **Kennwort** ein.
11. Geben Sie im Feld **Pfad** das Verzeichnis an, das zum Speichern der Sicherung auf dem Remoteserver verwendet werden soll. Sie müssen den absoluten Pfad zum Verzeichnis festlegen.
12. Klicken Sie auf **OK**.

    Nach Abschluss der Sicherung wird eine Bestätigungsmeldung 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.

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. Sie können ein Archiv der Sicherungsdateien erstellen. Sicherungsdateien, die an einem anderen Ort gespeichert sind, können an andere CC-SG-Einheiten gesendet und dann wiederhergestellt werden, um eine Konfiguration von einer CC-SG-Einheit zu einer anderen zu kopieren.

Durch das Löschen von unbenötigten Sicherungen haben Sie mehr Platz auf dem CC-SG.

Sicherungsdateien speichern

1. Wählen Sie **Systemwartung** > **CommandCenter wiederherstellen**.
2. Wählen Sie in der Tabelle **Verfügbare Sicherungen** eine Sicherung aus, die Sie auf Ihrem PC speichern möchten.
3. Klicken Sie auf **In Datei speichern**. Ein Speicherdialog wird angezeigt.
4. Geben Sie einen Namen für die Datei ein, und wählen Sie den Speicherort aus.
5. Klicken Sie auf Speichern.

   Die Sicherungsdatei wird an den festgelegten Speicherort kopiert.

Sicherungsdateien löschen

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 aus dem CC-SG-System zu löschen.

CC-SG wiederherstellen

➢ *So stellen Sie CC-SG wieder her:*

1. Wählen Sie **Systemwartung** > **Wiederherstellen**. Der Bildschirm **CommandCenter wiederherstellen** wird mit einer Tabelle mit Sicherungssitzungen für CC-SG angezeigt. Die Tabelle enthält die Sicherungsart, das Sicherungsdatum, die Beschreibung, welche CC-SG-Version verwendet wurde, sowie die Größe der Sicherungsdatei.
2. (Optional) Wenn Sie eine Sicherung wiederherstellen möchten, die nicht auf dem CC-SG-System gespeichert wurde, müssen Sie die Sicherungsdatei zunächst an CC-SG senden.
   a. Klicken Sie auf **Senden**. Ein Dialogbildschirm wird angezeigt.
   b. Suchen Sie nach der Sicherungsdatei, und wählen Sie sie im Dialogfenster aus. Sie können die Datei überall im Netzwerk des Client abrufen.
   c. Klicken Sie auf **Öffnen**, um diese Datei an CC-SG zu senden. 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 **Anwendungsdateien**, die in der Sicherungsdatei gespeichert sind, wieder her. 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** markieren. Markieren Sie jede der folgenden Optionen, um sie in der Wiederherstellung einzuschließen.
- **Daten**: CC-SG-Konfiguration, Geräte- und Knotenkonfiguration und Benutzerdaten.
- **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.

5. Geben Sie in das Feld **Wiederherstellen nach** 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**. CC-SG wartet den im Feld **Wiederherstellen nach** angegebenen Zeitraum, bevor die Konfiguration der ausgewählten Sicherung wiederhergestellt wird. Während der Wiederherstellung werden alle anderen Benutzer abgemeldet.

CC-SG zurücksetzen

Sie können CC-SG zurücksetzen, um die Datenbank zu leeren. Wenn die Datenbank geleert ist, sind alle Geräte, Knoten und Benutzer entfernt. Außerdem sind alle Authentifizierungs- und Autorisierungsserver entfernt.

Die Systemkonfigurationsdaten wie die IP-Adresse von CC-SG werden durch das Zurücksetzen nicht zurückgesetzt. Die folgenden Vorgänge werden durchgeführt, wenn Sie CC-SG zurücksetzen:

- CC-SG-Datenbank zurücksetzen
- SNMP-Konfiguration zurücksetzen
- zu Standardfirmware zurücksetzen
- Standardfirmware in die CC-SG-Datenbank laden
- Diagnosekonsole auf Standardwerte zurücksetzen

Vor dem Zurücksetzen von CC-SG sollten Sie eine Sicherung durchführen und die Sicherungsdatei an einem anderen Ort speichern.

➢ *So setzen Sie CC-SG zurück:*

1. Wählen Sie **Systemwartung** > **Zurücksetzen**.
2. Geben Sie Ihr CC-SG-**Kennwort** ein.
3. Broadcastnachricht: Geben Sie die Nachricht für Benutzer ein, die bei CC-SG abgemeldet werden.
4. Geben Sie die Dauer in Minuten von 0 bis 30 ein, die verstreichen sollen, bis CC-SG den Zurücksetzungsvorgang durchführt.
5. Klicken Sie auf **OK**, um CC-SG zurückzusetzen. Eine Meldung wird angezeigt, um das Zurücksetzen zu bestätigen.

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.

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 an der CC-SG-Einheit verwenden.

1. Wählen Sie **Systemwartung** > **Neu starten**.
2. Geben Sie Ihr Kennwort in das Feld **Kennwort** ein.

3. Broadcastnachricht: Geben Sie die Nachricht für Benutzer ein, die bei CC-SG abgemeldet werden.
4. Neustart nach (Min.): Geben Sie die Dauer in Minuten von 0 bis 30 ein, die verstreichen sollen, bis CC-SG neu startet.
5. Klicken Sie auf **OK**, um CC-SG neu zu starten.

CC-SG aktualisieren

Sie können die Firmware von CC-SG aktualisieren, wenn eine neuere Version veröffentlicht wird. Sie finden die Firmware-Dateien auf der Raritan-Website im Support-Bereich.

Laden Sie die Firmware-Datei auf Ihren Client-PC herunter, bevor Sie mit der Aktualisierung beginnen.

Sie sollten vor dem Aktualisieren eine Sicherheitskopie von CC-SG erstellen. Wenn Sie mit einem CC-SG-Cluster arbeiten, müssen Sie zuerst das Cluster entfernen und jeden Knoten einzeln aktualisieren.

Hinweis: Wenn Sie von 3.0.2 auf 3.1 aktualisieren und Active Directory verwenden, lesen Sie bitte in der Readme-Datei der Version 3.1 die besonderen Anleitungen.

Wichtig!

Wenn Sie sowohl CC-SG als auch ein Gerät oder eine Gerätegruppe aktualisieren müssen, aktualisieren Sie zuerst CC-SG und dann die Geräte.

CC-SG wird während des Aktualisierungsvorgangs von 3.1.1 auf 3.2 neu gestartet. Während der Aktualisierung dürfen Sie Folgendes NICHT: den Vorgang anhalten, die Einheit manuell neu starten, die Einheit ausschalten oder die Einheit aus- und einschalten.

➢ *So aktualisieren Sie CC-SG:*

1. Laden Sie die Datei mit der Firmware auf Ihren Client PC herunter.
2. ***Wartungsmodus starten*** (auf Seite 163)
3. Sobald sich CC-SG im Wartungsmodus befindet, wählen Sie **Systemwartung** > **Aktualisieren**.
4. Klicken Sie auf **Durchsuchen**. Wechseln Sie zur CC-SG-Firmwaredatei, wählen Sie diese aus, und klicken Sie auf **Öffnen**.
5. Klicken Sie auf **OK**, um die Firmwaredatei an CC-SG zu senden.

Nachdem die Firmwaredatei an CC-SG gesandt wurde, wird eine Erfolgsmeldung angezeigt. In dieser Meldung wird Ihnen mitgeteilt, dass CC-SG mit dem Aktualisierungsvorgang begonnen hat. Dazu werden alle Benutzer bei CC-SG abgemeldet.

6. Klicken Sie auf **OK**, um CC-SG zu verlassen und den Neustart durchzuführen. Sie müssen ca. 8 Minuten warten, während CC-SG neu startet.
7. Schließen Sie Ihr Browserfenster, und löschen Sie den Browser-Cache.
8. Öffnen Sie nach 8 Minuten ein neues Browserfenster, und starten Sie CC-SG.
9. Wählen Sie **Hilfe** > **Info zu Raritan Secure Gateway**. Überprüfen Sie die Versionsnummer, um zu bestätigen, 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.
10. ***Wartungsmodus beenden*** (auf Seite 163)

CC-SG herunterfahren

Wenn Sie CC-SG herunterfahren, wird die CC-SG-Software heruntergefahren, die CC-SG-Einheit wird jedoch nicht ausgeschaltet.

Nachdem CC-SG heruntergefahren wurde, sind alle Benutzer abgemeldet. Benutzer können sich erst wieder anmelden, nachdem Sie CC-SG entweder über die Diagnostic Console oder durch Aus- und Einschalten der CC-SG-Stromversorgung neu gestartet haben.

➢ *So fahren Sie CC-SG herunter:*

1. Wählen Sie **Systemwartung** > **CommandCenter herunterfahren**.
2. Geben Sie Ihr Kennwort in das Feld **Kennwort** ein.
3. Übernehmen Sie die Standardnachricht, oder geben Sie in das 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.

CC-SG nach dem Herunterfahren neu starten

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

- Über die Diagnostic Console: Weitere Informationen finden Sie unter ***Diagnostic Console*** (siehe "Diagnosekonsole" auf Seite 235).
- Schalten Sie die CC-SG-Einheit aus und dann wieder ein.

CC-SG herunterfahren

Wenn die Stromversorgung zu CC-SG unterbrochen wird, während das Gerät eingeschaltet ist und ausgeführt wird, merkt sich CC-SG den letzten Stromversorgungsstatus. Sobald die Stromversorgung wiederhergestellt ist, fährt CC-SG automatisch neu hoch. Wenn jedoch die Stromversorgung zu CC-SG unterbrochen wird, wenn das Gerät ausgeschaltet ist, bleibt CC-SG auch dann ausgeschaltet, wenn die Stromversorgung 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 fahren Sie CC-SG herunter:*

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 Stromversorgung alle Transaktionen beenden, die Datenbanken schließen und die Festplattenlaufwerke in einen sicheren Zustand versetzen.

CC-SG-Sitzung beenden

Eine CC-SG-Sitzung kann auf zwei Arten beendet werden.

Durch ***Abmelden*** (siehe "CC-SG verlassen" auf Seite 172), um Ihre Sitzung zu beenden, wobei das Client-Fenster geöffnet bleibt.

Durch ***Beenden*** (siehe "CC-SG beenden" auf Seite 172), um Ihre Sitzung zu beenden und das Client-Fenster zu schließen.

CC-SG verlassen

1. Wählen Sie **Secure Gateway** > **Abmelden**. Das Fenster **Abmelden** wird angezeigt.
2. Klicken Sie auf **Ja**, um CC-SG zu verlassen. Nach dem Abmelden wird das CC-SG-Anmeldefenster angezeigt.

CC-SG beenden

1. Wählen Sie **Secure Gateway** > **Beenden**.
2. Klicken Sie auf **Ja**, um CC-SG zu beenden.

Kapitel 15 Erweiterte Administration

In diesem Kapitel

Tipp des Tages konfigurieren

Mit dem Tipp des Tages können Sie allen Benutzern beim Anmelden eine Nachricht einblenden. Sie müssen über die Berechtigung **CC-Setup und -Steuerung** verfügen, um den Tipp des Tages zu konfigurieren.

➢ *So konfigurieren Sie den Tipp des Tages:*

1. Wählen Sie **Administration** > **Tipp des Tages einrichten**.
2. (Optional) 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 zum Speichern der Änderungen auf **OK**.

Anwendungen für den Zugriff auf Knoten konfigurieren

Anwendungen für den Zugriff auf Knoten

CC-SG bietet mehrere Anwendungen, mit denen Sie auf Knoten zugreifen können. Mit dem Anwendungsmanager können Sie Anwendungen anzeigen, neue Anwendungen hinzufügen, Anwendungen löschen und die Standardanwendung für jeden Gerätetyp einstellen.

➢ *So zeigen Sie in CC-SG verfügbare Anwendungen an:*

1. Wählen Sie **Administration** > **Anwendungen**.
2. Klicken Sie auf das Dropdown-Menü Anwendungsname, um die Liste der in CC-SG verfügbaren Anwendungen anzuzeigen.

Anwendungsversionen prüfen und aktualisieren

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

➢ *So überprüfen Sie eine Anwendungsversion:*

1. Wählen Sie **Administration** > **Anwendungen**.
2. Wählen Sie in der Liste einen **Anwendungsnamen** aus. Beachten Sie die Zahl im Feld **Version**. Für einige Anwendungen wird nicht automatisch eine Versionszahl angezeigt.

➢ *So aktualisieren Sie eine Anwendung:*

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. (Eine vollständige Liste der unterstützten Anwendungsversionen finden Sie in der **Kompatibilitätsmatrix** auf der Support-Website von Raritan.)

1. Speichern Sie die Datei mit der Anwendung auf Ihrem Client-PC.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Anwendungsname**, und wählen Sie die zu aktualisierende Anwendung in der Liste aus. Wenn Sie die Anwendung nicht sehen, müssen Sie die Anwendung zuerst hinzufügen. ***Anwendungen hinzufügen*** (auf Seite 175)
3. Klicken Sie auf **Durchsuchen**, und wählen Sie die Datei zur Anwendungsaktualisierung im angezeigten Dialogfeld zum Öffnen aus. Klicken Sie auf **Öffnen**.
4. Der Anwendungsname wird im **Anwendungsmanager** im Feld **Neue Anwendungsdatei** angezeigt.
5. Klicken Sie auf **Senden**. Eine Statusanzeige informiert über den Ladevorgang der neuen Anwendung. Nach dem Laden wird in einem neuen Fenster angezeigt, dass die Anwendung der CC-SG-Datenbank hinzugefügt wurde und nun verwendet werden kann.
6. Wenn das Feld **Version** nicht automatisch aktualisiert wird, geben Sie die neue Versionszahl in das Feld **Version** ein. Das Feld **Version** wird bei einigen Anwendungen automatisch aktualisiert.
7. Klicken Sie auf **Aktualisieren**.

Anwendungen hinzufügen

Wenn Sie CC-SG eine Anwendung hinzufügen, müssen Sie festlegen, mit welchen Gerätetypen die Anwendung verwendet wird. Bietet ein Gerät KVM- und seriellen Zugriff, wird es für beide Methoden aufgeführt.

1. Wählen Sie **Administration** > **Anwendungen**.
2. Klicken Sie auf **Hinzufügen**. Das Fenster **Anwendung hinzufügen** wird angezeigt.
3. Geben Sie den Namen der Anwendung in das Feld **Anwendungsname** ein.

4. Wählen Sie in der Liste **Verfügbar** die Raritan-Geräte für die Anwendung aus, und klicken Sie auf **Hinzufügen**, um sie der Liste **Ausgewählt** hinzuzufügen.
   - 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 **Entfernen**.
5. Klicken Sie auf **OK**. Ein Dialogfenster zum Öffnen wird angezeigt.
6. Navigieren Sie zur Anwendungsdatei (normalerweise eine JAR- oder CAB-Datei), wählen Sie die Datei aus und klicken Sie dann auf **Öffnen**.

   Die ausgewählte Anwendung wird in CC-SG geladen.

Anwendungen löschen

1. Wählen Sie **Administration** > **Anwendungen**.
2. Wählen Sie im Dropdown-Menü **Anwendungsname** eine Anwendung aus.
3. Klicken Sie auf **Löschen**. Ein Bestätigungsfeld wird angezeigt.
4. Klicken Sie auf **Ja**, um die Anwendung zu löschen.

Standardanwendungen konfigurieren

Standardanwendungen

Sie können festlegen, welche Anwendung CC-SG standardmäßig für jeden Gerätetyp verwenden soll.

Zuordnungen der Standardanwendung anzeigen

1. Wählen Sie **Administration** > **Anwendungen**.
2. 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.

Standardanwendung für Schnittstellen- oder Porttypen einstellen

1. Wählen Sie **Administration** > **Anwendungen**.

2. Klicken Sie auf die Registerkarte **Standardanwendungen**.
3. Wählen Sie den Schnittstellen- oder Porttyp aus, dessen Standardanwendung Sie einstellen möchten.
4. Doppelklicken Sie auf den Pfeil der **Anwendung**, der in der Zeile aufgeführt ist. Der Wert wird in einem Dropdown-Menü angezeigt. Abgeblendete Werte können nicht geändert werden.
5. Wählen Sie die Standardanwendung aus, die für die Verbindung zum ausgewählten Schnittstellen- oder Porttyp verwendet werden soll.
   - **Automatisch erkennen**: CC-SG wählt automatisch eine geeignete Anwendung basierend auf dem Clientbrowser aus.
6. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Gerätefirmware verwalten

CC-SG speichert Firmware für Raritan-Geräte, die Sie zum Aktualisieren der Geräte verwenden können, die von CC-SG gesteuert werden. Der Firmwaremanager wird verwendet, um die Geräte-Firmwaredateien an CC-SG zu senden oder in CC-SG zu löschen. Sobald eine Firmwaredatei gesendet wurde, können Sie auf die Datei zugreifen, um eine Geräteaktualisierung durchzuführen. ***Geräte aktualisieren*** (siehe "Gerät aktualisieren" auf Seite 45)

Upload

Sie können verschiedene Versionen von Gerätefirmware an CC-SG senden. Wenn neue Firmwareversionen verfügbar sind, werden sie auf der Website von Raritan veröffentlicht.

1. Wählen Sie **Administration** > **Firmware**.
2. Klicken Sie auf **Hinzufügen**, um eine neue Firmwaredatei hinzuzufügen. Ein Suchfenster wird angezeigt.
3. Wechseln Sie zur Firmwaredatei, die Sie an CC-SG senden möchten. Wählen Sie diese aus, und klicken Sie auf **Öffnen**. Nach dem Senden wird die neue Firmware im Feld **Firmwarename** angezeigt.

Firmware löschen

1. Wählen Sie **Administration** > **Firmware**.
2. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Firmwarename**, und wählen Sie die zu löschende Firmware aus.
3. Klicken Sie auf **Löschen**. Eine Bestätigungsmeldung wird angezeigt.

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

CC-SG-Netzwerk konfigurieren

Im Konfigurationsmanager können Sie die Netzwerkeinstellungen für Ihr vom CC-SG verwaltetes Netzwerk konfigurieren.

Netzwerkeinrichtung

CC-SG bietet zwei Modi für die Netzwerkeinrichtung:

- ***Primär-/Sicherungsmodus*** (siehe "Was ist der Primär-/Sicherungsmodus?" auf Seite 179)
- ***Aktiv/Aktivmodus*** (siehe "Was ist der Aktiv/Aktiv-Modus?" auf Seite 182)

CC-SG ermöglicht auch entweder statische oder mit DHCP zugeordnete IP-Adressen. Weitere Informationen zu optimalen Verfahren zur Verwendung von DHCP mit CC-SG finden Sie unter ***Empfohlene DHCP-Konfigurationen für CC-SG*** (auf Seite 184).

CC-SG-LAN-Ports

Ein CC-SG bietet zwei Haupt-LAN-Ports: Primäres LAN und Sekundäres LAN. Für die Modi Primär/Sicherung und Aktiv/Aktiv ist es erforderlich, dass Sie die CC-SG-LAN-Ports auf unterschiedliche Arten anschließen.

Lesen Sie die Tabellen unten, um die Position des primären und sekundären LAN-Ports auf Ihrem CC-SG-Modell zu überprüfen.

G1-LAN-Ports

Modell	Primäres LAN – Name	Primäres LAN – Position	Sekundäres LAN – Name	Sekundäres LAN – Position
G1	LAN0	Rechter LAN-Port	LAN1	Linker LAN-Port

V1-LAN-Ports

Modell	Primäres LAN – Name	Primäres LAN – Position	Sekundäres LAN – Name	Sekundäres LAN – Position
V1	LAN1	Linker LAN-Port	LAN2	Rechter LAN-Port

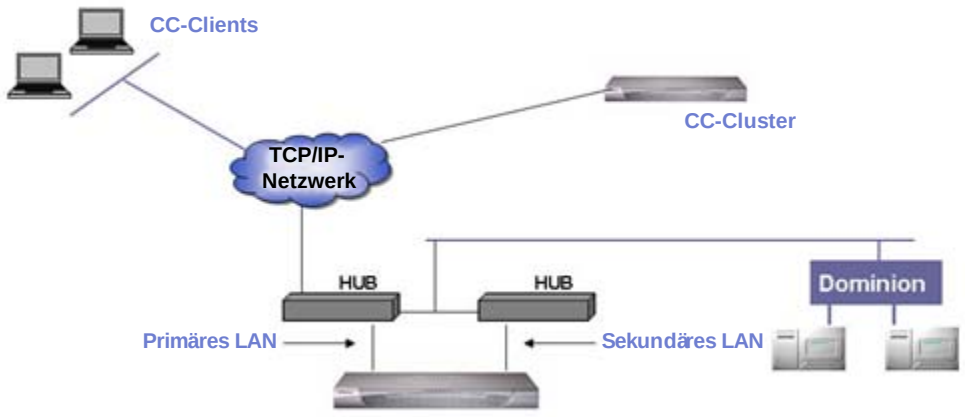
E1-LAN-Ports

Modell	Primäres LAN – Name	Primäres LAN – Position	Sekundäres LAN – Name	Sekundäres LAN – Position
E1	Nicht beschriftet	Oberer LAN-Port von 2 Ports in der Mitte der Einheitenrückseite	Nicht beschriftet	Unterer LAN-Port von 2 Ports in der Mitte der Einheitenrückseite

Was ist der Primär-/Sicherungsmodus?

Im Primär-/Sicherungsmodus können Sie zwei CC-SG-LAN-Ports verwenden, um Ausfallsicherung und Redundanz für das Netzwerk zu implementieren. In diesem Modus ist nur ein LAN-Port zurzeit aktiv.

Weitere Informationen zur Position des primären und sekundären LAN-Ports auf jedem CC-SG-Modell finden Sie unter ***CC-SG-LAN-Ports*** (auf Seite 178).



Wenn das primäre LAN angeschlossen ist und ein Verbindungsintegritätssignal erhält, verwendet CC-SG diesen LAN-Port für die Kommunikation. Wenn das primäre LAN die Verbindungsintegrität verliert und das sekundäre LAN angeschlossen ist, wird CC-SG die zugeordnete IP-Adresse zu Ausfallsicherungszwecken auf das sekundäre LAN verlegen. Das sekundäre LAN wird verwendet, bis das primäre LAN erneut dienstbereit ist. Wenn das primäre LAN wieder dienstbereit ist, verwendet CC-SG automatisch wieder das primäre LAN.

Solange eine LAN-Verbindung einsatzbereit ist, sollte ein Client keine Dienstunterbrechung bei Ausfällen feststellen.

➢ *Einrichtung für den Primär-/Sicherungsmodus*

Beim Implementieren des Primär-/Sicherungsmodus für Ihr CC-SG-Netzwerk gilt Folgendes:

- Beide CC-SG-LAN-Ports müssen an das gleiche LAN-Subnetzwerk angeschlossen sein.
- (Optional) Sie können jeden LAN-Port an einen anderen Switch oder ein anderes Hub im gleichen Subnetzwerk für bessere Zuverlässigkeit anschließen.

➢ *So konfigurieren Sie den Primär-/Sicherungsmodus in CC-SG:*

1. Wählen Sie **Administration** > **Konfiguration**.
2. Klicken Sie auf die Registerkarte **Netzwerkeinrichtung**.
3. Wählen Sie **Primär-/Sicherungsmodus**.
4. Geben Sie den CC-SG-Hostnamen in das Feld Hostname ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben. Wenn Sie zum Speichern der Konfiguration auf **Konfiguration aktualisieren** klicken, wird das Feld **Hostname** aktualisiert, um den vollständig qualifizierten Domänennamen (Fully-Qualified Domain Name, FQDN) anzuzeigen, wenn ein DNS und Domänensuffix konfiguriert wurden.
5. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Konfiguration**, und wählen Sie entweder **DHCP** oder **Statisch**.

   DHCP:

- Wenn Sie DHCP auswählen, werden die Felder Primärer DNS-Server, Sekundärer DNS-Server, Domänensuffix, IP-Adresse, Subnetzmaske und Standardgateway automatisch belegt (falls Ihr DHCP-Server für die Bereitstellung dieser Informationen konfiguriert wurde), sobald Sie diese Netzwerkeinrichtung speichern und CC-SG neu starten.
- Mithilfe der Informationen, die der DHCP-Server bereitstellt, wird CC-SG dynamisch beim DNS-Server registriert, wenn dieser dynamische Aktualisierungen annimmt.
- Weitere Informationen finden Sie unter ***Empfohlene DHCP-Konfigurationen für CC-SG*** (auf Seite 184).

Statisch:

- Wenn Sie **Statisch** auswählen, geben Sie den primären DNS-Server, den sekundären DNS-Server, das Domänensuffix, die IP-Adresse, die Subnetzmaske und das Standardgateway in die entsprechenden Felder ein.

6. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Adaptergeschwindigkeit**, und wählen Sie in der Liste eine Geschwindigkeit aus. Stellen Sie sicher, dass Ihre Auswahl mit der Adapterporteinstellung des Switch übereinstimmt.
7. Wenn Sie im Feld **Adaptergeschwindigkeit** die Option **Automatisch** ausgewählt haben, ist das Feld **Adaptermodus** deaktiviert. Die Option **Vollduplex** wurde automatisch ausgewählt. Wenn Sie eine andere Adaptergeschwindigkeit als Automatisch ausgewählt haben, klicken Sie auf den Pfeil neben der Dropdown-Liste **Adaptermodus**, und wählen Sie einen Duplexmodus in der Liste aus.
8. Klicken Sie auf **Konfiguration aktualisieren**, um die Änderungen zu speichern. Ihre Änderungen werden erst nach dem nächsten Neustart von CC-SG wirksam.
   - Klicken Sie auf **Jetzt neu starten**, wenn Sie CC-SG jetzt automatisch neu starten möchten.
   - Klicken Sie auf **Später neu starten**, wenn Sie CC-SG später ***neu starten*** (siehe "CC-SG neu starten" auf Seite 168) möchten.

- Klicken Sie auf **Abbrechen**, um zum Fensterbereich Netzwerkeinrichtung zurückzukehren, ohne die Änderungen zu speichern. Sie müssen auf **Konfiguration aktualisieren** klicken, und dann zum Speichern Ihrer Änderungen auf **Jetzt neu starten** oder **Später neu starten** klicken.

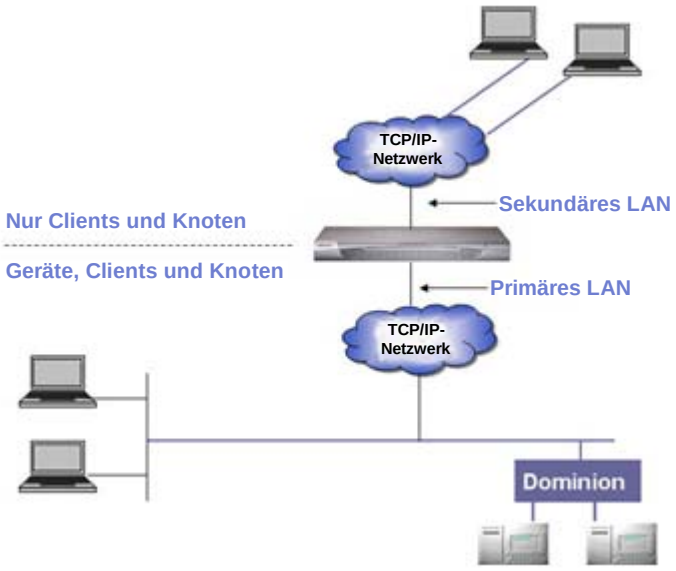
Hinweis: *Ist CC-SG mit DHCP konfiguriert, können Sie nach einer erfolgreichen Registrierung bei einem DNS-Server über den Hostnamen auf CC-SG zugreifen.*

Was ist der Aktiv/Aktiv-Modus?

Im Aktiv/Aktiv-Modus können Sie mit CC-SG Geräte und Knoten verwalten, die sich in zwei unterschiedlichen Netzwerken befinden. In diesem Modus verwaltet CC-SG den Verkehr zwischen den beiden unterschiedlichen IP-Domänen. Im Aktiv/Aktiv-Modus ist keine Ausfallsicherung verfügbar. Wenn eine LAN-Verbindung ausfällt, haben Benutzer keinen Zugriff.

Weitere Informationen zur Position des primären und sekundären LAN-Ports auf jedem CC-SG-Modell finden Sie unter ***CC-SG-LAN-Ports*** (auf Seite 178).

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



➢ *Einrichtung für den Aktiv/Aktiv-Modus*

Beim Implementieren des Aktiv/Aktiv-Modus für Ihr CC-SG-Netzwerk gilt Folgendes:

- Jeder CC-SG-LAN-Port muss an ein unterschiedliches Subnetzwerk angeschlossen sein.
- Raritan-Geräte dürfen nur an das primäre LAN angeschlossen werden.
- Clients und Knoten können an das primäre oder sekundäre LAN angeschlossen werden.
- Legen Sie in CC-SG im Fensterbereich Netzwerkeinrichtung höchstens ein Standardgateway fest. Verwenden Sie die Diagnostic Console, um bei Bedarf ***weitere statische Routen hinzuzufügen*** (siehe "Static Routes bearbeiten (Network Interfaces)" auf Seite 246).

➢ *So konfigurieren Sie den Aktiv/Aktiv-Modus in CC-SG:*

1. Wählen Sie Administration > Konfiguration.
2. Klicken Sie auf die Registerkarte Netzwerksetup.
3. Wählen Sie Aktiv/Aktiv-Modus.
4. Geben Sie den CC-SG-Hostnamen in das Feld Hostname ein. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben. Wenn Sie zum Speichern der Konfiguration auf Konfiguration aktualisieren klicken, wird das Feld Hostname aktualisiert, um den vollständig qualifizierten Domänennamen (Fully-Qualified Domain Name, FQDN) anzuzeigen, wenn ein DNS und Domänensuffix konfiguriert wurden.
5. Konfigurieren Sie das primäre LAN in der linken und das sekundäre LAN in der rechten Spalte:
6. Klicken Sie auf den Pfeil neben der Dropdown-Liste Konfiguration, und wählen Sie entweder DHCP oder Statisch.

   DHCP:

   - Wenn Sie DHCP auswählen, werden die Felder Primärer DNS-Server, Sekundärer DNS-Server, Domänensuffix, IP-Adresse, Subnetzmaske und Standardgateway automatisch belegt (falls Ihr DHCP-Server für die Bereitstellung dieser Informationen konfiguriert wurde), sobald Sie diese Netzwerkeinrichtung speichern und CC-SG neu starten.

- Mithilfe der Informationen, die der DHCP-Server bereitstellt, wird CC-SG dynamisch beim DNS-Server registriert, wenn dieser dynamische Aktualisierungen annimmt.
- Weitere Informationen finden Sie unter ***Empfohlene DHCP-Konfigurationen für CC-SG*** (auf Seite 184).

Statisch:

- Wenn Sie Statisch auswählen, geben Sie einen Wert für den primären DNS-Server, den sekundären DNS-Server, das Domänensuffix, die IP-Adresse und die Subnetzmaske in die entsprechenden Felder ein.
- Legen Sie nur ein Standardgateway fest.

7. Klicken Sie auf den Pfeil neben der Dropdown-Liste Adaptergeschwindigkeit, und wählen Sie in der Liste eine Geschwindigkeit aus. Stellen Sie sicher, dass Ihre Auswahl mit der Adapterporteinstellung des Switch übereinstimmt.
8. 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 Automatisch ausgewählt haben, klicken Sie auf den Pfeil neben der Dropdown-Liste Adaptermodus, und wählen Sie einen Duplexmodus in der Liste aus.
9. Klicken Sie auf Konfiguration aktualisieren, um die Änderungen zu speichern. CC-SG wird neu gestartet.

Empfohlene DHCP-Konfigurationen für CC-SG

Lesen Sie die folgenden empfohlenen DHCP-Konfigurationen. Stellen Sie sicher, dass Ihr DHCP-Server richtig eingerichtet ist, bevor Sie CC-SG zur Verwendung von DHCP konfigurieren.

- Konfigurieren Sie den DHCP-Server so, dass die IP-Adresse von CC-SG statisch zugeordnet wird.
- Konfigurieren Sie den DHCP- und DNS-Server so, dass sie CC-SG beim DNS-Server automatisch registrieren, wenn der DHCP-Server dem CC-SG eine IP-Adresse zuordnet.
- Konfigurieren Sie den DNS-Server so, dass es nicht authentifizierte dynamische Domain-Name-System (DDNS)-Registrierungsanforderungen von CC-SG annimmt.

Protokollaktivitäten konfigurieren

Sie können CC-SG so konfigurieren, dass Berichte auf externen Protokollservern erstellt werden. Sie können festlegen, welche Nachrichtenebene in jedem Protokoll enthalten sein soll.

➢ *So konfigurieren Sie die CC-SG-Protokollaktivität:*

1. Wählen Sie **Administration** > **Konfiguration**.
2. Klicken Sie auf die Registerkarte **Protokolle**.
3. Sie können einen externen Protokollserver, der von CC-SG verwendet werden soll, zuordnen, indem Sie die IP-Adresse in das Feld **Serveradresse** unter **Primärer Server** eingeben
4. Klicken Sie auf den Pfeil neben der Dropdown-Liste **Weiterleitungsebene**, und wählen Sie eine Schweregradebene für das Ereignis 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 Schweregradebene aus. Alle Ereignisse auf dieser Ebene oder höher werden an das interne Protokoll von CC-SG weitergeleitet.
7. Klicken Sie auf **Konfiguration aktualisieren**, um die Änderungen zu speichern.

Interne CC-SG-Protokolle leeren

Sie können interne CC-SG-Protokolle löschen. Bei diesem Vorgang werden keine Ereignisse gelöscht, die auf Ihren externen Protokollservern aufgezeichnet sind.

Hinweis: *Der Überwachungslistenbericht und Fehlerprotokollbericht basieren auf dem internen CC-SG-Protokoll. Wenn Sie das interne CC-SG-Protokoll leeren, werden diese beiden Berichte ebenfalls geleert. Sie können diese Berichte auch einzeln leeren.* **Berichtsdaten aus CC-SG leeren** *(auf Seite 149)*

➢ *So leeren Sie das interne CC-SG-Protokoll:*

1. Wählen Sie **Administration** > **Konfiguration**.
2. Klicken Sie auf die Registerkarte **Protokolle**.

3. Klicken Sie auf **Leeren**.
4. Klicken Sie auf **Ja**.

CC-SG-Serverzeit und -datum konfigurieren

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 unter *Aufgabenmanager* **(auf Seite 214). Die Uhrzeit, die auf Ihrem Client-PC eingestellt ist, unterscheidet sich eventuell von der auf CC-SG eingestellten Uhrzeit.**

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

In einer Clusterkonfiguration kann die Zeitzone nicht geändert werden.

➢ *So konfigurieren Sie die Serveruhrzeit und das Datum von CC-SG:*

1. Wählen Sie Administration >Konfiguration.
2. Klicken Sie auf die Registerkarte **Uhrzeit/Datum**.
   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 den Pfeil neben der 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. Wählen Sie **Systemwartung** > **Neu starten**, um CC-SG neu zu starten.

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.

Für die CC-SG-V1- oder -E1-Modelle steht kein Modem zur Verfügung und kann auch nicht konfiguriert werden.

CC-SG konfigurieren

1. Wählen Sie Administration > Konfiguration. Klicken Sie im Fenster Konfigurationsmanager auf die Registerkarte Modem.
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 Änderungen 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**.
2. Klicken Sie auf die Registerkarte **Modems**.
3. Klicken Sie auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Erweitert**.
5. Geben Sie einen Initialisierungsbefehl in das 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 zum Speichern der Änderungen auf **OK**.

Modemverbindungen konfigurieren

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

1. Wählen Sie **Start** > **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**.
4. Klicken Sie auf **Weiter**, **Verbindung mit dem Netzwerk am Arbeitsplatz herstellen**, **DFÜ-Verbindung**.
5. Geben Sie einen Namen für die Verbindung zu CC-SG ein.

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.
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. Klicken Sie im nächsten Fenster auf **Eigene Verwendung**, damit die Verbindung nur Ihnen zur Verfügung steht.
9. Klicken Sie im letzten Fenster auf **Fertig stellen**, um Ihre Änderungen zu speichern.

Rückrufverbindung konfigurieren

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

1. Wählen Sie **Start** > **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**.
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:

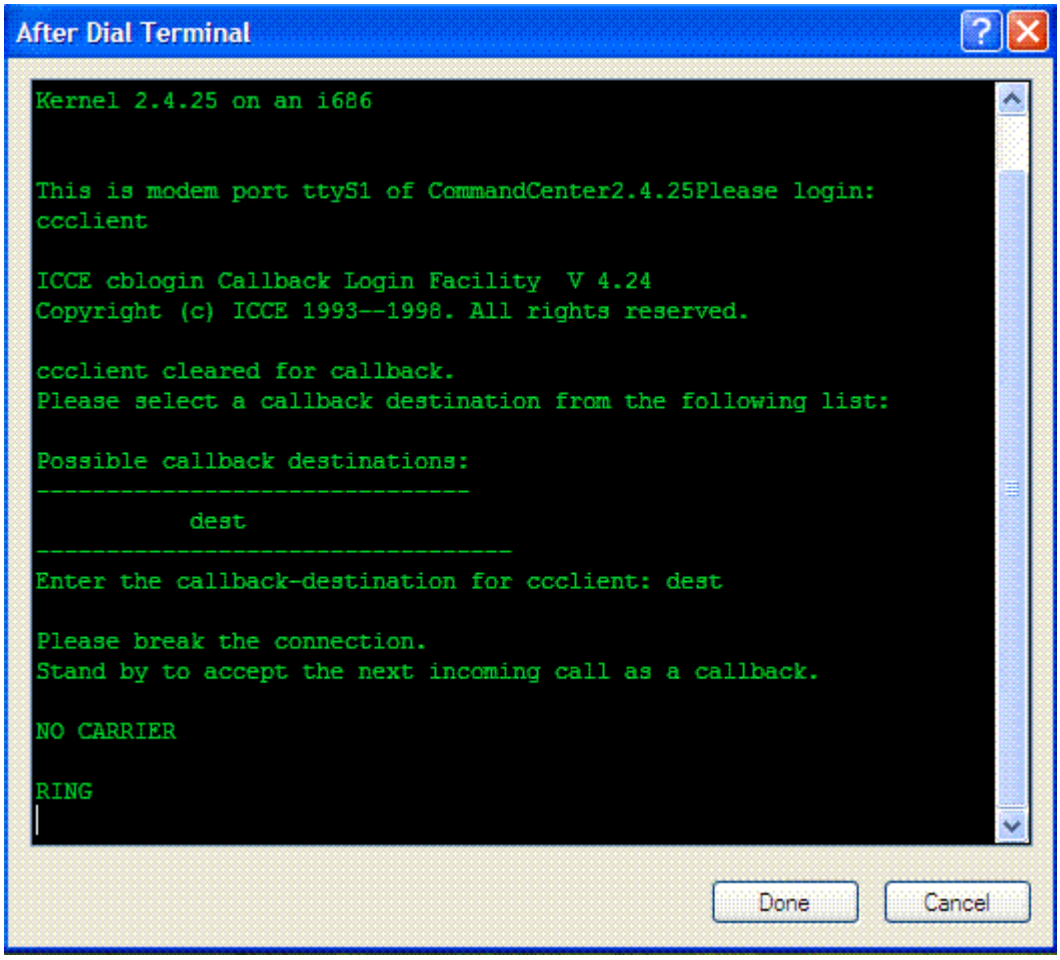
```
proc main
delay 1
waitfor "ogin:"
transmit "ccclient^M"
waitfor "client:"
transmit "dest^M"
waitfor "callback."
transmit "ATH^M"
waitfor "RING"
transmit "ATA^M"
waitfor "CONNECT"
waitfor "ogin:"
transmit "ccclient^M"
endproc
```

Mit CC-SG über ein Modem verbinden

➢ *So verbinden Sie mit CC-SG über ein Modem:*

1. Wählen Sie **Start** > **Netzwerkumgebung**.
2. Klicken Sie auf **Netzwerkverbindungen anzeigen**.
3. Doppelklicken Sie auf die erstellte Modemverbindung.
4. Geben Sie den Benutzernamen **ccclient** und das Kennwort **cbupass** ein.
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. Wenn **Terminalfenster einblenden** markiert war, wie es in **Rückrufverbindung konfigurieren** (auf Seite 189) beschrieben wurde, wird ein Terminal nach dem Wählen angezeigt.



8. Warten Sie 1 bis 2 Minuten. Geben Sie dann in einem unterstützten Browser die IP-Adresse von CC-SG ein, die auf dem CC-SG im **Konfigurationsmanager** auf der Registerkarte **Modem** als die **Serveradresse** konfiguriert wurde. Melden Sie sich dann bei CC-SG an.

Verbindungsmodi: Direkt und Proxy

Verbindungsmodi

CC-SG bietet drei Verbindungsmodi für Out-of-Band-Verbindungen zu Raritan-Geräteports: Direkt, Proxy und Beides, d. h. eine Kombination aus Direkt und Proxy.

- Im Direktmodus können Sie eine Verbindung direkt zu einem Knoten oder Port herstellen, ohne Daten durch CC-SG zu leiten. Der Direktmodus bietet im Allgemeinen schnellere Verbindungen.
- Im Proxymodus können Sie eine Verbindung zu einem Knoten oder Port herstellen, indem Sie alle Daten durch CC-SG leiten. Der Proxymodus erhöht die Last auf Ihren CC-SG-Server, wodurch eventuell langsamere Verbindungen verursacht werden. Der Proxymodus wird jedoch empfohlen, wenn Ihnen die Sicherheit der Verbindung sehr wichtig ist. Sie müssen jedoch nur die TCP-Ports des CC-SG (80, 443 und 2400) in der Firewall geöffnet lassen.
- Im Beides-Modus können Sie CC-SG so konfigurieren, dass eine Kombination aus dem Direkt- und Proxymodus verwendet wird. Im Beides-Modus ist der Proxymodus die Standardeinstellung. Sie können CC-SG jedoch so konfigurieren, den Direktmodus zu verwenden, wenn Verbindungen mit Client-IP-Adressen aus festgelegten Bereichen hergestellt werden.

Wichtig! Wenn CC-SG im Proxymodus oder im Beides-Modus ist, können Sie Benutzern keinen Zugriff auf virtuelle Medien geben.

Direktmodus für alle Client-Verbindungen konfigurieren

1. Wählen Sie **Administration** > **Konfiguration**.
2. Klicken Sie auf die Registerkarte **Verbindungsmodus**.
3. Wählen Sie **Direktmodus**.
4. Klicken Sie auf **Konfiguration aktualisieren**.

Proxymodus für alle Client-Verbindungen konfigurieren

1. Wählen Sie **Administration** > **Konfiguration**.
2. Klicken Sie auf die Registerkarte **Verbindungsmodus**.
3. Wählen Sie **Proxymodus**.
4. Klicken Sie auf **Konfiguration aktualisieren**.

Kombination aus Direktmodus und Proxymodus konfigurieren:

Wenn Sie CC-SG zur Verwendung einer Kombination aus Direktmodus und Proxymodus konfigurieren, ist der Proxymodus der Standardverbindungsmodus. Der Direktmodus wird für die Client-IP-Adressen verwendet, die Sie festlegen.

1. Wählen Sie **Administration** > **Konfiguration**.
2. Klicken Sie auf die Registerkarte **Verbindungsmodus**.
3. Wählen Sie **Beides**.
4. Legen Sie in den Feldern **Netzwerkadresse** und **Netzmaske** den Client-IP-Adressbereich fest, der eine Verbindung zu Knoten und Ports über den Direktmodus herstellen soll. Klicken Sie dann auf **Hinzufügen**.
5. Klicken Sie auf **Konfiguration aktualisieren**.

Geräteeinstellungen

1. Wählen Sie **Administration** > **Konfiguration**.
2. Klicken Sie auf die Registerkarte **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 Zeitlimitdauer eines Geräts geben Sie eine neue Zeitlimitdauer in das Feld **Heartbeat (Sek.)** ein.
5. Klicken Sie auf **Konfiguration aktualisieren**, um die Änderungen zu speichern. Eine Meldung wird zur Bestätigung angezeigt, dass alle zugewiesenen Geräteeinstellungen aktualisiert wurden.

SNMP konfigurieren

SNMP und CC-SG

Mit Simple Network Management Protocol (SNMP) sendet CC-SG SNMP-Traps (Ereignisbenachrichtigungen) zu einem SNMP-Manager im Netzwerk. Sie sollten Erfahrung im Umgang mit der SNMP-Infrastruktur haben, um CC-SG zur Verwendung mit SNMP zu konfigurieren.

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

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. ***SNMP-Traps*** (auf Seite 289). Sie finden die benutzerdefinierte MIB-Datei auf der Support-Website von Raritan.

So konfigurieren Sie SNMP in CC-SG:

1. Wählen Sie **Administration** > **Konfiguration**.
2. Klicken Sie auf die Registerkarte **SNMP**.
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 Lesezugriff** 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 Änderungen zu speichern.

5. Markieren Sie **SNMP-Traps aktivieren**, um das Senden von SNMP-Traps von CC-SG zu einem SNMP-Host zu aktivieren.
6. Markieren 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, beispielsweise einen Festplattenfehler, und **Anwendungsprotokoll**-Traps für Benachrichtigungen, die von Ereignissen in der CC-Anwendung erstellt werden, beispielsweise Änderungen des Benutzerkontos. Zum Aktivieren von Traps nach Typ markieren 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 unter **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 Fensterbereich **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. In dieser Liste können beliebig viele Manager festgelegt werden.
10. Klicken Sie auf **Trap-Konfiguration aktualisieren**, um die Änderungen zu speichern.

CC-SG-Cluster konfigurieren

Was ist ein CC-SG-Cluster?

Ein CC-SG-Cluster verwendet zwei CC-SG-Knoten: einen primären Knoten und einen sekundären Knoten, der zur Sicherheit dient, falls der primäre Knoten ausfällt. Für beide Knoten werden gemeinsame Daten für aktive Benutzer und Verbindungen verwendet, und alle Statusdaten werden zwischen den beiden Knoten repliziert.

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 verbundenen Geräte erkennen, dass der primäre Knoten nicht reagiert und reagieren auf Anforderungen des sekundären Knotens.

Anforderungen für CC-SG-Cluster

- Der primäre und sekundäre Knoten in einem Cluster müssen mit der gleichen Firmware und mit dem gleichen Hardware-Modell (G1, V1 oder E1) ausgeführt werden.
- CC-SG muss sich zur Verwendung von Clustering im **Primär-/Sicherungsmodus** befinden. Clustering funktioniert nicht, wenn die Konfiguration Aktiv/Aktiv ausgewählt wurde. Weitere Informationen finden Sie unter ***Netzwerkeinrichtung*** (auf Seite 178).
- Die Einstellungen für das Datum, die Uhrzeit und die Zeitzone werden nicht vom primären Knoten auf den sekundären Knoten übertragen. Sie müssen diese Einstellungen auf jedem CC-SG konfigurieren, bevor Sie den Cluster erstellen.

CC-SG-Cluster und CC-NOC

In einer Clusterkonfiguration kommuniziert nur der primäre Knoten mit CC-NOC. Wird ein CC-SG der primäre Knoten, wird seine IP-Adresse mit der IP-Adresse des sekundären Knotens 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.

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.

Wichtig: Vor dem Erstellen eines Clusters sollten Sie die Konfiguration auf beiden CC-SG-Einheiten sichern.

➢ *1. Primären CC-SG-Knoten einrichten*

1. Wählen Sie **Administration** > **Clusterkonfiguration**.
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**.
3. Geben Sie in das Feld **Clustername** einen Namen für diesen 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**. Eine Meldung wird angezeigt.
5. Klicken Sie auf **Ja**. Der CC-SG, den Sie gegenwärtig verwenden, wird der primäre Knoten.

➢ *2. 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**.
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 primären Knotens 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 Status Sekundär zuzuordnen.

   Wichtig! Wenn Sie den Verbindungsvorgang gestartet haben, sollten Sie keine weiteren Funktionen in CC-SG durchführen, bis der Verbindungsvorgang abgeschlossen ist.

6. Der neu ausgewählte sekundäre Knoten wird neu gestartet. Dieser Vorgang dauert einige Minuten. Nach dem abgeschlossenen Neustart wird eine Bestätigungsmeldung angezeigt.
7. Wählen Sie **Administration** > **Clusterkonfiguration**, um die aktualisierte Tabelle Clusterkonfiguration anzuzeigen.

Sekundären CC-SG-Knoten entfernen

Durch das Entfernen eines sekundären bzw. Sicherungsknotens wird die Zuweisung des sekundären Knotens entfernt. Die CC-SG-Sekundäreinheit wird nicht aus der Konfiguration gelöscht.

➢ *So entfernen Sie den Sekundärknotenstatus von einer CC-SG-Einheit:*

1. Markieren Sie den sekundären CC-SG-Knoten in der Tabelle Clusterkonfiguration.
2. Klicken Sie auf **Sicherungsknoten entfernen**.
3. Klicken Sie auf **Ja**, um den Sekundärknotenstatus zu entfernen.

Primären CC-SG-Knoten entfernen

Durch das Entfernen eines Clusters wird die primäre CC-SG-Einheit nicht aus der Konfiguration entfernt, sondern nur ihre Zuweisung als primärer Knoten. Cluster entfernen ist nur möglich, wenn kein Sicherungsknoten vorhanden ist.

➢ *So entfernen Sie den Primärknotenstatus von einer CC-SG-Einheit:*

1. Markieren Sie den primären CC-SG-Knoten in der Tabelle Clusterkonfiguration.
2. Klicken Sie auf **Cluster entfernen**.

3. Klicken Sie auf **Ja**, um den Primärknotenstatus zu entfernen.

Ausgefallenen CC-SG-Knoten wiederherstellen

Wenn ein Knoten ausfällt und Ausfallsicherheit eintritt, wird der ausgefallene Knoten im Status Warten wiederhergestellt. Befindet sich ein Knoten im Status Warten, kann er entweder im Modus Eigenständig oder im Modus Sicherungsknoten gestartet werden.

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 Status Sekundär zuzuordnen.
4. Der sekundäre Knoten wird neu gestartet. Dieser Vorgang dauert einige Minuten. Nach dem abgeschlossenen Neustart wird eine Bestätigungsmeldung angezeigt.

Erweiterte Clustereinstellungen

In einer Clusterkonfiguration können Sie die Zeitzone nicht ändern.

➢ *So konfigurieren Sie die erweiterten Clustereinstellungen:*

1. Wählen Sie den primären Knoten aus.
2. Klicken Sie auf **Erweitert**. Das Fenster **Erweiterte Einstellungen** wird angezeigt.
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. Sie sollten für Cluster mit weit voneinander entfernt liegenden Knoten lange Intervalle festlegen.

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 zum Speichern der Änderungen auf **OK**.

Sicherheitsmanager

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

Remoteauthentifizierung

Weitere Informationen zum Konfigurieren von Servern für die Remoteauthentifizierung finden Sie unter ***Remoteauthentifizierung*** (auf Seite 123).

AES-Verschlüsselung

Sie können CC-SG so konfigurieren, dass AES 128-Verschlüsselung zwischen dem Client und CC-SG-Server erforderlich ist. Wenn die AES-Verschlüsselung erforderlich ist, müssen alle Benutzer mit einem AES-fähigen Client auf CC-SG zugreifen. Wenn die AES-Verschlüsselung erforderlich ist und Sie versuchen, mit einem Browser, der nicht AES-fähig ist, auf CC-SG zuzugreifen, können Sie keine Verbindung mit CC-SG herstellen.

Browser auf AES-Verschlüsselung überprüfen

Wenn Sie nicht wissen, ob Ihr Browser AES verwendet, wenden Sie sich an den Browserhersteller.

Sie können auch die folgende Website mit dem Browser, dessen Verschlüsselungsmethode Sie überprüfen möchten, besuchen: ***https://www.fortify.net/sslcheck.html*** https://www.fortify.net/sslcheck.html. Diese Website erkennt die Verschlüsselungsmethode Ihres Browsers und zeigt einen Bericht an. Raritan ist dieser Website nicht angeschlossen.

AES-Verschlüsselung zwischen Client und CC-SG voraussetzen

Im Sicherheitsmanager können Sie CC-SG so konfigurieren, dass eine AES-Verschlüsselung für Sitzungen zwischen dem Client und CC-SG-Server vorausgesetzt wird.

1. Wählen Sie **Administration** > **Sicherheit**.

2. Öffnen Sie die Registerkarte **Verschlüsselung**.
3. Markieren Sie das Kontrollkästchen **AES-Verschlüsselung zwischen Client und Server voraussetzen**.
4. In einer Meldung werden Sie darüber informiert, dass die Clients AES-Verschlüsselung zur Verbindung zu CC-SG verwenden müssen, sobald diese Option ausgewählt wurde. Klicken Sie zum Bestätigen auf **OK**.
   - Im Feld **Schlüssellänge** wird 128 angezeigt. Die 128-Bit-Verschlüsselung wird zwischen dem Client und CC-SG-Server vorausgesetzt.
   - Im Feld **Browser-Verbindungsprotokoll** ist HTTPS/SSL ausgewählt.
5. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Browser-Verbindungsprotokoll konfigurieren: HTTP oder HTTPS/SSL

Im Sicherheitsmanager können Sie CC-SG so konfigurieren, dass entweder normale HTTP-Verbindungen von Clients verwendet oder HTTPS/SSL-Verbindungen vorausgesetzt werden. Sie müssen CC-SG neu starten, damit diese Einstellungen übernommen werden können.

1. Wählen Sie **Administration** > **Sicherheit**.
2. Öffnen Sie die Registerkarte **Verschlüsselung**.
3. Wählen Sie die Option **HTTP** oder **HTTPS/SSL**, um das Browser-Verbindungsprotokoll festzulegen, das Clients bei der Verbindung zu CC-SG verwenden sollen.
4. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Portnummer für SSH-Zugriff auf CC-SG einstellen

Im Sicherheitsmanager können Sie die Portnummer einstellen, die Sie für den SSH-Zugriff auf CC-SG verwenden möchten. Weitere Informationen finden Sie unter **SSH-Zugriff auf CC-SG** (auf Seite 226).

➢ *So stellen Sie die Portnummer für SSH-Zugriff auf CC-SG ein:*

1. Wählen Sie **Administration** > **Sicherheit**.
2. Geben Sie auf der Registerkarte **Verschlüsselung** die Portnummer für den Zugriff auf CC-SG über SSH in das Feld **SSH-Serverport** ein.
3. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Anmeldeeinstellungen

Auf der Registerkarte **Anmeldeeinstellungen** können Sie die **Einstellungen für sichere Kennwörter** und **Sperreinstellungen** konfigurieren.

Anmeldeeinstellungen anzeigen

1. Wählen Sie **Administration** > **Sicherheit**.
2. Klicken Sie auf die Registerkarte **Anmeldeeinstellungen**.

Sichere Kennwörter für alle Benutzer voraussetzen

1. Wählen Sie **Administration** > **Sicherheit**.
2. Öffnen Sie die Registerkarte **Anmeldeeinstellungen**.
3. Markieren Sie das Kontrollkästchen **Sichere Kennwörter für alle Benutzer erforderlich**.
4. Wählen Sie eine **Maximale Kennwortlänge**. Kennwörter müssen weniger als die maximale Anzahl an Zeichen enthalten.
5. Wählen Sie eine **Länge der Kennwortchronik**. Diese Zahl legt fest, wie viele vorherige Kennwörter in der Chronik gespeichert werden und nicht erneut verwendet werden können. Ist **Länge der Kennwortchronik** beispielsweise auf 5 festgelegt, können Benutzer keines ihrer vorherigen 5 Kennwörter verwenden.
6. Wählen Sie einen **Kennwort-Ablaufintervall**. Alle Kennwörter laufen nach einer festgelegten Anzahl an Tagen ab. Nachdem ein Kennwort abgelaufen ist, müssen Benutzer beim nächsten Anmelden ein neues Kennwort eingeben.
7. Wählen Sie **Anforderungen für sichere Kennwörter**:
   - 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.
8. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

CC-SG-Kennwörter

Alle Kennwörter müssen jedes Kriterium erfüllen, das der Administrator konfiguriert. Nach der Konfiguration der Regeln für sichere Kennwörter müssen alle zukünftigen Kennwörter diese Kriterien erfüllen. 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 verwaltet werden.

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

Regeln für sichere Kennwörter zwingen Benutzer beim Erstellen von Kennwörtern zur Beachtung strikter Richtlinien. Diese erschweren das Erraten von Kennwörtern und tragen damit zur Erhöhung der Kennwortsicherheit bei. Sichere Kennwörter sind standardmäßig nicht in CC-SG aktiviert. Ein sicheres Kennwort, das alle Parameter für sichere Kennwörter umfasst, ist für den CC-Superuser grundsätzlich erforderlich.

Sie können die Funktion **Tipp des Tages** verwenden, 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 an fehlgeschlagenen Anmeldeversuchen sperren. Diese Funktion gilt für Benutzer, die von CC-SG lokal authentifiziert und autorisiert werden. Sie gilt nicht für Benutzer, für die Remoteauthentifizierung auf externen Servern verwendet wird. Weitere Informationen finden Sie unter ***Remoteauthentifizierung konfigurieren*** (siehe "Remoteauthentifizierung" auf Seite 123).

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

➢ *So aktivieren Sie die Sperre:*

1. Wählen Sie Administration > Sicherheit.
2. Öffnen Sie die Registerkarte Anmeldeeinstellungen.

3. Markieren Sie Sperre aktiviert.
4. 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.
5. Wählen Sie eine Sperrstrategie aus:
   - Sperre für Zeitraum: Legen Sie den Zeitraum in Minuten fest, den Benutzer gesperrt werden, bevor sie sich wieder anmelden können. Der Standardwert ist 5 Minuten. Sie können einen Zeitraum von 1 Minute bis zu 1440 Minuten (24 Stunden) festlegen. 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.
   - Sperre, bis Administrator Zugriff zulässt: Benutzer werden gesperrt, bis ein Administrator die Sperre für das Benutzerkonto aufhebt.
6. (Optional) Geben Sie in das Feld E-Mail-Benachrichtigung über Sperre eine E-Mail-Adresse ein. Die Benachrichtigung wird an diese E-Mail-Adresse gesendet, wenn eine Sperre verhängt wurde. Ist das Feld leer, wird keine Benachrichtigung gesendet.
7. (Optional) Geben Sie in das Feld Telefonnummer des Administrators eine Telefonnummer ein. Die Telefonnummer wird in der E-Mail-Benachrichtigung, die bei einer Sperre gesendet wird, angezeigt.
8. Klicken Sie zum Speichern der Änderungen auf Aktualisieren.

➢ *So deaktivieren Sie die Sperre:*

Wenn Sie die Sperre deaktivieren, dürfen sich alle Benutzer, die zurzeit in CC-SG gesperrt sind, wieder anmelden.

1. Wählen Sie Administration > Sicherheit.
2. Öffnen Sie die Registerkarte Anmeldeeinstellungen.
3. Deaktivieren Sie das Kontrollkästchen Sperre aktiviert.
4. Klicken Sie zum Speichern der Änderungen auf Aktualisieren.

Gleichzeitige Anmeldung von Benutzern zulassen

Sie können mehrere gleichzeitige CC-SG-Sitzungen mit demselben Benutzernamen zulassen.

1. Wählen Sie **Administration** > **Sicherheit**.

2. Öffnen Sie die Registerkarte **Anmeldeeinstellungen**.
   - Markieren Sie **Superuser**, wenn Sie mehr als eine gleichzeitige Anmeldung mit dem CC-Superuser-Konto zulassen möchten.
   - Markieren Sie **Systemadministratoren**, wenn Sie gleichzeitige Anmeldungen von Benutzern der Benutzergruppe **Systemadministratoren** zulassen möchten.
   - Markieren Sie **Alle anderen Benutzer**, wenn Sie gleichzeitige Anmeldungen von allen anderen Benutzern zulassen möchten.
3. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Leerlaufzeitgeber konfigurieren

Sie können den Leerlaufzeitgeber konfigurieren, um festzulegen, wie lange eine CC-SG-Sitzung inaktiv bleiben kann, bevor der Benutzer bei CC-SG abgemeldet wird.

Wenn ein Benutzer Verbindungen zu Knoten offen hat, wird die Sitzung als aktiv betrachtet, und der Benutzer wird nicht abgemeldet, wenn der Leerlaufzeitgeber abläuft.

➢ *So konfigurieren Sie den Leerlaufzeitgeber:*

1. Wählen Sie **Administration** > **Sicherheit**.
2. Öffnen Sie die Registerkarte **Anmeldeeinstellungen**.
3. Geben Sie das gewünschte Zeitlimit in das Feld **Leerlaufzeit** ein.
4. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

Portal

Über Portaleinstellungen können Administratoren ein Logo und eine Zugriffsvereinbarung konfigurieren, die Benutzern beim Zugriff auf CC-SG angezeigt werden.

➢ *So konfigurieren Sie die Portaleinstellungen:*

1. Wählen Sie **Administration** > **Sicherheit**.
2. Öffnen Sie die Registerkarte **Portal**.

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 ein 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. Klicken Sie auf **Vorschau**, um das Logo anzuzeigen. Die ausgewählte Grafikdatei wird rechts angezeigt.
4. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**.

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.

➢ *So fügen Sie vertragliche Einschränkungen der Serviceleistungen zum CC-SG-Anmeldebildschirm hinzu:*

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. So geben Sie Ihre Meldung ein:
   a. Markieren Sie das Kontrollkästchen **Vertragliche Einschränkungen der Serviceleistungen - Meldung**, wenn Sie den Bannertext direkt eingeben möchten.

- Geben Sie die Meldung in das angezeigte Feld ein. Der Text darf höchstens 10.000 Zeichen umfassen.
- Klicken Sie auf das Dropdown-Menü **Schriftart**, und wählen Sie die Schriftart für die Meldung aus.
- Klicken Sie auf das Dropdown-Menü **Größe**, und wählen Sie die Schriftgröße für die Meldung aus.

b. Markieren Sie **Vertragliche Einschränkungen der Serviceleistungen - Datei**, wenn Sie eine Meldung aus einer Textdatei (TXT) verwenden möchten.

- Klicken Sie auf **Durchsuchen**. Ein Fenster wird angezeigt.
- Wählen Sie im Fenster die Textdatei mit der Meldung aus, die Sie verwenden möchten, und klicken Sie auf **Öffnen**. Der Text darf höchstens 10.000 Zeichen umfassen.
- Klicken Sie auf **Vorschau**, um den Text, der in der Datei enthalten ist, anzuzeigen. Die Vorschau wird im Feld für die Bannermeldung oben angezeigt.

3. Klicken Sie zum Speichern der Änderungen auf **Aktualisieren**. Die Neuigkeiten werden auf dem Anmeldebildschirm angezeigt, sobald ein Benutzer das nächste Mal auf CC-SG zugreift.

Zertifikate

Auf der Registerkarte Zertifikat können Sie eine Anforderung für die Zertifikatsignatur (certificate signing request, CSR), die zur Beantragung eines digitalen Identitätszertifikats an eine Zertifizierungsstelle gesendet wird, und ein selbstsigniertes Zertifikat erstellen oder Zertifikate und die entsprechenden privaten Schlüssel importieren und exportieren.

Zertifikate – Aufgaben

***Hinweis**: Die Schaltfläche unten im Bildschirm zeigt abhängig von der ausgewählten Zertifikatsoption **Exportieren**, **Importieren** oder **Erzeugen** an.*

➢ *Aktuelles Zertifikat und privaten Schlüssel exportieren*

1. Wählen Sie **Administration** > **Sicherheit**.
2. Klicken Sie auf die Registerkarte **Zertifikat**.
3. Wählen Sie **Aktuelles Zertifikat und privaten Schlüssel exportieren**.
4. Klicken Sie auf **Exportieren**.

Das Zertifikat wird im Fensterbereich **Zertifikat** und der private Schlüssel im Fensterbereich **Privater Schlüssel** angezeigt.

5. Markieren Sie in jedem Fensterbereich den Text, und drücken Sie dann Strg+C, um den Text zu kopieren. Anschließend können Sie den Text an jeder beliebigen Stelle einfügen.

➢ *Anforderung für die Zertifikatsignatur erstellen sowie eingefügtes Zertifikat und privaten Schlüssel importieren*

Die CSR wird an den Zertifikatserver übermittelt, der ein signiertes Zertifikat ausgibt. Außerdem wird ein Stammzertifikat vom Zertifikatserver exportiert und in einer Datei gespeichert. Nach dem Erhalt des signierten Zertifikats von der Zertifizierungsstelle für Zertifikate können Sie das signierte Zertifikat, das Stammzertifikat und den privaten Schlüssel importieren.

1. Wählen Sie **Administration** > **Sicherheit**.
2. Klicken Sie auf die Registerkarte **Zertifikat**.
3. Klicken Sie auf **Anforderung für Zertifikatsignatur erzeugen** und dann auf **Erzeugen**. Das Fenster Anforderung für Zertifikatsignatur erzeugen wird angezeigt.
4. Geben Sie die angeforderten Daten in die Felder ein.
   a. Verschlüsselungsmodus: Wenn nach Auswahl von Administration > Sicherheit > Verschlüsselung die Option **AES-Verschlüsselung zwischen Client und Server voraussetzen** ausgewählt wird, ist AES-128 die Standardeinstellung. Ist AES nicht erforderlich, ist 3DES die Standardeinstellung.
   b. Länge des privaten Schlüssels: Der Standardwert beträgt 1024.
   c. Gültigkeitsdauer (in Tagen): maximal 4 numerische Zeichen.
   d. Ländercode: CSR-Tag ist Country Name.
   e. Bundesland oder Kanton: maximal 64 Zeichen. Geben Sie den vollständigen Namen des Bundeslands oder Kantons ein. Abkürzungen sind nicht zulässig.
   f. Stadt/Ort: CSR-Tag ist Locality Name. Maximal 64 Zeichen.
   g. Name des registrierten Unternehmens: CSR-Tag ist Organization Name. Maximal 64 Zeichen.
   h. Abteilung: CSR-Tag ist Organization Unit Name. Maximal 64 Zeichen.

i. Vollständiger Name der Domäne (FQDN): CSR-Tag ist Common Name. Das registrierte Unternehmen muss den Domänennamen für Anforderungen für Zertifikatsignatur besitzen. Die Zertifizierungsstelle lehnt die Anforderung ab, wenn das registrierte Unternehmen den Domänennamen nicht besitzt.

j. Zusätzliches Kennwort: maximal 64 Zeichen.

k. E-Mail-Adresse des Administrators: Geben Sie die E-Mail-Adresse des Administrators ein, der für die Zertifikatsanforderung verantwortlich ist.

5. Klicken Sie zum Erzeugen der Anforderung für Zertifikatsignatur auf **OK**. Die Anforderung für Zertifikatsignatur und der private Schlüssel werden in den entsprechenden Feldern im Fenster **Zertifikat** angezeigt.
6. Markieren Sie den Text im Kästchen Zertifikatsanforderung, und drücken Sie dann Strg+C, um den Text zu kopieren. Öffnen Sie einen ASCII-Editor wie Editor, und fügen Sie die Anforderung für Zertifikatsignatur in eine Datei ein, die Sie dann mit der Erweiterung **.cer** speichern.
7. Markieren Sie den Text im Kästchen Privater Schlüssel, und drücken Sie dann Strg+C, um den Text zu kopieren. Öffnen Sie einen ASCII-Editor wie Editor, und fügen Sie den privaten Schlüssel in eine Datei ein, die Sie dann mit der Erweiterung **.txt** speichern.
8. Übermitteln Sie die **.cer-Datei** an den Zertifikatserver, um ein signiertes Zertifikat zu erhalten.
9. 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.
10. Klicken Sie neben **Zertifizierungsstellendatei** auf **Durchsuchen**, und wählen Sie die Stammzertifikatdatei aus.
11. Markieren Sie nach Erhalt des signierten Zertifikats vom Zertifikatserver **Eingefügtes Zertifikat und privaten Schlüssel importieren**.
12. Kopieren Sie den Text des signierten Zertifikats, und drücken Sie dann Strg+V, um den Text im Kästchen Zertifikat einzufügen.
13. Kopieren Sie den Text des privaten Schlüssels, der bereits als TXT-Datei gespeichert wurde, und drücken Sie dann Strg+V, um den Text im Kästchen Privater Schlüssel einzufügen.

14. Geben Sie **raritan** in das Feld **Kennwort** ein, wenn die Anforderung für Zertifikatsignatur 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*

1. Wählen Sie **Administration** > **Sicherheit**.
2. Klicken Sie auf die Registerkarte **Zertifikat**.
3. Markieren Sie **Selbstsigniertes Zertifikat erzeugen**, und klicken Sie dann auf **Erzeugen**. Das Fenster **Selbstsigniertes Zertifikat erzeugen** wird geöffnet.
4. Geben Sie die angeforderten Daten in die Felder ein.
   a. Verschlüsselungsmodus: Wenn nach Auswahl von Administration > Sicherheit > Verschlüsselung die Option **AES-Verschlüsselung zwischen Client und Server voraussetzen** ausgewählt wird, ist AES-128 die Standardeinstellung. Ist AES nicht erforderlich, ist 3DES die Standardeinstellung.
   b. Länge des privaten Schlüssels: Der Standardwert beträgt 1024.
   c. Gültigkeitsdauer (in Tagen): maximal 4 numerische Zeichen.
   d. Ländercode: CSR-Tag ist Country Name.
   e. Bundesland oder Kanton: maximal 64 Zeichen. Geben Sie den vollständigen Namen des Bundeslands oder Kantons ein. Abkürzungen sind nicht zulässig.
   f. Stadt/Ort: CSR-Tag ist Locality Name. Maximal 64 Zeichen.
   g. Name des registrierten Unternehmens: CSR-Tag ist Organization Name. Maximal 64 Zeichen.
   h. Abteilung: CSR-Tag ist Organization Unit Name. Maximal 64 Zeichen.

i. Vollständiger Name der Domäne (FQDN): CSR-Tag ist Common Name. Das registrierte Unternehmen muss den Domänennamen für Anforderungen für Zertifikatsignatur besitzen. Die Zertifizierungsstelle lehnt die Anforderung ab, wenn das registrierte Unternehmen den Domänennamen nicht besitzt.

j. Zusätzliches Kennwort: maximal 64 Zeichen.

k. E-Mail-Adresse des Administrators: Geben Sie die E-Mail-Adresse des Administrators ein, der für die Zertifikatsanforderung verantwortlich ist.

5. Klicken Sie zum Erzeugen des Zertifikats auf **OK**. Das Zertifikat und der private Schlüssel werden im Fenster **Zertifikat** in den entsprechenden Feldern verschlüsselt angezeigt.

Zugriffssteuerungsliste

In einer IP-Zugriffssteuerungsliste sind die Bereiche von Client-IP-Adressen festgelegt, für die Sie den Zugriff auf CC-SG verweigern oder zulassen möchten. Jeder Eintrag in der Zugriffssteuerungsliste wird eine Regel, die bestimmt, ob ein Benutzer in einer bestimmten Gruppe und mit einer bestimmten IP-Adresse auf CC-SG zugreifen kann. Sie können auch Regeln einstellen, die für das gesamte CC-SG-System (wählen Sie ein System anstelle einer Benutzergruppe) auf einer Betriebssystemebene gelten. Beim Erstellen von Regeln können Sie die Regeln in der Liste anordnen, um die Reihenfolge festzulegen, in der sie angewendet werden. Regeln am Listenanfang haben Vorrang vor Regeln, die weiter unten in der Liste stehen.

➢ *So zeigen Sie die Zugriffssteuerungsliste an:*

1. Wählen Sie Administration > Sicherheit.
2. Öffnen Sie die Registerkarte Zugriffssteuerungsliste.

➢ *So fügen Sie der Zugriffssteuerungsliste eine Regel hinzu:*

1. Wählen Sie Administration > Sicherheit.
2. Öffnen Sie die Registerkarte Zugriffssteuerungsliste.
3. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile, um eine neue Zeile in die Tabelle einzufügen. 

4. Legen Sie einen Bereich von IP-Adressen fest, auf den die Regel angewendet werden soll. Geben Sie hierzu den Wert für die erste IP-Adresse in das Feld Von IP-Adresse und den Wert für die letzte IP-Adresse in das Feld Bis IP-Adresse ein.
5. Klicken Sie auf den Pfeil neben der Dropdown-Liste Gruppe, um eine Benutzergruppe auszuwählen, auf die die Regel angewendet werden soll. Wenn Sie System auswählen, gilt die Regel für das gesamte CC-SG-System.
6. Klicken Sie auf den Pfeil neben der Dropdown-Liste Aktion, und wählen Sie Zulassen oder Verweigern aus, um festzulegen, ob die im IP-Bereich festgelegten Benutzer auf CC-SG zugreifen können.
7. Klicken Sie zum Speichern der Änderungen auf Aktualisieren.

➢ *So fügen Sie der Zugriffssteuerungsliste eine Regel hinzu, die den Zugriff auf einer Betriebssystemebene zulässt oder verweigert:*

1. Wählen Sie Administration > Sicherheit.
2. Öffnen Sie die Registerkarte Zugriffssteuerungsliste.
3. Klicken Sie auf das Symbol zum Einfügen einer neuen Zeile, um eine neue Zeile in die Tabelle einzufügen. 
4. Legen Sie einen Bereich von IP-Adressen fest, auf den die Regel angewendet werden soll. Geben Sie hierzu den Wert für die erste IP-Adresse in das Feld Von IP-Adresse und den Wert für die letzte IP-Adresse in das Feld Bis IP-Adresse ein.
5. Wählen Sie Gruppe > System.
6. Klicken Sie auf den Pfeil neben der Dropdown-Liste Aktion, und wählen Sie Zulassen oder Verweigern aus, um festzulegen, ob die im IP-Bereich festgelegten Benutzer auf CC-SG zugreifen können.
7. Klicken Sie zum Speichern der Änderungen auf Aktualisieren.

➢ *So ändern Sie die Reihenfolge, in der CC-SG Regeln anwendet:*

1. Wählen Sie Administration > Sicherheit.
2. Öffnen Sie die Registerkarte Zugriffssteuerungsliste.
3. Wählen Sie die Regel aus, die Sie in der Liste nach oben oder unten verschieben möchten.

4. Klicken Sie auf den Pfeil nach oben oder unten, bis sich die Regel an der richtigen Position befindet.
5. Klicken Sie zum Speichern der Änderungen auf Aktualisieren.

➢ *So entfernen Sie eine Regel aus der Zugriffssteuerungsliste:*

1. Wählen Sie Administration > Sicherheit.
2. Öffnen Sie die Registerkarte Zugriffssteuerungsliste.
3. Wählen Sie die Regel aus, die Sie entfernen möchten, und klicken Sie dann auf das Symbol zum Entfernen einer Zeile. 
4. Klicken Sie zum Speichern der Änderungen auf 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. ***Aufgabenmanager*** (auf Seite 214) Nach der Konfiguration des SMTP-Servers können Sie eine Test-E-Mail an den festgelegten Empfänger senden und ihn über das Testergebnis informieren.

Externe SMTP-Server konfigurieren

1. Wählen Sie **Administration** > **Benachrichtigungen**.
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*** (auf Seite 2) beschrieben.
4. Geben Sie eine gültige SMTP-Portnummer in das 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 in das Feld **Von** ein, die kennzeichnet, dass die Nachricht von CC-SG ist.
8. Geben Sie in das Feld **Sendewiederholungen** die Anzahl an Wiederholungen ein, die die E-Mail erneut gesendet werden soll, falls der Vorgang fehlschlägt.
9. Geben Sie die Anzahl an 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 beispielsweise Gerätesicherungen alle drei Wochen an einem Freitag oder eine E-Mail mit einem bestimmten Bericht 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:

- CC-SG sichern
- Gerätekonfiguration sichern (einzelne Geräte oder Gerätegruppen)
- Gerätekonfiguration kopieren (einzelne Geräte oder Gerätegruppen)
- Gruppenstromversorgungssteuerung
- Ausgangs-Stromversorgungssteuerung
- Protokolle löschen
- Gerät neu starten
- Gerätekonfiguration wiederherstellen (gilt nicht für Gerätegruppen)
- Gerätefirmware aktualisieren (einzelne Geräte oder Gerätegruppen)
- Alle Berichte erstellen (HTML- oder CSV-Format)

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 für Aufgaben

Nach dem Durchführen einer Aufgabe kann eine E-Mail-Nachricht an einen bestimmten Empfänger gesendet werden. Sie können im ***Benachrichtigungsmanager*** (auf Seite 213) angeben, wo und wie die E-Mail gesendet wird (z. B. sicher über SSL).

Geplante Berichte

Geplante Berichte werden per E-Mail an die festgelegten Empfänger gesendet.

Alle Berichte mit dem Status **Fertig gestellt** werden im CC-SG für 30 Tage gespeichert. Sie können die fertig gestellten Berichte im HTML-Format anzeigen, indem Sie im Menü **Berichte** die Option **Geplante Berichte** auswählen. Weitere Informationen finden Sie unter ***Geplante Berichte*** (auf Seite 159).

Aufgaben planen

In diesem Abschnitt werden die meisten planbaren Aufgaben behandelt. Weitere Informationen zum Planen von Firmware-Aktualisierungen für Geräte finden Sie unter ***Firmware-Aktualisierung für Geräte planen*** (auf Seite 219).

➢ *So planen Sie eine Aufgabe:*

1. Wählen Sie **Administration** > **Aufgaben**.
2. Klicken Sie auf **Neu**.
3. Geben Sie auf der Registerkarte **Hauptfenster** einen Namen (1 bis 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 die Aufgaben aus, die Sie planen möchten. Beachten Sie, dass die erforderlichen Felder von der ausgewählten Aufgabe abhängen. In den folgenden Abschnitten finden Sie weitere Informationen zu jeder Aufgabe:
   - ***CC-SG sichern*** (auf Seite 163)
   - ***Gerätekonfiguration sichern*** (auf Seite 46)
   - ***Gerätekonfiguration kopieren*** (auf Seite 49)
   - ***Gruppenstromversorgungssteuerung*** (siehe "Stromversorgung für Knotengruppe steuern" auf Seite 18)
   - Ausgangs-Stromversorgungssteuerung: Weitere Informationen finden Sie im CC-SG-Benutzerhandbuch.
   - ***Protokolle löschen*** (siehe "Protokollaktivitäten konfigurieren" auf Seite 185)
   - ***Gerät neu starten*** (auf Seite 50)
   - ***Gerätekonfiguration wiederherstellen*** (auf Seite 47) (gilt nicht für Gerätegruppen)
   - ***Alle Berichte erstellen*** (siehe "Berichte" auf Seite 147)
   - ***Gerätefirmware aktualisieren*** (siehe "Firmware-Aktualisierung für Geräte planen" auf Seite 219) (einzelnes Gerät oder Gerätegruppe)

6. Klicken Sie auf die Registerkarte **Serie**. Die Registerkarte **Serie** ist für die Aufgabe ***Gerätefirmware aktualisieren*** (siehe "Firmware-Aktualisierung für Geräte planen" auf Seite 219) deaktiviert.
7. Klicken Sie im Feld **Zeitraum** auf das Optionsfeld, das dem Zeitraum entspricht, nach dem die geplante Aufgabe wieder ausgeführt werden soll.
   a. **Einmal:** Wählen Sie über die Pfeile nach oben und unten die **Startzeit** für die Aufgabe aus.
   b. **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 in das Feld **Wiederholungsintervall** ein, der zwischen Wiederholungen liegen soll. Klicken Sie auf das Dropdown-Menü, und wählen Sie die Zeiteinheit in der Liste aus.
   c. **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.
   d. **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.
   e. **Monatlich:** Geben Sie das Datum, an dem die Aufgabe ausgeführt werden soll, in das Feld **Tage** ein, und markieren Sie das Kontrollkästchen neben jedem Monat, in dem die Aufgabe an dem bestimmten Datum wiederholt werden soll.
   f. **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. Für die Aufgaben **Täglich**, **Wöchentlich**, **Monatlich** und **Jährlich** müssen Sie im Bereich **Serienbereich** eine Start- und Endzeit für jede Aufgabe hinzufügen. Wählen Sie die Zeit **Start um** und das **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, in das 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. 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 Kontrollkästchen **Bei Fehler**, um Empfänger über fehlgeschlagene Aufgaben zu unterrichten.
13. Klicken Sie zum Speichern der Änderungen auf **OK**.

Firmware-Aktualisierung für Geräte planen

Sie können eine Aufgabe planen, um mehrere Geräte des gleichen Typs, z. B. KX oder SX, innerhalb einer Gerätegruppe zu aktualisieren. Sobald die Aufgabe beginnt, ist im Menü Berichte > Geplante Berichte der Bericht „Gerätefirmware aktualisieren“ verfügbar. In diesem Bericht können Sie den Aktualisierungsstatus in Echtzeit verfolgen. Dieser Bericht wird auch per E-Mail gesandt, wenn Sie die Option auf der Registerkarte Benachrichtigung festlegen.

Im Raritan-Benutzerhandbuch des jeweiligen Geräts finden Sie Informationen über die geschätzten Aktualisierungszeiten.

➢ *So planen Sie eine Firmwareaktualisierung für Geräte:*

1. Wählen Sie Administration > Aufgaben.
2. Klicken Sie auf Neu.
3. Geben Sie auf der Registerkarte Hauptfenster einen Namen und eine Beschreibung für die Aufgabe ein. Mit dem von Ihnen gewählten Namen werden die Aufgabe und der Bericht, der der Aufgabe zugewiesen ist, gekennzeichnet.
4. Öffnen Sie die Registerkarte Aufgabendaten.
5. Legen Sie die Details für die Geräteaktualisierung fest:
   a. Aufgabenvorgang: Wählen Sie Gerätefirmware aktualisieren.
   b. Gerätegruppe: Wählen Sie die Gerätegruppe, die die Geräte enthält, die Sie aktualisieren möchten.
   c. Gerätetyp: Wählen Sie den Gerätetyp, den Sie aktualisieren möchten. Wenn Sie mehr als einen Gerätetyp aktualisieren müssen, müssen Sie für jeden Typ eine Aufgabe planen.
   d. Gleichzeitige Aktualisierungen: Legen Sie die Anzahl der Geräte fest, die mit der Dateiübertragungsaufgabe der Aktualisierung gleichzeitig beginnen sollen. Die Höchstanzahl beträgt 10. Nach jeder Dateiübertragung wird eine neue Dateiübertragung begonnen. Auf diese Weise wird sichergestellt, dass nur die maximale Anzahl an gleichzeitigen Aktualisierungen zur selben Zeit durchgeführt wird.
   e. Aktualisierungsdatei: Wählen Sie die Firmwareversion, auf die Sie aktualisieren möchten. Es werden nur die verfügbaren Aktualisierungsdateien, die für den ausgewählten Gerätetyp geeignet sind, als Optionen angezeigt.
6. Legen Sie den Zeitraum für die Aktualisierung fest:

a. Startdatum/Startzeit: Wählen Sie das Datum und die Uhrzeit, zu der die Aufgabe beginnen soll. Das Startdatum und die Startzeit müssen in der Zukunft liegen.

b. Aktualisierungszeitfenster beschränken und Spätester Startzeitpunkt (Datum/Uhrzeit) für Aktualisierung: Wenn Sie alle Aktualisierungen innerhalb eines festgelegten Zeitfensters beenden müssen, verwenden Sie diese Felder, um das Datum und die Uhrzeit festzulegen, nach der keine neuen Aktualisierungen beginnen können. Wählen Sie Aktualisierungszeitfenster beschränken, um das Feld Spätester Startzeitpunkt (Datum/Uhrzeit) für Aktualisierung zu aktivieren.

7. Legen Sie fest, welche Geräte in welcher Reihenfolge aktualisiert werden. Platzieren Sie Geräte mit einer höheren Priorität an den Anfang der Liste:

   a. Wählen Sie in der Liste Verfügbar alle Geräte aus, die Sie aktualisieren möchten. Klicken Sie auf Hinzufügen, um das jeweilige Gerät in die Liste Ausgewählt zu verschieben.

   b. Wählen Sie in der Liste Ausgewählt ein Gerät aus, und verschieben Sie es mit den Pfeiltasten an die Position in der Reihenfolge, an der es aktualisiert werden soll.

8. Öffnen Sie die Registerkarte Wiederholen. Legen Sie fest, ob fehlgeschlagene Aktualisierungen wiederholt werden sollen.

   a. Wiederholungsanzahl: Geben Sie an, wie oft CC-SG eine fehlgeschlagene Aktualisierung wiederholen soll.

   b. Wiederholungsintervall: Geben Sie die Zeitdauer an, die zwischen den Versuchen verstreichen soll. Standardmäßig können 30, 60 und 90 Minuten ausgewählt werden. Dies sind die optimalen Wiederholungsintervalle.

9. Öffnen Sie die Registerkarte Benachrichtigung. Legen Sie E-Mail-Adressen fest, die Benachrichtigungen über eine erfolgreiche und fehlgeschlagene Ausführung empfangen sollen. Standardmäßig wird die E-Mail-Adresse des Benutzers verwendet, der zurzeit angemeldet ist. Die E-Mail-Adressen der Benutzer werden im Benutzerprofil konfiguriert.

   a. Klicken Sie auf Hinzufügen, geben Sie die E-Mail-Adresse in das eingeblendete Fenster ein, und klicken Sie dann auf OK.

   b. Wählen Sie Bei Fehler, wenn eine E-Mail gesendet werden soll, falls eine Aktualisierung fehlschlägt.

c. Wählen Sie Bei Erfolg, wenn eine E-Mail gesendet werden soll, falls alle Aktualisierungen erfolgreich abgeschlossen werden.

10. Klicken Sie zum Speichern der Änderungen auf OK.

Nach dem Beginn der Aufgabenausführung können Sie den Bericht „ Gerätefirmware aktualisieren “ jederzeit während des geplanten Zeitraums öffnen, um den Status der Aktualisierungen anzuzeigen. Weitere Informationen finden Sie unter ***Gerätefirmware aktualisieren – Bericht*** (siehe "Bericht „ Gerätefirmware aktualisieren “" auf Seite 160).

Aufgaben, Aufgabendetails und Aufgabenverlauf anzeigen

Wird eine Aufgabe geändert oder aktualisiert, wird der Verlauf ungültig und das Datum letzte Ausführung ist leer.

➢ *So zeigen Sie eine Aufgabe an:*

1. Wählen Sie **Administration** > **Aufgaben**.
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**. Weitere Informationen zu Registerkartenbeschreibungen finden Sie unter **Aufgaben planen**.

- 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**. Weitere Informationen zu Registerkartenbeschreibungen finden Sie unter ***Aufgaben planen*** (auf Seite 216) und ***Firmware-Aktualisierung für Geräte planen*** (auf Seite 219).

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 von CC-NOC finden Sie in der Dokumentation CommandCenter NOC von Raritan.

Damit Sie eine gültige Verbindung zwischen dem CC-SG und CC-NOC herstellen können, müssen Sie die Zeiteinstellungen auf beiden Geräten synchronisieren. CC-NOC und CC-SG müssen so konfiguriert werden, dass sie einen NTP-Server verwenden.

Ein CC-NOC hinzufügen

Sie müssen die erstellten 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.

1. Klicken Sie im Menü **Zugang** auf **CC-NOC-Konfiguration**.
2. Klicken Sie auf **Hinzufügen**.
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 auf der Support-Website von Raritan.

4. Geben Sie einen beschreibenden Namen für CC-NOC in das Feld **Name** ein. Der Name darf aus maximal 50 alphanumerischen Zeichen bestehen.
5. Geben Sie die IP-Adresse oder den Hostnamen von CC-NOC in das Feld **CC-NOC-IP/Hostname** ein. Dieses Feld muss ausgefüllt werden. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) 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. CC-SG weist CC-NOC an, Ereignisse für diese Geräte in diesem IP-Bereich 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.

Hinweis: Verwenden Sie den CC-NOC-Synchronisation-Bericht, um Ziele anzuzeigen, die CC-SG abonniert. In dem Bericht werden auch neue Ziele angezeigt, die von CC-NOC erkannt wurden. Weitere Informationen finden Sie unter ***CC-NOC-Synchronisation-Bericht*** (auf Seite 160).

1. Geben Sie einen **Synchronisierungszeitpunkt** 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.
2. Geben Sie in das Feld **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.
3. Geben Sie im Feld **Heartbeat-Fehlversuche** 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.
4. Klicken Sie auf **Weiter**.
5. 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.

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.

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. Sie müssen diesen Vorgang wiederholen.

Hinweis: *CommandCenter NOC kann nur eigenständigen CC-SG-Einheiten oder primären Knoten von gruppierten CC-SG-Einheiten hinzugefügt werden.*

Ein CC-NOC bearbeiten

➢ *So bearbeiten Sie ein CC-NOC:*

1. Wählen Sie **Zugang** > **CC-NOC-Konfiguration**.
2. Markieren Sie ein CC-NOC in der Liste, und klicken Sie auf **Bearbeiten**.
3. Ändern Sie die Konfiguration nach Bedarf.

CC-NOC starten

➢ *So starten Sie CC-NOC in CC-SG:*

1. Wählen Sie **Zugang** > **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

1. Wählen Sie **Zugang** > **CC-NOC-Konfiguration**.
2. Wählen Sie in CC-SG ein CC-NOC aus, und klicken Sie auf **Löschen**. Eine Bestätigungsmeldung wird angezeigt.
3. Klicken Sie auf **Ja**, um das CC-NOC zu löschen. Eine Meldung wird eingeblendet, wenn das CC-NOC gelöscht wurde.

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.

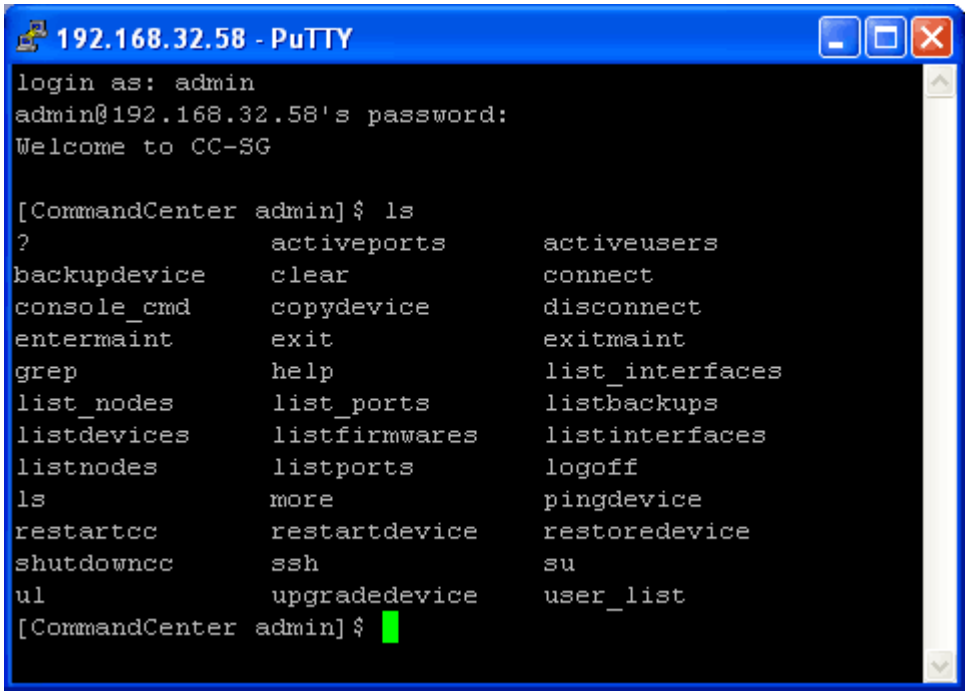
Der Benutzer des SSH-Clients wird von CC-SG authentifiziert, in dem vorhandene Authentifizierungs- und Autorisierungsrichtlinien auf den SSH-Client angewendet werden. Die für den SSH-Client verfügbaren Befehle werden von den Berechtigungen für die Benutzergruppen bestimmt, denen der Benutzer des SSH-Clients 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 ***Sicherheit konfigurieren*** (siehe "Sicherheitsmanager" auf Seite 200).
3. Melden Sie sich 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.



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.

Geben Sie einen Befehl mit dem Switch **–h** ein, wird die Hilfe für den Befehl angezeigt (z. B. **listfirmwares –h**).

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]` CC-SG neu starten
`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.

Tipps zu Befehlen

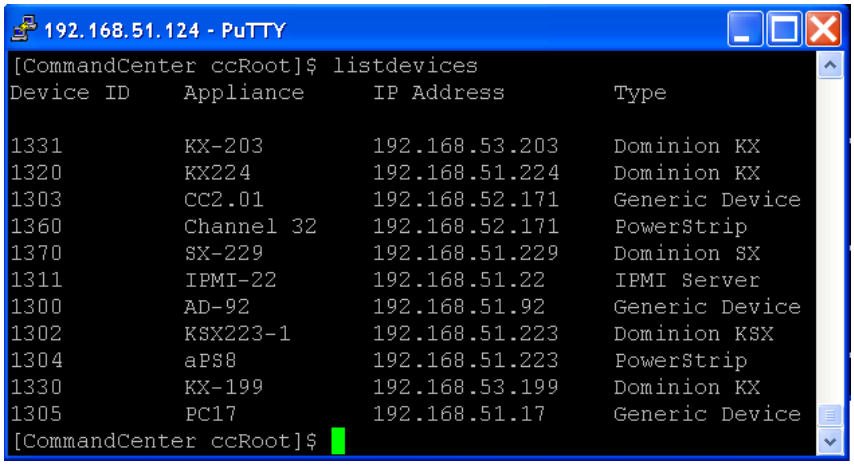
- Bei Befehlen, die eine IP-Adresse weiterleiten (z. B. `upgradedevice`), können Sie den Hostnamen für eine IP-Adresse einsetzen. Die Regeln zur Vergabe von Hostnamen werden unter ***Terminologie/Abkürzungen*** (auf Seite 2) beschrieben.
- Die Befehle `copydevice` und `restartdevice` gelten nur für einige Raritan-Geräte wie Dominion SX. IPMI-Server und generische Geräte unterstützen diese Befehle nicht.

SSH-Verbindung zu einem SX-Gerät herstellen

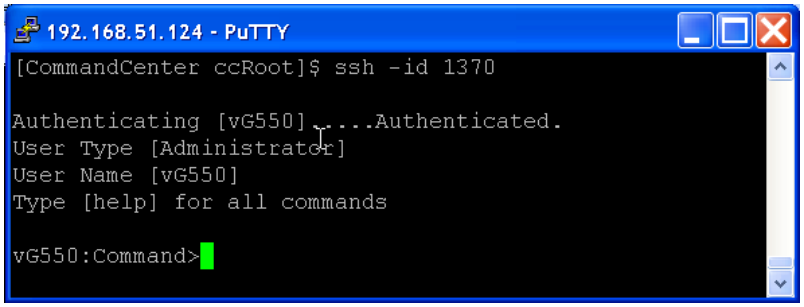
Sie können eine SSH-Verbindung zu einem SX-Gerät herstellen, um administrative Aufgaben auf dem Gerät durchzuführen. Nach dem Verbindungsaufbau stehen die administrativen Befehle zur Verfügung, die vom SX-Gerät unterstützt werden.

***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-Gerät zu CC-SG hinzugefügt wurde.



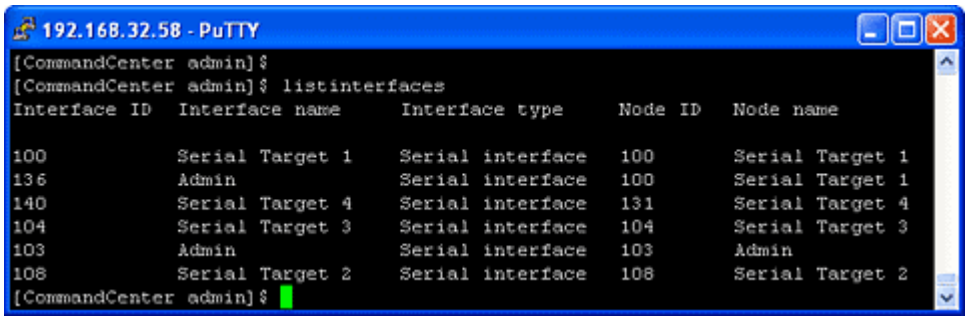
2. Stellen Sie eine Verbindung zum SX-Gerät her, indem Sie `ssh -id <Geräte-ID>` eingeben. Für das oben gezeigte Beispiel können Sie eine Verbindung zu SX-229 herstellen, indem Sie `ssh -id 1370` eingeben.



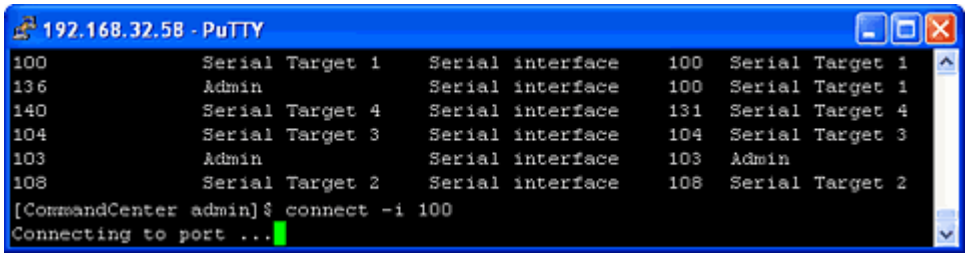
Verbindung zum Knoten mit SSH über serielle Out-of-Band-Schnittstelle herstellen

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.



2. Geben Sie `connect -i <Schnittstellen-ID>` ein, um eine Verbindung zu dem Knoten herzustellen, der mit der Schnittstelle verknüpft ist.



3. Geben Sie nach dem Verbindungsaufbau zum Knoten die standardmäßige Escape-Tastenfolge ‚~' gefolgt von ‚.' ein. Bei der angezeigten Eingabeaufforderung können Sie bestimmte Befehle oder Aliasse 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.

SSH-Sitzungen beenden

Sie können die Verbindung zwischen SSH und CC-SG trennen, indem Sie `exit` eingeben.

Serieller Administrationsport

Der serielle Administrationsport am CC-SG kann direkt an ein serielles Raritan-Gerät wie Dominion SX oder Dominion KSX angeschlossen werden.

Sie können mit einem Terminalemulationsprogramm wie HyperTerminal oder PuTTy über die IP-Adresse eine Verbindung zum SX- oder KSX-Gerät herstellen. Stellen Sie im Terminalemulationsprogramm eine Baudrate ein, die mit der Baudrate des SX- oder KSX-Geräts identisch ist.

- *G1 – Serieller Administrationsport:*

- *V1 – Serieller Administrationsport:*

- *E1 – Serieller Administrationsport:*

Terminalemulationsprogramme

HyperTerminal ist auf vielen Windows-Betriebssystemen verfügbar. HyperTerminal ist nicht auf Windows Vista verfügbar.

PuTTy ist ein kostenloses Programm, das Sie im Internet herunterladen können.

Web Services-API

Die Web Services-Programmierschnittstelle (WS-API) kann gegenwärtig nicht aktiviert werden. Aktualisierte Informationen zu dieser Funktion finden Sie unter http://www.raritan.com/web-services-api.

Kapitel 16 Diagnosekonsole

Die Diagnosekonsole ist eine nicht grafische Schnittstelle, die lokalen Zugriff auf CC-SG bereitstellt. Sie können auf die ***Diagnosekonsole über einen seriellen oder KVM-Port*** (siehe "Auf die Diagnosekonsole über VGA-/Tastatur-/Mausport zugreifen" auf Seite 236) oder über einen ***SSH-Client (Secure Shell)*** (siehe "Über SSH auf die Diagnosekonsole zugreifen" auf Seite 236) wie PuTTy oder OpenSSH-Client zugreifen.

Die Diagnosekonsole bietet zwei Benutzeroberflächen: ***Statuskonsole*** (siehe "Die Statuskonsole" auf Seite 237) und ***Administratorkonsole*** (siehe "Die Administratorkonsole" auf Seite 238).

Hinweis: *Wenn Sie über SSH auf die Diagnosekonsole zugreifen, übernehmen die Statuskonsole und Administratorkonsole die in Ihrem SSH-Client konfigurierten Anzeigeeinstellungen sowie die Tastaturbindungen. Diese Anzeigeeinstellungen unterscheiden sich eventuell von denen dieser Dokumentation.*

In diesem Kapitel

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. Drücken Sie die Eingabetaste, um eine Anmeldeaufforderung auf dem Bildschirm anzuzeigen.

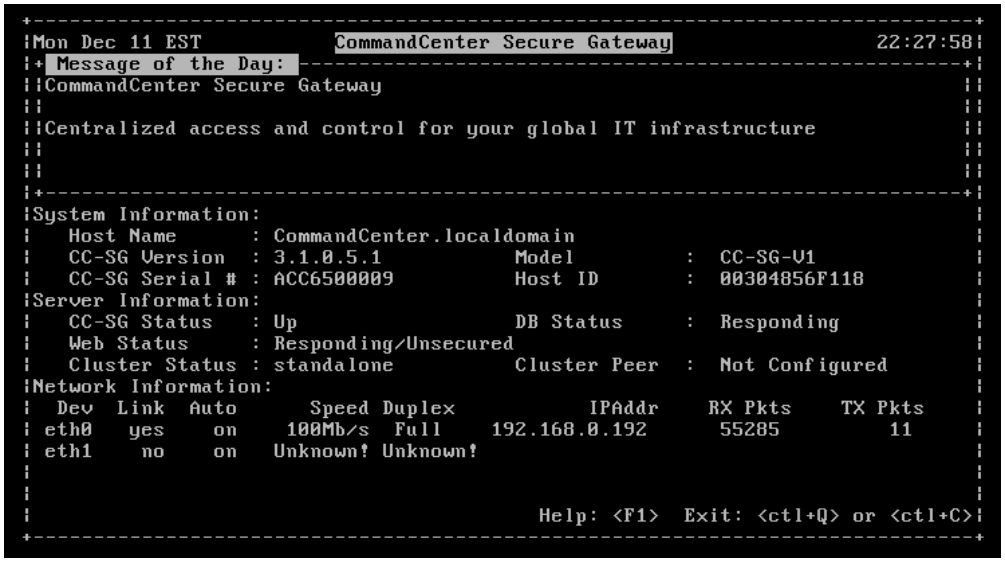
Über SSH auf die Diagnosekonsole zugreifen

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.

- Geben Sie beim Anmeldebildschirm **status** ein. Die Statuskonsole wird mit Lesezugriff angezeigt.



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.

Die Statuskonsole

Über die Statuskonsole können Sie den Zustand von CC-SG, die verschiedenen Dienste, die von CC-SG verwendet werden, sowie das angeschlossene Netzwerk feststellen.

Für die Statuskonsole ist standardmäßig kein Kennwort erforderlich.

Auf die Statuskonsole zugreifen

➢ *So greifen Sie auf die Statuskonsole zu:*

1. Geben Sie in der Anmeldeaufforderung den Wert **status** ein.
2. Die aktuellen Systeminformationen werden angezeigt.

Die Administratorkonsole

Über die Administratorkonsole können Sie Anfangsparameter festlegen, Erstkonfigurationen für das Netzwerk bereitstellen, Protokolldateien debuggen, einige eingeschränkte Diagnosefunktionen ausführen und CC-SG neu starten.

Die Standard-Anmeldeinformationen für die Administratorkonsole sind:

- Benutzername: **admin**
- Kennwort: **raritan**

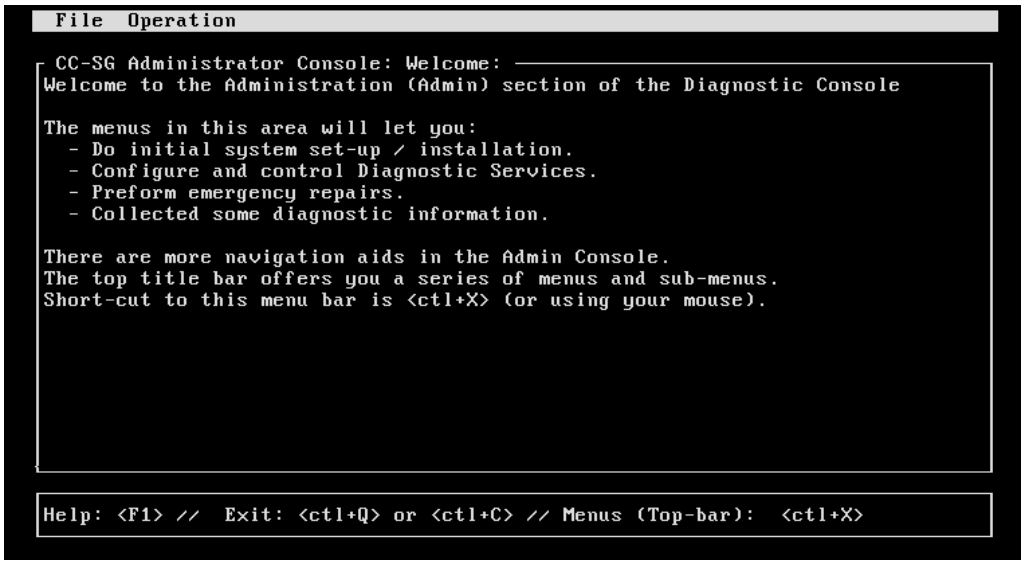
Das Konto **admin** der Diagnosekonsole unterscheidet sich von dem Konto **admin** und Kennwort des CC-Superusers, die für den Java-basierten CC-SG-Administrations-Client und HTML-basierten Zugriffs-Client verwendet werden. Wenn Sie ein Kennwort ändern, wird das andere davon nicht betroffen.

Auf die Administratorkonsole zugreifen

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 zur Einstellung der Kennwortsicherheitsstufe finden Sie unter ***Kennwörter für die Diagnosekonsole (Admin)*** (siehe "Kennworteinstellungen der Diagnosekonsole" auf Seite 259).

Der Hauptbildschirm der Administratorkonsole wird angezeigt.



Die Administratorkonsole navigieren

In der folgenden Tabelle sind die verschiedenen Navigationsmöglichkeiten für die Menüs der Diagnosekonsole aufgeführt. In einigen Sitzungen können Sie auch mit der Maus navigieren. Gegebenenfalls funktioniert die Maus 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.
Eingabetaste	Auswählen der aktuellen Option.
Pfeil	Bewegen zu anderen Feldern innerhalb einer Option.

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.

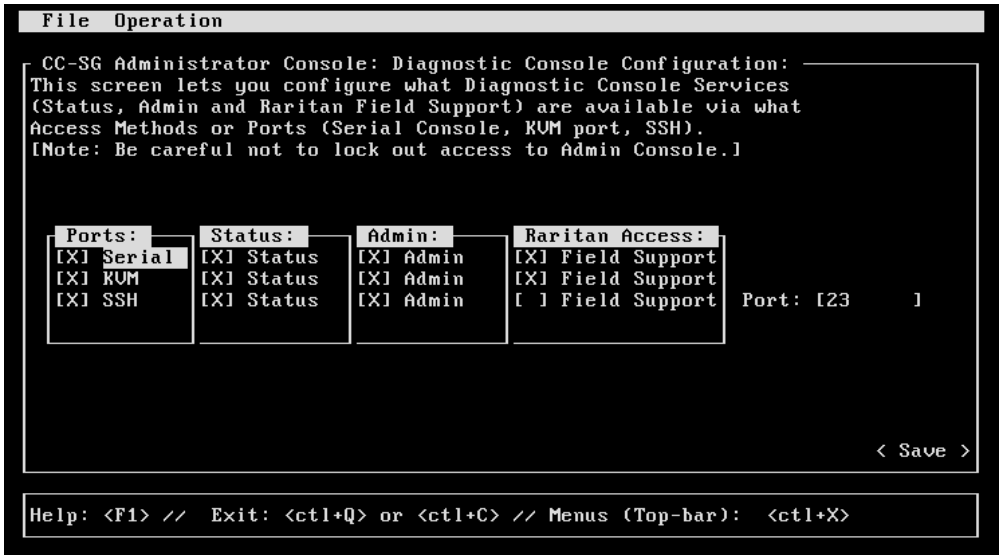
Wichtig: Stellen Sie sicher, dass Sie nicht den Admin- oder Field Support-Zugriff vollständig sperren.

➢ *So bearbeiten Sie die Konfiguration der Diagnosekonsole:*

1. Wählen Sie **Operation** > **Diagnostic Console Config**.
2. Bestimmen Sie, wie die Diagnosekonsole konfiguriert und auf die Diagnosekonsole zugegriffen werden soll.

   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**.



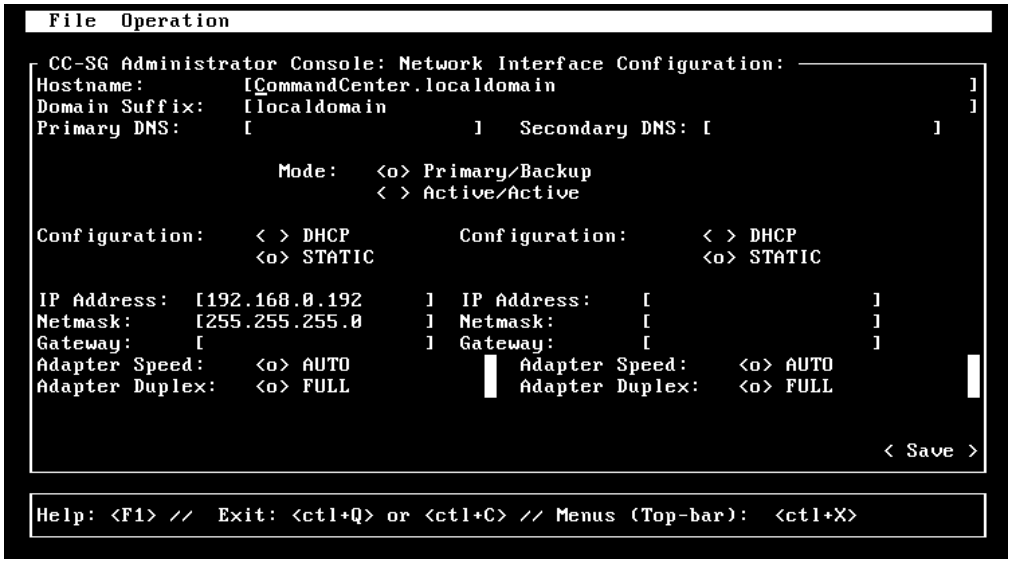
4. Klicken Sie auf **Save**.

Netzwerkschnittstellenkonfiguration bearbeiten (Network Interfaces)

Über die Netzwerkschnittstellenkonfiguration können Sie Erstkonfigurationsaufgaben wie die Einstellung des Hostnamens und der IP-Adresse von CC-SG durchführen.

1. Wählen Sie **Operation** > **Network Interfaces** > **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**.



3. Geben Sie Ihren Hostnamen in das 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*** (auf Seite 2) beschrieben.

4. Wählen Sie im Modusfeld **Primary/Backup Mode** oder **Active/Active Mode** aus. Weitere Informationen finden Sie unter ***Netzwerkeinrichtung*** (auf Seite 178).

   - Wählen Sie im Konfigurationsfeld entweder DHCP oder Static aus.
   - 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.

5. Wählen Sie über **Adapter Speed** eine Geschwindigkeit aus. Die Werte 10, 100 und 1000 MBit/s werden in einer Liste aufgeführt (in der nur ein Wert gleichzeitig angezeigt wird). Verwenden Sie die Pfeiltasten ⚜⚜, um die Werte anzuzeigen. Drücken Sie die Leertaste, um die angezeigte Option auszuwählen.
6. 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.
7. Wiederholen Sie diese Schritte für die zweite Netzwerkschnittstelle, wenn **Active/Active Mode** aktiviert ist.
8. Wählen Sie **Save**. CC-SG wird erneut gestartet und meldet alle Benutzer der grafischen Benutzeroberfläche von CC-SG ab und beendet ihre Sitzungen. Ein Warnhinweis wird angezeigt, der auf die bevorstehende Netzwerkkonfiguration und die damit verbundenen Auswirkungen auf CC-SG-Benutzer hinweist. Wählen Sie zum Fortfahren <**YES**>.

   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 stehen über <**F1**> bis <**F6**> bereit.

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, wenn ein Ping-Versuch fehlschlägt.*

1. Wählen Sie Operation > Network Interfaces > 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) Wählen Sie:

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. (Optional) Sie können 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 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. Weitere Informationen finden Sie unter ***Traceroute verwenden*** (siehe "Static Routes bearbeiten (Network Interfaces)" auf Seite 246).
6. Drücken Sie Strg+C, um die Ping-Sitzung zu beenden.

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. Wählen Sie **Operation** > **Network Interfaces** > **Traceroute**.
2. Geben Sie die IP-Adresse oder den Hostnamen des Ziels, das Sie prüfen möchten, in das Feld **Traceroute Target** ein.
3. (Optional) Wählen Sie:

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.

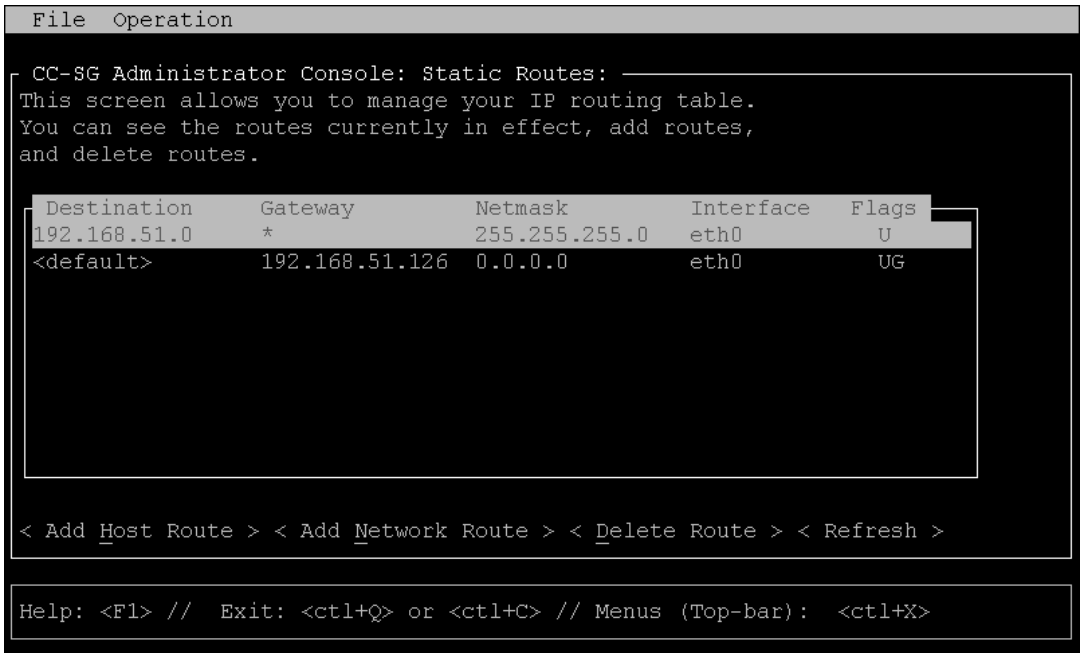
4. (Optional) Sie können Werte eingeben, wie viele Teilstrecken der Befehl traceroute bei ausgehenden Prüfpaketen verwendet (der Standardwert lautet 30), wie viele Teilstrecken der UDP-Zielport für Prüfpakete verwendet (der Standardwert lautet 33434) und wie groß die traceroute-Pakete sein sollen. Werden 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 ***Netzwerkeinrichtung*** (auf Seite 178). Klicken Sie mit der Maus, oder verwenden Sie die Tabulator- und Pfeiltasten zum Navigieren, und drücken Sie zum Auswählen eines Werts die **Eingabetaste**.

➢ *So zeigen Sie eine statisch Route an oder bearbeiten sie:*

1. Wählen Sie **Operation** > **Network Interfaces** > **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.



Protokolldateien in der Diagnosekonsole anzeigen (Admin)

Sie können eine oder mehrere Protokolldateien in LogViewer anzeigen sowie mehrere Dateien gleichzeitig durchsuchen, um die Systemaktivität zu untersuchen.

Die Liste der Protokolldateien wird nur aktualisiert, wenn die verknüpfte Liste aktiviert wird. Dies tritt ein, wenn ein Benutzer beispielsweise in den Listenbereich der Protokolldateien wechselt oder eine neue Sortieroption ausgewählt wird. Entweder wird ein Zeitstempel vor den Dateinamen angezeigt, um zu kennzeichnen, wann neue Daten für die Protokolldatei eingegangen sind, oder die Größe der Protokolldatei.

➢ *Abkürzungen für Zeitstempel und Dateigröße:*

Zeitstempel:

- s = Sekunden
- m = Minuten
- h = Stunden
- d = Tage

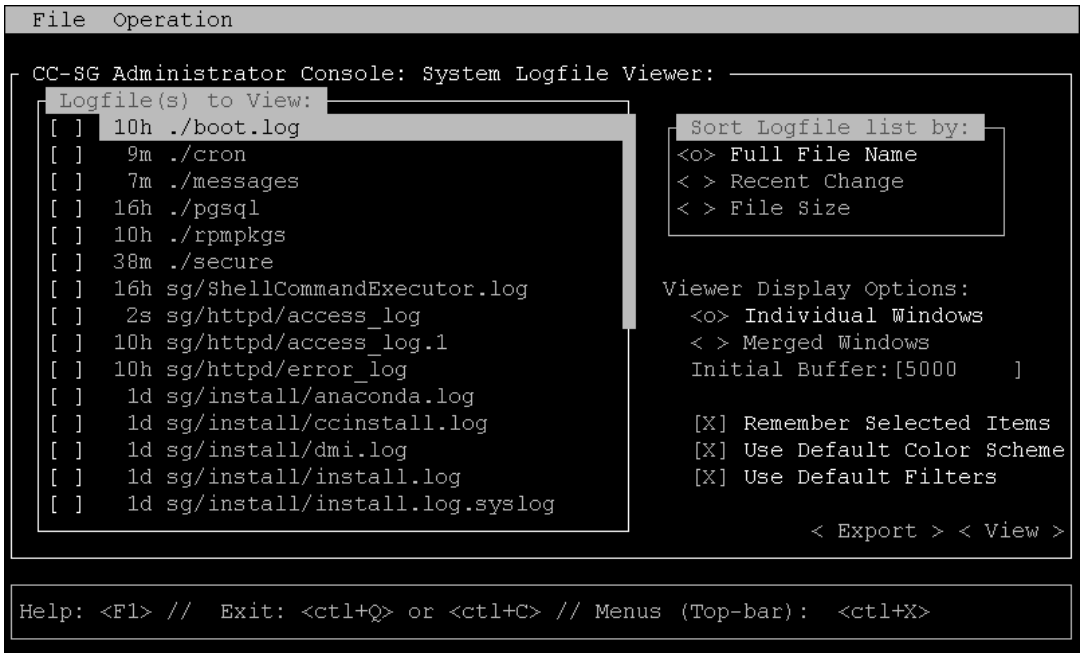
Dateigrößen:

- B = Byte
- K = Kilobyte (1.000 Byte)
- M = Megabyte (1.000.000 Byte)
- G = Gigabyte (1.000.000.000 Byte)

➢ *So zeigen Sie Protokolldateien an:*

1. Wählen Sie **Operation** > **Admin** > **System Logfile Viewer**.
2. Der Logviewer-Bildschirm ist in 4 Hauptbereiche 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.
   - 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.



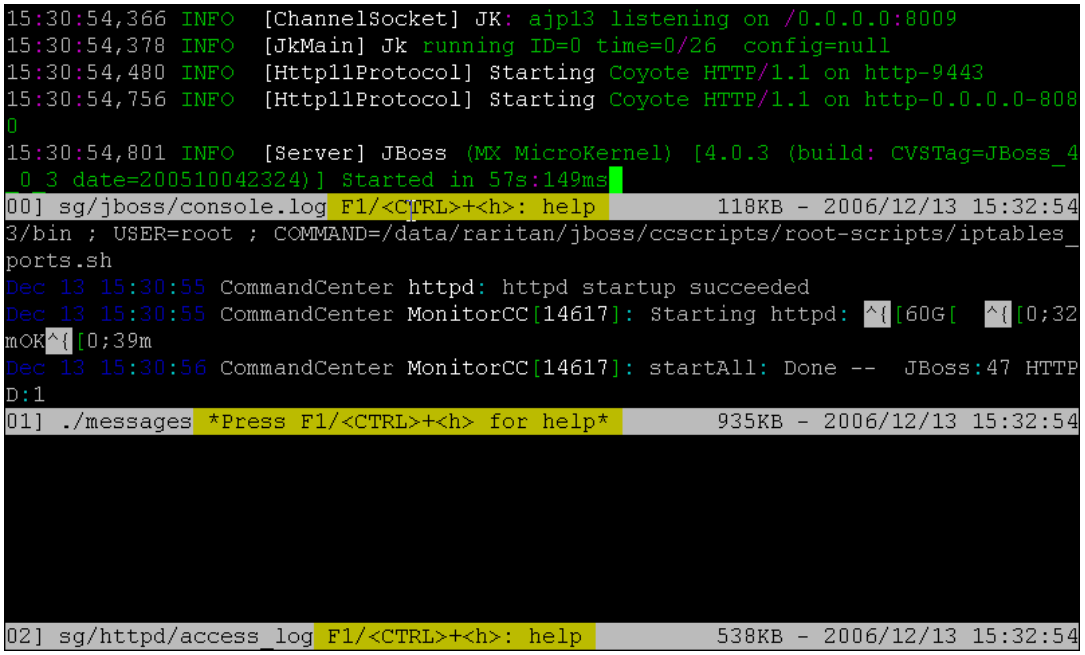
➢ *So sortieren Sie die Liste Logfiles to View:*

Mit den Optionen unter **Sort Logfile list by** bestimmen Sie die Reihenfolge, in der Protokolldateien in der Liste **Logfile to View** angezeigt werden.

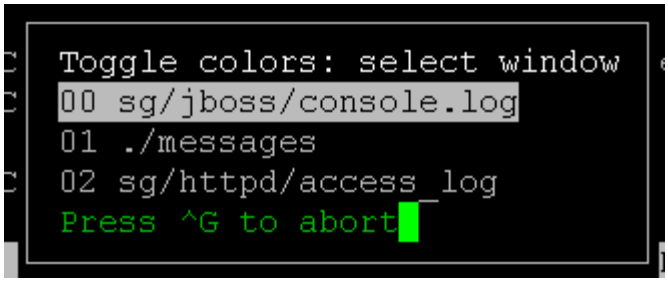
Option	Beschreibung
Individual Windows	Zeigt die ausgewählten Protokolle in einzelnen Unterfenstern an.
Merged Windows	Zeigt die ausgewählten Protokolle in einem Fenster an.
Initial Buffer	Legt die anfängliche Puffer- oder Verlaufsgröße fest. Der Standardwert beträgt **5000**. Das System ist so konfiguriert, 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:



- Drücken Sie beim Anzeigen von Protokolldateien **Q, Strg+Q** oder **Strg+C**, um zum vorherigen Bildschirm zu wechseln.
- Sie können die Farben in einer Protokolldatei ändern, um wichtige Daten hervorzuheben. Geben Sie **c** ein, um die Farben einer Protokolldatei zu ändern, und wählen Sie ein Protokoll in der Liste aus.

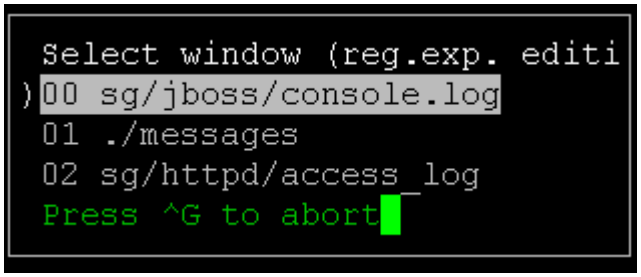


- Geben Sie **i** zur Anzeige von Systeminformationen ein.

Hinweis: *Die Systemauslastung ist zu Beginn der Administratorkonsole-Sitzung statisch. Verwenden Sie das TOP-Dienstprogramm, um die Systemressourcen dynamisch zu überwachen.*

➢ *So filtern Sie eine Protokolldatei mit einem regulären Ausdruck:*

1. 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.



2. 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.

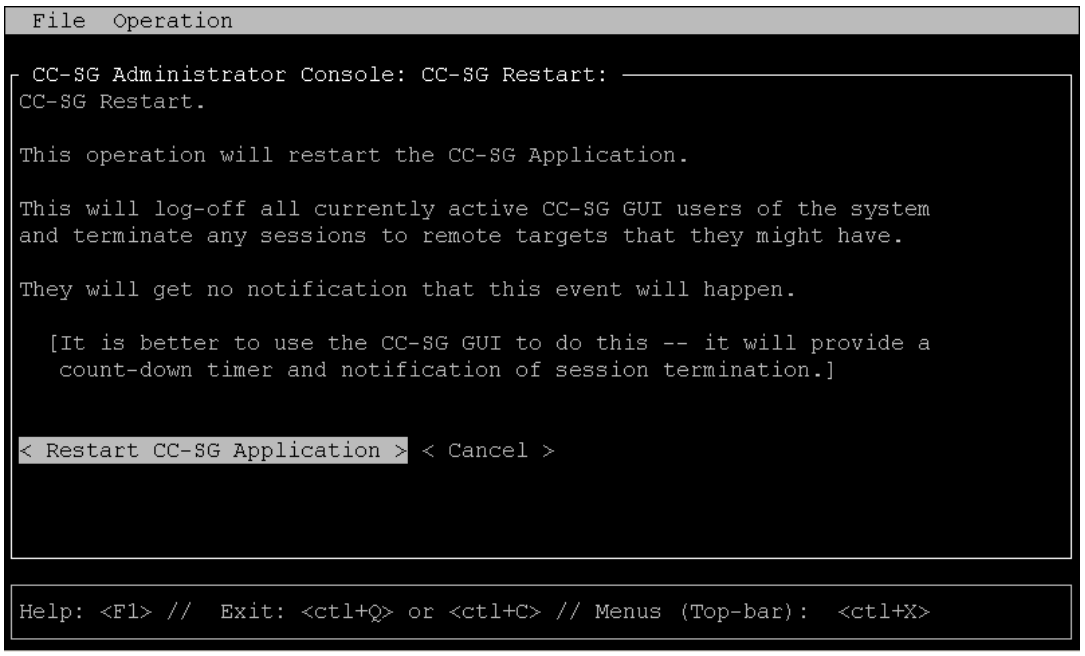
CC-SG mit der Diagnosekonsole neu starten

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 auf dem Java-basierten Administrations-Client neu zu starten, wenn es nicht absolut notwendig ist, den Neustart in der Diagnosekonsole auszuführen. Weitere Informationen finden Sie unter *CC-SG neu starten* **(auf Seite 168). Beim Neustarten von CC-SG in der Diagnosekonsole werden die Benutzer der grafischen Benutzeroberfläche über den Neustart NICHT informiert.**

➢ *So starten Sie CC-SG mit der Diagnosekonsole neu:*

1. Wählen Sie **Operation** > **Admin** > **CC-SG Restart**.
2. Klicken Sie auf **Restart CC-SG Application**, oder drücken Sie die **Eingabetaste**. Bestätigen Sie den Neustart im nächsten Bildschirm.

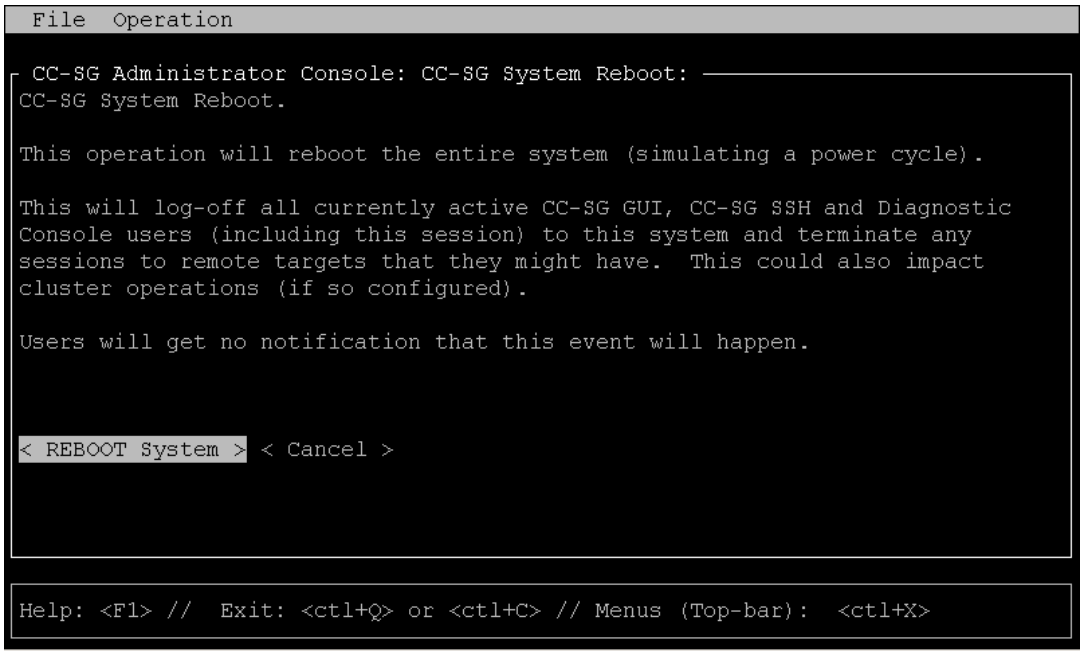


CC-SG mit der Diagnosekonsole neu hochfahren

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. Wählen Sie **Operation** > **Admin** > **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.



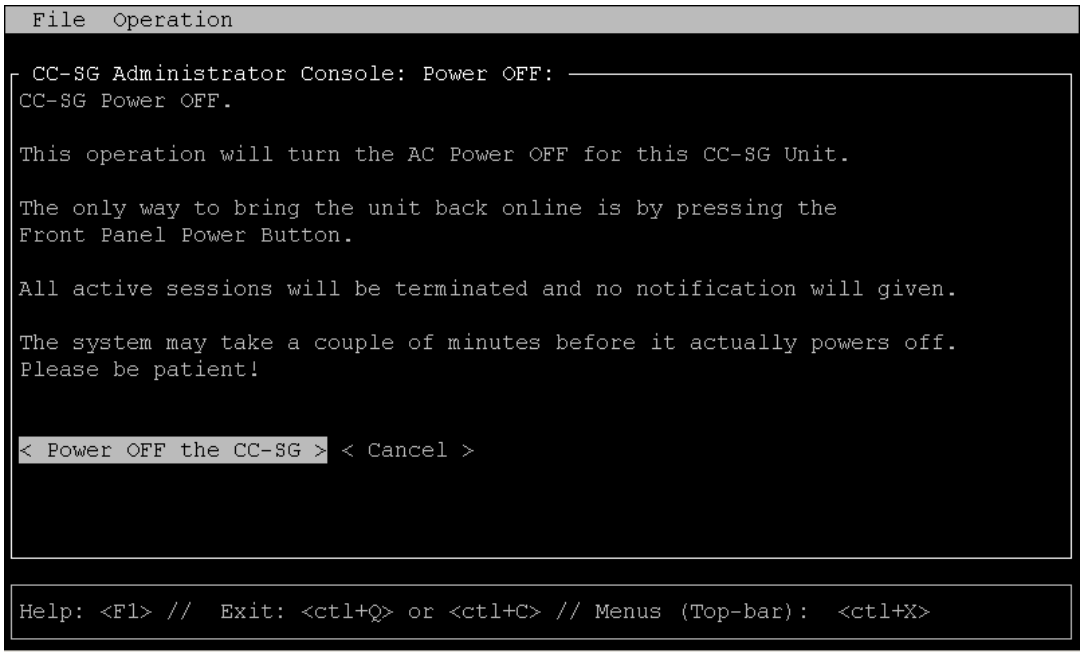
CC-SG-System in der Diagnosekonsole ausschalten

Mit dieser Option schalten Sie die CC-SG-Einheit aus. Angemeldete 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 betätigen.

➢ *So schalten Sie CC-SG aus:*

1. Wählen Sie **Operation** > **Admin** > **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.



Kennwort des CC-Superusers mit der Diagnosekonsole zurücksetzen

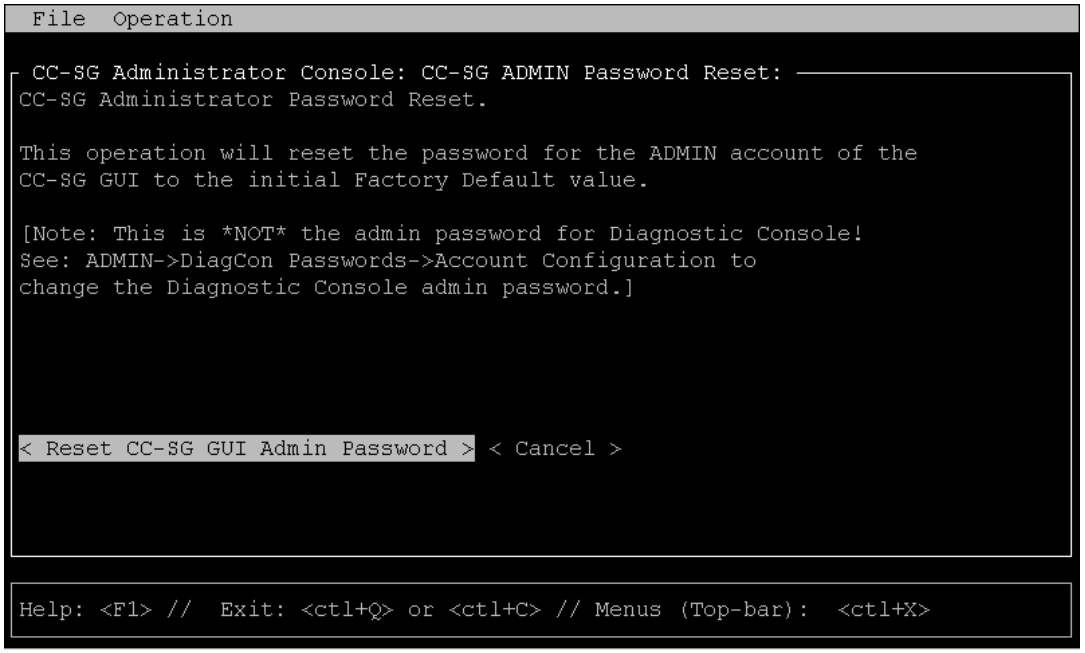
Mit dieser Option setzen Sie das Kennwort für das CC-Superuser-Konto auf den werksseitigen Standardwert zurück.

Werksseitiges Standardkennwort: **raritan**

Hinweis: *Dies ist nicht das Kennwort für den Benutzer admin der Diagnosekonsole. Weitere Informationen finden Sie unter* **Kennworteinstellungen der Diagnosekonsole** *(auf Seite 259).*

➢ *So setzen Sie das admin Kennwort der grafischen Benutzeroberfläche von CC-SG zurück:*

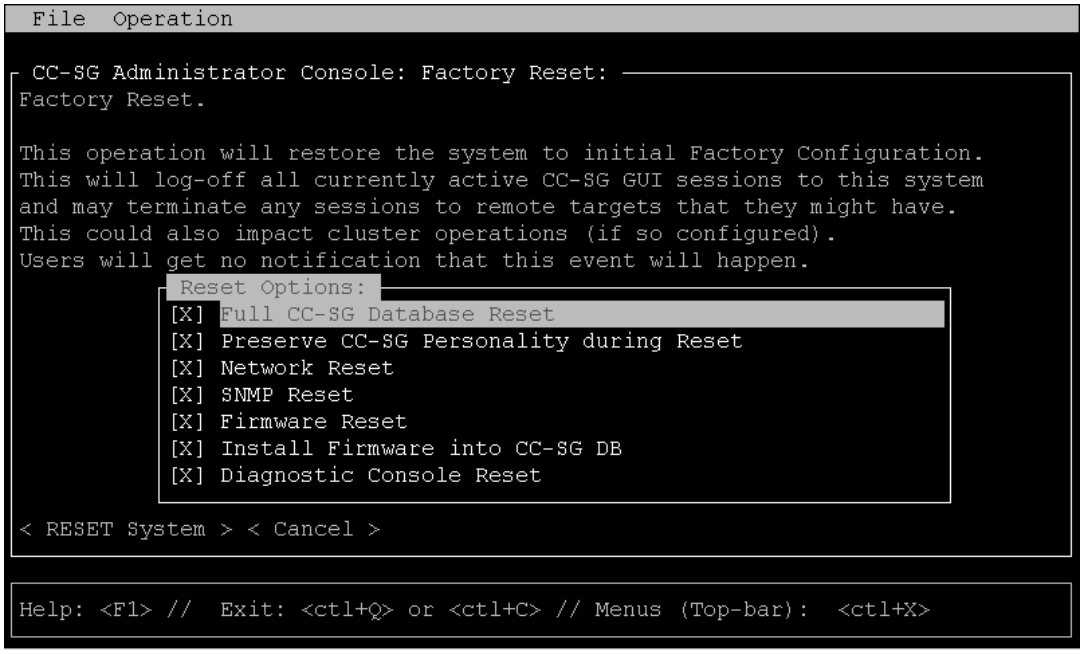
1. Wählen Sie Operation > Admin > CC-SG ADMIN Password Reset.
2. Klicken Sie auf Reset CC-SG GUI Admin Password, oder drücken Sie die Eingabetaste, um das admin Kennwort auf die werksseitige Standardeinstellung zurückzusetzen. Bestätigen Sie das Zurücksetzen im nächsten Bildschirm.



Werksseitig eingestellte 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 des Administrators und nicht über die Diagnosekonsole zurücksetzen. Die Option Admin Client Reset kann alle hier aufgeführten Funktionen außer des Zurücksetzens der Netzwerkwerte durchführen.

1. Wählen Sie **Operation** > **Admin** > **Factory Reset**. Folgender Bildschirm wird mit sieben Optionen zum Zurücksetzen angezeigt.



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 sich abmelden. 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.

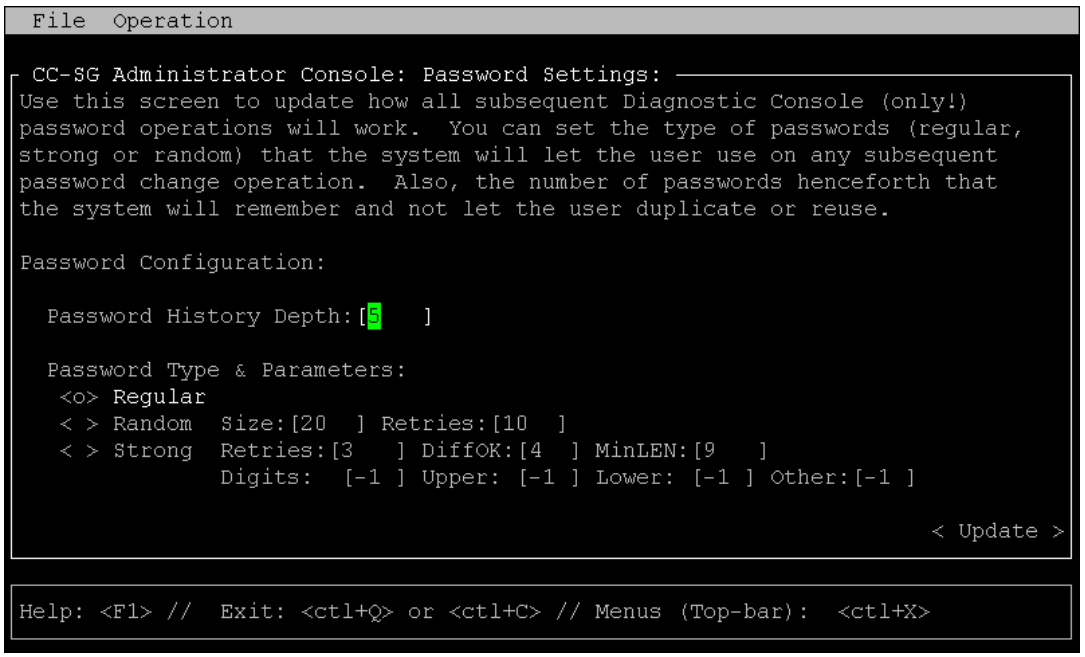
Network Reset	Diese Option setzt die Netzwerkwerte auf die werksseitigen Standardwerte zurück: Hostname = CommandCenter Domänenname = localdomain Modus = Primary / Backup Konfiguration = Static IP-Adresse = 192.168.0.192 Netzmaske = 255.255.255.0 Gateway = <kein> Primärer DNS-Server = <keiner> Sekundärer 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. Änderungen an der CC-SG-Datenbank werden nicht vorgenommen.
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.

Kennworteinstellungen der Diagnosekonsole

Mit dieser Option können Sie die Sicherheitsstärke von Kennwörtern (status und admin) sowie Kennwortattribute konfigurieren. Dazu gehören die Höchstanzahl an 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 (status und admin) und Kennwörter der Diagnosekonsole. Sie haben keine Auswirkungen auf normale CC-SG-Konten oder -Kennwörter der Benutzeroberfläche.

➢ *Password Configuration*

1. Wählen Sie **Operation** > **Admin** > **DiagCon Passwords** > **Password Configuration**.
2. Geben Sie in das Feld Länge der Kennwortchronik die Anzahl an Kennwörtern ein, die gespeichert werden sollen. Die Standardeinstellung ist **5**.



3. Wählen Sie **Regular**, **Random** oder **Strong** für die Kennwörter **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 an „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.

➢ *So konfigurieren Sie Konten:*

1. Wählen Sie **Operation** > **Admin** > **DiagCon Passwords** > **Account Configuration**.
2. Auf dem Bildschirm werden die Einstellungen für jedes Konto **Status**, **Admin**, **FS1** und **FS2** angezeigt.

```
 File  Operation

┌ CC-SG Administrator Console: Account Settings: ──────────────────────────
Account Configuration:
Field: \ User: Status:        Admin:         FS1:           FS2:
User Name:     status         admin          fs1            fs2
Last Changed:  Dec 12, 2006   Dec 12, 2006   Dec 13, 2006   Dec 13, 2006
Expire:        Never          Never          Never          Never

Mode:          < > Disabled                  < > Disabled   <o> Disabled
               < > Enabled                   <o> Enabled    < > Enabled
               <o> NoPassword
Min Days:      [0      ]      [0      ]
Max Days:      [99999  ]      [99999  ]
Warn:          [7      ]      [7      ]
Max # Logins:  [-1     ]      [2      ]      [1      ]      [0      ]
Update Param:   <UPDATE>       <UPDATE>       <UPDATE>       <UPDATE>
New Password:  <New Password> <New Password>

                                    < RESET to Factory Password Configuration >

Help: <F1> //  Exit: <ctl+Q> or <ctl+C> // Menus (Top-bar):  <ctl+X>
```

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 Konto **Status** 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.

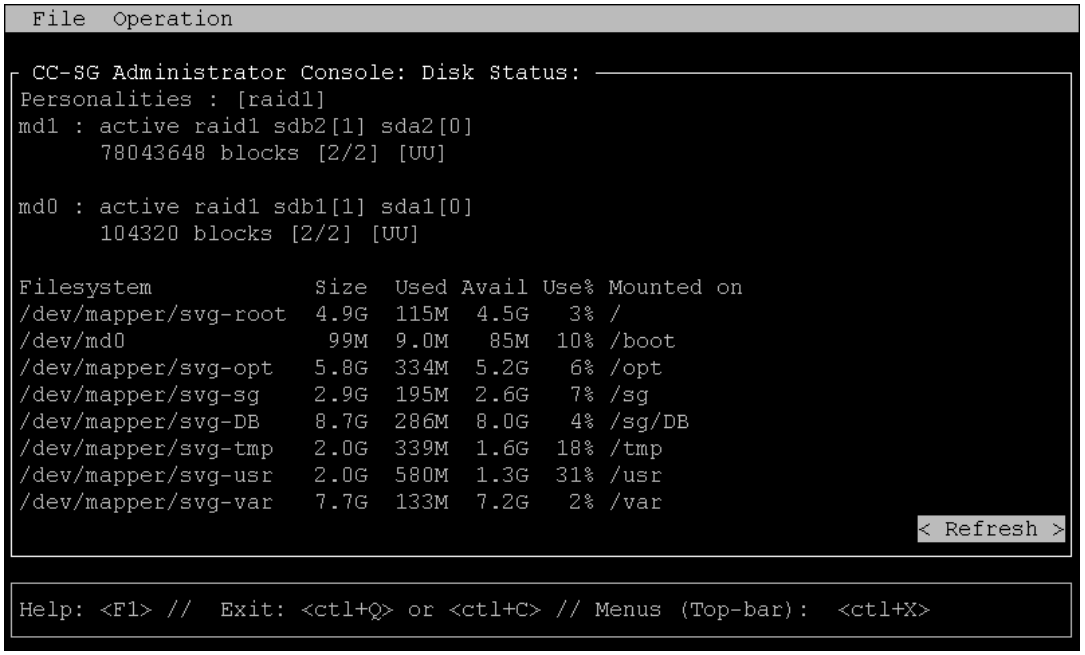
Disk Status anzeigen (Utilities)

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. Wählen Sie **Operation** > **Utilities** > **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.



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.*

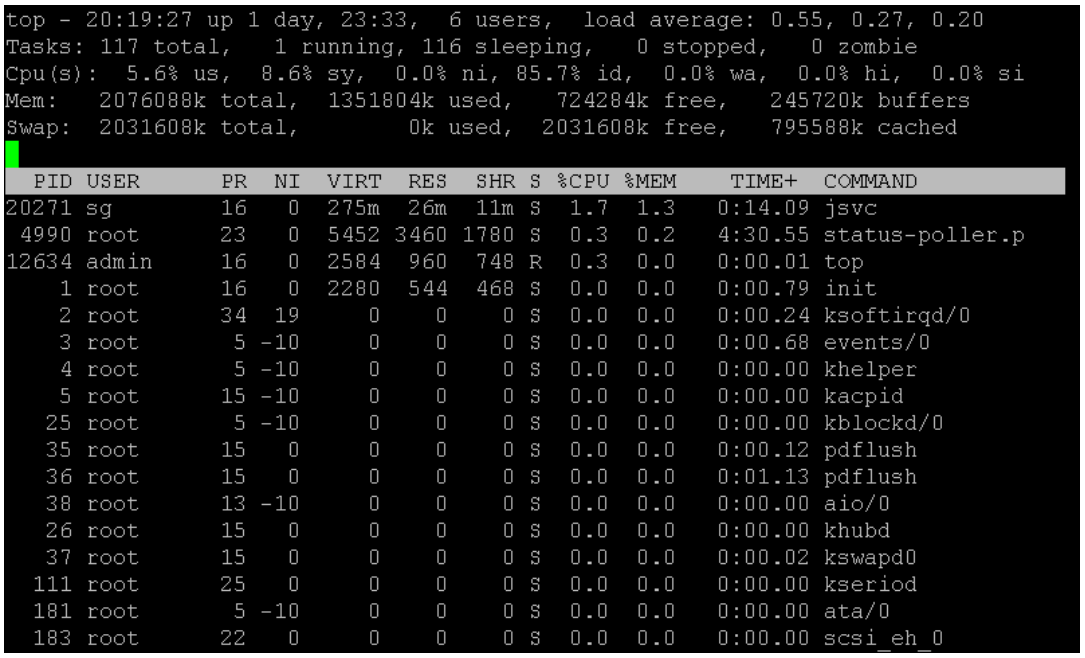
Top Display mit der Diagnosekonsole anzeigen

Mit Top Display können Sie die Prozessliste und die Attribute, die zurzeit unter CC-SG ausgeführt werden, sowie den allgemeinen Systemzustand anzeigen.

➢ *So zeigen Sie die Prozesse an, die unter CC-SG ausgeführt werden:*

1. Wählen Sie **Operation** > **Utilities** > **Top Display**.

2. Zeigen Sie die Gesamtanzahl der Prozesse an, die ausgeführt werden, ruhen oder unterbrochen wurden.



3. Geben Sie **h** ein, um eine Hilfeseite für den Befehl top anzuzeigen. Die Hilfetaste **F1** funktioniert in diesem Fall nicht.

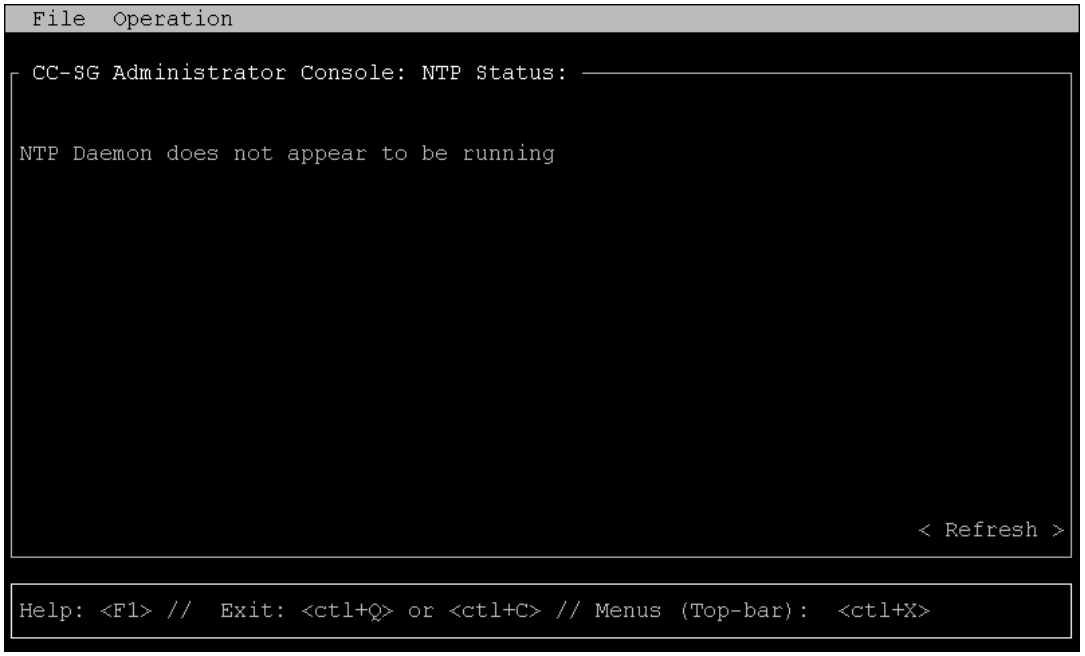
NTP Status anzeigen (Utilities)

Sie können den Status des NTP-Zeitdaemons anzeigen, falls dieser konfiguriert wurde und unter CC-SG ausgeführt wird. Der NTP-Daemon kann nur über die grafische Benutzeroberfläche des CC-SG-Administrations-Client konfiguriert werden.

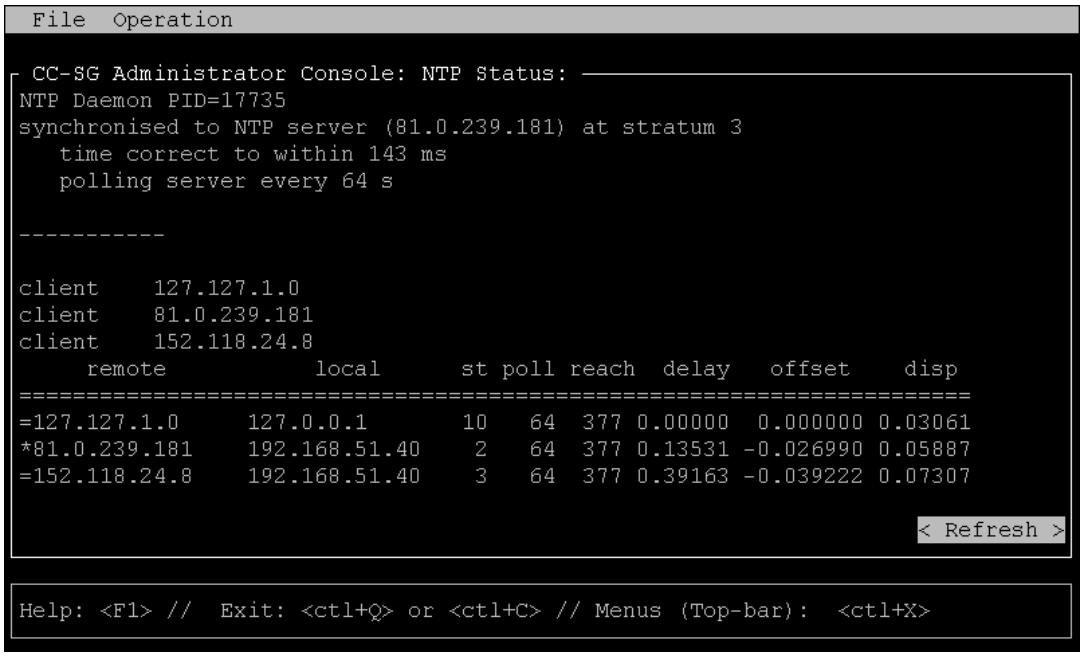
➢ *So zeigen Sie den Status des NTP-Daemons in CC-SG an:*

1. Wählen Sie **Operation** > **Utilities** > **NTP Status Display**.

- NTP ist nicht aktiviert oder ordnungsgemäß konfiguriert:



- NTP ist ordnungsgemäß konfiguriert und wird ausgeführt:



Anhang A Technische Daten für G1, V1 und E1

In diesem Kapitel

G1-Modell

G1 – 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

G1 – 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

G1 – 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 bis 30° C
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-Modell

V1 – 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° - 35° (50°- 95°)
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

V1 – 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

V1 – 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° - +60° (-40°-140°)
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-Modell

E1 – 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 bis 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

E1 – 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

E1 – Umgebungsanforderungen

Betrieb	
Luftfeuchtigkeit	5-90 %, nicht-kondensierend
Höhe über NN	Meeresspiegel bis 213.360,00 cm

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° bis 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

Anhang B CC-SG und Netzwerkkonfiguration

In diesem Kapitel

Anhang

Dieser Anhang enthält die Netzwerkanforderungen (Adressen, Protokolle und Ports) für eine typische CC-SG-Implementierung. 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.

Die folgenden Tabellen enthalten die Protokolle und Ports, die von CC-SG und den verknüpften Komponenten benötigt werden.

Erforderliche geöffnete Ports für CC-SG-Netzwerke: Übersicht

Die folgenden Ports müssen geöffnet sein:

Portnummer	Protokoll	Zweck
80	TCP	HTTP-Zugriff auf CC-SG
443	TCP	HTTP-(SSL-)Zugriff auf CC-SG
8080	TCP	CC-SG <-> Zugriffs-Client
2400	TCP	Knotenzugriff (Proxymodus und In-Band-Zugriff)

5000	TCP	Knotenzugriff (Direktmodus) 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.
51000	TCP	SX-Zielzugriff (Direktmodus)

Mögliche Ausnahmen:

Port 80 kann ausgeschlossen werden, falls der Zugriff auf CC-SG vollständig über HTTPS-Adressen läuft.

Ports 5000 und 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.

CC-SG-Kommunikationskanäle

Die Kommunikationskanäle sind wie folgt aufgeteilt:

- CC-SG zu Raritan-Geräten
- CC-SG zu CC-SG-Clustering (optional)
- CC-SG zu Infrastrukturdiensten
- Clients zu CC-SG
- Clients zu Zielen (Direktmodus)
- Clients zu Zielen (Proxymodus)
- Clients zu Zielen (In-Band)
- CC-SG zu 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 zu Lokaler Broadcast	5000	UDP	ja
CC-SG zu Remote LAN IP	5000	UDP	ja
CC-SG zu Raritan-Gerät	5000	TCP	ja
Raritan-Geräte zu CC-SG	5001	UDP	nein

CC-SG Clustering

Wenn die optionale CC-SG Clustering-Funktion verwendet wird, müssen die folgenden Ports für die miteinander verbundenen Subnetzwerke verfügbar sein. Wird die optionale Clustering-Funktion nicht verwendet, müssen diese Ports nicht geöffnet sein.

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 zu Lokaler Broadcast	10000	UDP	nein
CC-SG zu Remote LAN IP	10000	UDP	nein
CC-SG zu CC-SG	5432	TCP	nein
CC-SG zu CC-SG	8732	TCP	nein
CC-SG zu 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 zu CC-SG	68	UDP	nein
CC-SG zu DHCP-Server	67	UDP	nein
NTP-Server zu CC-SG	123	UDP	nein
CC-SG zu DNS	53	UDP	nein

Verbindung von PC-Clients mit CC-SG

PC-Clients verwenden für die Verbindung zu CC-SG einen dieser drei Modi:

- Grafische Benutzeroberfläche eines Administrations- oder Zugriffs-Clients über einen Webbrowser
- Befehlszeilenschnittstelle (Command Line Interface, CLI) über SSH
- Diagnosekonsole

Kommunikationsrichtung	Portnummer	Protokoll	Konfigurierbar?
PC-Client zu CC-SG-Benutzeroberfläche	443	TCP	nein
PC-Client zu CC-SG-Benutzeroberfläche	80	TCP	nein
PC-Client zu CC-SG-Benutzeroberfläche	8080	TCP	nein
PC-Client zu CLI SSH	22	TCP	ja
PC-Client zur 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 Knoten. Diese Knoten 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 zu CC-SG über Proxy zum Ziel	2400 (an CC-SG)	TCP	nein
Client zu Raritan-Ziel (Direktmodus)	5000 (am Gerät)	TCP	ja
Client zu Dominion SX zu Ziel (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 zu IPMI	623	UDP	nein
CC-SG zu iLO/RILOE (verwendet HTTP-Ports)	80 oder 443	UDP	nein

CC-SG zu DRAC	80 oder 443	UDP	nein
CC-SG zu 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 zu CC-SG	161	UDP	ja
CC-SG zu SNMP Manager	162	UDP	ja

CC-SG und CC-NOC

CC-NOC ist eine optionale Appliance, die in Verbindung mit CC-SG implementiert 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 zu 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
- 8093

  Außer diesen Ports verwendet CC-SG ggf. TCP- und UDP-Ports im Bereich 32xxx (oder höher). 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. Die Firewall muss auch für externe Verbindungen zu den Ports 80 (kein-SSL) oder 443 (SSL), 8080 und 2400 so konfiguriert sein, dass an CC-SG weitergeleitet wird (da der PC-Client die Sitzungen an diesen Ports startet).

Hinweis: *Nicht-SSL-Verkehr sollte nicht über eine Firewall abgewickelt werden.*

Alle In-Band-Verbindungen verwenden CC-SG als Proxy-Verbindung. Es ist keine weitere Konfiguration erforderlich.
Out-of-Band-Verbindungen, die die Firewall verwenden, müssen so konfiguriert werden, dass sie den Proxymodus verwenden. Weitere Informationen finden Sie unter ***Verbindungsmodi: Direkt und Proxy*** (auf Seite 192). CC-SG stellt 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.

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	Benutzerverwaltung	
	(Benutzer bearbeiten)	Benutzerverwaltung	Über Benutzerprofil
	> Benutzer löschen	Benutzerverwaltung	
	> Benutzer aus Gruppe löschen	Benutzerverwaltung	
	> Benutzer abmelden	Benutzerverwaltung	
	> Massenkopieren	Benutzerverwaltung	
> Benutzer-gruppen manager	> Benutzergruppe hinzufügen	Benutzerverwaltung	
	(Benutzergruppen bearbeiten)	Benutzerverwaltung	Über Benutzergruppenprofil
	> Benutzergruppe löschen	Benutzerverwaltung	
	> Benutzer der Gruppe zuweisen	Benutzerverwaltung	
	> Benutzer abmelden	Benutzerverwaltung	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
Geräte	**Dieses Menü und die Benutzerstrukturansicht stehen nur Benutzern mit folgenden Berechtigungen zur Verfügung:** Device-, Port- and Node Management Device Configuration and Upgrade Management		
	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
	> Gerät löschen	Device-, Port- and Node Management	
	> Massenkopieren	Device-, Port- and Node Management	
	> Gerät aktualisieren	Device Configuration and Upgrade Management	
>> Konfiguration	>> Sicherung	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	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
	> 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	
	> Gerätestrom-manager	Device-, Port- and Node Management	
	> Administration starten	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
	> Benutzerstation-Administration starten		
	> Benutzer trennen	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
	> Topologieansicht	Device-, Port- and Node Management	
> Ansicht ändern	> Benutzer-definierte 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	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
> 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	
	> 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 Node In-Band Access (In-Band Knotenzugriff) Node Out-of-Band Access (Out-of-Band Knotenzugriff) Node Power Control		
	Knoten hinzufügen	Device-, Port- and Node Management	
	(Knoten bearbeiten)	Device-, Port- and Node Management	Über das Knotenprofil
	Knoten löschen	Device-, Port- and Node Management	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
	<Schnittstellenname>	In-Band-Zugriff oder Out-of-Band-Zugriff	
	Trennen	In-Band-Zugriff oder Out-of-Band-Zugriff	
	Strom-Versorgungssteue-rung	Strom-Versorgungssteue-rung	
	Gruppen-strom-Versorgungssteue-rung	Strom-versorgungssteuerung	
> Knoten-sortieroptionen	> Nach Knotenname	Eine der Folgenden: Device-, Port- and Node Management In-Band-Zugriff oder Out-of-Band-Zugriff oder Stromversorgungssteuerung	
	> 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	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
	> 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	
> 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.

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
	> 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	CC Setup And Control	
	Verfügbarkeits-bericht	Device-, Port- and Node Management oder Device Configuration and Upgrade Management	
> Benutzer	> Aktive Benutzer	Benutzerverwaltung	
	> Gesperrte Benutzer	CC Setup And Control	
	> Benutzerdaten	Zum Anzeigen aller Benutzerdaten: Benutzerverwaltung Zum Anzeigen Ihrer eigenen Benutzerdaten: Keine	
	> Benutzer in Gruppen	Benutzerverwaltung	
	> Gruppendaten	User Security Management	
> Geräte	Anlagenverwaltung	Device-, Port- and Node Management	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
> 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	
> Active Directory	AD-Benutzergruppen-bericht		
	Geplante Berichte	CC Setup And Control	
	CC-NOC-Synchronisation	CC Setup And Control	
Zugang			
	CC-NOC-Konfiguration	CC Setup And Control	
Administration	**Dieses Menü steht nur Benutzern mit einer der folgenden Berechtigung zur Verfügung:** CC Setup And Control 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	

Menü > Untermenü	Menüelement	Erforderliche Berechtigung	Beschreibung
	Firmware	Device-, Port- and Node Management	
	Konfiguration	CC Setup And Control	
	Sicherheit	CC Setup And Control	
	Benachrichtigungen	CC Setup And Control	
	Aufgaben	CC Setup And Control	
	Kompatibilitäts-matrix	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	
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.

Anhang D SNMP-Traps

CC-SG stellt die folgenden SNMP-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.

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.

In diesem Kapitel

Clientbrowser-Anforderungen

Eine vollständige Liste der unterstützten Browser finden Sie in der **Kompatibilitätsmatrix** auf der Support-Website von Raritan.

Anhang F Zwei-Faktoren-Authentifizierung

CC-SG kann 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.

In diesem Kapitel

Unterstützte Umgebungen für die Zwei-Faktoren-Authentifizierung

Die folgenden Komponenten der 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 für die Zwei-Faktoren-Authentifizierung

Die folgenden Aufgaben müssen für ein Zwei-Faktoren-Authentifizierungs-Setup abgeschlossen werden. Weitere Informationen finden Sie in der RSA-Dokumentation.

1. Token importieren
2. CC-SG-Benutzer erstellen und Token dem Benutzer zuordnen
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 bei der Zwei-Faktoren-Authentifizierung

Der Modus RSA RADIUS „New PIN“, der ein Herausforderungskennwort/PIN erfordert, funktioniert nicht. Benutzern in diesem Schema müssen stattdessen festgelegte Kennwörter zugeordnet werden.

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 implementierter Server und Netzwerkgeräte, die an einem IT-fähigen Raritan-Gerät angeschlossen sind.
Wozu kann ich CC-SG einsetzen?	Mit zunehmender Anzahl an 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?	Bitte lesen Sie die CC-SG-Kompatibilitätsmatrix auf der Support-Website von Raritan.
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?	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.

Frage	Antwort
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 an 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 Knoten tatsächlich angeschlossen werden können.
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*** (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 zugeordnet. 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 zugeordneten Knoten anzuzeigen. Vergessen Sie nicht, dass beim Aktualisieren von CC-SG alle derzeitigen Konsolensitzungen geschlossen werden.

Frage	Antwort
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.
Authentifizierung	

Frage	Antwort
Wie viele Benutzerkonten können für CC-SG erstellt werden?	Überprüfen Sie die Bestimmungen in Ihrer Lizenz. Für die Anzahl an Benutzerkonten, die für CC-SG erstellt werden können, liegt keine festgelegte Beschränkung vor. Es kann jedoch auch keine unbegrenzte Anzahl an 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 zuordnen?	Ja, wenn Sie Administratorberechtigungen besitzen. Administratoren haben die Möglichkeit, jedem Benutzer bestimmte Knoten zuzuordnen.
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.

Frage	Antwort
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.
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.

Frage	Antwort
Leistung	
Als CC-SG-Administrator habe ich über 500 Knoten hinzugefügt, die ich alle mir zugeordnet habe. Das Anmelden in CC-SG nimmt jetzt sehr viel Zeit in Anspruch.	Wenn Sie sich als Administrator viele Knoten zugeordnet 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 an Knoten zugeordnet 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.
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.

Frage	Antwort
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 sollte der Tausch von CIMS auf physischer Ebene mit Änderungen in der logischen Datenbank gehandhabt werden?	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 Kommunikationsprotokolle für diese Switches nicht veröffentlichen. Je nach Fähigkeiten der KVM-Switches von Drittanbietern variiert der Grad der Integration.

Frage	Antwort
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.
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 Java-basierten Administrations-Client verwendet werden.

Vorgang	Tastenkombinationen
Aktualisieren	F5
Fenster drucken	Strg + P
Hilfe	F1
Zeile in Verknüpfungstabelle einfügen	Strg + I

Anhang I Benennungsregeln

Dieser Anhang enthält Informationen zu den Benennungsregeln, die in CC-SG verwendet werden. Beachten Sie die maximale Zeichenlänge beim Benennen aller Teile der CC-SG-Konfiguration.

CC-SG-Beschränkungen	
Feld in CC-SG:	Zulässige Anzahl an Zeichen in CC-SG
Gerätename	32
Gerätegruppe	40
Portname	32
Benutzername	20
Benutzergruppenname	64
Kennwort (kein sicheres Kennwort)	16
Kennwort (sicheres Kennwort)	Konfigurierbar Minimum: 8 Maximum: 64 Standardminimum: 8 Standardmaximum: 16
Kategoriename	64
Elementname	31
Knotenname	66
Knotengruppenname	40
Richtlinienname	56

Index

A

B

C

D

E

F

G

H

I

K

L

M

N

P

R

S

T

U

V

W

Z

➢ *USA/Kanada/Lateinamerika*

Montag bis Freitag
08:00 bis 20:00 Uhr ET (Eastern Time)
Tel.: 800-724-8090 oder 732-764-8886
CommandCenter NOC: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 1.
CommandCenter Secure Gateway: Drücken Sie auf Ihrem Telefon die Zifferntaste 6 und dann die Zifferntaste 2.
Fax: 732-764-8887
E-Mail-Adresse für CommandCenter NOC: tech-ccnoc@raritan.com
E-Mail-Adresse für alle anderen Produkte: tech@raritan.com

➢ *Großbritannien*

Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +44-20-7614-77-00

➢ *Japan*

Montag bis Freitag
09:30 bis 17:30 Uhr Ortszeit
Tel.: +81-3-3523-5994
E-Mail: support.japan@raritan.com

➢ *Korea*

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +82-2-5578730

➢ *Melbourne, Australien*

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +61-3-9866-6887

➢ *Shanghai*

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-21-5425-2499

➢ *Taiwan*

Montag bis Freitag
09:00 bis 18:00 Uhr GMT -5 Standardzeit -4 Sommerzeit
Tel.: +886-2-8919-1333
E-Mail: tech.rap@raritan.com

➢ *Beijing*

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-10-88091890

➢ *Europa*

Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +31-10-2844040
E-Mail: tech.europe@raritan.com

➢ *Frankreich*

Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +33-1-47-56-20-39

➢ *Deutschland*

Montag bis Freitag
08:30 bis 17:00 Uhr GMT+1 MEZ
Tel.: +49-20-17-47-98-0

➢ *GuangZhou*

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +86-20-8755-5561

➢ *Indien*

Montag bis Freitag
09:00 bis 18:00 Uhr Ortszeit
Tel.: +91-124-410-7881