Cisco Business Dashboard und Probe, Administratorhandbuch, Version 2.2.x

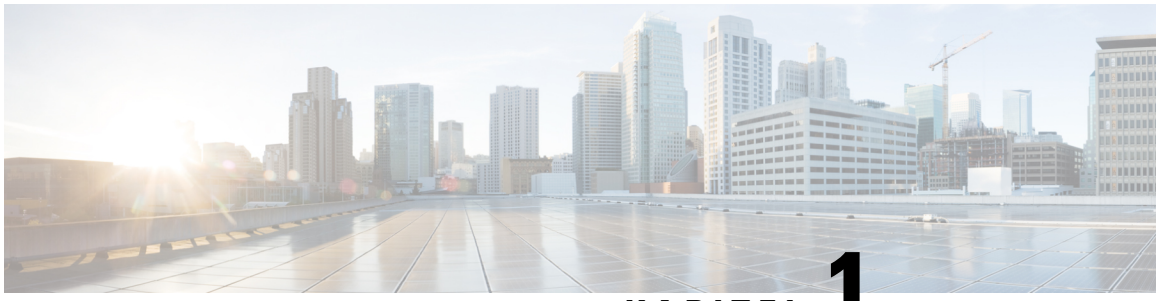
Erste Veröffentlichung: 14 Juli 2020

Letzte Änderung: 2 September 2020

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883


Das Java-Logo ist eine Marke oder eingetragene Marke von Sun Microsystems, Inc. in den Vereinigten Staaten oder anderen Ländern.

INHALTSVERZEICHNIS



KAPITEL 1

Cisco Business Dashboard Übersicht

Dieses Kapitel enthält folgende Abschnitte:

Allgemeines zu Cisco Business Dashboard

Cisco Business Dashboard bietet Tools für die Überwachung und Verwaltung Ihres Cisco Business-Netzwerks. Cisco Business Dashboard führt eine automatische Netzwerkerkennung durch und ermöglicht Ihnen die Konfiguration und Überwachung aller unterstützten Cisco Business-Geräte, beispielsweise Switches, Router und Wireless-Access-Points von Cisco. Außerdem werden Sie benachrichtigt, wenn Firmwareupdates verfügbar sind und wenn die Garantie oder der Supportvertrag von Geräten abgelaufen ist.

Cisco Business Dashboard ist eine verteilte Anwendung, die aus zwei separaten Komponenten bzw. Anwendungen besteht: die Cisco Business Dashboard-Hauptanwendung, die als *Dashboard* bezeichnet wird, und eine oder mehrere Instanzen der Cisco Business Dashboard Probe, die als *Probe* bezeichnet wird.

Eine einzelne Instanz von Cisco Business Dashboard wird an einem geeigneten Standort im Netzwerk installiert. Über die Dashboard-Schnittstelle können Sie eine zentrale Ansicht des Status aller Standorte in Ihrem Netzwerk abrufen oder sich auf einen einzelnen Standort oder ein Gerät konzentrieren und nur die Informationen für diesen Standort oder dieses Gerät anzeigen.

Eine Instanz von Cisco Business Dashboard Probe wird an jedem Standort im Netzwerk installiert und dem Dashboard zugeordnet. Die Probe führt eine Netzwerkerkennung durch und kommuniziert direkt mit jedem verwalteten Gerät im Namen des Dashboards.

Unterstützung für bestimmte Netzwerkgeräte ist direkt dem Dashboard zugeordnet und kann ohne Probe verwaltet werden. Wenn Netzwerkgeräte auf diese Weise direkt verwaltet werden, stehen alle Management-Funktionen für das Gerät zur Verfügung, der Prozess zur Netzwerkerkennung ist jedoch möglicherweise nicht so umfassend wie mit einer Probe-Anwendung.

Zielgruppe

Dieses Handbuch richtet sich in erster Linie an Netzwerkadministratoren, die für die Softwareinstallation und das Management von Cisco Business Dashboard verantwortlich sind.

Verwandte Dokumente

Die Dokumentation für Cisco Business Dashboard besteht aus einer Reihe separater Handbücher. Dazu gehören:

- **Administratorhandbuch (das vorliegende Dokument)**: Dies ist ein Referenzhandbuch mit Informationen zu allen Funktionen und Optionen der Software sowie zu deren Konfiguration und Nutzung.
- **Device Support List** (Liste der unterstützten Geräte): Diese Liste enthält Details zu den von Cisco Business Dashboard unterstützten Geräten und den für die einzelnen Gerätetypen verfügbaren Funktionen. Eine Liste aller von Cisco Business Dashboard unterstützten Geräten finden Sie unter Cisco Business Dashboard − Liste der unterstützten Geräte.
- **Kurzanleitung**: Dieses Handbuch enthält Informationen zum Durchführen der Ersteinrichtung für Cisco Business Dashboard mit den am häufigsten ausgewählten Optionen. Eine Übersicht der für die Verwaltung eines Netzwerks erforderlichen grundlegenden Aufgaben finden Sie in der Kurzanleitung zu Cisco Business Dashboard.
- **Installationshandbücher**

  In der folgenden Tabelle sind alle Installationshandbücher zur Cisco Business Dashboard-Software aufgeführt, die auf verschiedenen Plattformen bereitgestellt werden kann. Weitere Informationen finden Sie unter dem Pfad in der Spalte „Location“ (Standort):

Unterstützte Plattformen	Standort
Amazon Web Services	Cisco Business Dashboard – Installationshandbuch für Amazon Web Services
Oracle VirtualBox	Cisco Business Dashboard – Installationshandbuch für Oracle VirtualBox
Microsoft Hyper-V	Cisco Business Dashboard – Installationshandbuch für Microsoft Hyper-V
VMware vSphere, Workstation und Fusion	Cisco Business Dashboard – Installationshandbuch für VMWare
Ubuntu Linux (Dashboard und Probe) und Raspbian Linux (nur Probe)	Cisco Business Dashboard − Installationshandbuch für Linux

Terminologie

Begriff	Beschreibung
Hyper-V	Eine von der Microsoft Corporation bereitgestellte Virtualisierungsplattform
OVF (Open Virtualization Format)	Ein TAR-Archiv mit einem oder mehreren virtuellen Systemen im OVF-Format. Es handelt sich dabei um eine plattformunabhängige Methode zum Verpacken und Verteilen von virtuellen Systemen (Virtual Machines, VMs).
OVA-Datei (Open Virtual Appliance oder Open Virtual Application)	Ein Paket, das die folgenden Dateien zum Beschreiben eines virtuellen Systems enthält, die in einem TAR-Archiv gespeichert sind: • Descriptor-Datei (.OVF) • Manifestdatei (.MF) und Zertifikatsdateien (optional)
Raspberry Pi	Ein sehr kostengünstiger Einplatinencomputer, der von der Raspberry Pi Foundation entwickelt wurde. Weitere Informationen finden Sie unter *https://www.raspberrypi.org/*.
Raspbian	Eine Debian-basierte Linux-Distribution, die für den Raspberry Pi optimiert ist. Weitere Informationen finden Sie unter *https://www.raspbian.org/*.
VirtualBox	Eine von der Oracle Corporation bereitgestellte Virtualisierungsplattform
VHD (Virtual Hard Disk, virtuelle Festplatte)	VHD ist ein Format für Laufwerks-Images zum Speichern des gesamten Inhalts einer Festplatte.
VM (Virtual Machine, virtuelles System)	Eine virtuelle Computing-Umgebung, in der ein Gastbetriebssystem und entsprechende Anwendungssoftware ausgeführt werden können. Auf einem Hostsystem können mehrere VMs gleichzeitig betrieben werden.
• VMware ESXi • VMware Fusion • vSphere Server • VMware Workstation	Eine von VMware Inc. bereitgestellte Virtualisierungsplattform

Begriff	Beschreibung
vSphere-Client	Eine Benutzeroberfläche, über die Benutzer von jedem Windows-PC aus eine Remoteverbindung zu vCenter Server oder ESXi herstellen können. Über die Hauptoberfläche von vSphere Client können Sie VMs, deren Ressourcen und die zugehörigen Hosts erstellen, verwalten und überwachen. Außerdem bietet sie Konsolenzugriff auf VMs.

Systemvoraussetzungen für Cisco Business Dashboard

Cisco Business Dashboard wird als Image für virtuelle Computer und als Installationsprogramm zur Verwendung mit der Ubuntu Linux-Distribution angeboten und ist über den AWS Marketplace (*https://aws.amazon.com/marketplace*) für Amazon Web Services (AWS) verfügbar.

Wenn Sie Cisco Business Dashboard auf einem virtuellen Computer ausführen, muss einer der folgenden Hypervisoren genutzt werden:

- Microsoft Hyper-V, Version 10.0 oder höher
- Oracle VirtualBox, Version 6.1 oder höher
- VMware
    - ESXi, Version 6.0 oder höher
    - Fusion, Version 11.5 oder höher
    - Workstation, Version 15.1 oder höher

Für die Ausführung von Cisco Business Dashboard unter Ubuntu Linux muss in Ihrer Umgebung Ubuntu Version 16.04.x (Xenial Xerus) auf einer 64-Bit-Intel-Architekturplattform ausgeführt werden. Cisco empfiehlt, die Ubuntu-Serververteilung zu verwenden und nur die für Cisco Business Dashboard erforderlichen Pakete zu installieren.

In Tabelle 1 sind die für Cisco Business Dashboard erforderlichen Computerressourcen nach Anzahl der verwalteten Geräte aufgeführt.

Tabelle 1: Cisco Business Dashboard Anforderungen an die Computerressourcen

Unterstützte Geräteanzahl	Anzahl vCPUs	RAM	Festplattenspeicher
Bis zu 300	2	4 GB	60 GB
Bis zu 2.500	12	24 GB	60 GB

Zum Ausführen von Cisco Business Dashboard in AWS benötigen Sie ein AWS-Konto. Die folgenden AWS-Instanztypen werden unterstützt:

- c5.large − bis zu 300 verwaltete Geräte
- c5.4xlarge – bis zu 2.500 verwaltete Geräte

Cisco Business Dashboard wird über eine webbasierte Benutzeroberfläche verwaltet. Dazu benötigen Sie einen der folgenden Browser:

- Apple Safari (nur MacOS) − zwei aktuelle Hauptversionen
- Google Chrome − aktuelle Version
- Microsoft Edge − zwei aktuelle Hauptversionen
- Mozilla Firefox − aktuelle Version

Hinweis Wenn Sie Safari verwenden, stellen Sie sicher, dass für das von Cisco Business Dashboard Probe bereitgestellte Zertifikat **Always Trust** (Immer vertrauen) ausgewählt ist. Andernfalls treten bei bestimmten Funktionen, die die Verwendung sicherer WebSockets voraussetzen, höchstwahrscheinlich Fehler auf. Das ist eine Einschränkung bei der Verwendung von Safari.

Ihr Netzwerk muss alle Instanzen von Cisco Business Dashboard Probe zulassen, um eine TCP-Netzwerkverbindung zu Cisco Business Dashboard herstellen zu können. Detaillierte Informationen zu den verwendeten Ports und Protokollen finden Sie im Kapitel Häufig gestellte Fragen.

Systemvoraussetzungen für Cisco Business Dashboard Probe

Cisco Business Dashboard Probe wird als Image für virtuelle Computer und als Installationsprogramm zur Verwendung mit folgenden Betriebssystemen angeboten:

- Ubuntu Linux-Distribution auf einem PC
- Raspbian Linux-Distribution auf einem Raspberry Pi

Cisco Business Dashboard Probe ist auch als eingebettete Funktion ausgewählter Cisco Produkte der Serien 100 bis 500 erhältlich.

Wenn Sie Cisco Business Dashboard Probe als virtuellen Computer ausführen möchten, müssen in Ihrer Umgebung die folgenden Voraussetzungen erfüllt sein:

- Hypervisor:
  - Microsoft Hyper-V, Version 10.0 oder höher
  - Oracle VirtualBox, Version 6.1 oder höher
  - VMware
    - ESXi, Version 6.0 oder höher
    - Fusion, Version 11.5 oder höher
    - Workstation, Version 15.1 oder höher
  - Ressourcenanforderungen des virtuellen Systems:
    - CPU: 1x 64-Bit-Intel-Architektur
    - Arbeitsspeicher: 512 MB

- Festplattenspeicher: 5 GB

Wenn Sie Cisco Business Dashboard unter dem Betriebssystem Ubuntu Linux ausführen möchten, müssen in Ihrer Umgebung die folgenden Voraussetzungen erfüllt sein:

- Ubuntu Version 16.04.x (Xenial Xerus)
- CPU: 1x 64-Bit-Intel-Architektur
- Arbeitsspeicher: 512 MB
- Festplattenspeicher: 5 GB

Wenn Sie Cisco Business Dashboard Probe unter einem Raspberry Pi-Betriebssystem ausführen möchten, müssen in Ihrer Umgebung die folgenden Voraussetzungen erfüllt sein:

- Hardware: Raspberry Pi 3 Model B/B+ oder Raspberry Pi 4 Model B
- Festplattenspeicher: 5 GB
- Betriebssystem: Raspbian Buster

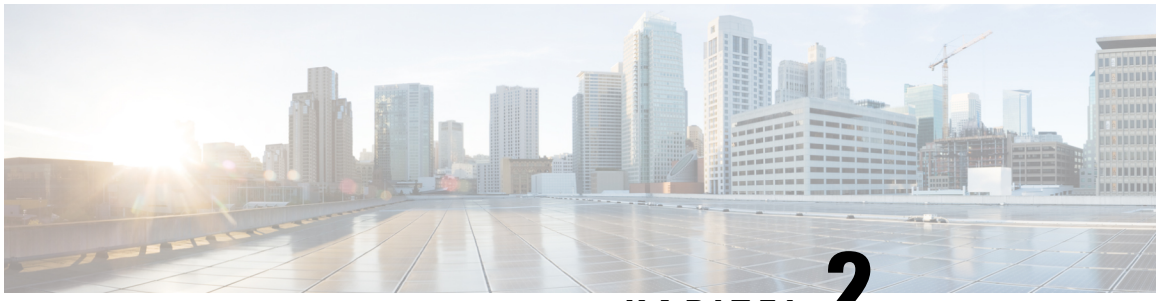
Um Cisco Business Dashboard Probe als eingebettete Anwendung auf einem Cisco Produkt auszuführen, benötigen Sie ein unterstütztes Produkt, auf dem eine Firmware-Version ausgeführt wird, die die Cisco Business Dashboard Probe-Funktion unterstützt. Weitere Informationen zu den Hardware- und Versionsanforderungen finden Sie hier: Cisco Business Dashboard – Liste der unterstützten Geräte. Weitere plattformspezifische Anforderungen können Sie dem Administratorhandbuch zum Produkt entnehmen.

Cisco Business Dashboard Probe wird über eine webbasierte Benutzeroberfläche verwaltet. Dazu benötigen Sie einen der folgenden Browser:

- Apple Safari (nur MacOS) − zwei aktuelle Hauptversionen
- Google Chrome − aktuelle Version
- Microsoft Edge − zwei aktuelle Hauptversionen
- Mozilla Firefox − aktuelle Version

Cisco Business Dashboard Probe überwacht Netzwerkgeräte, die die folgenden Anforderungen erfüllen, und greift darauf zu:

- Sie müssen sich im selben Subnetz wie der PC befinden, auf dem Cisco Business Dashboard Probe ausgeführt wird, oder direkt mit einem verwalteten Gerät verbunden und über TCP/IP erreichbar sein.
- Muss ein unterstütztes Cisco Business- oder Cisco Small Business-Gerät der Serie 100 bis 500 sein



KAPITEL 2

Verwenden von Cisco Business Dashboard und Probe

Dieses Kapitel enthält folgende Abschnitte:

Verwenden der Cisco Business Dashboard-GUI

Übersicht der GUI von Cisco Business Dashboard mit einer Beschreibung der Links im Navigationsbereich

Startseite

Abbildung 1: Cisco Business Dashboard –Startseite

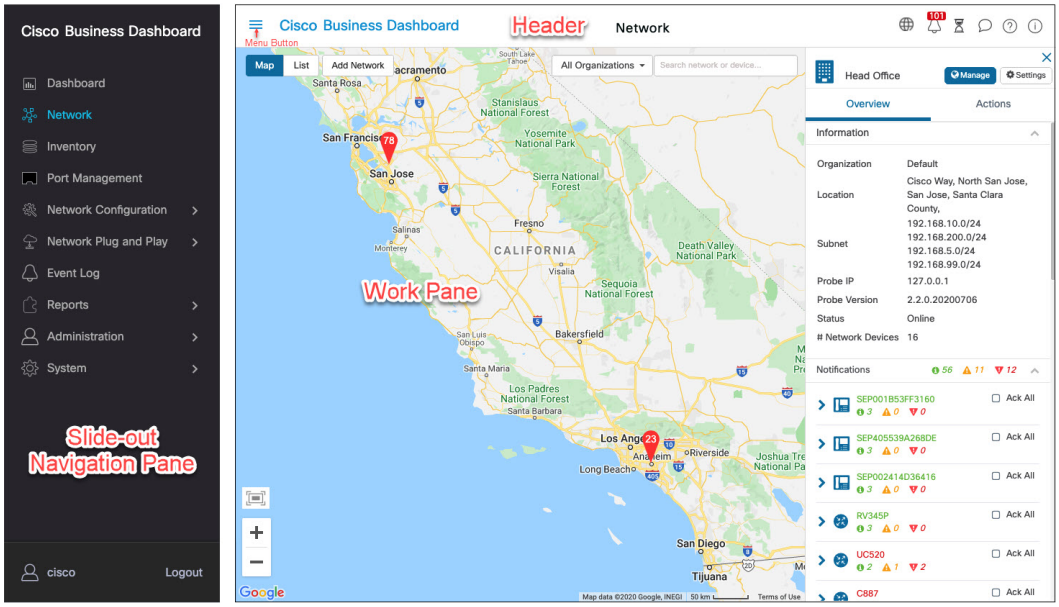


Tabelle 2: Cisco Business Dashboard –Startseite

Name	Beschreibung
Navigationsbereich	Bietet Zugriff auf die Funktionen von Cisco Business Dashboard. Der Navigationsbereich wird angezeigt, wenn auf das **Menü**-Symbol geklickt wird und es nach einer Auswahl ausgeblendet wird. Der aktuell angemeldete Benutzer wird unten im Navigationsbereich angezeigt.
Arbeitsbereich	In diesem Bereich wird die Benutzeroberfläche der Funktionen angezeigt. Wenn Sie im **Navigationsbereich** auf eine Option klicken, wird das entsprechende Fenster in diesem Bereich geöffnet.
Kopfleiste	Die Symbolleiste im Kopfbereich enthält folgende Optionen: • Eine Menüschaltfläche zum Anzeigen des Navigationsbereichs • Kopfzeilentext • eine Reihe von Symbolen für Funktionen wie Sprachauswahl, Benachrichtigungen, Aufgabenaktivitäten, Feedback, Kontexthilfe und Versionsinformationen

Optionen im Navigationsbereich

Der **Navigationsbereich** enthält Optionen zum Zugriff auf die Hauptfunktionen von Cisco Business Dashboard.

Tabelle 3: Optionen im Navigationsbereich

Symbol	Name	Beschreibung
	**Dashboard**	Im **Dashboard** können Sie die Leistung Ihres Netzwerks im zeitlichen Verlauf anzeigen. Zudem lassen sich hier das Datenverkehrsaufkommen und die Anzahl der verbundenen Geräte sowie weitere Netzwerkdetails überwachen.
	**Netzwerk**	Zeigt eine Übersicht aller Standorte im Netzwerk in Karten- oder Listenform an. Enthält verschiedene Ansichten der einzelnen Netzwerke und der erkannten Netzwerkgeräte. Sie können u. a. die Netzwerktopologie und einen Etagenplan mit dem physischen Layout des Netzwerks anzeigen.
	**Bestand**	Unter **Inventory** (Bestand) finden Sie eine Liste aller Geräte im Netzwerk. Dort können Sie detaillierte Informationen zu den Geräten anzeigen und Aktionen wie Firmware-Updates, Konfigurations-Backups und Neustarts durchführen.
	**Portverwaltung**	Unter **Port Management** (Portverwaltung) erhalten Sie eine Ansicht der Vorderseiten der Netzwerkgeräte. Sie können Details zu den einzelnen Ports anzeigen und die Konfiguration ändern.

Symbol	Name	Beschreibung
	**Netzwerkkonfiguration**	Auf der Seite **Network Configuration** (Netzwerkkonfiguration) können Sie die Konfigurationsprofile für Ihr Netzwerk verwalten.
	**Network Plug and Play**	Mithilfe von **Network Plug and Play** können Netzwerkgeräte völlig ohne Benutzerinteraktion bereitgestellt werden. Firmware und Konfigurationsdateien werden während der Installation automatisch von Cisco Business Dashboard heruntergeladen.
	**Ereignisprotokoll**	Auf der Seite **Event Log** (Ereignisprotokoll) finden Sie eine Liste aller Ereignisse, die im Netzwerk eingetreten sind. Mithilfe von Filtern können Sie diese Liste auf die Ereignisse eingrenzen, die für Sie von Interesse sind.
	**Berichte**	Unter der Überschrift „Berichte“ finden Sie eine Reihe von Berichten mit Informationen zum Lebenszyklus Ihrer Netzwerkgeräte, u. a. End-of-Life-Bulletins, Garantieinformationen und Details zum Servicevertrag.
	**Verwaltung**	Auf den Seiten unter „Administration“ (Verwaltung) können Sie Cisco Business Dashboard verwalten.
	**System**	Die Seiten unter **System** dienen zum Verwalten der Cisco Business Dashboard-Anwendung.
	**Benutzeroptionen**	Der aktuell angemeldete Benutzer wird unten in der Navigationsleiste zusammen mit einer Option zum **Abmelden** angezeigt. Klicken Sie auf den Benutzernamen, um die Profilseite des Benutzers anzuzeigen.

Optionen in der Kopfleiste

Über die **Kopfleiste** können Sie auf andere Systemfunktionen zugreifen. Außerdem werden dort Systembenachrichtigungen angezeigt.

Tabelle 4: Optionen in der Kopfleiste

Symbol	Option	Beschreibung
	**Menü-Taste**	Befindet sich oben links in der Kopfleiste. Durch Klicken auf diese Schaltfläche wird der Navigationsbereich angezeigt.
	**Sprachauswahl**	In diesem Dropdown-Menü können Sie die Sprache für die Benutzeroberfläche auswählen.

Symbol	Option	Beschreibung
	**Benachrichtigungscenter**	Dieses Symbol zeigt die Anzahl und den Schweregrad der ausstehenden Benachrichtigungen aus Cisco Business Dashboard an. Klicken Sie auf dieses Symbol, um den Benachrichtigungsbereich anzuzeigen. In diesem Bereich können Sie die angezeigten Benachrichtigungsereignisse filtern. Weitere Informationen finden Sie in diesem Leitfaden unter Anzeigen und Filtern aktueller Gerätebenachrichtigungen, auf Seite 101.
	**Job Center**	Zeigt den Status der aktuell ausgeführten Jobs und den Verlauf der vergangenen Jobs an. Zu den Jobs gehören alle von Cisco Business Dashboard ausgeführten Aktionen, einschließlich Jobs, die von Benutzern initiiert wurden, und Systemjobs. Klicken Sie auf dieses Symbol, um ausstehende, laufende und abgeschlossene Jobs anzuzeigen.
	**Feedback**	Über diese Schaltfläche können Sie Feedback zu Ihren Erfahrungen mit Cisco Business Dashboard und ggf. Verbesserungsvorschläge übermitteln.
	**Hilfe**	Über diese Schaltfläche gelangen Sie zur Onlinehilfe für Cisco Business Dashboard.
	**Informationen zu Cisco Business Dashboard**	Mit einem Klick auf dieses Symbol können Sie Informationen zu Cisco Business Dashboard abrufen, beispielsweise die aktuelle Version. Ist eine neue Version verfügbar, wird das Symbol mit einer Kennzeichnung versehen. Im zugehörigen Popup-Fenster finden Sie dann einen Link, über den Sie das Update installieren können.

Verwenden der Cisco Business Dashboard Probe-GUI

Wenn Sie sich bei Cisco Business Dashboard Probe angemeldet haben, wird die **Startseite** angezeigt.

Abbildung 2: Cisco Business Dashboard –Startseite

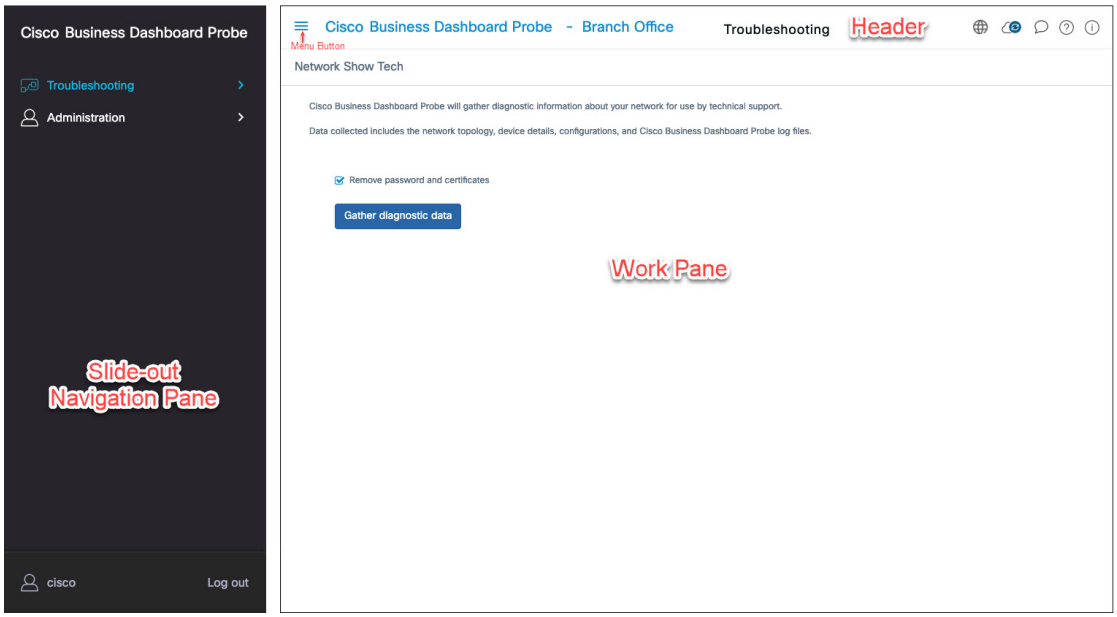


Tabelle 5: Cisco Business Dashboard –Startseite

Name	Beschreibung
Navigationsbereich	Bietet Zugriff auf die Funktionen von Cisco Business Dashboard Probe. Der Navigationsbereich wird angezeigt, wenn auf die Menü-Schaltfläche geklickt wird und es nach einer Auswahl ausgeblendet wird. Der aktuell angemeldete Benutzer wird unten im Navigationsbereich angezeigt.
Arbeitsbereich	In diesem Bereich wird die Benutzeroberfläche der Funktionen angezeigt. Wenn Sie im **Navigationsbereich** auf eine Option klicken, wird das entsprechende Fenster in diesem Bereich geöffnet.
Kopfleiste	Die Symbolleiste im Kopfbereich enthält folgende Optionen: • Eine Menüschaltfläche zum Anzeigen des Navigationsbereichs • Kopftext, u. a. den Standortnamen von Probe • ein Dropdown-Menü zur Sprachauswahl • eine Reihe von Symbolen für Funktionen wie Benachrichtigungen, Feedback und Kontexthilfe

Optionen im Navigationsbereich

Der **Navigationsbereich** enthält Optionen zum Zugriff auf die Hauptfunktionen von Cisco Business Dashboard Probe.

Tabelle 6: Optionen im Navigationsbereich

Symbol	Name	Beschreibung
	**Fehlerbehebung**	Im Abschnitt **Fehlerbehebung** finden Sie Diagnosetools, die Ihnen beim Ermitteln von Problemen im Netzwerk helfen können.
	**Verwaltung**	Auf der Seite „Administration“ (Verwaltung) können Sie die Cisco Business Dashboard Probe-Netzwerkanwendung verwalten.
	**Benutzeroptionen**	Der aktuell angemeldete Benutzer wird unten in der Navigationsleiste zusammen mit einer Option zum **Abmelden** angezeigt. Klicken Sie auf den Benutzernamen, um die Profilseite des Benutzers anzuzeigen.

Optionen in der Kopfleiste

Über die **Kopfleiste** können Sie auf andere Systemfunktionen zugreifen. Außerdem werden dort Systembenachrichtigungen angezeigt.

Tabelle 7: Optionen in der Kopfleiste

Symbol	Option	Beschreibung
	**Menü-Taste**	Befindet sich oben links in der Kopfleiste. Durch Klicken auf diese Schaltfläche wird der Navigationsbereich angezeigt.
	**Sprachauswahl**	In diesem Dropdown-Menü können Sie die Sprache für die Benutzeroberfläche auswählen.
	**Dashboard-Status**	Der Status der Verbindung zwischen Cisco Business Dashboard und Probe. Klicken Sie auf dieses Symbol, um die Dashboard-Benutzeroberfläche zu öffnen.
	**Feedback**	Über diese Schaltfläche können Sie Feedback zu Ihren Erfahrungen mit Cisco Business Dashboard Probe und ggf. Verbesserungsvorschläge übermitteln.
	**Hilfe**	Über diese Schaltfläche gelangen Sie zur Onlinehilfe für Cisco Business Dashboard Probe.
	**Über Cisco Business Dashboard Probe**	Mit einem Klick auf dieses Symbol können Sie Informationen zu Cisco Business Dashboard Probe abrufen, beispielsweise die aktuelle Version. Ist eine neue Version verfügbar, wird das Symbol mit einer Kennzeichnung versehen. Im zugehörigen Popup-Fenster finden Sie dann einen Link, über den Sie das Update installieren können.

Aktualisieren von Cisco Business Dashboard und Probe

Von Zeit zu Zeit veröffentlicht Cisco neue Versionen und Updates für Cisco Business Dashboard und Probe, die im Software Center auf cisco.com bereitgestellt werden. Cisco Business Dashboard überprüft das Software Center regelmäßig auf Updates. Wird ein Update gefunden, wird im Kopfzeilenbereich der Benutzeroberfläche unter **About Cisco Business Dashboard** (Über Business Cisco Dashboard) eine Kennzeichnung angezeigt. Wenn Sie auf diesen Link klicken, lädt das Dashboard das Update herunter und installiert es. Alternativ können Sie Updates auch selbst herunterladen und manuell installieren.

Gehen Sie folgt vor, wenn das Dashboard das Update herunterladen und installieren soll:

1. Klicken Sie auf **About Cisco Business Dashboard**, um das Popup **About Cisco Business Dashboard** zu öffnen. Wenn Updates für das Dashboard oder eine oder mehrere dem Dashboard zugeordneten Probe-Instanzen verfügbar sind, werden sie in diesem Fenster aufgeführt.
2. Sollte ein Update für das Dashboard verfügbar sein: Aktivieren Sie das zu dem Update gehörende Optionsfeld und klicken Sie auf **Upgrade** (Aktualisieren).

   Das Dashboard lädt das Update herunter und installiert es. Den Fortschritt des Vorgangs können Sie jederzeit im Popup-Fenster **About Cisco Business Dashboard** mitverfolgen. Nach erfolgreicher Installation des Updates wird die Dashboard-Anwendung neu gestartet.

Gehen Sie wie folgt vor, um ein Dashboard-Update manuell zu installieren:

1. Laden Sie die Cisco Business Dashboard-Linux-Installationsdatei herunter, indem Sie zu *https://cisco.com/go/cbd-sw* navigieren und im Produktauswahlbereich unten rechts die Option **Download Software** (Software herunterladen) auswählen.
2. Kopieren Sie die Installationsprogrammdatei in das Dateisystem von Dashboard.
3. Geben Sie den Befehl `sh <filename of installer>` ein, um das Installationsprogramm auszuführen. Beispiel: `sh cisco-business-dashboard-2.2-ubuntu-xenial-amd64.sh`. Geben Sie Ihr Kennwort ein, falls sudo Sie dazu auffordert. Während dieses Vorgangs wird die Dashboard-Anwendung neu gestartet.

Sie können über das Dashboard auch Updates auf alle Probe-Instanzen im Netzwerk anwenden. Dabei können Sie entweder alle Network Probe-Instanzen gleichzeitig aktualisieren oder auch nur einzelne Network Probe-Instanzen.

Gehen Sie wie folgt vor, um über das Dashboard alle Probe-Instanzen gleichzeitig zu aktualisieren:

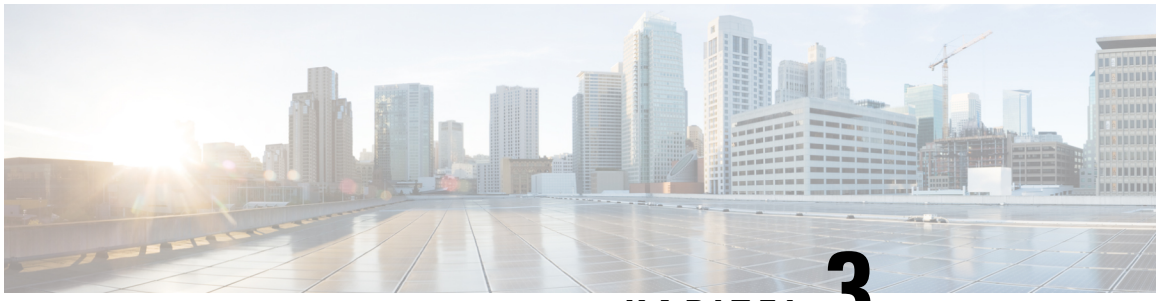
1. Klicken Sie auf **About Cisco Business Dashboard**, um das Popup **About Cisco Business Dashboard** zu öffnen. Wenn Updates für das Dashboard oder eine oder mehrere dem Dashboard zugeordneten Probe-Instanzen verfügbar sind, werden sie in diesem Fenster aufgeführt.
2. Falls ein Update für das Dashboard verfügbar ist: Installieren Sie dieses Update, bevor Sie die Probe-Instanzen aktualisieren. Sollten Sie versuchen, die Network Probe-Instanzen zuerst zu aktualisieren, wird eine Fehlermeldung angezeigt.
3. Aktivieren Sie das Optionsfeld neben dem Network Probe-Update, und klicken Sie auf **Upgrade**.
4. Den Fortschritt des Updates können Sie auf der Network Probe-Benutzeroberfläche mitverfolgen.

Gehen Sie wie folgt vor, um über das Dashboard eine einzelne Probe-Instanz zu aktualisieren:

1. Falls ein Update für das Dashboard verfügbar ist: Installieren Sie dieses Update, bevor Sie die Probe-Instanzen aktualisieren. Sollten Sie versuchen, die Probe-Instanz zu aktualisieren, bevor das Dashboard aktualisiert wurde, wird eine Fehlermeldung angezeigt.
2. Klicken Sie im Navigationsbereich auf **Network** (Netzwerk). Wählen Sie unter **Kartenansicht** oder in der **Listenansicht** das Netzwerk aus, das aktualisiert werden soll.
3. Klicken Sie im Bereich **Basic Info** (Basisinformationen) des Netzwerks auf die Registerkarte **Actions** (Aktionen).
4. Klicken Sie auf **Upgrade**.

   Den Fortschritt des Updates können Sie im Jobcenter mitverfolgen.

Hinweis Wenn Sie eine eingebettete Probe-Instanz verwenden, die auf einem Netzwerkgerät ausgeführt wird, finden Sie in der Dokumentation für dieses Gerät Informationen zum Durchführen von Updates. Einige Geräte unterstützen keine von der Geräte-Firmware unabhängige Aktualisierung der Probe-Anwendung.



KAPITEL 3

Überwachungs-Dashboard

Dieses Kapitel enthält folgende Abschnitte:

Informationen zum Überwachungs-Dashboard

Auf der Seite **Dashboard** in Cisco Business Dashboard können Sie die Leistung des Netzwerks und der zugehörigen Geräte in Echtzeit anzeigen und die Daten in einem grafischen Format abrufen. Das Überwachungs-Dashboard besteht aus einer anpassbaren Zusammenstellung aus von den Benutzern auswählbaren Widgets. Folgende Widgets sind standardmäßig im Dashboard enthalten:

- Widget **Inventory Summary** (Bestandszusammenfassung): Zeigt eine Aufschlüsselung der im Netzwerk erkannten Geräte an.
- Widget **Device Health** (Geräteintegrität): Zeigt die Gesamtintegrität der Geräte im Netzwerk an.
- Widget **WLAN Client Count** (Anzahl WLAN-Clients): Zeigt die Anzahl der dem ausgewählten Wireless-Netzwerk zugeordneten Geräte an.
- Widget **Device Client Count** (Anzahl Geräte-Clients): Zeigt die Anzahl der dem ausgewählten Wireless Access Point zugeordneten Geräte an.
- Widget **Wireless-Top Ten**: Zeigt die zehn Wireless-Netzwerke, Access Points oder Clients mit dem höchsten Datenverkehrsaufkommen bzw. den meisten Clients an.
- Widget **Traffic** (Verkehr): Zeigt ein Diagramm des durch die ausgewählte Schnittstelle fließenden Datenverkehrs an.

Mit den Steuerungen der einzelnen Widgets können Sie anpassen, welche Daten angezeigt werden. Über die Dropdown-Liste „Organization“ (Organisation) oben rechts im **Dashboard** können Sie die angezeigten Informationen auf eine bestimmte Organisation beschränken.

In den grafischen Widgets können Sie auf die Beschriftungen in der Legende im Diagramm klicken, um die Anzeige des jeweiligen Datensatzes umzuschalten. So können Sie die angezeigten Daten weiter verfeinern.

Hinzufügen eines Widgets

Mithilfe dieser Funktionen können Sie ein oder mehrere Widgets zu den im Dashboard angezeigten Standard-Widgets hinzufügen, um bestimmte Aufgaben auf einem Gerät oder in einem Netzwerk zu überwachen.

Schritt 1 Klicken Sie auf das Zahnradsymbol oben rechts im Dashboard-Fenster, und wählen Sie **Add Widget** (Widget hinzufügen) aus.

Schritt 2 Wählen Sie den gewünschten Widget-Typ aus der Popup-Liste aus Das neu ausgewählte Widget wird im Dashboard angezeigt.

Schritt 3 Ziehen Sie das neue Widget an die gewünschte Position im Dashboard, und ändern Sie die Größe bei Bedarf.

Schritt 4 Klicken Sie erneut auf das Zahnradsymbol, und wählen Sie **View Mode** (Ansichtsmodus) aus, um die Änderungen zu übernehmen.

Ändern eines Widgets

Schritt 1 Verwenden Sie die Dropdown-Listen im neuen Widget, um diejenigen Daten auszuwählen, die Sie anzeigen möchten.

Schritt 2 Klicken Sie auf das Zahnradsymbol oben rechts im Widget, um Parameter wie Probenintervalle oder Schwellenwerte zu ändern. Sie können auch auf das Bearbeitungssymbol klicken, das im Widget angezeigt wird, wenn sich das Dashboard im **Bearbeitungsmodus** befindet, um den Titel des Widgets zu ändern.

Löschen eines Widgets

Schritt 1 Klicken Sie auf das Zahnradsymbol oben rechts im Dashboard-Fenster, und wählen Sie **Edit Mode** (Bearbeitungsmodus) aus.

Schritt 2 Klicken Sie oben rechts auf das Symbol **Widget entfernen**, um das Widget zu entfernen. Ordnen Sie die verbleibenden Widgets nach Belieben neu an.

Schritt 3 Klicken Sie erneut auf das Zahnradsymbol, und wählen Sie **View Mode** (Ansichtsmodus) aus, um die Änderungen zu übernehmen.

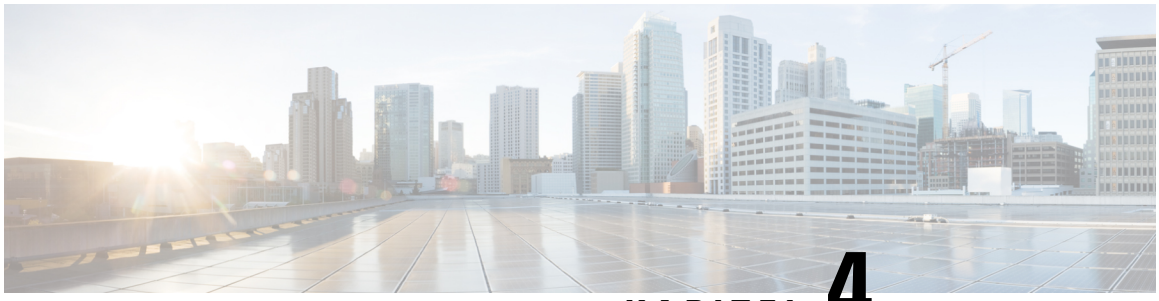
Ändern des Dashboard-Layouts

Das Layout des **Dashboards** kann mit den folgenden Schritten einfach angepasst werden:

Schritt 1 Klicken Sie auf das Zahnradsymbol oben rechts im Dashboard-Fenster, und wählen Sie **Edit Mode** (Bearbeitungsmodus) aus.

Schritt 2 Klicken Sie in die Kopfzeile eines Widgets, und verschieben Sie das Widget im **Dashboard** durch Ziehen. Die anderen Widgets passen sich dynamisch an, um Platz zu schaffen. Klicken und ziehen Sie am Rand oder an der Ecke eines Widgets, um die Größe zu ändern. Wenn Sie das Layout neu anordnen, wird die Größe des Dashboards dynamisch an die verfügbare Breite angepasst.

Schritt 3 Klicken Sie erneut auf das Zahnradsymbol, und wählen Sie **View Mode** (Ansichtsmodus) aus, um die Änderungen zu übernehmen.



KAPITEL 4

Vermittlung

Dieses Kapitel enthält folgende Abschnitte:

Informationen zu „Network“ (Netzwerk)

Auf der Seite **Network** (Netzwerk) finden Sie eine Übersicht über das gesamte Netzwerk, wahlweise in Form einer Standortliste oder in Form einer Landkarte, auf der die geografische Position und der Status jedes Standorts verzeichnet sind. In der **Kartenansicht** weisen Zahlen bei den Netzwerksymbolen Sie darauf hin, wie viele unbestätigte Benachrichtigungen für einen Standort vorliegen. Dabei können Sie an der Farbe des Symbols erkennen, welchen Schweregrad die unbestätigte Nachricht mit der höchsten Priorität hat. In der **Listenansicht** finden Sie dieselben Informationen in der letzten Spalte der Tabelle. Wenn Sie genauere Informationen zu einem Netzwerk einsehen möchten, klicken Sie auf das Netzwerksymbol oder auf die Tabellenzeile des entsprechenden Standorts.

Wenn zwei oder mehr Netzwerksymbole zu eng auf der Karte positioniert sind, um sie leicht zu unterscheiden, werden sie durch ein einzelnes Clustersymbol ersetzt. Wenn Sie auf das Clustersymbol klicken, wird die Karte automatisch auf eine Ebene gezoomt, auf der die Netzwerke in diesem Cluster getrennt betrachtet werden können.

In der **Netzwerkübersicht** stehen folgende Steuerelemente zur Verfügung:

- Auswahl **Map/List** (Karte/Liste): Verwenden Sie dieses Steuerelement, um Netzwerke auf einer Karte oder in einer Tabelle anzuzeigen.
- Schaltfläche **Add Network** (Netzwerk hinzufügen): Verwenden Sie diese Schaltfläche, um einen neuen Netzwerkdatensatz zu erstellen, bevor Sie eine Probe-Instanz für dieses Netzwerk bereitstellen.
- Dropdown-Liste **Organization** (Organisation): Wählen Sie eine einzelne Organisation aus der Dropdown-Liste aus, um die angezeigten Netzwerke einzuschränken.

- Feld **Search** (Suchen): In diesem Feld können Sie den Namen, die Adresse oder die IP-Adresse eines Netzwerks vollständig oder teilweise eingeben, um das Netzwerk auf der Karte zu lokalisieren. Alternativ können Sie den Namen, die IP-Adresse, die Seriennummer oder die MAC-Adresse eines Geräts vollständig oder teilweise eingeben, um herauszufinden, in welchem Netzwerk sich das Gerät befindet. Bereits während der Eingabe wird eine Liste passender Suchergebnisse angezeigt. Wenn mit dem Mauszeiger auf ein Ergebnis zeigen, wird das zugehörige Netzwerk hervorgehoben. Sobald Sie ein Ergebnis auswählen, wird das zugehörige Netzwerk ausgewählt und zum Mittelpunkt der Ansicht gemacht.
- **Zoom**-Steuerelemente: Mit diesen Steuerelementen können Sie die Kartenansicht vergrößern und verkleinern. Klicken Sie zum Vergrößern auf das Pluszeichen (**+**) und zum Verkleinern auf das Minuszeichen (**−**).
- Schaltfläche **Fit-to-view** (Ansicht anpassen): Mit dieser Schaltfläche wird die Karte automatisch so gezoomt, dass alle Netzwerkmarkierungen angezeigt werden können.

Sie können auch überall im Kartenbereich klicken und ziehen, um die Karte im **Arbeitsbereich** zu verschieben.

In der **Listenansicht** sind folgende Steuerelemente verfügbar:

- Auswahl **Map/List** (Karte/Liste): Verwenden Sie dieses Steuerelement, um Netzwerke auf einer Karte oder in einer Tabelle anzuzeigen.
- Symbol **Column Select** (Spaltenauswahl): Über dieses Symbol können Sie die anzuzeigenden Spalten auswählen. Sie können auf die Spaltenüberschriften klicken, um die Tabelle zu sortieren.
- **Add Network** (Netzwerk hinzufügen): Klicken Sie auf das Pluszeichen (**+**), um ein neues Netzwerk hinzuzufügen, bevor Sie eine Probe-Instanz für dieses Netzwerk bereitstellen.
- **Refresh** (Aktualisieren): Klicken Sie auf diese Schaltfläche, um die Tabelle zu aktualisieren und die aktuellsten Informationen anzuzeigen.
- Dropdown-Liste **Organization** (Organisation): Wählen Sie eine einzelne Organisation aus der Dropdown-Liste aus, um die angezeigten Netzwerke einzuschränken.
- Feld **Search** (Suchen): In diesem Feld können Sie den Namen, die Adresse oder die IP-Adresse eines Netzwerks vollständig oder teilweise eingeben, um nur die diesen Kriterien entsprechenden Netzwerke in der Tabelle anzuzeigen.

Wenn Sie auf ein Netzwerksymbol oder eine Netzwerkzeile klicken, wird der Bereich **Basic Info** (Basisinformationen) für das betreffende Netzwerk geöffnet. Der Bereich **Basic Info** (Basisinformationen) enthält folgende Angaben:

- Netzwerkname
- Die Organisation, zu der das Netzwerk gehört
- Die physische Adresse des Netzwerks
- Die Probe-IP-Adresse des Netzwerks und alle im Netzwerk erkannten IP-Subnetze
- Die Version der Network Probe-Software
- Den Verbindungsstatus
- Die Anzahl verwalteter Geräte im jeweiligen Netzwerk
- Eine Liste aller aktuellen, noch unbestätigten Benachrichtigungen für das Netzwerk

- Eine Liste der in den letzten 24 Stunden für dieses Netzwerk erfassten Ereignisse

Sie können über den Bereich **Basic Info** (Basisinformationen) auch folgende Aktionen für ein Netzwerk ausführen:

- Klicken Sie auf **Manage** (Verwalten), um detaillierte Informationen zum Netzwerk anzuzeigen, u. a. die Netzwerktopologie und Etagenpläne.
- Klicken Sie auf **Settings** (Einstellungen), um den Bereich **Network Detail** (Netzwerkdetails) anzuzeigen. Weitere Informationen über den Bereich **Network Detail** (Netzwerkdetail) finden Sie unter Informationen zu „Network Detail“ (Netzwerkdetails), auf Seite 21.
- Klicken Sie auf die Registerkarte **Actions** (Aktionen), um weitere für das Netzwerk verfügbare Aktionen anzuzeigen.
  - Klicken Sie auf **Remove** (Entfernen), um das Netzwerk und alle ihm zugeordneten Daten aus dem Dashboard zu löschen.
  - Klicken Sie auf **Upgrade**, um die in diesem Netzwerk installierte Probe-Software zu aktualisieren.
  - Klicken Sie auf **Show Tech** (Technische Informationen), um ein Archiv mit technischen Netzwerkinformationen für dieses Netzwerk zu generieren.

Informationen zu „Network Detail“ (Netzwerkdetails)

Im Bereich **Network Detail** (Netzwerkdetails) können Sie Informationen anzeigen und aktualisieren, die für dieses Netzwerk spezifisch sind. Zu diesen Informationen zählen:

- Wichtige Netzwerkparameter, einschließlich Netzwerkname, Beschreibung, Organisation und Standardgerätegruppe
- Standort des Netzwerks
- Anmeldeinformationen, die beim Hochladen von Bestandsinformationen in Cisco Active Advisor für das Netzwerk verwendet werden sollen
- Protokollierungskonfiguration für Probe in diesem Netzwerk. Weitere Informationen zum Konfigurieren von Probe-Protokollen finden Sie unter Verwalten der Probe-Protokolleinstellungen, auf Seite 104.

Informationen zu „Network View“ (Netzwerkansicht)

Klicken Sie im Bereich **Basic Info** (Basisinformationen) des Netzwerks auf **Manage** (Verwalten), um die **Netzwerkansicht** des Netzwerks anzuzeigen. Die **Netzwerkansicht** bietet mehrere Ansichten des Netzwerks:

- Ansicht **Topology** (Topologie): Zeigt eine logische Topologie aller erkannten Geräte im Netzwerk an. Es werden Informationen zu den einzelnen Geräten angezeigt, und Sie können Aktionen für ausgewählte Produkte von Cisco durchführen.
- Ansicht **Floor Plan** (Etagenplan): Dokumentiert die physischen Standorte der Netzwerkgeräte in Ihrer Umgebung.

Nachfolgend sind die zusätzlichen Steuerelemente aufgeführt, die in der **Netzwerkansicht** für alle Aufgaben zur Verfügung stehen:

- **Auswahlmöglichkeiten für Organisation und Netzwerk**: Mit diesen Dropdown-Listen können Sie zwischen Netzwerken und Organisationen wechseln, ohne zur Hauptseite des Netzwerks zurückzukehren. Um die Topologie oder den Etagenplan für ein anderes Netzwerk anzuzeigen, wählen Sie einfach dieses Netzwerk mithilfe der Dropdown-Liste aus.
- Dropdown-Liste **Network Actions** (Netzwerkaktionen): Über diese Dropdown-Liste können Sie ausgewählte Aktionen für alle Geräte im Netzwerk durchführen, die diese Aktion unterstützen. So können Sie beispielsweise die Konfigurationen aller Netzwerkgeräte mit nur einem Klick sichern. Außerdem können Sie über die Dropdown-Liste **Network Actions** (Netzwerkaktionen) den Erkennungsprozess für das Netzwerk erneut starten und Ihren Bestand bei Cisco Active Advisor (*https://www.ciscoactiveadvisor.com*) hochladen. Weitere Informationen zu Cisco Active Advisor finden Sie unter *https://help.ciscoactiveadvisor.com*

Übersicht der Topologiekarte und der zugehörigen Tools

Über die Topologiekarte

Cisco Business Dashboard fragt Details zur Netzwerkverbindung von den erkannten Geräten ab und erstellt anhand der so erfassten Informationen eine Grafik oder Topologie. Zu den erfassten Daten zählen Informationen zu CDP- und LLDP-Nachbarn, MAC-Adresstabellen und Tabellen der zugehörigen Geräte für Cisco Switches, Router und Wireless-Access-Points. Anhand dieser Informationen wird der Aufbau des Netzwerks ermittelt. Wenn im Netzwerk Infrastrukturgeräte vorhanden sind, die aus gewissen Gründen nicht verwaltet werden können, versucht Cisco Business Dashboard, die Topologie auf Grundlage der erfassbaren Informationen abzuleiten.

Sie können in der Topologie auf ein Gerät oder einen Link klicken, um den zugehörigen Bereich **Basic Info** (Basisinformationen) anzuzeigen. Im Bereich **Basic Info** (Basisinformationen) finden Sie detailliertere Informationen zu dem betreffenden Gerät oder Link und können unterschiedliche Aktionen für das Gerät durchführen.

Wenn Sie in der **Topologiekarte** auf **Overlays** klicken, wird der Bereich **Overlays & Filter** (Overlays und Filter) angezeigt. In diesem Bereich können Sie die Anzahl der in der Topologie angezeigten Geräte nach Gerätetyp oder Tag begrenzen. Sie können dort auch die Topologie erweitern, damit zusätzliche Informationen wie der aktuelle Datenverkehr für Verbindungen oder die Konfiguration eines bestimmten VLAN im Netzwerk angezeigt werden.

Zugreifen auf die Topologiekarte

Um auf die **Topologiekarte** zuzugreifen, wählen Sie in der **Navigation** den Eintrag **Network** (Netzwerk) aus, klicken Sie auf das Symbol oder die Tabellenzeile für das Netzwerk, an dem Sie interessiert sind, und klicken Sie dann auf **View** (Anzeigen). Die **Topologiekarte** für das betreffende Netzwerk wird im Arbeitsbereich angezeigt.

Topologiesteuerelemente

Die Topologiesteuerelemente befinden sich oben links in der **Topologiekarte**.

Tabelle 8: Topologiesteuerelemente

Symbol	Symbolname	Beschreibung
	**Vergrößern**	Passt die Ansicht im Fenster **Toplogy** (Topologie) an. Klicken Sie auf das Plussymbol (**+**) in der Menüleiste, um den Netzwerkausschnitt im Anzeigebereich zu vergrößern.
	Verkleinern	Passt die Ansicht im Fenster **Toplogy** (Topologie) an. Klicken Sie auf das Minussymbol (**−**), um den Netzwerkausschnitt im Anzeigebereich zu verkleinern.
	**Topologielayout aktualisieren**	Stellt automatisch das ursprüngliche Layout der Topologie wieder her, nachdem es durch manuelle Änderungen deaktiviert wurde. Zeichnet die Topologie mithilfe des automatischen Layoutalgorithmus neu.
	**Auswahl vergrößern/verkleinern**	Wählen Sie per Klicken und Ziehen den Bereich aus, der vergrößert werden soll.
	**An Anzeigebereich anpassen**	Vergrößert oder verkleinert die Anzeige, bis das gesamte Netzwerk im Anzeigebereich zu sehen ist.
	**Vollbildmodus**	Zeigt die Benutzeroberfläche von Cisco Business Dashboard bildschirmfüllend an.
	**Topologie exportieren**	Exportiert die aktuelle Topologieansicht als Bilddatei im PNG-Format. Das Bild wird am Standard-Downloadspeicherort des verwendeten Browsers gespeichert.
	**Topologieeinstellungen**	Erlaubt die Anpassung der Beschriftung der einzelnen Topologiesymbole.

Topologiesymbole

Die nachfolgend beschriebenen Symbole sind im Fenster **Topology** (Topologie) zu finden.

Tabelle 9: Topologiesymbole

Symbol	Netzwerkelement	Beschreibung
	**Access Point**	Steht für einen Wireless Access Point.
	**Cloud**	Steht für ein nicht von Cisco Business Dashboard verwaltetes Netzwerk oder einen entsprechenden Netzwerkbereich.

Symbol	Netzwerkelement	Beschreibung
	**Links**	Verbindungen sind Verbindungslinien zwischen Geräten. Klicken Sie auf eine Verbindung, um die Namen des Quell- und des Zielgeräts und andere grundlegende Details wie die Geschwindigkeit anzuzeigen. Die Dicke des Verbindungslinie repräsentiert die Geschwindigkeit der Leitung, wobei eine dünne Linie für eine Geschwindigkeit von maximal 100 Mbit/s steht und eine dicke Linie für eine Geschwindigkeit von mindestens 1 Gbit/s. Eine gestrichelte Linie symbolisiert eine Wireless-Verbindung.
	**Router**	Steht für einen Router.
	**Switch**	Steht für einen Switch.
	**Gastgeber**	Steht für einen per Kabelverbindung an das Netzwerk angebundenen Host.
	**Wireless-Host**	Steht für einen per Wireless-Verbindung an das Netzwerk angebundenen Host.

Bereich „Overlays & Filter“ (Overlays und Filter)

Dieser Bereich wird rechts neben der Karte **Toplogy** (Topologie) angezeigt, wenn Sie auf **Overlays** klicken. Den Link **Overlays** finden Sie rechts oben in der Topologie, neben dem **Suchfeld**.

Tabelle 10: Bereich „Overlays & Filter“ (Overlays und Filter)

Nummer	Beschreibung
Overlay auswählen	Mit dieser Funktion wird die Karte **Topology** (Topologie) auf Grundlage der ausgewählten Ansicht um zusätzliche Informationen erweitert. Folgende Werte sind möglich: • **Verbindungsauslastungsansicht**: Die aktuelle Netzwerkleistung wird durch die Überwachung des Datenverkehrsaufkommens ermittelt. Dieser Datenverkehr wird in der Karte **Topology** (Topologie) in Form farbcodierter Links angezeigt. Die Farbe gibt an, zu wie viel Prozent die Verbindung ausgelastet ist. Grün steht für Verbindungen, die nur mäßig ausgelastet sind, während Orange und Rot für Verbindungen stehen, die sich den Kapazitätsgrenzen nähern. Mithilfe der angezeigten Steuerelemente können Sie die Schwellenwerte für die verschiedenen Farben anpassen. • **VLAN-Ansicht**: Zeigt, wo ein VLAN im Netzwerk aktiviert ist. Anhand dieser Darstellung können Sie ein partitioniertes VLAN oder eine andere Fehlkonfiguration ermitteln. Wenn Sie im Dropdown-Menü „Overlay“ die Option **VLAN View** (VLAN-Ansicht) auswählen, wird unter diesem Feld ein zweites Dropdown-Menü angezeigt, in dem Sie die anzuzeigende VLAN-ID auswählen können. • **PoE-Ansicht**: In dieser Ansicht werden auf der Topologiekarte Verbindungen hervorgehoben, bei denen die Geräte derzeit über einen PoE-fähigen Switch mit Strom versorgt werden. • **L2-Pfadverfolgung**: Zeigt den Layer-2-Pfad, über den der Datenverkehr zwischen zwei ausgewählten Geräten im Netzwerk geleitet wird. Zur Auswahl der gewünschten Geräte können Sie deren Hostnamen, MAC-Adresse oder IP-Adresse in das jeweils dafür vorgesehene Feld eingeben oder in der Topologiekarte bei gedrückter Umschalttaste auf zwei Geräte klicken.
Tag auswählen	Geben Sie im Textfeld unter der Beschriftung **Select Tag** (Tag auswählen) ein **Geräte-Tag** an, um die Topologie zu filtern und nur Geräte anzuzeigen, die dem angegebenen Tag entsprechen. Geräte-Tags werden im Bereich **Detailed Info** (Detaillierte Informationen) zugewiesen.
Nur anzeigen: • **Router** • **Switches** • **Wireless** • **Hosts** • **Andere**	Aktivieren Sie die Kontrollkästchen neben den Geräten aus der Liste, die auf der Karte **Topology** (Topologie) angezeigt werden sollen. Mit dieser Funktion können Sie die auf der Karte anzuzeigenden Geräte filtern. In der Liste nicht aktivierte Geräte werden nicht auf der Karte angezeigt.

Anzeigen der Basisinformationen eines Geräts

Klicken Sie auf ein Netzwerkgerät wie einen Switch, einen Router oder eine Verbindung zwischen zwei Geräten, um Basisinformationen zu dem Gerät anzuzeigen. Dazu gehören unter anderem ausstehende Benachrichtigungen und ausführbare Aktionen. Im Bereich **Basic Info** (Basisinformationen) können Sie detailliertere Informationen zu einem Gerät abrufen und direkt auf die Verwaltungsoberfläche des Geräts zugreifen.

Hinweis Detaillierte Informationen zu einem Gerät finden Sie unter Anzeigen detaillierter Geräteinformationen, auf Seite 30.

Weitere Informationen zum Zugriff auf die Verwaltungsoberfläche eines Geräts finden Sie unter Zugreifen auf die Verwaltungsoberfläche des Geräts, auf Seite 30.

In der Tabelle im folgenden Abschnitt sind die Arten der angezeigten Gerätedetails aufgeführt. So rufen Sie die Basisinformationen eines Geräts auf:

Schritt 1 Wählen Sie auf der Seite **Network** (Netzwerk) ein Netzwerk aus, und klicken Sie auf **Manage** (Verwalten), um die Topologie anzuzeigen.

Schritt 2 Klicken Sie in der Topologieübersicht auf ein Netzwerkgerät wie einen Switch oder einen Router, für das Sie die Details anzeigen möchten.

Schritt 3 Die Gerätedetails werden im Bereich **Basic Info** (Basisinformationen) auf der Registerkarte **Overview** (Übersicht) angezeigt. Jedes Element wird in der folgenden Tabelle beschrieben.

Tabelle 11: Basisinformationen eines Geräts

Artikelbezeichnung	Beschreibung
Informationsbereich	
Modell	Modellname des Geräts
Beschreibung	Beschreibung des Geräts oder Produkts
Firmware-Version	Firmwareversion des Geräts
PID-VID	Produkt-ID und Versions-ID
MAC-Adresse	Bei der *MAC-Adresse (Media Access Control)* handelt es sich um eine standardisierte Sicherungsschichtadresse, die für bestimmte Netzwerkschnittstellen erforderlich ist. Diese Adressen sind für jedes Gerät eindeutig und werden nicht von anderen Geräten im Netzwerk verwendet.
Seriennummer	Die Geräteseriennummer.
Status	Gerätestatus „Online“ oder „Offline“
Domäne	Der Domänenname des Geräts
Anbieter	Der Hersteller des Geräts

Artikelbezeichnung	Beschreibung
Netzwerk	Der Name des Netzwerks, in dem sich das Gerät befindet
Organisation	Die Organisation, zu der das Gerät gehört.
Bereich „Benachrichtigungen“	
Kopf des Bereichs „Benachrichtigungen“: Im Kopf des Bereichs „Benachrichtigungen“ wird angezeigt, wie viele unbestätigte Benachrichtigungen für das Gerät vorliegen. **Hauptfeld des Bereichs „Benachrichtigungen“**: Im Hauptfeld des Bereichs „Benachrichtigungen“ werden alle unbestätigten Benachrichtigungen für das Gerät aufgeführt. Die vollständige Liste aller Gerätebenachrichtigungen finden Sie unter Anzeigen und Filtern aktueller Gerätebenachrichtigungen, auf Seite 101. Aktivieren Sie das Kontrollkästchen für eine Benachrichtigung, um sie zu bestätigen und aus der Liste zu entfernen. Sie können Benachrichtigungen auch filtern, um beispielsweise bestätigte Nachrichten anzuzeigen.	
Bereich „Ereignisse“	
Im Bereich „Ereignisse“ sind alle Benachrichtigungen und sonstigen Ereignisse aufgeführt, die in den letzten 24 Stunden für das betreffende Gerät eingegangen sind bzw. gemeldet wurden. Eine vollständige Liste aller Ereignisse für alle Geräte finden Sie im Ereignisprotokoll. Dort stehen ebenfalls Filteroptionen zur Verfügung.	
Bereich „PoE“	
Der Bereich „PoE“ wird auf PoE-fähigen Switches angezeigt und liefert eine Übersicht über den Stromverbrauch der einzelnen Anschlüsse des Geräts.	
Bereich „Stackinformationen“	
Der Bereich „Stackinformationen“ wird für Switch-Stacks angezeigt. Hier finden Sie die Hardwaredetails aller Stackmitglieder, inklusive Modellinformationen, Seriennummer und MAC-Adresse.	
Service	
Listet die auf dem Gerät identifizierten Netzwerkdienste auf.	
Verbundenes Gerät	
Bei Host-Geräten gibt es den Bereich **Connected Devices** (Verbundene Geräte). In diesem Bereich wird angezeigt, wie der Host mit dem Netzwerk verbunden ist. Dabei werden das Upstream-Netzwerkgerät und ggf. der Port angegeben, mit dem der Host verbunden ist.	

Zusätzlich zur Registerkarte **Overview** (Übersicht) finden Sie im Bereich **Basic Info** (Basisinformationen) auch die Registerkarte **Actions** (Aktionen), auf der Sie verschiedene Aufgaben für das betreffende Gerät durchführen können. Details finden Sie unter Ausführen von Geräteaktionen, auf Seite 27.

Ausführen von Geräteaktionen

Aktionen wie Firmware-Updates, Konfigurations-Backups und -Wiederherstellungen und Neustarts können für Geräte im Netzwerk ganz einfach durchgeführt werden. So führen Sie diese Aktionen aus:

Schritt 1 Klicken Sie in der **Topologiekarte** oder auf der Seite **Inventory** (Bestand) auf ein Netzwerkgerät wie einen Switch oder einen Router, für das Sie die Aktion durchführen möchten.

Schritt 2 Klicken Sie im Bereich **Basic Info** (Basisinformationen) auf die Registerkarte **Actions** (Aktionen). Abhängig von den Gerätefunktionen sind die folgenden Aktionen verfügbar:

Firmwareupgrade auf neueste Version	Ermöglicht Ihnen, das neueste Firmware-Update auf das Gerät anzuwenden. Cisco Business Dashboardlädt das Update von Cisco herunter und lädt es dann auf das Gerät hoch. Das Gerät wird nach Abschluss des Vorgangs neu gestartet.
Upgrade aus lokaler Quelle	Ermöglicht Ihnen, eine Firmware-Upgrade-Datei von Ihrem lokalen Laufwerk hochzuladen. Cisco Business Dashboard lädt die Datei auf das Gerät hoch und das Gerät wird nach Abschluss des Updates neu gestartet.
Konfiguration sichern	Mit dieser Aktion können Sie eine Kopie Ihrer aktuellen Gerätekonfiguration im Dashboard speichern. **1.** Klicken Sie auf **Konfiguration sichern**. **2.** Fügen Sie im Textfeld **Backup Configuration** (Konfiguration sichern) optional einen Hinweis zu der Sicherung ein, die Sie durchführen möchten. **Hinweis** Dieser Hinweis wird angezeigt, wenn die Sicherung in der Benutzeroberfläche aufgelistet wird. **3.** Klicken Sie auf **Save Backup** (Sicherung speichern), um diese Aktion abzuschließen, oder auf **Cancel** (Abbrechen), falls Sie die Aktion nicht durchführen möchten. Ein Auftrag zum Sichern der Konfiguration wird erstellt und kann im **Task Center** (Aufgaben-Center) angezeigt werden.

Konfiguration wiederherstellen	Damit können Sie eine zuvor gesicherte Konfiguration auf Ihrem Gerät wiederherstellen. Klicken Sie auf **Restore Configuration**. Folgende Optionen für Backup-Konfigurationen sind verfügbar: • **Sicherungen für *Gerätename*** – Liste aller verfügbaren Sicherungen, mit denen ein gegebenes Gerät konfiguriert werden kann • **Sicherungen für andere Geräte** – Liste aller verfügbaren Sicherungen zur Konfiguration anderer Geräte desselben Typs oder mit derselben Produkt-ID • **Sicherungen für andere kompatible Geräte** – Liste all verfügbaren Sicherungen zur Konfiguration anderer Geräte der Serie, die mit dem ausgewählten Gerät kompatibel sind So führen Sie eine Backup-Konfiguration aus: **1.** Wählen Sie im Fenster **Restore Configuration** (Konfiguration wiederherstellen) das Backup aus, das Sie auf dem Gerät wiederherstellen möchten. Scrollen Sie nach unten, um alle verfügbaren Sicherungen durchzusehen, und klicken Sie dann auf das gewünschte Optionsfeld. Dadurch wird die Schaltfläche **Restore Configuration** (Konfiguration wiederherstellen) aktiviert. Alternativ können Sie auch eine Konfigurationsdatei hochladen. Verschieben Sie dazu die Konfigurationsdatei per Drag-and-Drop in den gewünschten Bereich, oder klicken Sie auf den Bereich, und wählen Sie dann eine Datei aus dem Dateisystem aus. **2.** Klicken Sie auf **Restore Configuration** (Konfiguration wiederherstellen), um die Aktion abzuschließen. Ein Auftrag zum Wiederherstellen der Konfiguration wird erstellt und kann im **Task Center** (Aufgaben-Center) angezeigt werden.
Neustart	Startet das Gerät neu **Hinweis** Wenn Sie auf diese Schaltfläche klicken, werden Sie aufgefordert, diesen Schritt zur Bestätigung zu wiederholen.
Aktuelle Konfiguration speichern	Auf Geräten, die separate aktuelle Konfigurationen und Startkonfigurationen unterstützen, wird bei dieser Aktion die aktuelle Konfiguration in die Startkonfiguration kopiert. Dadurch werden beim nächsten Neustart des Geräts die Konfigurationsänderungen beibehalten.
Löschen	Mit dieser Aktion können Sie Offline-Geräte aus der Topologie und dem Bestand löschen.

Zugreifen auf die Verwaltungsoberfläche des Geräts

In bestimmten Fällen müssen Sie unter Umständen auf die Verwaltungsoberfläche eines Netzwerkgeräts direkt zugreifen. So greifen Sie auf die Verwaltungsoberfläche zu:

Schritt 1 Klicken Sie auf der Seite **Topology** (Topologie) oder **Inventory** (Bestand) auf ein Netzwerkgerät wie einen Switch oder einen Router, für das Sie die Verwaltungsschnittstelle aufrufen möchten.

Schritt 2 Klicken Sie im Bereich **Basic Info** (Basisinformationen) in der oberen rechten Ecke auf **View** (Anzeigen). In Ihrem Browser wird ein neues Fenster mit der Verwaltungsoberfläche des Geräts geöffnet.

Hinweis Wenn Sie die Verwaltungsschnittstelle durch Klicken auf **View** (Anzeigen) aufrufen, stellt Ihr Browser über das Dashboard eine Verbindung zum Gerät her. Wenn Sie Ihr Netzwerk also per Remotezugriff aufrufen, muss nur das Dashboard von einem externen Standort aus direkt erreichbar sein.

Da diese Verbindungen alle über denselben Host ausgeführt werden, nämlich das Dashboard, werden die Cookies für ein Gerät auch an andere Geräte gesendet. Daher können sie unter Umständen von anderen Geräten aktualisiert werden, wenn der Name identisch ist. Als Folge davon wird die Browsersitzung auf dem ersten Gerät sofort abgemeldet, nachdem die Verbindung zum zweiten Gerät hergestellt wurde, da das Cookie aktualisiert wurde.

Anzeigen detaillierter Geräteinformationen

Schritt 1 Klicken Sie auf der Seite **Topology** (Topologie) oder **Inventory** (Bestand) auf ein Netzwerkgerät wie einen Switch oder einen Router, für das Sie nähere Informationen anzeigen möchten.

Schritt 2 Klicken Sie im Bereich **Basic Info** (Basisinformationen) in der oberen rechten Ecke auf **More** (Mehr).

Schritt 3 Im Bereich **Detailed Info** (Detaillierte Informationen) finden Sie eine detaillierte Liste der Geräteinformationen auf der linken Seite und weitere Funktionen unter den folgenden Registerkarten:

- **Dashboard**: Zeigt eine Reihe von Dashboard-Widgets speziell für das Gerät an.
- **Port Management** (Portverwaltung): In diesem Bereich können Sie die Konfiguration der Switch-Ports verwalten.

  Hinweis Diese Informationen sind nur für Geräte mit Switch-Anschlüssen verfügbar.

- **Wireless LANs**: Hier werden die für das Gerät konfigurierten Wireless LANs aufgelistet.

  Hinweis Diese Informationen sind nur für Wireless-Geräte verfügbar.

- **Event Log** (Ereignisprotokoll): Hier finden Sie eine Liste aller in der Vergangenheit für das Gerät durchgeführten Aktionen sowie aller in der Vergangenheit für das Gerät empfangenen Benachrichtigungen.
- **Config Backups** (Konfig.-Backups): In diesem Bereich können Sie eine Liste der Backup-Konfigurationen für Geräte abrufen und verschiedene Aktionen durchführen, z. B. eine Konfiguration wiederherstellen, speichern oder löschen.

Hinweis Diese Informationen sind nur für Geräte verfügbar, die die Vorgänge der Backup-Konfiguration unterstützen.

- **Pending Config** (Ausstehende Konfig.): Vergleicht die gewünschte Konfiguration anhand der definierten Konfigurationsprofile mit der aktuellen Konfiguration auf dem Gerät und hebt alle Unterschiede hervor.

  Hinweis Dieser Bereich wird nur für Geräte angezeigt, die für Konfigurationsvorgänge unterstützt werden, bei denen die aktuelle Konfiguration nicht mit der gewünschten Konfiguration übereinstimmt.

Diese werden in den folgenden Schritten beschrieben:

Schritt 4 Eine detaillierte Liste mit Informationen über das Gerät wird auf der linken Seite angezeigt. Diese Liste enthält die folgenden Informationen:

Tabelle 12: Detaillierte Geräteinformationen

Artikelbezeichnung	Beschreibung
Hostname	Klicken Sie neben dem Gerätenamen auf **Edit** (Bearbeiten), um den Geräte-Hostnamen zu ändern. Klicken Sie auf **Save** (Speichern), um die Änderungen zu speichern.
Modell	Modellname des Geräts
MAC-Adresse	Bei der *MAC-Adresse (Media Access Control)* handelt es sich um eine standardisierte Sicherungsschichtadresse, die für bestimmte Netzwerkschnittstellen erforderlich ist. Diese Adressen sind für jedes Gerät eindeutig und werden nicht von anderen Geräten im Netzwerk verwendet.
Status	Der aktuelle Status des Geräts, beispielsweise ob es online oder offline ist
Maßnahmen	Über die Dropdown-Liste **Actions** (Aktionen) und das Symbol **Open Device GUI** (Geräte-GUI öffnen) im Bereich **Detailed Info** (Detaillierte Informationen) können Sie mit dem Gerät interagieren.
IP	IP-Adressen des Geräts
Domäne	Der Domänenname des Geräts
PID-VID	Produkt-ID und Versions-ID
Seriennummer	Seriennummer des Geräts
Anbieter	Der Hersteller des Geräts
Beschreibung	Beschreibung des Geräts oder Produkts
Gerätegruppe	Die Gerätegruppe, zu der dieses Gerät gehört
Netzwerk	Das Netzwerk, zu dem dieses Gerät gehört
Organisation	Die Organisation, zu der dieses Gerät gehört

Artikelbezeichnung	Beschreibung
PnP-Parameter	Das Image und die Konfigurationsdatei, die per Network Plug and Play an das Gerät übermittelt werden sollen. Klicken Sie auf das Symbol **Edit** (Bearbeiten), um Änderungen vorzunehmen, und klicken Sie dann auf das Symbol **Save** (Speichern), um die Änderungen anzuwenden, oder auf **Cancel** (Abbrechen), um den Vorgang ohne Speichern abzuschließen.
Tags	Geben Sie im Feld „Tags“ beliebige alphanumerische Zeichen ein, und drücken Sie dann die **Eingabetaste**, um neue Tags für dieses Gerät zu erstellen. Um ein bestehendes Tag zu löschen, klicken Sie im Tag auf das Symbol ✖. Klicken Sie auf **Save** (Speichern), um die Änderungen zu speichern. Anhand von Tags können Sie Geräte mit üblichen Merkmalen identifizieren. Sie können Tags auch in anderen Bereichen von Cisco Business Dashboard Probe einsetzen, um die Netzwerkansichten auf die Anzeige einer Untergruppe von Geräten zu beschränken.
Firmware-Version	Die Version der derzeit auf dem Gerät ausgeführten Firmware. Wenn eine höhere Version verfügbar ist, wird diese in Klammern neben der aktuellen Version angezeigt. Über die Symbole können Sie die Versionshinweise zum Update aufrufen und für das Gerät übernehmen.
Erkennungsmethode	Die Protokolle und Geräte, anhand derer das Gerät erkannt wurde
Ausstehende Konfig.	Zeigt den Status der Gerätekonfiguration an und zeigt, ob Unterschiede zwischen der aktuellen Konfiguration für das Gerät und der erwarteten Konfiguration bestehen.

Schritt 5 Klicken Sie auf **Dashboard**, um eine Reihe von Widgets anzuzeigen, die den aktuellen Status des Geräts anzeigen. Nähere Informationen finden Sie unter Informationen zum Überwachungs-Dashboard.

Schritt 6 Klicken Sie auf **Port Management** (Portverwaltung), um die Konfiguration der Switch-Ports auf dem Gerät abzurufen und zu verwalten. Es wird eine visuelle Repräsentation des Geräts angezeigt, die der auf der Seite **Port Management** (Portverwaltung) ähnelt.

In diesem Fenster werden die Anschlussdetails für das Gerät in einer visuellen Repräsentation dargestellt. Über dem Bild werden das Modell und die Seriennummer des Geräts angezeigt, unter dem Bild eine tabellarische Ansicht der Ports. Weitere Informationen dazu finden Sie unter Allgemeines zur Portverwaltung, auf Seite 39.

Schritt 7 Klicken Sie auf **WLAN**, um die auf diesem Gerät konfigurierten Funkeinstellungen und Wireless LANs anzuzeigen.

Schritt 8 Klicken Sie auf **Event Log** (Ereignisprotokoll), um eine Liste aller in der Vergangenheit empfangenen Benachrichtigungen und sonstigen Ereignisse aufzurufen, die für dieses Gerät aufgezeichnet wurden. Die angezeigten Einträge lassen sich mithilfe von Filtern eingrenzen. Nähere Informationen finden Sie unter Allgemeines zum Ereignisprotokoll.

Schritt 9 Klicken Sie auf **Config Backups** (Konfig.-Backups), um die Konfigurations-Backups für dieses Gerät aufzurufen und zu verwalten. Auf dieser Registerkarte wird eine Tabelle mit allen in Network Probe gespeicherten Sicherungen angezeigt, einschließlich der folgenden Details:

Tabelle 13: Konfig.-Backups

Nummer	Beschreibung
Zeitstempel	Datum und Uhrzeit der Konfigurationssicherung
Kommentar	Dies sind Hinweise, die der Benutzer bei der Sicherungserstellung angegeben hat.

Nummer	Beschreibung
Gesichert von	Benutzer, der die Konfiguration erstellt hat
Maßnahmen	Wählen Sie eine der folgenden Sicherungsaktionen aus: • **Restore configuration to device** (Konfiguration auf Gerät wiederherstellen): Mit dieser Option wird das ausgewählte Backup auf dem Gerät wiederhergestellt. • **Save configuration to PC** (Konfiguration auf PC speichern): Mit dieser Option wird das Backup als ZIP-Datei auf dem lokalen Laufwerk Ihres PCs gespeichert. • **Delete configuration** (Konfiguration löschen): Mit dieser Option wird das Backup entfernt. • **View configuration** (Konfiguration anzeigen): Hilft beim Anzeigen des Inhalts des Konfigurations-Backups im Browser.

Sie können auch ein Konfigurations-Backup über die Registerkarte auslösen, indem Sie auf **Backup Configuration** (Konfiguration sichern) klicken.

Schritt 10 Klicken Sie auf **Pending Config** (Ausstehende Konfig.), um einen direkten Vergleich zwischen der aktuellen Gerätekonfiguration und der erwarteten Konfiguration anhand der auf das Gerät angewendeten Konfigurationsprofile anzuzeigen. Die Konfigurationen werden in einem geräteunabhängigen Format dargestellt, und alle Unterschiede werden hervorgehoben. Sie können die Schaltflächen oben auf der Seite verwenden, um alle ausstehenden Änderungen anzuwenden, die aktuelle Gerätekonfiguration zu akzeptieren oder die aktuelle Gerätekonfiguration erneut einzulesen.

Verwenden von Etagenplänen

In der Etagenplanansicht können Sie die physischen Standorte Ihrer Netzwerkgeräte verfolgen. Sie können für jede Etage in den Gebäuden einen Plan hochladen und die einzelnen Netzwerkgeräte auf dem Plan positionieren. So finden Sie die Geräte schnell, wenn sie gewartet werden müssen. In seiner Funktionsweise ähnelt der Etagenplan der Topologiekarte. Die auf dem Etagenplan platzierten Geräte können so behandelt werden wie Geräte auf der Topologiekarte.

Erstellen eines neuen Etagenplans

1. Navigieren Sie zu **Network View** (Netzwerkansicht), und klicken Sie auf **Floor Plan** (Etagenplan). Wenn ein vorhandener Etagenplan angezeigt wird, klicken Sie im Etagenplan oben links auf das Symbol für die **Startseite**.
2. Wenn das Gebäude, für das Sie einen Etagenplan hinzufügen möchten, bereits erstellt wurde, fahren Sie mit dem nächsten Schritt fort. Wurde das Gebäude noch nicht erstellt, geben Sie im Feld **Neues Gebäude** einen Namen für das Gebäude ein, in dem sich die Etage befindet. Klicken Sie auf das Symbol zum **Speichern**.
3. Ziehen Sie eine Bilddatei mit dem Etagenplan per Drag-and-Drop in den Zielbereich für die neue Etage, oder klicken Sie in den Zielbereich, um eine Datei für den Upload anzugeben. Unterstützt werden die Bildformate `.png`, `.gif` und .jpg. Die Bilddateien dürfen maximal 500 KB groß sein.

4. Geben Sie im Feld **New Floor** (Neue Etage) einen Namen für die Etage ein. Klicken Sie auf das Symbol zum **Speichern**.
5. Wiederholen Sie die Schritte 2 bis 4 für jede Etage jedes Gebäudes, auf der sich Netzwerkgeräte befinden.

Platzieren von Netzwerkgeräten auf einem Etagenplan

1. Navigieren Sie zu **Network View** (Netzwerkansicht), und klicken Sie auf **Floor Plan** (Etagenplan). Wenn der relevante Etagenplan noch nicht angezeigt wird, öffnen Sie ihn durch Klicken.
2. Klicken Sie auf **Add Devices** (Geräte hinzufügen), und suchen Sie dann mithilfe des Suchfelds unten links das zu platzierende Gerät. Sie können anhand des Hostnamens, des Gerätetyps oder der IP-Adresse suchen. Bei der Eingabe werden unter dem Suchfeld passende Geräte angezeigt. Graue Symbole stehen für Geräte, die bereits auf einem Etagenplan platziert wurden.
3. Klicken Sie auf ein Gerät, und ziehen Sie es auf die richtige Position, um es dem Etagenplan hinzuzufügen. Wenn Sie ein Gerät auswählen, das bereits auf einem anderen Etagenplan platziert wurde, wird es entfernt und dem aktuellen Plan hinzugefügt.
4. Wiederholen Sie Schritt 2 und 3, bis alle Geräte im Etagenplan enthalten sind.

Entfernen von Geräten aus einem Etagenplan

1. Navigieren Sie zu **Network View** (Netzwerkansicht), und klicken Sie auf **Floor Plan** (Etagenplan). Wenn der relevante Etagenplan noch nicht angezeigt wird, öffnen Sie ihn durch Klicken.
2. Wählen Sie das zu entfernende Gerät durch Klicken aus.
3. Klicken Sie auf das angezeigte rote Kreuz, um das Gerät aus dem Etagenplan zu entfernen.

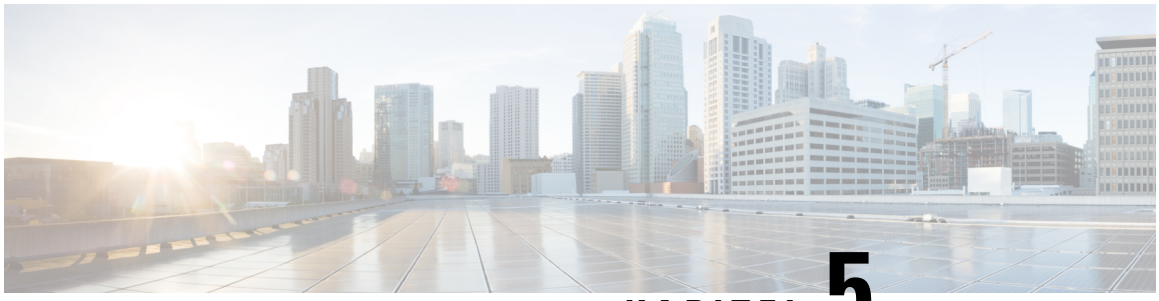
Ändern des Etagenplans

1. Navigieren Sie zu **Network View** (Netzwerkansicht), und klicken Sie auf **Floor Plan** (Etagenplan). Wenn ein vorhandener Etagenplan angezeigt wird, klicken Sie im Etagenplan oben links auf das Symbol für die **Startseite**.
2. Um einen Gebäudenamen zu ändern, klicken Sie neben dem Namen auf das Symbol zum **Bearbeiten**. Klicken Sie nach Abschluss der Änderungen auf das Symbol zum **Speichern**.
3. Um einen Etagenplan zu ändern, klicken Sie neben dem Etagennamen auf das Symbol zum **Bearbeiten**. Sie können den Etagenplan ändern, indem Sie eine neue Bilddatei in den Zielbereich ziehen oder indem Sie in den Zielbereich klicken und eine neue Datei vom PC hochladen. Sie können auch den Namen des Etagenplans ändern. Klicken Sie nach Abschluss der Änderungen auf das Symbol zum **Speichern**.

Entfernen eines Etagenplans

1. Navigieren Sie zu **Network View** (Netzwerkansicht), und klicken Sie auf **Floor Plan** (Etagenplan). Wenn ein vorhandener Etagenplan angezeigt wird, klicken Sie im Etagenplan oben links auf das Symbol für die **Startseite**.
2. Identifizieren Sie den zu entfernenden Etagenplan, und klicken Sie auf das **Löschsymbol** in der oberen rechten Ecke des Zielbereichs.

3. Wenn Sie ein ganzes Gebäude mit allen enthaltenen Etagenplänen entfernen möchten, klicken Sie neben dem Gebäudenamen auf das Symbol zum **Löschen**.



KAPITEL 5

Bestand

Dieses Kapitel enthält folgende Abschnitte:

Anzeigen des Gerätebestands

Auf der Seite **Inventory** (Bestand) wird eine vollständige tabellarische Auflistung aller Geräte mit den zugehörigen Informationen. Ebenso stehen Ihnen hier Aktionsschaltflächen zur Verfügung, über die Sie für unterstützte Geräte Konfigurationsaufgaben durchführen und die neuesten Firmwareupdates installieren können. Die folgende Tabelle enthält Details zu den angezeigten Informationen.

Tabelle 14: Details zum Bestand

Nummer	Beschreibung
Hostname	Der Name des Geräts
Typ	Typ des Geräts, z. B. Switch, Router oder Wireless Access Point (WAP)
Tags	Auflistung aller dem Gerät zugeordneten Tags
IP	Die IP-Adresse des Geräts
MAC (standardmäßig ausgeblendet)	Bei der MAC-Adresse (Media Access Control) handelt es sich um eine standardisierte Sicherungsschichtadresse, die für bestimmte Netzwerkschnittstellen erforderlich ist. Diese Adressen sind für jedes Gerät eindeutig und werden nicht von anderen Geräten im Netzwerk verwendet.
Seriennummer	Seriennummer des Geräts
Version	Aktuelle Firmwareversion auf dem Gerät
Hersteller (Standardmäßig ausgeblendet)	Der Anbieter, der das Gerät hergestellt hat.
Modell	Modellname des Geräts
Organisation	Die Organisation, zu der das Gerät gehört.

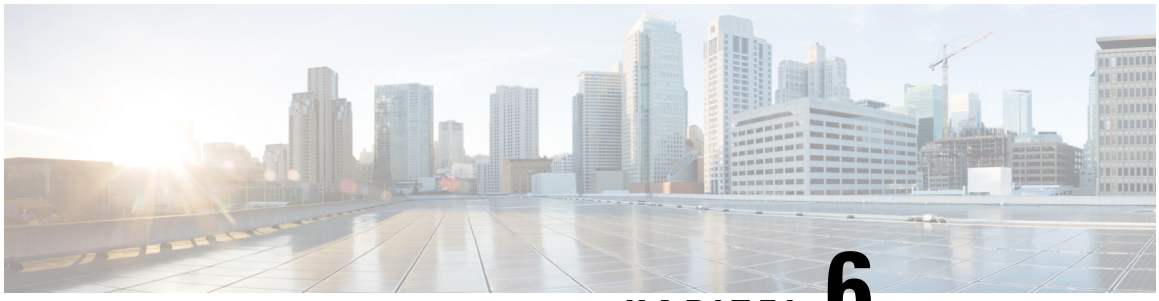
Nummer	Beschreibung
Netzwerk	Das Netzwerk, zu dem das Gerät gehört
Benachrichtigung	Die Anzahl der ausstehenden Benachrichtigungen für das Gerät
PnP-Status (standardmäßig ausgeblendet)	Der aktuelle Network Plug and Play-Status für das Gerät. Weitere Informationen finden Sie auf den Seiten zu **Network Plug and Play**.

Die folgenden zusätzlichen Steuerelemente sind auf der Seite **Inventory** (Bestand) verfügbar:

- Schaltfläche **Select columns** (Spalten auswählen): Verwenden Sie diese Schaltfläche oben links in der Tabelle, um auszuwählen, welche Spalten angezeigt werden sollen.
- **Filterfeld**: Über das **Filterfeld** können Sie die Liste eingrenzen, beispielsweise anhand des Gerätenamens, des Gerätetyps oder der Seriennummer. Standardmäßig wird der Bestand so gefiltert, dass nur Netzwerkgeräte angezeigt werden.
- Symbol **Add** (Hinzufügen): Klicken Sie auf das Pluszeichen (**+**), um dem Bestand neue Geräte hinzuzufügen, bevor das jeweilige Gerät erkannt wird. Wenn Sie dem Bestand manuell ein Gerät hinzufügen, können Sie grundlegende Informationen zum Gerät bereitstellen, einschließlich Identitätsinformationen, Organisation und Gerätegruppe sowie PnP-Einstellungen. Wenn Sie diese Informationen im Voraus angeben, stellen Sie damit sicher, dass das Gerät ordnungsgemäß verwaltet wird, sobald es mit dem Netzwerk verbunden ist.
- Schaltfläche **Refresh** (Aktualisieren): Klicken Sie auf diese Schaltfläche, um die Tabelle zu aktualisieren, damit die neuesten verfügbaren Informationen angezeigt werden.
- Schaltflächen für **Aktionen**: Mit den folgenden Aktionsschaltflächen können Sie Aktionen auf einem oder mehreren ausgewählten Geräten ausführen:
  - **Aktuellste Firmware herunterladen**
  - **Firmwareupgrade von lokal auf Gerät anwenden**
  - **Konfiguration sichern**
  - **Konfiguration wiederherstellen**
  - **Gerät neu starten**
  - **Aktuelle Konfiguration speichern**
  - **Löschen**

  Aktionsschaltflächen werden nur angezeigt, wenn mindestens ein Gerät ausgewählt ist, das Aktionen unterstützt.

Hinweis Nähere Informationen zu diesen Aktionen finden Sie unter Ausführen von Geräteaktionen auf Seite 19.



KAPITEL 6

Portverwaltung

Dieses Kapitel enthält folgende Abschnitte:

Allgemeines zur Portverwaltung

Unter **Port Management** (Portverwaltung) finden Sie eine Ansicht der Vorderseiten aller Geräte mit Switch-Ports, die von Cisco Business Dashboard konfiguriert werden können. Auf dieser Seite können Sie den Status der Anschlüsse mit Verkehrszählern anzeigen und die Anschlusskonfiguration ändern. Außerdem können Sie auf dieser Seite die Smartport-Rollen für Ports von Geräten mit Smartport-Unterstützung anzeigen und konfigurieren. Über das Suchfeld können Sie die angezeigten Geräte eingrenzen. Geben Sie einen Gerätenamen, eine Produkt-ID oder eine Seriennummer ganz oder teilweise ein, um das gewünschte Gerät zu suchen.

Zusätzlich ist eine Listenansicht mit denselben Informationen vorhanden, in der alle Switch-Ports in einem tabellarischen Format angezeigt werden. Bei der Ansicht der Gerätevorderseiten unter **Port Management** (Portverwaltung) stehen zwei verschiedene Ansichten für Geräte zur Verfügung:

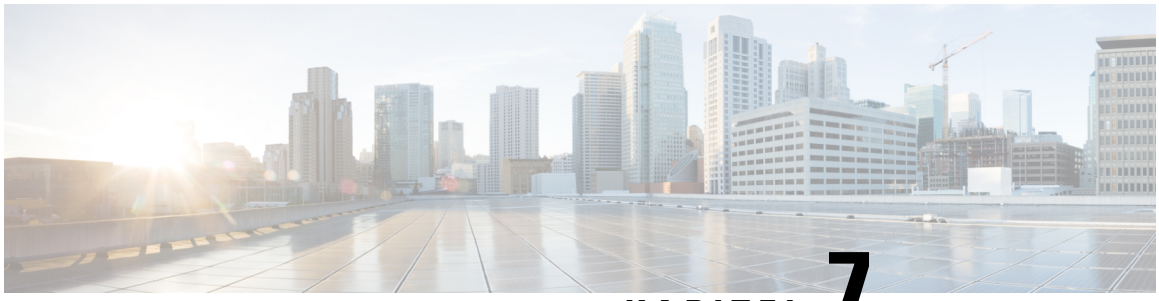
- **Physical** (Physisch): In dieser Ansicht können Sie den Status des Anschlusses anzeigen und seine Konfiguration auf der physischen Ebene ändern. Sie können die Einstellungen für Geschwindigkeit, Duplex, EEE (Energy Efficient Ethernet), PoE (Power over Ethernet) und VLANs anzeigen und ändern. Zu jedem Anschluss wird eine grüne LED für die Verbindung und eine gelbe LED für die Stromversorgung des angeschlossenen Geräts angezeigt.
- **Smartports**: In dieser Ansicht können Sie die aktuellen Smartport-Rollen der einzelnen Ports anzeigen und ändern. Über jedem Anschluss wird ein Symbol für die aktuelle Rolle angezeigt.

Hinweis Ein Smartport ist eine Schnittstelle, auf die eine integrierte (oder benutzerdefinierte) Vorlage angewendet werden kann. Diese Vorlagen sollen eine schnelle Konfiguration des Geräts ermöglichen, um so die Kommunikationsanforderungen zu unterstützen und die Funktionen verschiedener Arten von Netzwerkgeräten zu nutzen.

Um den Status eines Ports anzuzeigen, klicken Sie in der Vorderseiten- oder Listenansicht auf den Port. Der Bereich **Basic Info** (Basisinformationen) für den Anschluss wird angezeigt. Hier finden Sie folgende Bereiche:

- **General** (Allgemein): Im Bereich **General** (Allgemein) wird der Status des Ports auf der physischen Ebene angezeigt und Sie können den Port aktivieren oder herunterfahren.
- **Ethernet**: Ermöglicht die Steuerung der Geschwindigkeits- und Duplex-Einstellungen.
- **VLAN**: Im Bereich **VLAN** werden alle aktuell am Port konfigurierten VLANs angezeigt. Klicken Sie auf die Schaltfläche **Select VLAN** (VLAN auswählen) oder auf die Schaltfläche **Create VLAN** (VLAN erstellen), wenn Sie diese Konfiguration ändern möchten.
- **PoE**: Der Bereich **PoE** wird nur bei PoE-fähigen Ports angezeigt. Hier können Sie die PoE-Einstellungen des Ports konfigurieren. Über die Schaltfläche zur Leistungsumschaltung haben Sie außerdem die Möglichkeit, angebundene PoE-Geräte an- und wieder auszuschalten.
- **Green Ethernet**: Im Bereich **Green Ethernet** können Sie die EEE-Konfiguration (Energy Efficient Ethernet) des Ports verwalten.
- **Smartports**: Im Bereich **Smartports** werden die für den Port verfügbaren Smartport-Rollen aufgeführt. Klicken Sie auf eine Rolle, um die zugehörige Konfiguration auf den Port anzuwenden. Die aktuell konfigurierte Rolle wird hervorgehoben.

Um Änderungen an den Porteinstellungen vorzunehmen, klicken Sie oben rechts in dem Bereich, der diese Einstellung enthält, auf das Symbol **Edit** (Bearbeiten). Klicken Sie nach Abschluss der Änderungen auf das Symbol **Save** (Speichern).



KAPITEL 7

Netzwerkkonfiguration

Dieses Kapitel enthält folgende Abschnitte:

Über die Netzwerkkonfiguration

Auf den Seiten **Network Configuration** (Netzwerkkonfiguration) können Sie verschiedene Parameter definieren, die üblicherweise für einige oder alle Geräte im Netzwerk gelten. Zu diesen Parametern zählen Aspekte der Konfiguration wie Zeiteinstellungen, Domain Name Services, Administratorauthentifizierung, virtuelle LANs (VLANs) und Wireless LANs (WLANs). Sie können Konfigurationsprofile für die einzelnen Bereiche separat erstellen oder mit dem Assistenten Profile für jeden Bereich innerhalb eines Workflows erstellen. Die Konfigurationsprofile werden auf eine oder mehrere Gerätegruppen angewendet und danach auf die Geräte übertragen.

Verwenden des Assistenten

Mit dem Assistenten können Sie in einem einzigen Arbeitsablauf Konfigurationsprofile für die einzelnen Elemente der Netzwerkkonfiguration erstellen und diese Profile einer oder mehreren Gerätegruppen zuweisen.

Verwenden des Assistenten

1. Navigieren Sie zu **Network Configuration** > **Wizard** (Netzwerkkonfiguration > Assistent).
2. Geben Sie im Fenster **Device Group Selection** (Gerätegruppenauswahl) einen Profilnamen für diese Konfiguration ein, wählen Sie eine Organisation aus, und wählen Sie eine oder mehrere Gerätegruppen zur Konfiguration aus. Klicken Sie auf **Next** (Weiter).
3. Wählen Sie in den nachfolgenden Fenstern die erforderlichen Konfigurationsoptionen aus. Nähere Informationen zu diesen Parametern erhalten Sie in den folgenden Abschnitten.

4. Wenn Sie mit den Einstellungen in einem Fenster fertig sind, klicken Sie jeweils auf **Next** (Weiter). Wenn Sie in einem bestimmten Fenster keine Einstellungen für das Profil konfigurieren möchten, klicken Sie auf **Skip** (Überspringen). Klicken Sie auf **Back** (Zurück), um zum vorherigen Fenster zurückzukehren. Sie können auch links auf die Überschriften klicken.
5. Schließen Sie die Konfiguration ab, und prüfen Sie im letzten Fenster die Einstellungen. Klicken Sie auf **Finish** (Fertigstellen), um die Konfiguration auf die ausgewählten Geräte anzuwenden.

Konfigurieren der Zeitverwaltung

Auf der Seite **Time Management** (Zeitverwaltung) können Sie Zeitzonen, den Wechsel zwischen Sommer- und Winterzeit sowie NTP-Server für das Netzwerk konfigurieren. In den folgenden Abschnitten finden Sie Anweisungen zum Erstellen, Ändern und Löschen des Konfigurationsprofils für Zeiteinstellungen.

Erstellen eines Konfigurationsprofils für die Zeitverwaltung

1. Navigieren Sie zu **Network Configuration** > **Time Management** (Netzwerkkonfiguration > Zeitverwaltung).
2. Klicken Sie auf das Plussymbol (**+**), um ein neues Profil hinzuzufügen.
3. Geben Sie im Abschnitt **Device Group Selection** (Gerätegruppenauswahl) einen Profilnamen für diese Konfiguration ein, wählen Sie eine Organisation aus, und wählen Sie eine oder mehrere Gerätegruppen zur Konfiguration aus.
4. Wählen Sie im Abschnitt **Time Setting** (Zeiteinstellung) die passende Zeitzone aus dem Dropdown-Menü aus.
5. Aktivieren Sie bei Bedarf die Option **Daylight Saving** (Sommerzeit), indem Sie das Kontrollkästchen aktivieren, und legen Sie die Parameter für die Sommerzeit in den entsprechenden Feldern fest. Sie können entweder feste Daten oder ein Serienmuster angeben. Sie können auch festlegen, um wie viele Stunden die Zeit verschoben werden soll.
6. Aktivieren Sie im Abschnitt **Use NTP** (NTP verwenden) bei Bedarf NTP (Network Time Protocol) zur Zeitsynchronisierung, indem Sie das Kontrollkästchen aktivieren. Geben Sie in den entsprechenden Feldern mindestens eine NTP-Serveradresse ein.
7. Klicken Sie auf **Save** (Speichern).

Ändern eines Konfigurationsprofils für die Zeitverwaltung

1. Aktivieren Sie das Optionsfeld neben dem zu ändernden Profil, und klicken Sie dann auf das Symbol zum **Bearbeiten**.
2. Nehmen Sie die erforderlichen Änderungen an den Profileinstellungen vor, und klicken Sie auf **Update** (Aktualisieren).

Entfernen eines Konfigurationsprofils für die Zeitverwaltung

1. Aktivieren Sie das Optionsfeld neben dem zu entfernenden Profil.
2. Klicken Sie auf das Symbol zum **Löschen**.

Konfigurieren der DNS-Resolver

Auf der Seite **DNS-Resolver** können Sie den Domänennamen und die DNS-Server für das Netzwerk konfigurieren. In den folgenden Abschnitten finden Sie Anweisungen zum Erstellen, Ändern und Löschen des Konfigurationsprofils für DNS-Resolver.

Erstellen eines Konfigurationsprofils für DNS-Resolver

1. Navigieren Sie zu **Network Configuration** > **DNS Resolvers** (Netzwerkkonfiguration > DNS-Resolver).
2. Klicken Sie auf das Plussymbol (**+**), um ein neues Profil hinzuzufügen.
3. Geben Sie im Abschnitt **Device Group Selection** (Gerätegruppenauswahl) einen Profilnamen für diese Konfiguration ein, wählen Sie eine Organisation aus, und wählen Sie eine oder mehrere Gerätegruppen zur Konfiguration aus.
4. Geben Sie den Domänennamen für das Netzwerk an.
5. Geben Sie mindestens eine DNS-Serveradresse ein.
6. Klicken Sie auf **Save** (Speichern).

Ändern eines Konfigurationsprofils für DNS-Resolver

1. Aktivieren Sie das Optionsfeld neben dem zu ändernden Profil, und klicken Sie dann auf das Symbol zum **Bearbeiten**.
2. Nehmen Sie die erforderlichen Änderungen an den Profileinstellungen vor, und klicken Sie auf **Update** (Aktualisieren).

Entfernen eines Konfigurationsprofils für DNS-Resolver

1. Aktivieren Sie das Optionsfeld neben dem zu entfernenden Profil.
2. Klicken Sie auf das Symbol zum **Löschen**.

Konfigurieren der Authentifizierung

Auf der Seite **Authentication** (Authentifizierung) können Sie den Zugriff von Administratorbenutzern auf die Netzwerkgeräte konfigurieren. In den folgenden Abschnitten finden Sie Anweisungen zum Erstellen, Ändern und Löschen des Konfigurationsprofils für die Authentifizierung.

Erstellen eines Konfigurationsprofils für die Authentifizierung

1. Navigieren Sie zu **Network Configuration** > **Authentication** (Netzwerkkonfiguration > Authentifizierung).
2. Klicken Sie auf das Plussymbol (**+**), um ein neues Profil hinzuzufügen.

3. Geben Sie im Abschnitt **Device Group Selection** (Gerätegruppenauswahl) einen Profilnamen für diese Konfiguration ein, wählen Sie eine Organisation aus, und wählen Sie eine oder mehrere Gerätegruppen zur Konfiguration aus.
4. Legen Sie mindestens eine Kombination aus Benutzername und Kennwort für die Authentifizierung lokaler Benutzer fest. Sie können weitere Benutzer durch Klicken auf das Plussymbol (✚) erstellen.
5. Bei Bedarf können Sie die Verwendung komplexer Kennwörter vorschreiben.
6. Klicken Sie auf **Save** (Speichern).

Ändern eines Konfigurationsprofils für die Authentifizierung

1. Aktivieren Sie das Optionsfeld neben dem zu ändernden Profil, und klicken Sie dann auf das Symbol zum **Bearbeiten**.
2. Nehmen Sie die erforderlichen Änderungen an den Profileinstellungen vor, und klicken Sie auf **Update** (Aktualisieren).

Entfernen eines Konfigurationsprofils für die Authentifizierung

1. Aktivieren Sie das Optionsfeld neben dem zu entfernenden Profil.
2. Klicken Sie auf das Symbol zum **Löschen**.

Konfigurieren von virtuellen LANs (VLANs)

Auf der Seite **Virtual LANs** (Virtuelle LANs) können Sie Ihr Switch-Netzwerk in mehrere virtuelle Netzwerke (VLANs) unterteilen. Die bereits vorhandenen, nicht von Cisco Business Dashboard konfigurierten VLANs im Netzwerk werden auf dieser Seite in einer separaten Tabelle angezeigt. In den folgenden Abschnitten finden Sie Anweisungen zum Erstellen, Ändern und Löschen von Konfigurationsprofilen für virtuelle LANs.

Erstellen eines VLAN

1. Navigieren Sie zu **Network Configuration** > **Virtual LANs** (Netzwerkkonfiguration > Virtuelle LANs).
2. Klicken Sie auf das Plussymbol (✚), um ein neues VLAN hinzuzufügen.
3. Geben Sie im Abschnitt **Device Group Selection** (Gerätegruppenauswahl) einen Profilnamen für diese Konfiguration ein, wählen Sie eine Organisation aus, und wählen Sie eine oder mehrere Gerätegruppen zur Konfiguration aus.
4. Geben Sie einen beschreibenden Namen für das VLAN und die zu verwendende VLAN-ID an. Die VLAN-ID sollte eine Zahl zwischen 1 und 4094 sein.
5. Sie können mehrere VLANs mit einem einzigen Profil erstellen. Wenn Sie zusätzliche VLANs in diesem Profil erstellen möchten, klicken Sie auf **Add Another** (Weitere hinzufügen), und fahren Sie mit Schritt 4 fort.
6. Klicken Sie auf **Save** (Speichern). Das neue VLAN wird in den ausgewählten Gruppen auf allen VLAN-fähigen Geräten erstellt.

Wenn die VLAN-ID des neu erstellten VLAN mit einem vorhandenen VLAN übereinstimmt, das bereits auf Geräten in der Gerätegruppe vorhanden ist, wird dieses VLAN von Cisco Business Dashboard übernommen und aus der Tabelle der erkannten virtuellen LANs entfernt.

Ändern eines VLAN

1. Aktivieren Sie die Optionsschaltfläche neben dem zu ändernden VLAN, und klicken Sie dann auf das Symbol **Edit** (Bearbeiten).
2. Nehmen Sie die erforderlichen Änderungen an den VLAN-Einstellungen vor, und klicken Sie dann auf **Update** (Aktualisieren).

Entfernen eines VLAN

Aktivieren Sie die Optionsschaltfläche neben dem zu entfernenden VLAN, und klicken Sie dann auf das Symbol **Delete** (Löschen).

Entfernen eines nicht von erstellten VLAN Cisco Business Dashboard

Klicken Sie in der Tabelle der erkannten VLANs neben den zu entfernenden VLANs auf das Symbol zum **Löschen**.

Hinweis VLAN 1 kann nicht gelöscht werden.

Konfigurieren von WLANs

Auf der Seite **Wireless LANs** können Sie die Wireless-Netzwerke in Ihrer Umgebung verwalten. Die bereits vorhandenen, nicht von Cisco Business Dashboard konfigurierten WLANs im Netzwerk werden in einer separaten Tabelle angezeigt. In den folgenden Abschnitten finden Sie Anweisungen zum Erstellen, Ändern und Löschen von Konfigurationsprofilen für Wireless LANs.

Erstellen eines WLAN

1. Navigieren Sie zu **Network Configuration** > **Wireless LANs** (Netzwerkkonfiguration > Wireless LANs).
2. Klicken Sie auf das Plussymbol (**+**), um ein neues WLAN hinzuzufügen.
3. Geben Sie im Abschnitt **Device Group Selection** (Gerätegruppenauswahl) einen Profilnamen für diese Konfiguration ein, wählen Sie eine Organisation aus, und wählen Sie eine oder mehrere Gerätegruppen zur Konfiguration aus.
4. Geben Sie einen SSID-Namen für das Wireless LAN an, und geben Sie die VLAN-ID an, der es zugeordnet werden soll. Die VLAN-ID muss eine Zahl aus dem Bereich von 1 bis 4095 sein. Existiert die angegebene VLAN-ID noch nicht im Netzwerk, wird automatisch ein neues VLAN erstellt.
5. Optional können Sie die Einstellungen für **Enable** (Aktivieren), **Broadcast**, **Security** (Sicherheit) und **Radio** (Funk) ändern.

6. Sie können mehrere Wireless LANs mit einem einzigen Profil erstellen. Wenn Sie zusätzliche Wireless LANs in diesem Profil erstellen möchten, klicken Sie auf **Add Another** (Weitere hinzufügen), und fahren Sie mit Schritt 3 fort.
7. Geben Sie je nach dem ausgewählten Sicherheitsmodus – **Enterprise** (Unternehmen) oder **Personal** (Persönlich) – entweder den RADIUS-Server für die Authentifizierung oder einen vorab geteilten Schlüssel ein.
8. Klicken Sie auf **Save** (Speichern). Das neue WLAN wird auf allen Geräten mit Funktionen für Wireless Access Points in den ausgewählten Gruppen erstellt.

Wenn die Wireless LAN-Konfiguration des neu erstellten Profils mit einem vorhandenen Wireless LAN übereinstimmt, das bereits auf Geräten in der Gerätegruppe vorhanden ist, wird dieses Wireless LAN vom Cisco Business Dashboard übernommen und aus der Tabelle der erkannten Wireless LANs entfernt.

Ändern eines WLAN

1. Aktivieren Sie die Optionsschaltfläche neben dem zu ändernden Wireless LAN, und klicken Sie dann auf das Symbol **Edit** (Bearbeiten).
2. Nehmen Sie die erforderlichen Änderungen an den Wireless LAN-Einstellungen vor, und klicken Sie dann auf **Update** (Aktualisieren).

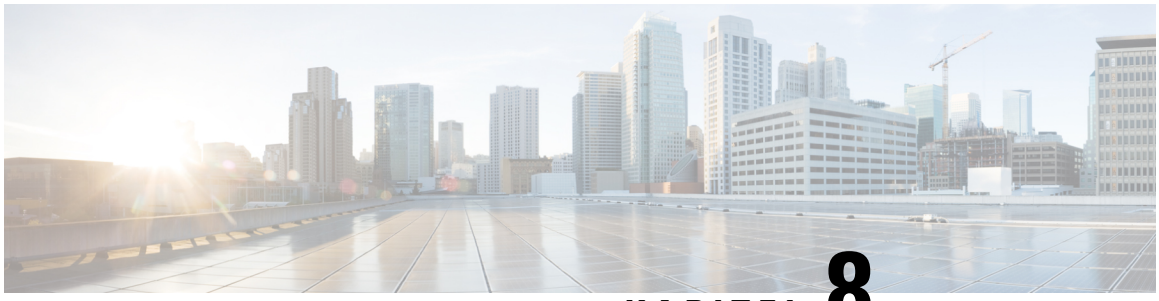
Entfernen eines WLAN

Aktivieren Sie die Optionsschaltfläche neben den zu entfernenden Wireless LANs, und klicken Sie dann auf das Symbol **Delete** (Löschen).

Hinweis Wenn beim Erstellen des Wireless LAN automatisch ein virtuelles LAN erstellt wurde, wird das virtuelle LAN nicht automatisch zusammen mit dem Wireless LAN gelöscht. Sie können das virtuelle LAN auf der Seite **Virtual LANs** (Virtuelle LANs) löschen.

Entfernen eines nicht von erstellten WLAN Cisco Business Dashboard

Klicken Sie in der Tabelle der erkannten Wireless LANs auf die Optionsschaltfläche für das zu entfernende Wireless LAN, und klicken Sie dann auf das Symbol **Delete** (Löschen). In manchen Fällen kann eine WLAN nicht von bestimmten Geräten gelöscht werden. In diesen Fällen müssen Sie die Gerätekonfiguration direkt ändern.



KAPITEL 8

Network Plug and Play

Dieses Kapitel enthält folgende Abschnitte:

Allgemeines zu Network Plug and Play

Network Plug and Play ist ein Service, über den die Firmware und Konfiguration Network Plug and Play-fähiger Geräte zentral verwaltet werden kann und der die Bereitstellung neuer Netzwerkgeräte ohne Benutzereingriffe ermöglicht. Geräte können direkt über das Network Plug-and-Play-Protokoll bereitgestellt werden oder indirekt, wenn sie von einer dem Dashboard zugeordneten Probe-Instanz erkannt werden.

Wenn ein Network Plug and Play-fähiges Gerät installiert wird, identifiziert es den Network Plug and Play-Server entweder per manueller Konfiguration oder durch DHCP, DNS bzw. den Plug and Play Connect-Service. Die folgenden Abschnitte stellen die Konfiguration des Network Plug and Play-Service in Cisco Business Dashboard genauer vor.

Netzwerkanforderungen

Network Plug and Play-Geräte verwenden eine der nachfolgend beschriebenen Methoden zur automatischen Erkennung der Adresse des Network Plug and Play-Servers. Dabei werden die Methoden nacheinander angewendet, bis eine Adresse erkannt wird oder alle Methoden fehlgeschlagen sind. Es werden folgende Methoden verwendet (in der angegebenen Reihenfolge):

- **Manuelle Konfiguration**: Die Adresse des Servers kann manuell über die Verwaltungsoberfläche des Network Plug and Play-fähigen Geräts eingetragen werden.
- **DHCP**: Die Adresse des Servers kann über die DHCP-Option „Vendor-specific Information“ (Herstellerspezifische Informationen) an das Gerät übergeben werden.
- **DNS**: Wird über DHCP kein Wert für die DHCP-Option „Vendor-specific Information“ übermittelt, versucht das Gerät den Server per DNS-Lookup unter Verwendung eines bekannten Hostnamens zu erkennen.

- **Plug and Play Connect-Service**: Sind alle anderen Methoden fehlgeschlagen, versucht das Gerät, eine Verbindung mit dem Plug and Play Connect-Service herzustellen. Dieser Service leitet das Gerät dann an Ihren zuständigen Server weiter.

Sobald das Gerät den Server identifiziert hat, stellt es eine Verbindung her und aktualisiert die Firmware sowie die Konfigurationseinstellungen nach den auf dem Server hinterlegten Vorgaben.

Einrichten der DHCP-basierten Erkennung

Zur Erkennung der Serveradresse per DHCP sendet das Gerät eine DHCP-Erkennungsnachricht mit der Option 60. Diese Nachricht enthält die Zeichenfolge „ciscopnp“. Der DHCP-Server muss daraufhin eine Antwort senden, die die DHCP-Option „Vendor-specific Information“ (Option 43) enthält. Das Gerät extrahiert die Serveradresse aus dieser Option und stellt über diese Adresse eine Verbindung mit dem Server her. „5A1N;B2;K4;I172.19.45.222;J80“ wäre ein Beispiel für eine solche in Option 43 übermittelte Zeichenfolge mit der Adresse eines Network Plug and Play-Servers.

Die Zeichenfolge in Option 43 setzt sich aus folgenden Komponenten zusammen, jeweils voneinander getrennt durch einen Strichpunkt:

- 5A1N: Gibt die DHCP-Unteroption für Plug and Play an und besagt, dass der Server aktiv ist, dass er Version 1 verwendet und dass keine Debugginginformationen vorliegen. Dieser Teil der Zeichenfolge muss nicht geändert werden.
- B2: Steht für den IP-Adress-Typ:
  - B1 = Hostname
  - B2 = IPv4
- Ixxx.xxx.xxx.xxx: großgeschriebenes I, gefolgt von der IP-Adresse oder dem Hostnamen des Servers (IP-Adresse in diesem Beispiel: 172.19.45.222)
- Jxxxx: Nummer des Ports, über den die Verbindung zum Server hergestellt werden soll. (Portnummer in diesem Beispiel: 80) Der Standardport für HTTP ist Port 80, der Standardport für HTTPS Port 443.
- K4: das Transportprotokoll, das für die Verbindung zwischen dem Cisco Plug and Play Agent und dem Server verwendet werden soll:
  - K4 = HTTP (Standard)
  - K5 = HTTPS
- T*trustpoolBundleURL*: optionaler Parameter, der die externe URL des Trustpool-Bundles angibt, falls dieses von einem anderen Speicherort als dem Server abgerufen werden muss. Soll das Bundle beispielsweise von einem TFTP-Server mit der Adresse 10.30.30.10 heruntergeladen werden, müsste als Wert für den Parameter Folgendes angegeben werden: Ttftp://10.30.30.10/ca.p7b
- Wenn Sie Trustpool als Sicherheitsvorkehrung nutzen und den T-Parameter nicht angeben, ruft das Gerät das Trustpool-Bundle vom Server ab.
- Zxxx.xxx.xxx.xxx: die IP-Adresse des NTP-Servers. Dieser Parameter muss angegeben werden, wenn Trustpool als Sicherheitsvorkehrung genutzt wird. Nur dann ist gewährleistet, dass alle Geräte synchronisiert werden.

Detaillierte Informationen zur Konfiguration der DHCP-Optionen finden Sie in der Dokumentation Ihres DHCP-Servers.

Einrichten der DNS-basierten Erkennung

Wenn die IP-Adresse des Servers nicht per DHCP erkannt werden kann, greift das Gerät auf einen DNS-Lookup zurück. Ausgehend von dem vom DHCP-Server zurückgegebenen Netzwerkdomänennamen generiert das Gerät einen vollqualifizierten Domänennamen (FQDN, Fully Qualified Domain Name) für den Server. Dabei verwendet es den vordefinierten Hostnamen „pnpserver“.

Gibt der DHCP-Server beispielsweise den Domänennamen „example.com“ zurück, generiert das Gerät den FQDN „pnpserver.example.com“. Anschließend nutzt es den lokalen Nameserver, um die IP-Adresse dieses FQDN aufzulösen.

Zertifikatanforderungen

Beim Herstellen einer Verbindung mit einem Network Plug and Play-Server überprüft der Client, ob das vom Server vorgelegte Zertifikat gültig und vertrauenswürdig ist. Damit das Zertifikat akzeptiert wird und der Verbindungsaufbau fortgesetzt werden kann, muss das Zertifikat die folgenden Bedingungen erfüllen:

- Das Zertifikat muss von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) signiert werden, oder das Zertifikat selbst muss vom Client als vertrauenswürdig eingestuft werden. Ein Zertifikat, das über die per DHCP übermittelte TrustpoolBundleURL oder den Plug and Play Connect-Service heruntergeladen wurde, wird vom Client als vertrauenswürdig eingestuft.
- Wenn die Serveridentität unter Verwendung von manueller Konfiguration, DHCP oder Plug and Play Connect erkannt wird und eine IP-Adresse ist, muss entweder das Feld **Common Name** (Allgemeiner Name) oder das Feld **Subject Alt Name** diese IP-Adresse enthalten.
- Wenn die Serveridentität unter Verwendung von manueller Konfiguration, DHCP oder Plug and Play Connect erkannt wird und ein Hostname ist, muss entweder das Feld **Common Name** (Allgemeiner Name) oder das Feld **Subject Alt Name** diesen Hostnamen enthalten.
- Wenn die Serveridentität unter Verwendung von DNS-Erkennung erkannt wird, muss entweder das Feld **Common Name** (Allgemeiner Name) oder das Feld **Subject-Alt-Name** die IP-Adresse enthalten, die dem wohlbekannten Hostnamen „pnpserver.<*lokale Domäne*>“ entspricht.

Hinweis Bei einigen der älteren Network Plug and Play-Client-Implementierungen wird das Vorhandensein der Serveridentität im Zertifikat nicht überprüft.

Einrichten der Netzwerkerkennung über Plug and Play Connect

Plug and Play Connect ist ein von Cisco bereitgestellter Service, der von Network Plug and Play-fähigen Geräten als letzte Methode zur Servererkennung verwendet wird, falls alle anderen Erkennungsmethoden fehlgeschlagen sind. Damit Plug and Play Connect zur Servererkennung verwendet werden kann, müssen Sie zunächst ein Controller-Profil für den PnP-Server erstellen und jedes Ihrer Geräte beim Plug and Play Connect-Service registrieren.

Zugreifen auf den Plug and Play Connect-Service

Gehen Sie wie folgt vor, um auf den Plug and Play Connect-Service zuzugreifen:

1. Rufen Sie in einem Webbrowser die Seite *https://software.cisco.com* auf.

2. Klicken Sie oben rechts auf dem Bildschirm auf **Log In** (Anmelden). Melden Sie sich mit der cisco.com-ID Ihres Cisco Smart Account an.
3. Klicken Sie unter **Network Plug and Play** auf **Plug and Play Connect**. Die Hauptseite des Service **Plug and Play Connect** wird angezeigt.

Erstellen eines Controller-Profils

Gehen Sie wie folgt vor, um ein Controller-Profil für den PnP-Server zu erstellen:

1. Öffnen Sie in Ihrem Browser die Webseite von Plug and Play Connect, und wählen Sie falls erforderlich den korrekten Virtual Account aus.
2. Klicken Sie auf „Controller Profiles“ (Controller-Profile) und anschließend auf die Schaltfläche „Add Profile“ (Profil hinzufügen).
3. Wählen Sie aus der Dropdown-Liste „Controller Type“ (Controller-Typ) die Option „PNP SERVER“ (PNP-SERVER) aus. Klicken Sie dann auf „Next“ (Weiter).
4. Geben Sie einen Namen für das Profil ein. Optional können Sie auch eine Beschreibung eingeben.
5. Legen Sie unter „Primary Controller“ (Primärer Controller) mithilfe der Dropdown-Liste fest, ob Sie den Server über seinen Namen oder seine IP-Adresse angeben möchten. Geben Sie den Namen oder die Adressen des Servers in die dafür vorgesehenen Felder ein.
6. Wählen Sie das Protokoll aus, das zur Kommunikation mit dem Server verwendet werden soll. Zur Gewährleistung der Integrität des Bereitstellungsprozesses empfehlen wir dringend, HTTPS zu verwenden.
7. Wenn das ausgewählte Protokoll HTTPS ist, sollte das vom Server verwendete Zertifikat mithilfe der bereitgestellten Steuerelemente hochgeladen werden. Details zum Download des Zertifikats aus Cisco Business Dashboard finden Sie unter Verwalten von Zertifikaten, auf Seite 86.
8. Geben Sie optional einen sekundären Controller an.
9. Klicken Sie auf **Next** (Weiter), und überprüfen Sie die vorgenommenen Einstellungen. Klicken Sie anschließend auf **Submit** (Senden).

Registrieren von Geräten

Bei einem Kauf direkt von Cisco werden bestimmte Produkte möglicherweise bereits zum Zeitpunkt der Bestellung mit Ihrem Cisco Smart Account verknüpft. Diese Produkte werden Plug and Play Connect automatisch hinzugefügt. Die meisten Plug and Play-fähigen Cisco Produkte müssen jedoch manuell registriert werden. Gehen Sie wie folgt vor, um Geräte bei Plug and Play Connect zu registrieren:

1. Öffnen Sie in Ihrem Browser die Webseite von Plug and Play Connect, und wählen Sie falls erforderlich den korrekten Virtual Account aus.
2. Klicken Sie auf **Devices** (Geräte) und anschließend auf **Add Devices** (Geräte hinzufügen). Möglicherweise muss Ihnen zunächst die Berechtigung erteilt werden, dem Account manuell Geräte hinzuzufügen. Dabei handelt es sich um einen einmaligen Vorgang. Sollte dies nötig sein, werden Sie per E-Mail informiert, sobald die Berechtigung erteilt wurde.
3. Wählen Sie aus, ob Sie die Geräte manuell hinzufügen möchten oder ob Sie eine CSV-Datei mit Geräteinformationen hochladen möchten, um mehrere Geräte gleichzeitig hinzuzufügen. Klicken Sie auf den entsprechenden Link, um eine exemplarische CSV-Datei herunterzuladen. Wenn Sie eine CSV-Datei

hochladen möchten: Klicken Sie auf die Schaltfläche **Browse** (Durchsuchen), und wählen Sie die gewünschte Datei aus. Klicken Sie dann auf **Next** (Weiter).

4. Wenn Sie manuell Geräte hinzufügen möchten: Klicken Sie auf **Identify Device** (Gerät identifizieren). Geben Sie die Seriennummer und die Produkt-ID des Geräts ein, das Sie hinzufügen möchten. Wählen Sie aus der Dropdown-Liste ein Controller-Profil aus. Optional können Sie auch eine Beschreibung des Geräts eingeben.
5. Wiederholen Sie Schritt 4 für alle Geräte, die Sie hinzufügen möchten. Klicken Sie dann auf **Next** (Weiter).
6. Überprüfen Sie alle hinzugefügten Geräte, und klicken Sie anschließend auf **Submit** (Senden).

Konfigurieren des Network Plug and Play-Service

Bei der Einrichtung des Network Plug and Play-Service in Ihrer Umgebung müssen Sie möglicherweise verschiedene Aufgaben durchführen. Dazu gehören unter anderem der Upload von Konfigurationen und Images, das Hinzufügen und Konfigurieren von Geräten zur Verwendung von Network Plug and Play und das Management von mit dem Service verbundenen Geräten, die noch nicht beim Service registriert sind. In den nachfolgenden Abschnitten werden diese Aufgaben detailliert beschrieben.

Verwenden des Network Plug and Play-Dashboards

Im **Network Plug and Play**-Dashboard finden Sie einen Überblick über alle Geräte, die aktuell per Network Plug and Play bereitgestellt werden. Es werden drei Diagramme angezeigt, die den Gerätestatus nach Gerätegruppe, PnP-fähigem Gerät und dem Cisco Business Dashboard-Bestand unbekannten Geräten (nicht beanspruchten Geräten) verdeutlichen. Bei jedem Diagramm wird angegeben, wie viele Geräte bzw. Gruppen sich jeweils im betreffenden Status befinden. Durch einen Klick auf die Statusüberschrift eines Diagramms können Sie eine detaillierte Liste aller Geräte oder Gruppen aufrufen, die in die betreffende Kategorie fallen. Die folgende Tabelle zeigt die verschiedenen Status:

Tabelle 15: Netzwerk Plug and Play-Dashboard – Statusdefinitionen

Status	Beschreibung
Gruppen	
Vorab bereitgestellt	Gerätegruppen mit PnP-fähigen Geräten nur im Status „Ausstehend“.
In Bearbeitung	Gerätegruppen mit einigen PnP-fähigen Geräten im Status „Ausstehend“ und einigen im Status „Bereitstellung“ oder „Wurde bereitgestellt“
Wurde bereitgestellt	Gerätegruppen, in denen sich alle PnP-fähigen Geräte im Status „Wurde bereitgestellt“ befinden
Fehler	Gerätegruppen mit einem oder mehreren PnP-fähigen Geräten im Status „Fehler“
Aktivierte Geräte	
Ausstehend	Geräte im Bestand, die für PnP aktiviert wurden, aber noch keine Verbindung zum PnP-Server hergestellt haben

Status	Beschreibung
Bereitstellung	Geräte, die den PnP-Server kontaktiert und mit der Bereitstellung begonnen haben, aber den Bereitstellungsprozess nicht abgeschlossen haben
Wurde bereitgestellt	Geräte, die erfolgreich über PnP bereitgestellt wurden
Fehler	Geräte, bei denen der PnP-Bereitstellungsprozess fehlgeschlagen ist
Nicht beanspruchte Geräte	
Nicht beansprucht	Geräte, die den PnP-Server kontaktiert haben, aber nicht im Bestand definiert sind
Ignored (Ignoriert)	Nicht beanspruchte Geräte, die vom Benutzer explizit ignoriert wurden

Über die Dropdown-Liste „Organization“ (Organisation) oben rechts im Dashboard können Sie die angezeigten Informationen auf eine bestimmte Organisation beschränken. Geben Sie beim Anzeigen von Gerätegruppen einen Gruppennamen ganz oder teilweise im Suchfeld ein, um die in der Tabelle angezeigten Gruppen einzuschränken. Analog hierzu können Sie beim Anzeigen von Bereitstellungsregeln im Suchfeld einen Gerätenamen, eine Produkt-ID oder eine Seriennummer eingeben, um den aktuellen Status eines einzelnen Geräts abzurufen.

Hinweis Das Diagramm für nicht angeforderte Geräte wird nur **Administratoren** angezeigt, die Daten für **alle Organisationen** anzeigen.

Verwalten von aktivierten Geräten

Aktivierte Geräte sind Geräte im Bestand, die für die Bereitstellung mit einer Image- oder Konfigurationsdatei konfiguriert wurden oder zuvor von Cisco Business Dashboard erkannt wurden und versucht haben, eine Verbindung über Network Plug and Play herzustellen. Bei einem aktivierten Gerät, das mit einer Image- oder Konfigurationsdatei konfiguriert wurde, wird dieses Image und/oder diese Konfiguration bei der nächsten Gelegenheit auf das Gerät angewendet. Wenn das Gerät mit dem Dashboard verbunden und verwaltet wird, werden die Änderungen sofort angewendet. Andernfalls werden die Änderungen übernommen, wenn das Gerät das nächste Mal verbunden wird − entweder über eine Probe oder direktes Management − oder wenn es sich über das Network Plug and Play-Protokoll anmeldet.

Gehen Sie wie folgt vor, um ein neues aktiviertes Gerät zu erstellen:

1. Navigieren Sie zu **Network Plug and Play** > **Enabled Devices** (Aktivierte Geräte).
2. Klicken Sie auf das Pluszeichen (**✚**), um dem Bestand ein neues aktiviertes Gerät hinzuzufügen.
3. Füllen Sie das Formular **Add New Device** (Neues Gerät hinzufügen) mit den angeforderten Parametern aus, einschließlich Details zum Gerät, der Organisation, dem Netzwerk und der Gerätegruppe, zu der es gehören soll, und klicken Sie dann auf **Next** (Weiter).
4. Wählen Sie optional ein Firmware-Image aus, das auf das Gerät angewendet werden soll. Wenn Sie als Image **Default** (Standard) auswählen, verwendet das Gerät das für die jeweilige Produkt-ID als Standard-Image festgelegte Image, sobald es sich mit dem Server verbindet.
5. Wählen Sie optional eine Konfiguration, die auf das Gerät angewendet werden soll, sowie die Version der Konfiguration aus, falls es mehrere Versionen gibt. Wenn es sich bei der Konfiguration um eine

Vorlage mit Platzhaltern handelt, wird ein Formular angezeigt, in dem die für dieses Gerät zu verwendenden Werte eingegeben werden müssen. Füllen Sie diese Felder bei Bedarf aus. Wenn die Vorlage vom System definierte Parameter verwendet, können Sie das Kontrollkästchen aktivieren, um die zu verwendenden Werte anzuzeigen.

6. Klicken Sie auf **Next** (Weiter), um zum Bildschirm **Summary** (Zusammenfassung) zu gelangen. Überprüfen Sie die eingegebenen Daten. Im Vorschaufenster unten können Sie auch die endgültige Gerätekonfiguration überprüfen. Wenn Sie zufrieden sind, klicken Sie auf **Finish** (Fertigstellen).

Gehen Sie wie folgt vor, um ein vorhandenes Gerät zu bearbeiten:

1. Navigieren Sie zu **Network Plug and Play** > **Enabled Devices** (Aktivierte Geräte).
2. Aktivieren Sie das Kontrollkästchen für das zu ändernde Gerät und klicken Sie auf **Edit** (Bearbeiten). Alternativ können Sie auf den Namen des Geräts klicken.
3. Klicken Sie auf **Next** (Weiter), um den Bildschirm **Provision Device** (Gerät bereitstellen) anzuzeigen. Ändern Sie bei Bedarf das Image und/oder die Konfigurationsdatei und nehmen Sie alle Änderungen an den mit der Konfiguration verbundenen Parameterwerten vor.
4. Klicken Sie auf **Next** (Weiter), um zum Bildschirm **Summary** (Zusammenfassung) zu gelangen. Überprüfen Sie die eingegebenen Daten. Im Vorschaufenster unten können Sie auch die endgültige Gerätekonfiguration überprüfen. Wenn Sie zufrieden sind, klicken Sie auf **Finish** (Fertigstellen).

Hinweis Wenn die Einstellungen für die Image- oder Konfigurationsdatei für ein Gerät geändert werden, das schon bereitgestellt wurde, wird der Status dieses Geräts auf „Pending“ (Ausstehend) zurückgesetzt, und das Gerät wird beim nächsten Einchecken beim Dashboard erneut bereitgestellt.

Gehen Sie wie folgt vor, um ein aktiviertes Gerät zu entfernen:

1. Navigieren Sie zu **Network Plug and Play** > **Enabled Devices** (Aktivierte Geräte).
2. Markieren Sie ein oder mehrere Kontrollkästchen für die zu entfernenden Geräte und klicken Sie auf das Symbol zum **Löschen**.

Hinweis Wenn ein aktiviertes Gerät gelöscht wird, dieses Gerät jedoch dem Dashboard anderweitig bekannt ist und das Gerät online ist, werden nur die Einstellungen für die Image- und Konfigurationsdateien für dieses Gerät entfernt. Das Gerät verbleibt im Bestand, ähnlich wie jedes andere verwaltete Gerät. Wenn ein Gerät anschließend über PnP eine Verbindung mit dem Dashboard herstellt, wird der Tabelle der aktivierten Geräte ein neuer Eintrag hinzugefügt.

Nicht angeforderte Geräte

Hinweis Die Seite **Unclaimed Devices** (Nicht angeforderte Geräte) ist nur für Administratoren verfügbar.

Nicht angeforderte Geräte sind Geräte, die eine Verbindung mit dem Service hergestellt haben, für die jedoch im Bestand kein passender Gerätedatensatz vorhanden ist. Gehen Sie wie folgt vor, um eine Liste aller nicht

angeforderten Geräte aufzurufen und nicht angeforderte Geräte anzufordern, damit sie mit Network Plug and Play verwaltet werden können:

1. Navigieren Sie zu **Network Plug and Play** > **Unclaimed Devices** (Nicht angeforderte Geräte), und wechseln Sie zur Registerkarte **Unclaimed** (Nicht angefordert).
2. Klicken Sie auf die Schaltfläche „Claim“ (Anfordern), um das Gerät zu verwalten.
3. Füllen Sie das Formular „Unclaimed Device“ (Nicht beanspruchtes Gerät) mit den angeforderten Parametern aus, einschließlich der Organisation, dem Netzwerk und der Gerätegruppe, zu der es gehören soll, und klicken Sie dann auf **Next** (Weiter).
4. Wählen Sie optional ein Firmware-Image aus, das auf das Gerät angewendet werden soll. Wenn Sie als Image **Default** (Standard) auswählen, verwendet das Gerät das für die jeweilige Produkt-ID als Standard-Image festgelegte Image, sobald es sich mit dem Server verbindet.
5. Wählen Sie alternativ eine Konfiguration, die auf das Gerät angewendet werden soll, sowie die Version der Konfiguration aus, falls es mehrere Versionen gibt. Wenn es sich bei der Konfiguration um eine Vorlage mit Platzhaltern handelt, wird ein Formular angezeigt, in dem die für dieses Gerät zu verwendenden Werte eingegeben werden müssen. Füllen Sie diese Felder bei Bedarf aus.

   Wenn die Vorlage vom System definierte Parameter verwendet, können Sie das Kontrollkästchen aktivieren, um die zu verwendenden Werte anzuzeigen.
6. Klicken Sie auf **Next** (Weiter), um zum Bildschirm **Summary** (Zusammenfassung) zu gelangen. Überprüfen Sie die eingegebenen Daten. Im Vorschaufenster unten können Sie auch die endgültige Gerätekonfiguration überprüfen. Wenn Sie zufrieden sind, klicken Sie auf **Finish** (Fertigstellen).

Gehen Sie wie folgt vor, um Geräte aus der Liste „Unclaimed“ (Nicht angefordert) zu entfernen, ohne sie bereitzustellen:

1. Navigieren Sie zu **Network Plug and Play** > **Unclaimed Devices** (Nicht angeforderte Geräte), und wechseln Sie zur Registerkarte **Unclaimed** (Nicht angefordert).
2. Klicken Sie für das Gerät, das Sie aus der Liste entfernen möchten, auf **Ignore** (Ignorieren) .

Die Geräte werden in die Liste **Ignored** (Ignoriert) verschoben. Es werden keine weiteren Aktionen für sie durchgeführt. Gehen Sie wie folgt vor, um ein ignoriertes Gerät erneut anzufordern:

1. Navigieren Sie zu **Network Plug and Play** > **Unlaimed Devices** (Nicht angeforderte Geräte), und wechseln Sie zur Registerkarte **Ignored** (Ignoriert).
2. Klicken Sie auf die Schaltfläche **Unignore** (Ignorieren aufheben), um das Gerät wieder anzufordern.

Die Geräte werden in die Liste **Unclaimed** (Nicht angefordert) verschoben, und Sie können die Geräte wie oben beschrieben anfordern.

Automatisches Anfordern von Geräten

Hinweis Die Seite **Auto Claim** (Automatische Anforderung) ist nur für Administratoren verfügbar.

Sie können eine Regel zur automatischen Anforderung für eine Produkt-ID erstellen, damit Geräte mit dieser ID automatisch vom Server angefordert und bereitgestellt werden. Gehen Sie wie folgt vor, um eine Regel zur automatischen Anforderung zu erstellen:

1. Navigieren Sie zu **Network Plug and Play** > **Auto Claim Devices** (Geräte automatisch anfordern).
2. Klicken Sie auf das Pluszeichen (✚), um eine neue Regel zur **automatischen Anforderung** zu erstellen.
3. Füllen Sie das Formular „Auto Claim Device“ (Automatisches Anfordern von Geräten) mit den angeforderten Parametern aus, einschließlich der zu vergleichenden Produkt-ID (PID), der Organisation, dem Netzwerk und der Gerätegruppe, zu der das neu angeforderte Gerät gehören soll, und klicken Sie dann auf **Next** (Weiter).
4. Wählen Sie optional ein Firmware-Image aus, das auf das Gerät angewendet werden soll. Wenn Sie als Image **Default** (Standard) auswählen, verwendet das Gerät das für die jeweilige Produkt-ID als Standard-Image festgelegte Image, sobald es sich mit dem Server verbindet.
5. Wählen Sie alternativ eine Konfiguration, die auf das Gerät angewendet werden soll, sowie die Version der Konfiguration aus, falls es mehrere Versionen gibt. Wenn es sich bei der Konfiguration um eine Vorlage mit Platzhaltern handelt, wird ein Formular angezeigt, in dem die für dieses Gerät zu verwendenden Werte eingegeben werden müssen. Füllen Sie diese Felder bei Bedarf aus.

   Wenn die Vorlage vom System definierte Parameter verwendet, können Sie das Kontrollkästchen aktivieren, um die zu verwendenden Werte anzuzeigen.
6. Klicken Sie auf **Next** (Weiter), um zum Bildschirm **Summary** (Zusammenfassung) zu gelangen. Überprüfen Sie die eingegebenen Daten. Im Vorschaufenster unten können Sie auch die endgültige Gerätekonfiguration überprüfen. Wenn Sie zufrieden sind, klicken Sie auf **Finish** (Fertigstellen).

Neue Geräte, die nicht im Bestand enthalten sind, werden mit der Liste der Regeln zur automatischen Anforderung abgeglichen. Wird hier eine passende Regel gefunden, wird im Bestand ein neuer Gerätedatensatz mit dem von der Regel zur **automatischen Anforderung** vorgegebenen Image und der entsprechenden Konfigurationsdatei erstellt. Anschließend wird das Gerät entsprechend bereitgestellt. Passt keine der Regeln zur **automatischen Anforderung** auf das Gerät, wird das Gerät der Liste der nicht angeforderten Geräte hinzugefügt, und es wird keine weitere Aktion durchgeführt.

Geräte-Firmware-Images

Auf der Seite **Images** können Sie Firmware-Images hochladen, die dann auf Geräten bereitgestellt werden können. Dabei können Sie Firmware-Images als Standard-Image für bestimmte Plattformen festlegen. So lässt sich die Firmware ganzer Gerätefamilien später sehr einfach aktualisieren. Firmware-Images sind organisationsspezifisch und dürfen nur für Bereitstellungsgeräte verwendet werden, die derselben Organisation zugeordnet sind.

Gehen Sie wie folgt vor, um ein Firmware-Image hochzuladen:

1. Navigieren Sie zu **Network Plug and Play** > **Images**.
2. Klicken Sie auf das Plussymbol (✚).
3. Wählen Sie die Organisation für das Image aus der Dropdown-Liste aus.
4. Ziehen Sie ein Firmware-Image von Ihrem PC in den Zielbereich im Fenster **Upload File** (Datei hochladen). Alternativ können Sie in den Zielbereich klicken und ein Firmware-Image zum Hochladen auswählen.
5. Klicken Sie auf **Upload** (Hochladen).

Sie können ein Image als Standard-Image für einen oder mehrere Gerätetypen festlegen. Gehen Sie wie folgt vor, um ein Image als Standard-Image festzulegen:

1. Navigieren Sie zu **Network Plug and Play** > **Images**.

2. Aktivieren Sie in der Tabelle **Images** die Optionsschaltfläche für das Image, und klicken Sie dann auf **Edit** (Bearbeiten).
3. Geben Sie in das Feld **Default Image for Product IDs** (Standard-Image für Produkt-IDs) eine Liste von Produkt-IDs ein, jeweils durch Komma voneinander getrennt. Produkt-IDs dürfen Fragezeichen (?) als Platzhalter für einzelne Zeichen enthalten und Sterne (*) als Platzhalter für Zeichenfolgen.
4. Klicken Sie auf **Save** (Speichern).

Gehen Sie wie folgt vor, um Images zu entfernen:

1. Navigieren Sie zu **Network Plug and Play** > **Images**.
2. Aktivieren Sie die Optionsschaltfläche für das zu löschende Image, und klicken Sie dann auf **Delete** (Löschen).

Gerätekonfigurationsdateien

Auf der Seite „Configurations“ (Konfigurationen) können Sie Konfigurationsdateien hochladen oder erstellen, die dann auf den Geräten bereitgestellt werden können. Konfigurationsdateien sind organisationsspezifisch und dürfen nur für Bereitstellungsgeräte verwendet werden, die derselben Organisation zugeordnet sind.

Konfigurationsdateien können einfache Textdateien sein oder Platzhalter und zugehörige Metadaten enthalten, so dass dieselbe Konfigurationsdatei mit mehreren Geräten verwendet werden kann, während gleichzeitig eindeutige Parameter für jedes einzelne Gerät eingestellt werden können. Eine einzige Konfigurationsvorlage kann beispielsweise auf mehrere Geräte angewendet werden, wobei der Hostname jedoch für jedes Gerät einzeln angegeben werden kann. Weitere Einzelheiten zu Konfigurationsvorlagen finden Sie unter Verwaltung von Konfigurationsvorlagen in Anhang A.

Eine Auswahl von Konfigurationsvorlagen für verschiedene Gerätetypen ist in der Dashboard-Anwendung enthalten. Diese Vorlagen können unverändert übernommen, geändert oder kopiert und als Grundlage für neue Vorlagen verwendet werden.

Um eine neue Konfiguration manuell zu erstellen, gehen Sie wie folgt vor:

1. Navigieren Sie zu **Network Plug and Play** > **Configurations** (Konfigurationen).
2. Klicken Sie auf das Plussymbol (✚).
3. Der Vorlageneditor startet mit einem leeren Bereich für die Konfiguration auf der linken Seite und einem Formular auf der rechten Seite zur Verwaltung der mit der Vorlage verbundenen Metadaten.

   Geben Sie in das Feld oben links einen Namen für die Konfiguration ein. Wählen Sie eine Organisation aus und geben Sie in den Feldern rechts eine durch Komma getrennte Liste von Produkt-IDs ein, die diese Konfiguration unterstützen. Optional können Sie eine Beschreibung eingeben. Produkt-IDs dürfen Fragezeichen (?) als Platzhalter für einzelne Zeichen enthalten und Sterne (*) als Platzhalter für Zeichenfolgen.
4. Erstellen Sie die Konfiguration durch Eingeben oder Einfügen von Text in den Textbereich auf der linken Seite. Nehmen Sie ggf. mit den Bedienelementen auf der rechten Seite die entsprechenden Änderungen an den Metadaten vor. Weitere Einzelheiten zur Vorlagensyntax und zu den Metadaten finden Sie unter Verwaltung von Konfigurationsvorlagen.

   Sie können die Schaltfläche **Preview** (Vorschau) verwenden, um zu sehen, wie die Konfigurationsvorlage aussieht, wenn sie einem Gerät zugeordnet wird.
5. Wenn Sie mit der Konfiguration zufrieden sind, klicken Sie auf **Save** (Speichern).

Gehen Sie wie folgt vor, um eine Konfigurationsdatei hochzuladen:

1. Navigieren Sie zu **Network Plug and Play** > **Configurations** (Konfigurationen).
2. Klicken Sie auf das Symbol zum **Hochladen**.
3. Wählen Sie die Organisation für die Konfiguration aus der Dropdown-Liste aus. Geben Sie einen Namen für die Konfiguration an und fügen Sie optional eine Beschreibung hinzu.
4. Ziehen Sie eine Konfigurationsdatei von Ihrem PC in den Zielbereich im Fenster **Upload File** (Datei hochladen). Alternativ können Sie in den Zielbereich klicken und eine Konfigurationsdatei zum Hochladen auswählen.
5. Klicken Sie auf **Upload** (Hochladen).

Bei Bedarf können Sie auf den Dateinamen der hochgeladenen Konfigurationsdatei klicken, um deren Inhalte im Vorlageneditor zu sehen.

Gehen Sie wie folgt vor, um Konfigurationsdateien zu entfernen:

1. Navigieren Sie zu **Network Plug and Play** > **Configurations** (Konfigurationen).
2. Markieren Sie ein oder mehrere Kontrollkästchen für die zu entfernenden Konfigurationen und klicken Sie auf das Symbol zum **Löschen**.

Verwalten der Einstellungen

Auf der Seite mit den Network Plug and Play-Einstellungen können Sie steuern, wie das Network Plug and Play-Protokoll arbeitet. Der Parameter **Check In Time Interval** (Check-in-Zeitintervall) legt fest, wie häufig ein Gerät nach der Erstbereitstellung eine Verbindung mit dem Network Plug and Play-Service herstellt. Gehen Sie wie folgt vor, um diesen Parameter zu ändern:

1. Navigieren Sie zu **Network Plug and Play** > **Settings** (Einstellungen).
2. Geben Sie das gewünschte Zeitintervall für den Verbindungsaufbau in das dafür vorgesehene Feld ein. Das Intervall wird in Minuten angegeben. Der Standardwert ist 2.880 Minuten (oder 2 Tage).
3. Klicken Sie auf **Save** (Speichern).

Das **Check-in-Zeitintervall** wird für das System als Ganzes festgelegt, kann aber auf Organisationsebene überschrieben werden. Wenn kein Intervall für die Organisation festgelegt ist, wird der Systemwert verwendet.

Konfigurieren des Zertifikats

Das Zertifikat, das von Cisco Business Dashboard beim ersten Start automatisch generiert wird, ist ein selbstsigniertes Zertifikat. In den meisten Fällen reicht dies nicht aus, damit das Zertifikat vom Network Plug and Play-Client akzeptiert wird, und es muss ein neues Zertifikat generiert werden. Beim Generieren eines neuen selbstsignierten Zertifikats oder einer neuen Zertifikatsignierungsanforderung (Certificate Signing Request, CSR) berücksichtigt das Dashboard neben den in der GUI im Feld **Subject Alternative Name** festgelegten Werten auch den Inhalt des Felds **Common Name** (Allgemeiner Name) im Feld **Subject Alternative Name**.

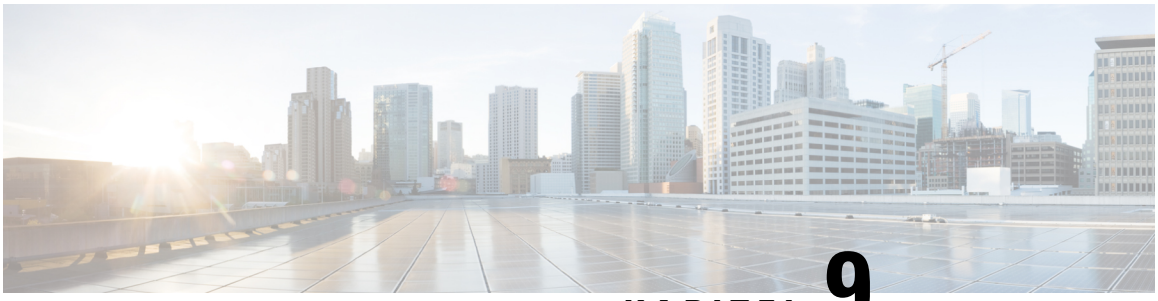
Weitere Informationen zum Konfigurieren des Zertifikats für das Dashboard finden Sie unter Verwalten von Zertifikaten, auf Seite 86.

Überwachen von Network Plug and Play

Alle Geräte, die im Network Plug and Play-Service als erkannt geführt werden, werden entweder auf der Seite **Enabled Devices** (Aktivierte Geräte) oder auf der Seite **Unclaimed Devices** (Nicht angeforderte Geräte) mit ihrem Status angezeigt. Sie können diesen Status auch auf der Seite **Inventory** (Bestand) anzeigen, indem Sie die Anzeige der Spalte **PnP Status** (PnP-Status) aktivieren. Das Statusfeld gibt den aktuellen Status des Geräts an und enthält einen der in der nachfolgenden Tabelle aufgeführten Werte. Durch einen Klick auf das Statusfeld können Sie weitere Details abrufen, beispielsweise einen chronologischen Verlauf der Gerätestatusänderungen.

Tabelle 16: Network Plug and Play: Gerätestatus

Status	Beschreibung
AUSSTEHEND	Das Gerät ist im Service definiert, hat aber noch keine Verbindung mit dem Service hergestellt.
BEREITSTELLUNG	Das Gerät hat die Erstverbindung mit dem Service hergestellt.
PROVISIONING_IMAGE	Das Gerät stellt ein Firmware-Image bereit.
PROVISIONED_IMAGE_REBOOTING	Das Gerät führt einen Neustart durch, um die neue Firmware auszuführen.
PROVISIONED_IMAGE	Die neue Firmware wurde erfolgreich installiert.
PROVISIONING_CONFIG	Eine Konfigurationsdatei wird auf das Gerät angewendet.
PROVISIONED_CONFIG	Eine Konfigurationsdatei wurde erfolgreich auf das Gerät angewendet. Je nach Gerätetyp wird ein Geräteneustart durchgeführt, damit die Konfigurationseinstellungen wirksam werden.
FEHLER	Es ist ein Fehler aufgetreten. Weitere Details finden Sie in den Protokolldateien.
BEREITGESTELLT	Die Bereitstellung des Geräts ist abgeschlossen.



KAPITEL 9

Ereignisprotokoll

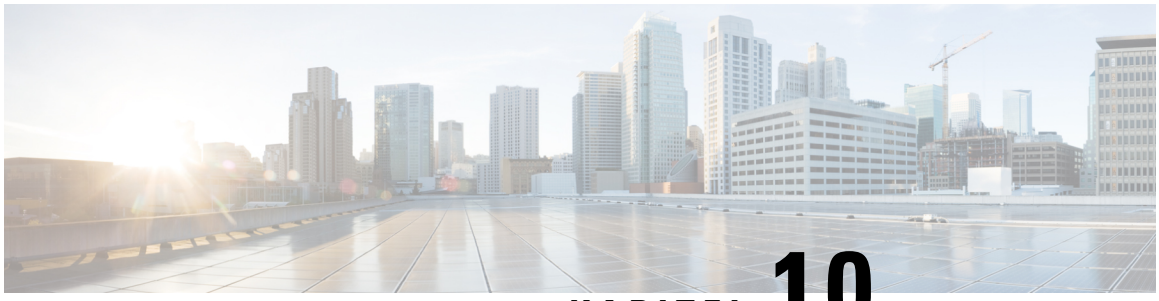
Dieses Kapitel enthält folgende Abschnitte:

Allgemeines zum Ereignisprotokoll

Das Ereignisprotokoll gibt Ihnen eine durchsuchbare und sortierbare Liste aller im Netzwerk generierten Ereignisse an die Hand. Über die zur Verfügung gestellten Filtersteuerelemente können Sie mithilfe einer beliebigen Kombination der folgenden Parameter eingrenzen, welche Ereignisse angezeigt werden:

- **Time** (Uhrzeit): Mithilfe dieses Parameters können Sie den Startzeitpunkt und den Endzeitpunkt einer Zeitspanne festlegen, nach der gefiltert werden soll. Es werden dann nur Ereignisse angezeigt, die während dieser Zeitspanne eingetreten sind.
- **Severity** (Prioritätsstufe): Mithilfe dieses Parameters können Sie festlegen, dass nur Ereignisse einer bestimmten Prioritätsstufe angezeigt werden. Aktivieren Sie das Kontrollkästchen *Higher* (Höher), wenn jeweils auch Ereignisse mit höherer Prioritätsstufe angezeigt werden sollen.
- **Type** (Typ): Wählen Sie einen oder mehrere Ereignistypen aus, die angezeigt werden sollen. Die verschiedenen Typen sind in Form einer Baumstruktur angeordnet. Wenn Sie einen Ereignistyp auswählen, werden automatisch auch alle ihm in der Baumstruktur untergeordneten Typen eingeschlossen.
- **Network** (Netzwerk): Wählen Sie eines oder mehrere Netzwerke aus, für die Ereignisse angezeigt werden sollen. Sobald Sie mit der Eingabe beginnen, werden passende Standorte vorgeschlagen.
- **Device** (Gerät): Mithilfe dieses Parameters können Sie festlegen, dass nur die für ein bestimmtes Gerät erfassten Ereignisse angezeigt werden. Sie können ein oder mehrere Geräte auswählen. Sobald Sie mit der Eingabe beginnen, werden passende Geräte vorgeschlagen. Zur Geräteauswahl können Sie den Namen, die IP-Adresse oder die MAC-Adresse des Geräts eingeben.

Ereignisse, die den Filterbedingungen entsprechen, werden in der Tabelle unter den Filteroptionen angezeigt. Die Tabelleneinträge lassen sich per Klick auf die Spaltenüberschriften sortieren.



KAPITEL 10

Berichte

Dieses Kapitel enthält folgende Abschnitte:

Allgemeines zu Berichten

Mit der Option **Reports** (Berichte) in Cisco Business Dashboard können Sie eine Reihe von Berichten über Ihr Netzwerk abrufen. Unter anderen stehen folgende Berichte zur Verfügung:

- **Lifecycle Report** (Lebenszyklusbericht): Bietet eine Übersicht über den Status der Geräte im Netzwerk.
- **End of Life Report** (End-of-Life-Bericht): Führt alle Geräte auf, für die ein End-of-Life-Bulletin veröffentlicht wurde.
- **Maintenance Report** (Wartungsbericht): Listet alle Geräte mit Garantiestatus und ggf. aktivem Supportvertrag auf.
- **Wireless Network** (Wireless-Netzwerk): Enthält Informationen zur Wireless-Umgebung, unter anderem zu SSIDs, Access Points und der Spektrumnutzung.
- **Wireless Client** (Wireless-Client): Enthält Details zu allen Wireless-Clients, die im Netzwerk erkannt wurden.

Anzeigen des Lebenszyklusberichts

Der **Lebenszyklusbericht** bietet einen Überblick über den Status der Netzwerkgeräte, wobei der Software- und der Hardwarelebenszyklusstatus berücksichtigt werden. In der folgenden Tabelle werden die enthaltenen Informationen erläutert.

Tabelle 17: Lebenszyklusbericht

Feld	Beschreibung
Netzwerkname	Der Name des Netzwerks, in dem sich das Gerät befindet
Organisation	Die Organisation, zu der das Gerät gehört
Hostname	Hostname des Geräts
Gerätetyp	Typ des Geräts
Modell	Modellnummer des Geräts.
Herstellungswoche	Das Herstellungsdatum des Geräts, angezeigt als Kalenderwoche und Jahr
Firmwareupgrade verfügbar	Neueste für das Gerät verfügbare Firmwareversion oder ein Hinweis, dass die Firmware des Geräts aktuell ist
Firmware-Version	Aktuell auf dem Gerät ausgeführte Firmwareversion
End-of-Life-Status	Gibt an, ob für das Gerät ein End-of-Life-Bulletin veröffentlicht wurde und an welchem Datum der nächste wichtige Meilenstein im End-of-Life-Prozess erreicht wird.
Wartungsstatus	Gibt an, ob für das Gerät aktuell eine Garantie oder ein Supportvertrag gilt.

Wenn ein Gerät möglicherweise Ihr Eingreifen erfordert, verdeutlicht die Zeilenfarbe die Dringlichkeit. So wird beispielsweise ein Gerät, für das ein End-of-Life-Bulletin veröffentlicht wurde, orangefarben markiert, wenn der End-of-Support-Meilenstein noch nicht erreicht ist. Wenn Cisco keinen Support mehr für das Gerät anbietet, wird es rot markiert.

Mit dem Suchfeld oben in jedem Bericht können Sie die Ergebnisse filtern. Geben Sie im Feld Suchen Text ein, um nur die Einträge mit dem entsprechenden Text anzuzeigen. Über die Dropdown-Liste „Organization“ (Organisation) können Sie die Ergebnisse auf eine bestimmte Organisation begrenzen.

Über das Spaltenauswahl-Symbol oben links im Bericht können Sie die angezeigten Informationen anpassen. Klicken Sie auf das Symbol, und wählen Sie dann mithilfe der angezeigten Kontrollkästchen die gewünschten Spalten für den Bericht aus.

Anzeigen des End-of-Life-Berichts

Im **End-of-Life-Bericht** sind alle Geräte aufgeführt, für die ein **End-of-Life**-Bulletin veröffentlicht wurde, inklusive der wichtigsten End-of-Life-Termine und der empfohlenen Ersatzplattform. In der folgenden Tabelle werden die enthaltenen Informationen erläutert.

Tabelle 18: End-of-Life-Bericht

Feld	Beschreibung
Netzwerkname	Der Name des Netzwerks, in dem sich das Gerät befindet
Organisation	Die Organisation, zu der das Gerät gehört
Produkt-ID	Produkt-ID oder Teilenummer des Geräts
Hostname	Hostname des Geräts
Gerätetyp	Typ des Geräts
Aktueller Status	Aktueller Status des End-of-Life-Prozesses für das Produkt
Ankündigungsdatum	Veröffentlichungsdatum des End-of-Life-Bulletins
Letztes Verkaufsdatum	Datum, nach dem das Produkt nicht mehr von Cisco verkauft wird
Letztes Datum für Softwareversionen	Datum, nach dem keine weiteren Softwareversionen mehr für das Produkt veröffentlicht werden
Letztes Datum für neuen Servicevertrag	Letztes Datum, an dem Sie einen neuen Supportvertrag für das Gerät abschließen können
Letztes Datum für Verlängerung des Servicevertrags	Letztes Datum, an dem Sie einen vorhandenen Supportvertrag für das Gerät verlängern können
Letztes Support-Datum	Datum, nach dem Cisco keinen Support mehr für das Produkt anbietet
Empfohlener Ersatz	Empfohlenes Ersatzprodukt
Produktneuheiten	Produkt-Bulletin-Nummer und Link zum Bulletin auf der Cisco Website

Die Zeilen der Tabelle haben unterschiedliche Farben, die den Status des End-of-Life-Prozesse für das Gerät angeben. So wird beispielsweise ein Gerät, bei dem das letzte Verkaufsdatum bereits überschritten ist, das letzte Supportdatum jedoch noch nicht, orangefarben markiert. Ein Gerät, bei dem bereits das letzte Supportdatum überschritten ist, wird rot markiert.

Mit dem Suchfeld oben in jedem Bericht können Sie die Ergebnisse filtern. Geben Sie im Feld Suchen Text ein, um nur die Einträge mit dem entsprechenden Text anzuzeigen. Über die Dropdown-Liste „Organization“ (Organisation) können Sie die Ergebnisse auf eine bestimmte Organisation begrenzen.

Über das Spaltenauswahl-Symbol oben links im Bericht können Sie die angezeigten Informationen anpassen. Klicken Sie auf das Symbol, und wählen Sie dann mithilfe der angezeigten Kontrollkästchen die gewünschten Spalten für den Bericht aus.

Anzeigen des Wartungsberichts

Im **Wartungsbericht** sind alle Netzwerkgeräte mit Informationen zum Status der Garantie und des Supportvertrags aufgeführt. In der folgenden Tabelle werden die enthaltenen Informationen erläutert.

Tabelle 19: Wartungsbericht

Feld	Beschreibung
Netzwerkname	Der Name des Netzwerks, in dem sich das Gerät befindet
Organisation	Die Organisation, zu der das Gerät gehört
Hostname	Hostname des Geräts
Gerätetyp	Typ des Geräts
Modell	Modellnummer des Geräts
Seriennummer	Seriennummer des Geräts
Status	Aktueller Supportstatus des Geräts
Abdeckung – Enddatum	Datum, an dem der aktuelle Supportvertrag ausläuft
Enddatum der Garantie	Datum, an dem die Garantie für das Gerät ausläuft

Die Zeilen der Tabelle haben unterschiedliche Farben, die den Supportstatus für das Gerät angeben. So wird beispielsweise ein Gerät, bei dem das Enddatum der Garantie oder des Supportvertrags naht, orangefarben markiert. Ein Gerät, bei dem die Garantie bereits abgelaufen ist und für das kein aktueller Supportvertrag vorhanden ist, wird rot markiert.

Mit dem Suchfeld oben in jedem Bericht können Sie die Ergebnisse filtern. Geben Sie im Feld Suchen Text ein, um nur die Einträge mit dem entsprechenden Text anzuzeigen. Über die Dropdown-Liste „Organization“ (Organisation) können Sie die Ergebnisse auf eine bestimmte Organisation begrenzen.

Über das Spaltenauswahl-Symbol oben links im Bericht können Sie die angezeigten Informationen anpassen. Klicken Sie auf das Symbol, und wählen Sie dann mithilfe der angezeigten Kontrollkästchen die gewünschten Spalten für den Bericht aus.

Anzeigen des Wireless-Netzwerkberichts

Der **Wireless-Netzwerkbericht** enthält Details zum Wireless-Netzwerk, aufgeschlüsselt nach SSID, Nutzung des Wireless-Spektrums und Access Point. Außerdem liefert er eine Liste aller nicht autorisierten Access Points, die erkannt wurden. Mithilfe der Steuerelemente oben auf der Seite können Sie festlegen, dass Berichte für bestimmte Zeiträume (zwischen täglich und wöchentlich) generiert werden sollen.

Mehrere der Datensätze enthalten ein Diagramm, in dem die Inhalte der ausgewählten Zeile im zeitlichen Verlauf aufgeschlüsselt werden. Sie können auf die Beschriftungen in der Legende im Diagramm klicken, um die Anzeige des jeweiligen Datensatzes umzuschalten.

In der folgenden Tabelle werden die in den verschiedenen Abschnitten des Berichts enthaltenen Informationen erläutert:

Tabelle 20: Wireless-Netzwerkbericht

Feld	Beschreibung
Wireless Networks-Tabelle	
SSID	Der Name des Wireless-Netzwerks
Network (Netzwerk) (standardmäßig ausgeblendet)	Das Netzwerk, in dem sich die SSID befindet
Organization (Organisation) (standardmäßig ausgeblendet)	Die Organisation, zu der die SSID gehört
Gast	Information, ob die SSID für Gastzugriff konfiguriert ist
Security	Die für die SSID konfigurierte Sicherheitsmethode
Clientanzahl (Höchstwert)	Die Höchstanzahl von Clients, die während des Berichtszeitraums gleichzeitig der SSID zugeordnet waren
Clientanzahl (Durchschnitt)	Die durchschnittliche Anzahl von Clients, die während des Berichtszeitraums gleichzeitig der SSID zugeordnet waren
Datenverkehr (Höchstwert)	Das höchste aggregierte Datenverkehrsvolumen, das während des Berichtszeitraums über die SSID übertragen wurde
Datenverkehr (Durchschnitt)	Das durchschnittliche aggregierte Datenverkehrsvolumen, das während des Berichtszeitraums über die SSID übertragen wurde
Tabelle „Spektrumnutzung“	
Funkfrequenz	Das verwendete Frequenzband (2,4 GHz oder 5 GHz)
Vermittlung	Das Netzwerk, für das die angezeigten Spektrumnutzungsdaten gelten
Organisation	Die Organisation, für die die Spektrumnutzungsdaten gelten
Clientanzahl (Höchstwert)	Die Hochstanzahl von Clients, die während des Berichtszeitraums gleichzeitig das Frequenzband verwendet haben
Clientanzahl (Durchschnitt)	Die durchschnittliche Anzahl von Clients, die während des Berichtszeitraums gleichzeitig das Frequenzband verwendet haben
Datenverkehr (Höchstwert)	Das maximale aggregierte Datenverkehrsvolumen, das während des Berichtszeitraums über das Frequenzband übertragen wurde

Feld	Beschreibung
Datenverkehr (Durchschnitt)	Das durchschnittliche aggregierte Datenverkehrsvolumen, das während des Berichtszeitraums über das Frequenzband übertragen wurde
Wireless Access Points-Tabelle	
Access Point	Der Name des Access Points
Network (Netzwerk) (standardmäßig ausgeblendet)	Das Netzwerk, in dem sich der Access Point befindet
Organization (Organisation) (standardmäßig ausgeblendet)	Die Organisation, zu der der Access Point gehört
Modell	Das Modell des Access Points
Version	Die auf dem Access Point ausgeführte Firmware-Version
Clientanzahl (Höchstwert)	Die Höchstanzahl von Clients, die während des Berichtszeitraums gleichzeitig dem Access Point zugeordnet waren
Clientanzahl (Durchschnitt)	Die durchschnittliche Anzahl von Clients, die während des Berichtszeitraums gleichzeitig dem Access Point zugeordnet waren
Datenverkehr (Höchstwert)	Das höchste aggregierte Datenverkehrsvolumen, das während des Berichtszeitraums über den Access Point übertragen wurde
Datenverkehr (Durchschnitt)	Das durchschnittliche aggregierte Datenverkehrsvolumen, das während des Berichtszeitraums über den Access Point übertragen wurde
Rogue Access Points-Tabelle	
SSID	Die erkannte SSID
Network (Netzwerk) (standardmäßig ausgeblendet)	Das Netzwerk, in dem sich der für die Erkennung zuständige Access Point befindet
Organization (Organisation) (standardmäßig ausgeblendet)	Die Organisation, zu der der für die Erkennung zuständige Access Point gehört
MAC	Die MAC-Adresse des nicht autorisierten Access Points
Erstmals bemerkt	Der Zeitpunkt, zu dem der nicht autorisierte Access Point erstmals erkannt wurde
Letzte Erkennung	Der Zeitpunkt, zu dem der nicht autorisierte Access Point letztmals erkannt wurde
Gesamtzeit sichtbar	Der Gesamtzeitraum, während dessen der nicht autorisierte Access Point online war

Feld	Beschreibung
Kanal	Der von dem nicht autorisierten Access Point verwendete Wireless-Kanal
Durchschnittliche Signalstärke	Die vom für die Erkennung zuständigen Access Point verzeichnete durchschnittliche Signalstärke des nicht autorisierten Access Points
Erkannt von	Die Access Points, die den nicht autorisierten Access Point erkannt haben

Anzeigen des Berichts „Wireless-Client“

Der Bericht **Wireless-Client** enthält Details zu den Wireless-Clients im Netzwerk. Mithilfe der Steuerelemente oben auf der Seite können Sie festlegen, dass Berichte für bestimmte Zeiträume (zwischen täglich und wöchentlich) generiert werden sollen.

Alle Datensätze enthalten Diagramme, in denen die Inhalte der ausgewählten Zeile im zeitlichen Verlauf aufgeschlüsselt werden. Sie können auf die Beschriftungen in der Legende im Diagramm klicken, um die Anzeige des jeweiligen Datensatzes umzuschalten.

In der folgenden Tabelle werden die enthaltenen Informationen erläutert.

Tabelle 21: Tabelle zu Wireless-Clients

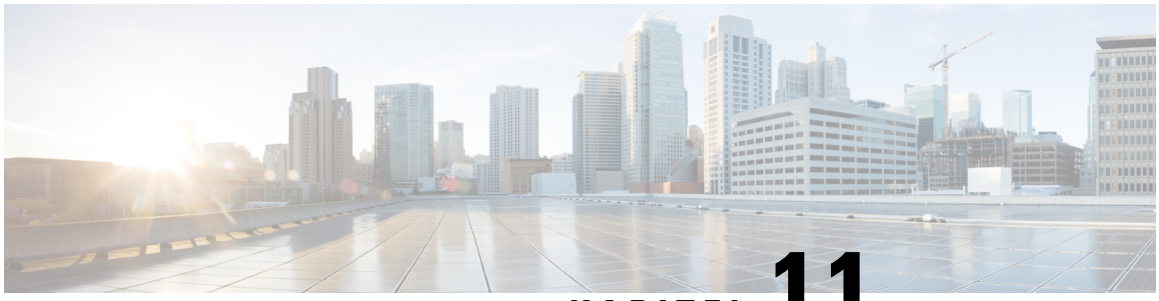
Wireless Clients-Tabelle	
MAC	Die MAC-Adresse des Clients
Hostname	Der Hostname des Clients, sofern verfügbar
Organisation	Die Organisation, in der der Client zuletzt vorhanden war
Vermittlung	Das Netzwerk, in dem der Client zuletzt vorhanden war
SSID	Die SSID, der der Client zuletzt zugeordnet war
802.11-Typ	Die vom Client verwendete 802.11-Variante
Häufigkeit	Das vom Client verwendete 802.11-Frequenzband
Max. Datenrate	Die vom Client verwendete maximale Datenrate
Hochladen	Das vom Client hochgeladene Datenvolumen
Herunterladen	Das vom Client heruntergeladene Datenvolumen
Gesamt-	Das insgesamt vom Client gesendete und empfangene Datenvolumen
Erstmals bemerkt	Der Zeitpunkt, zu dem der Client erstmals erkannt wurde
Letzte Erkennung	Der Zeitpunkt, zu dem der Client letztmals erkannt wurde

Wireless Clients-Tabelle	
Zeit online	Der Gesamtzeitraum, während dessen der Client online war
% Online-Zeit	Der prozentuale Anteil der Online-Zeit am Gesamtzeitraum, während dessen der Client im Netzwerk als erkannt geführt wurde

Tabelle 22: Tabelle „Wireless Guests“ (Wireless-Gäste)

Tabelle „Wireless Guests“ (Wireless-Gäste)	
MAC	Die MAC-Adresse des Clients
Hostname	Der Hostname des Clients, sofern verfügbar
Benutzername	Der Benutzername, den der Client im Gastportal eingetragen hat
Organisation	Die Organisation, in der der Client zuletzt vorhanden war
Vermittlung	Das Netzwerk, in dem der Client zuletzt vorhanden war
SSID	Die SSID, der der Client zuletzt zugeordnet war
802.11-Typ	Die vom Client verwendete 802.11-Variante
Häufigkeit	Das vom Client verwendete 802.11-Frequenzband
Max. Datenrate	Die vom Client verwendete maximale Datenrate
Hochladen	Das vom Client hochgeladene Datenvolumen
Herunterladen	Das vom Client heruntergeladene Datenvolumen
Gesamt-	Das insgesamt vom Client gesendete und empfangene Datenvolumen
Erstmals bemerkt	Der Zeitpunkt, zu dem der Client erstmals erkannt wurde
Letzte Erkennung	Der Zeitpunkt, zu dem der Client letztmals erkannt wurde
Zeit online	Der Gesamtzeitraum, während dessen der Client online war
% Online-Zeit	Der prozentuale Anteil der Online-Zeit am Gesamtzeitraum, während dessen der Client im Netzwerk als erkannt geführt wurde

Hinweis Die Zeitstempel **First Seen** (Zuerst erkannt) und **Last Seen** (Zuletzt erkannt) sind die vom Access Point angegebenen Zeitpunkte. Es wird empfohlen, für alle Netzwerkgeräte die Taktsynchronisierung mithilfe eines Mechanismus wie dem Network Time Protocol (NTP) zu implementieren.



KAPITEL 11

Verwaltung

Dieses Kapitel enthält folgende Abschnitte:

Über die Verwaltung

Mit der Option **Administration** (Verwaltung) in Cisco Business Dashboard können Sie den Betrieb der Anwendung auf Organisationsebene steuern. Diese Option ist in die folgenden Seiten unterteilt:

- **Organizations** (Organisationen): Erstellen und Verwalten von Organisationen in Cisco Business Dashboard
- **Device Groups** (Gerätegruppen): Zuweisen von Netzwerkgeräten zu Gruppen für eine einfachere Verwaltung
- **Device Credentials** (Anmeldeinformationen des Geräts): Eingeben der Anmeldeinformationen für den Zugriff auf Netzwerkgeräte
- **Users** (Benutzer): Definieren des Benutzerzugriffs auf Cisco Business Dashboard
- **Notification Defaults** (Benachrichtigungs-Standardeinstellungen): Ändern des Standardbenachrichtigungsverhaltens für Cisco Business Dashboard.
- **Login Attempts** (Anmeldeversuche): Protokoll des gesamten Benutzerzugriffs auf Cisco Business Dashboard
- **Report Settings** (Berichtseinstellungen): Ändern der Einstellungen, die steuern, wie Berichte generiert werden

Nicht alle Seiten sind für alle Rollen sichtbar. Bediener können keine Benutzereinstellungen verwalten. Die Seiten **Notification Defaults** (Benachrichtigungs-Standardeinstellungen) und **Report Settings** (Berichtseinstellungen) sind nur für Administratoren sichtbar.

Verwalten von Organisationen

Organisationen werden in Cisco Business Dashboard verwendet, um Netzwerke, Benutzer und Geräte in Gruppen aufzuteilen, die in der Regel separat verwaltet werden. Jedes Netzwerk oder Gerät gehört zu einer Organisation, und jeder Benutzer kann eine oder mehrere Organisationen verwalten. Eine Organisation kann für einen Kunden, eine Abteilung oder eine Region stehen – je nachdem, was für Ihr Unternehmen am besten passt. In jedem Fall ermöglicht die Verwendung von Organisationen eine detailliertere Kontrolle darüber, wer die verschiedenen Teile des Netzwerks anzeigen und verwalten kann. Eine einzelne Organisation wird standardmäßig erstellt, wenn Cisco Business Dashboard installiert wird.

Erstellen einer neuen Organisation

Gehen Sie wie folgt vor, um eine neue Organisation zu erstellen:

1. Navigieren Sie zu **Administration** > **Organizations** (Verwaltung > Organisationen).
2. Klicken Sie oben in der Tabelle auf das Pluszeichen (✚).
3. Geben Sie einen Namen für die Organisation an, und geben Sie die erforderlichen Details ein.
4. Geben Sie einen Namen für eine neue Gerätegruppe ein, die als Standardgruppe für neu erkannte Geräte verwendet werden soll. Die neue Gerätegruppe wird zusammen mit der Organisation erstellt.
5. Klicken Sie auf **Save** (Speichern).
6. Wiederholen Sie die oben genannten Schritte für jede Organisation, die Sie erstellen möchten.

Ändern einer vorhandenen Organisation

Gehen Sie wie folgt vor, um eine vorhandene Organisation zu ändern:

1. Navigieren Sie zu **Administration** > **Organizations** (Verwaltung > Organisationen).
2. Aktivieren Sie die Optionsschaltfläche für die zu ändernde Organisation, und klicken Sie dann auf das Symbol **Edit** (Bearbeiten).
3. Nehmen Sie die erforderlichen Änderungen vor, und klicken Sie dann auf **Save** (Speichern).

Löschen einer Organisation

Gehen Sie wie folgt vor, um eine Organisation zu löschen:

1. Navigieren Sie zu **Administration** > **Organizations** (Verwaltung > Organisationen).
2. Aktivieren Sie die Optionsschaltfläche für die zu ändernde Organisation, und klicken Sie dann auf das Symbol **Delete** (Löschen).

Verwalten von Überwachungsprofilen für eine Organisation

Mit Überwachungsprofilen können Sie steuern, wie die Überwachung von Netzwerkgeräten in der gesamten Organisation durchgeführt wird. Die auf Organisationsebene ausgewählten Profile werden in allen Netzwerken der Organisation angewendet.

Gehen Sie wie folgt vor, um die Überwachungsprofile für eine Organisation zu ändern:

1. Navigieren Sie zu **Administration** > **Organizations** (Verwaltung > Organisationen).
2. Klicken Sie auf den Namen der zu ändernden Organisation und wählen Sie die Registerkarte **Monitoring Profiles** (Überwachungsprofile) aus.
3. Verwenden Sie die Dropdown-Listen, um das entsprechende Überwachungsprofil auszuwählen, das auf Geräte des entsprechenden Typs angewendet werden soll. Weitere Informationen zum Erstellen von Überwachungsprofilen finden Sie unter Verwalten von Überwachungsprofilen, auf Seite 78.

   Sie können auch festlegen, dass das auf Systemebene definierte Verhalten gelten soll. Aktivieren Sie dazu das Kontrollkästchen **Inherit from Monitoring Defaults** (Übernehmen von Überwachungs-Standardeinstellungen) für einzelne Gerätetypen oder die gesamte Organisation.
4. Klicken Sie auf **Save** (Speichern).

Hinweis Unter Verwalten von Überwachungsprofilen finden Sie weitere Informationen zu den möglichen Überwachungsarten und deren Verwaltung. Weitere Informationen zum Ändern von Überwachungsprofilen auf Systemebene finden Sie unter Ändern von Überwachungsstandards, auf Seite 78.

Verwalten von Benutzern, die einer Organisation zugeordnet sind

Benutzer mit einer Rolle als **Organisationsadministrator** oder niedriger müssen explizit einer Organisation zugeordnet sein, um Geräte in dieser Organisation anzeigen oder verwalten zu können.

Gehen Sie wie folgt vor, um einen Benutzer der Organisation zuzuordnen:

1. Navigieren Sie zu **Administration** > **Organizations** (Verwaltung > Organisationen).
2. Klicken Sie auf den Namen der zu ändernden Organisation, und wählen Sie die Registerkarte **Users** (Benutzer) aus.
3. Klicken Sie auf das Plussymbol (**+**). Wählen Sie den Benutzer aus der Dropdown-Liste aus.

Hinweis Benutzer auf **Administratorebene** sind implizit allen Organisationen zugeordnet und werden nicht in der Dropdown-Liste angezeigt.

Gehen Sie wie folgt vor, um einen Benutzer aus der Organisation zu entfernen:

1. Navigieren Sie zu **Administration** > **Organizations** (Verwaltung > Organisationen).
2. Klicken Sie auf den Namen der zu ändernden Organisation, und wählen Sie die Registerkarte **Users** (Benutzer) aus.
3. Klicken Sie in der Tabelle neben dem Benutzer auf das Symbol **Delete** (Löschen).

Verwalten von Netzwerken, die einer Organisation zugeordnet sind

Jedes Netzwerk in Cisco Business Dashboard gehört zu einer einzigen Organisation. Sie können eine Liste der einer Organisation zugeordneten Netzwerke anzeigen, indem Sie auf der Seite **Organization Detail** (Organisationsdetails) die Registerkarte **Networks** (Netzwerke) auswählen.

Die Zuordnung eines Netzwerks zu einer Organisation erfolgt, wenn das Netzwerk zum ersten Mal erstellt wird. Gehen Sie wie folgt vor, um die Organisation zu ändern, der ein Netzwerk zugeordnet ist:

1. Navigieren Sie zu **Network** (Netzwerk), und wählen Sie das Netzwerk aus, das Sie ändern möchten. Klicken Sie auf **More** (Mehr), um den Bereich **Network Detail** (Netzwerkdetails) anzuzeigen.
2. Klicken Sie neben dem Netzwerknamen auf das Symbol **Edit** (Bearbeiten).
3. Wählen Sie die neue Organisation aus der Dropdown-Liste aus.
4. Klicken Sie auf **OK**.

Sie können in dieser Ansicht neue Netzwerke für eine Organisation erstellen. Klicken Sie auf das Pluszeichen (✚), um ein neues Netzwerk zu erstellen und im daraufhin angezeigten Formular die entsprechenden Werte anzugeben.

Verwalten von Gerätegruppen

Cisco Business Dashboard nutzt zum Ausführen der meisten Konfigurationsaufgaben Gerätegruppen. Mehrere Netzwerkgeräte werden in Gruppen zusammengefasst und können dann mit einer einzigen Aktion zusammen konfiguriert werden.

Eine Gerätegruppe kann Geräte verschiedener Art enthalten. Wenn eine Konfiguration auf eine Gerätegruppe angewendet wird, erfolgt dies nur für die Geräte aus der Gruppe, die die jeweilige Funktion unterstützen. Wenn beispielsweise eine Gerätegruppe Wireless Access Points, Switches und Router enthält, wird die Konfiguration für eine neue Wireless-SSID auf die Wireless Access Points angewendet, jedoch nicht auf die Switches. Auf die Router wird sie nur angewendet, wenn es sich um Wireless-Router handelt.

Gerätegruppen können Geräte aus mehreren Netzwerken umfassen, wobei jedoch alle Geräte derselben Organisation angehören müssen. Eine Gerätegruppe kann als Standardgruppe für eine Organisation oder ein Netzwerk festgelegt werden. Alle neu erkannten Geräte für dieses Netzwerk oder diese Organisation werden dann der Standardgerätegruppe hinzugefügt.

Erstellen einer neuen Gerätegruppe

Gehen Sie wie folgt vor, um eine neue Gerätegruppe zu erstellen:

1. Navigieren Sie zu **Administration** > **Device Groups** (Verwaltung > Gerätegruppen).
2. Klicken Sie auf das Plussymbol (✚), um eine neue Gruppe zu erstellen.
3. Geben Sie eine Organisation, einen Namen und eine Beschreibung für die Gruppe ein. Klicken Sie auf **Save** (Speichern).
4. Optional können Sie der Gerätegruppe Geräte hinzufügen, indem Sie auf das Pluszeichen (✚) klicken und das Suchfeld verwenden, um Geräte auszuwählen, die der Gruppe hinzugefügt werden sollen. Sie können Geräte einzeln oder pro Netzwerk hinzufügen. Wenn das ausgewählte Gerät bereits Mitglied einer anderen Gruppe ist, wird es aus dieser Gruppe entfernt. Jedes Gerät kann nur zu einer einzigen Gruppe gehören.

Bearbeiten einer Gerätegruppe

Gehen Sie wie folgt vor, um eine vorhandene Gerätegruppe zu ändern:

1. Navigieren Sie zu **Administration** > **Device Groups** (Verwaltung > Gerätegruppen).
2. Aktivieren Sie das Optionsfeld neben der zu ändernden Gruppe, und klicken Sie dann auf das Symbol **Edit** (Bearbeiten).
3. Ändern Sie ggf. den Namen und die Beschreibung. Klicken Sie auf **Save** (Speichern).
4. Fügen Sie je nach Bedarf Geräte der Gruppe hinzu, oder entfernen Sie Geräte aus der Gruppe. Um ein Gerät zu entfernen, das der Gruppe zuvor hinzugefügt wurde, klicken Sie neben dem Gerät auf das **Papierkorbsymbol**. Das Gerät wird in die **Standardgruppe** für das jeweilige Netzwerk oder die Organisation verschoben.

Hinweis Sie können keine Geräte aus der Gruppe **Standard** löschen. Um ein Gerät aus der Gruppe **Standard** zu entfernen, müssen Sie es einer neuen Gruppe hinzufügen.

Löschen einer Gerätegruppe

Gehen Sie wie folgt vor, um eine Gerätegruppe zu löschen:

1. Navigieren Sie zu **Administration** > **Device Groups** (Verwaltung > Gerätegruppen).
2. Klicken Sie auf die Optionsschaltfläche neben der zu entfernenden Gerätegruppe, und klicken Sie dann auf das Symbol **Delete** (Löschen).

Hinweis Die **Standardgruppe** kann nicht gelöscht werden.

Verwalten der Anmeldeinformationen für Geräte

Damit Cisco Business Dashboard das Netzwerk vollständig erkennen und verwalten kann, müssen Anmeldeinformationen zur Authentifizierung gegenüber den Netzwerkgeräten zur Verfügung stehen. Bei der ersten Erkennung eines Geräts verwendet Probe zum Versuch der Authentifizierung gegenüber dem Gerät den Standardbenutzernamen: `cisco`, Kennwort: `cisco`, SNMP-Community: `public`. Wenn dieser Versuch fehlschlägt, wird eine Benachrichtigung generiert, und der Benutzer muss gültige Anmeldeinformationen bereitstellen. Gehen Sie wie folgt vor, um die gültigen Anmeldeinformationen anzugeben:

1. Navigieren Sie zu **Administration** > **Device Credentials** (Verwaltung > Geräteanmeldeinformation). In der ersten Tabelle auf dieser Seite sind alle erkannten Geräte aufgeführt, die Anmeldeinformationen erfordern.
2. Geben Sie in den Feldern **Username/Password** (Benutzername/Kennwort), **SNMP Community** und **SNMPv3** gültige Anmeldeinformationen ein (füllen Sie je nach Bedarf alle oder nur einzelne Felder aus). Durch Klicken auf das Plussymbol (✚) neben dem jeweiligen Feld können Sie für jeden Anmeldeinformationstyp bis zu drei Angaben machen. Kennwörter müssen in Klartext eingegeben werden.

Hinweis Für die **SNMPv3**-Anmeldeinformationen werden optional die Authentifizierungsprotokolle MD5 und SHA unterstützt. Als Verschlüsselungsprotokolle werden DES und AES unterstützt.

3. Klicken Sie auf **Apply** (Anwenden). Die Anmeldeinformationen werden von den Probes für alle Geräte getestet, die diese Art von Anmeldeinformationen erfordern. Wenn die Anmeldeinformationen gültig sind, werden sie zur späteren Verwendung für das Gerät gespeichert.
4. Wiederholen Sie bei Bedarf die Schritte 2 und 3, bis für jedes Gerät die gültigen Anmeldeinformationen gespeichert sind.

Gehen Sie wie folgt vor, um Anmeldeinformationen einzeln für ein bestimmtes Gerät anzugeben:

1. Klicken Sie in der Tabelle der erkannten Geräte neben dem Gerät auf das Symbol **Edit** (Bearbeiten). Es wird ein Popup-Fenster angezeigt, in dem Sie zum Eingeben von Anmeldeinformationen aufgefordert werden, die zum ausgewählten Anmeldeinformationstyp passen.
2. Geben Sie in den entsprechenden Feldern einen Benutzernamen und ein Kennwort oder SNMP-Anmeldeinformationen ein.
3. Klicken Sie auf **Apply** (Anwenden). Um das Fenster zu schließen, ohne die Änderungen anzuwenden, klicken Sie in der oberen rechten Ecke des Popup-Fensters auf das ✖.

Unter dem Abschnitt **Neue Anmeldeinformationen hinzufügen** finden Sie eine Tabelle mit den Identitäten der Geräte, für die Network Probe gültige Anmeldeinformationen gespeichert hat. In dieser Tabelle ist auch das Datum angegeben, an dem die jeweiligen Anmeldeinformationen zuletzt genutzt wurden. Um die gespeicherten Anmeldeinformationen für ein Gerät anzuzeigen, können Sie neben dem Gerät auf das Symbol **Show Password** (Kennwort anzeigen) klicken. Um die Anmeldeinformationen wieder auszublenden, klicken Sie auf das Symbol **Hide Password** (Kennwort verbergen). Mit der Schaltfläche oben in der Tabelle können Sie auch die Anmeldeinformationen für alle Geräte auf einmal ein- und ausblenden. Sie können Anmeldeinformationen löschen, wenn sie nicht mehr benötigt werden. Gehen Sie wie folgt vor, um gespeicherte Anmeldeinformationen zu löschen:

1. Navigieren Sie zu **Administration** > **Device Credentials** (Verwaltung > Geräteanmeldeinformation).
2. Aktivieren Sie in der Tabelle **Saved Credentials** (Gespeicherte Anmeldeinformationen) die Kontrollkästchen neben den zu löschenden Anmeldeinformationen. Wenn alle Anmeldeinformationen ausgewählt werden sollen, können Sie auch das Kontrollkästchen oben in der Tabelle aktivieren.
3. Klicken Sie auf **Delete Selected Credentials** (Ausgewählte Anmeldeinformationen löschen).

Um die Anmeldeinformationen für ein einzelnes Gerät zu löschen, können Sie auch neben dem Gerät auf das Symbol **Delete** (Löschen) klicken.

Benutzer verwalten

Auf der Seite **User Management** (Benutzerverwaltung) können Sie steuern, welche Benutzer auf Cisco Business Dashboard zugreifen dürfen. Außerdem können Sie hier die Einstellungen anpassen, die regeln, wie diese Benutzer mit dem Dashboard interagieren.

Cisco Business Dashboard unterstützt vier Benutzertypen:

- **Administrator**: Administratoren haben vollen Zugriff auf die Funktionen des Dashboards, einschließlich der Möglichkeit zur Systemwartung.
- **Organization Administrator** (Organisationsadministrator): Organisationsadministratoren sind auf die Verwaltung einer oder mehreren Organisationen beschränkt und können keine Änderungen am System vornehmen.
- **Operator** (Bediener): Bediener haben ähnliche Berechtigungen wie Organisationsadministratoren, können jedoch keine Benutzer verwalten.
- **Readonly** (Schreibgeschützt): Diese Benutzer können nur die Netzwerkinformationen anzeigen. Sie können keinerlei Änderungen vornehmen.

Cisco Business Dashboard ermöglicht die Authentifizierung von Benutzern anhand der lokalen Benutzerdatenbank. Ab Version 2.2.1 können Benutzer auch anhand einer Microsoft Azure Active Directory-Instanz authentifiziert werden.

Bei der Erstinstallation von Cisco Business Dashboard wird ein standardmäßiger **Administrator** in der lokalen Benutzerdatenbank mit `cisco` als Benutzername und Kennwort erstellt.

Hinweis Die Benutzereinstellungen können nur von **Administratoren** und **Organisationsadministratoren** verwaltet werden.

Hinzufügen eines neuen Benutzers zur lokalen Benutzerdatenbank

Gehen Sie wie folgt vor, um einen neuen Benutzer hinzuzufügen:

1. Navigieren Sie zu **Administration** > **Users** (Verwaltung > Benutzer), und wählen Sie die Registerkarte **Users** (Benutzer) aus.
2. Klicken Sie auf das Plussymbol (✚), um einen neuen Benutzer zu erstellen.
3. Geben Sie in den dafür vorgesehenen Feldern einen Benutzernamen, einen Anzeigenamen, eine E-Mail-Adresse und ein Kennwort ein, und wählen Sie einen Benutzertyp aus. Sie können auch Kontaktdaten für den Benutzer angeben.
4. Klicken Sie auf **Save** (Speichern).

Wenn der Benutzer kein **Administrator** ist, müssen Sie den Benutzer einer oder mehreren Organisationen hinzufügen. Wählen Sie dazu die Registerkarte **Organizations** (Organisationen) aus, und klicken Sie auf das Pluszeichen (✚). Wählen Sie die gewünschte Organisation aus der Dropdown-Liste aus.

Ändern eines Benutzers

Gehen Sie wie folgt vor, um einen vorhandenen Benutzer zu ändern:

1. Navigieren Sie zu **Administration** > **Users** (Verwaltung > Benutzer), und wählen Sie die Registerkarte **Users** (Benutzer) aus.
2. Aktivieren Sie das Optionsfeld neben dem zu ändernden Benutzer, und klicken Sie dann auf das Symbol **Edit** (Bearbeiten).
3. Nehmen Sie die erforderlichen Änderungen vor.

4. Klicken Sie auf **Save** (Speichern).

Um den Benutzer einer neuen Organisation hinzuzufügen, wählen Sie die Registerkarte **Organizations** (Organisationen) aus, und klicken Sie auf das Pluszeichen (✚). Wählen Sie die gewünschte Organisation aus der Dropdown-Liste aus. Um ihn aus einer Organisation zu entfernen, klicken Sie in der Tabelle neben der Organisation auf das Symbol **Delete** (Löschen).

Löschen eines Benutzers

Gehen Sie wie folgt vor, um einen vorhandenen Benutzer zu löschen:

1. Navigieren Sie zu **Administration** > **Users** (Verwaltung > Benutzer), und wählen Sie die Registerkarte **Users** (Benutzer) aus.
2. Aktivieren Sie das Optionsfeld neben dem zu löschenden Benutzer, und klicken Sie dann oben in der Tabelle auf das Symbol **Delete** (Löschen).

Ändern der Kennwortkomplexität

Gehen Sie wie folgt vor, um Anforderungen an die Kennwortkomplexität festzulegen oder diese zu ändern:

1. Navigieren Sie zu **Administration** > **Users** (Verwaltung > Benutzer), und wählen Sie die Registerkarte **User Settings** (Benutzereinstellungen) aus.
2. Wählen Sie die Registerkarte **Local** (Lokal) unter **Authentication Source** (Authentifizierungsquelle). Andern Sie die Einstellungen unter **User Password Complexity** (Kennwortkomplexität für Benutzer) je nach Bedarf und klicken Sie dann auf **Save** (Speichern).

Hinweis Bei der Authentifizierung anhand einer Azure Active Directory-Instanz wird die Kennwortkomplexität in Active Directory verwaltet.

Aktivieren der Active Directory-Authentifizierung

Cisco Business Dashboard unterstützt die Benutzerauthentifizierung anhand einer Microsoft Azure Active Directory-Instanz. Active Directory-Benutzern werden Rollen und Organisationslisten auf der Basis der Active Directory-Gruppen zugewiesen, in denen der Benutzer Mitglied ist.

Gehen Sie wie folgt vor, um Azure Active Directory als Authentifizierungsquelle zu aktivieren:

1. Erstellen Sie in **Azure Active Directory** eine neue App-Registrierung für Cisco Business Dashboard, weisen Sie delegierte Berechtigungen für User.Read und Domain.Read.All über die **Microsoft Graph-API** zu und erstellen Sie einen **geheimen Client-Schlüssel**. Notieren Sie sich die Anwendungs-ID (Client-ID), den geheimen Client-Schlüssel und die Verzeichnis-ID (Tenant-ID).
2. Öffnen Sie die Cisco Business Dashboard-Web-GUI und navigieren Sie zu **Administration** > **Users** (Verwaltung > Benutzer). Wählen Sie die Registerkarte **User Settings** (Benutzereinstellungen) und dann die Registerkarte **Azure AD** unter **Authentication Source**(Authentifizierungsquelle) aus.
3. Aktivieren Sie das Kontrollkästchen **Enable** (Aktivieren).
4. Geben Sie die in Schritt 1 erfasste **Client-ID**, den **geheimen Client-Schlüssel** und die **Tenant-ID** in das entsprechende Feld ein.

5. Geben Sie optional eine durch Kommas getrennte Liste von Domänen an, die auf das Dashboard zugreifen dürfen. Klicken Sie auf **Save** (Speichern).
6. Klicken Sie auf das Pluszeichen **(+)** unter der Kopfzeile **User Group Mappings** (Benutzergruppenzuordnungen), um eine neue Gruppenzuordnung zu erstellen. Geben Sie die **Objekt-ID** für die Active Directory-Gruppe in das dafür vorgesehene Feld ein und wählen Sie dann eine Rollen- und Organisationsliste aus, die auf Benutzer in dieser Gruppe angewendet werden soll. Wiederholen Sie diesen Schritt für alle Gruppen, die zugeordnet werden müssen.
7. Notieren Sie sich die **Redirect URL** (Weiterleitungs-URL), die unter dem Kontrollkästchen **Enable** (Aktivieren) angezeigt wird. Kehren Sie zu Azure Active Directory zurück und fügen Sie die URL zur Liste der Weiterleitungs-URIs für die App-Registrierung hinzu.

Hinweis Der in der Weiterleitungs-URL angezeigte Host und Port sollten über die Webbrowser der Benutzer erreichbar sein, die auf das Dashboard zugreifen. Wenn die aktuell angezeigten Werte nicht erreichbar sind, aktualisieren Sie die entsprechenden Felder auf der Registerkarte **System Variables** (Systemvariablen) auf der Seite **System** > **Plattform Settings**(Plattformeinstellungen).

Verwalten der lokalen Authentifizierung

Die Authentifizierung anhand der lokalen Benutzerdatenbank ist standardmäßig aktiviert. Gehen Sie wie folgt vor, um die lokale Authentifizierung zu deaktivieren:

1. Stellen Sie sicher, dass die Authentifizierung anhand Azure Active Directory wie oben beschrieben eingerichtet wurde. Melden Sie sich mit einem durch Active Directory authentifizierten Administratorkonto am Dashboard an.
2. Navigieren Sie zu **Administration** > **Users**(Verwaltung> Benutzer) und wählen Sie die Registerkarte **User Settings** (Benutzereinstellungen) aus. Wählen Sie unter **Authentication Source** (Authentifizierungsquelle) die Registerkarte **Local** (Lokal) aus.
3. Deaktivieren Sie das Kontrollkästchen **Enable** (Aktivieren) und klicken Sie auf **Save** (Speichern).

Gehen Sie wie folgt vor, um die lokale Authentifizierung wieder zu aktivieren:

1. Navigieren Sie zu **Administration** > **Users**(Verwaltung > Benutzer) und wählen Sie die Registerkarte **User Settings** (Benutzereinstellungen) aus. Wählen Sie unter **Authentication Source** (Authentifizierungsquelle) die Registerkarte **Local** (Lokal) aus.
2. Aktivieren Sie das Kontrollkästchen **Enable** (Aktivieren) und klicken Sie auf **Save** (Speichern).

Wiederherstellen des Zugriffs, wenn der gesamte Administratorzugriff verloren gegangen ist

Gehen Sie wie folgt vor, wenn der Administratorzugriff auf die Cisco Business Dashboard-Anwendung verloren geht:

1. Melden Sie sich über die Konsole oder über SSH beim Host-Betriebssystem an.
2. Geben Sie den Befehl **cisco-business-dashboard restorepassword** ein.

Nach Eingabe des Befehls wird die lokale Benutzerauthentifizierung aktiviert und der Standardadministrator mit dem Benutzernamen **cisco** und dem Kennwort **cisco** wiederhergestellt.

Ändern von Sitzungstimeouts

Gehen Sie wie folgt vor, um den Leerlauftimeout und den absoluten Timeout für Benutzersitzungen zu ändern:

1. Navigieren Sie zu **Administration** > **Users** (Verwaltung > Benutzer), und wählen Sie die Registerkarte **User Settings** (Benutzereinstellungen) aus.
2. Ändern Sie die Parameter für **User Session** (Benutzersitzung) nach Bedarf, und klicken Sie dann auf **Save** (Speichern). Wenn Sie den Mauszeiger über den Hilfesymbolen platzieren, werden die zulässigen Bereiche für die verschiedenen Parameter angezeigt.

Ändern von Überwachungsstandards

Mit **Überwachungsprofilen** können Sie steuern, wie die Überwachung von Geräten im Netzwerk durchgeführt wird. Überwachungsprofile können auf Organisationsebene oder auf Systemebene angewendet werden. Bei Organisationen, die die auf Systemebene festgelegten Überwachungsprofile übernehmen sollen, wird das Verhalten über die Seite **Monitoring Defaults** (Überwachungs-Standardeinstellungen) gesteuert.

Gehen Sie wie folgt vor, um die im System angewendeten **Überwachungsprofile** zu ändern:

1. Navigieren Sie zu **Administration** > **Monitoring Defaults** (Verwaltung > Überwachungs-Standardeinstellungen).
2. Verwenden Sie die Dropdown-Listen, um das entsprechende Überwachungsprofil auszuwählen, das auf Geräte des entsprechenden Typs angewendet werden soll. Weitere Informationen zum Erstellen von Überwachungsprofilen finden Sie unter „Verwalten von Überwachungsprofilen“.
3. Klicken Sie auf **Save** (Speichern).

Unter Verwalten von Überwachungsprofilen finden Sie weitere Informationen zu den möglichen Überwachungsarten und deren Verwaltung. Weitere Informationen zum Ändern der Überwachungseinstellungen auf Organisationsebene finden Sie unter Verwalten von Organisationen, auf Seite 70.

Verwalten von Überwachungsprofilen

Überwachungsprofile steuern die Daten, die von Geräten erfasst werden, und die Benachrichtigungen, die generiert werden. Profile können auf verschiedene Gerätetypen innerhalb einer Organisation oder im gesamten System angewendet werden. Innerhalb eines Profils werden zwei Arten von Monitoren unterstützt: **Benachrichtigungsmonitore** und **Berichtsmonitore**.

Mit Benachrichtigungsmonitoren werden Benachrichtigungen und Warnungen generiert, in der Regel aufgrund einer Änderung des Gerätezustands oder eines Parameters, der einen Grenzwert überschreitet. Benachrichtigungen haben unterschiedliche Schweregrade (Information, Warnung und Alert) und können Popup-Meldungen auf der Benutzeroberfläche und E-Mail-Benachrichtigungen generieren. Aktive Benachrichtigungen werden auch im **Benachrichtigungscenter** angezeigt und in den Ansichten mit Geräteinformationen angezeigt. Änderungen an Benachrichtigungen werden ebenfalls im **Ereignisprotokoll** aufgezeichnet.

Hinweis Wenn Sie E-Mail-Benachrichtigungen festlegen, achten Sie darauf, dass die E-Mail-Einstellungen richtig konfiguriert sind. Nähere Informationen finden Sie unter Verwalten der E-Mail-Einstellungen.

Berichtsmonitore erfassen die Daten, die für Wireless-Berichte und Datenverkehrsdiagramme im Überwachungs-Dashboard verwendet werden.

Es können mehrere Überwachungsprofile erstellt und verschiedenen Gerätetypen können unterschiedliche Profile auf System- oder Organisationsebene zugewiesen werden. Weitere Informationen zum Zuweisen von Überwachungsprofilen zu Geräten finden Sie unter Verwalten von Organisationen, auf Seite 70 und Ändern von Überwachungsstandards, auf Seite 78.

Hinzufügen von neuen Überwachungsprofilen

Gehen Sie wie folgt vor, um ein neues Überwachungsprofil hinzuzufügen:

1. Navigieren Sie zu **Administration** > **Monitoring Defaults**(Verwaltung > Überwachungs-Standardeinstellungen).
2. Klicken Sie auf das Plussymbol **(+)**, um ein neues Profil zu erstellen.
3. Geben Sie einen Namen für das Profil und eine Organisation an, der das Profil zugeordnet werden soll. Sie können hier auch „All Organizations“ (Alle Organisationen) angeben, sodass das Profil mit jeder Organisation oder als Standard auf Systemebene verwendet werden kann.
4. Sie können auch eine Beschreibung für das Profil und eine durch Kommas getrennte Liste mit E-Mail-Adressen angeben, um Benachrichtigungen zu erhalten.
5. Klicken Sie auf **Save** (Speichern).
6. Der Bildschirm wird aktualisiert, um die verschiedenen Benachrichtigungs- und Berichtsmonitore anzuzeigen. Sie können einzelne Monitore mithilfe der bereitgestellten Steuerelemente aktivieren und deaktivieren.
7. Die Benachrichtigungsmonitore haben zusätzliche Einstellungen, die durch Klicken auf das Symbol zum **Bearbeiten** für den Monitor geändert werden können. Die Einstellungen variieren je nach Monitor, umfassen jedoch die Benachrichtigungstypen, die generiert werden sollen, den Schweregrad der Benachrichtigung und die Grenzwerte, die die Benachrichtigung auslösen sollen.

Kopieren eines vorhandenen Überwachungsprofils

Gehen Sie wie folgt vor, um ein vorhandenes Überwachungsprofil zu kopieren:

1. Navigieren Sie zu **Administration > Monitoring Defaults** (Verwaltung > Überwachungs-Standardeinstellungen).
2. Aktivieren Sie das Kontrollkästchen neben dem zu kopierenden Profil und klicken Sie auf das Symbol zum **Speichern unter**.
3. Aktualisieren Sie bei Bedarf den Profilnamen, die Beschreibung, die Organisation und die E-Mail-Adresse(n) und klicken Sie dann auf **Save** (Speichern).
4. Nehmen Sie bei Bedarf Änderungen an den Benachrichtigungs- und Berichtsmonitoren vor. Sie können die Monitoreinstellungen auf die Standardeinstellungen zurücksetzen, indem Sie auf die Schaltfläche **Reset to defaults** (Auf Standardeinstellungen zurücksetzen) klicken.

Ändern eines Überwachungsprofils

Gehen Sie wie folgt vor, um ein vorhandenes Überwachungsprofil zu ändern:

1. Navigieren Sie zu **Administration > Monitoring Defaults** (Verwaltung > Überwachungs-Standardeinstellungen).
2. Aktivieren Sie das Kontrollkästchen neben dem zu kopierenden Profil und klicken Sie auf das Symbol zum **Speichern**.
3. Aktualisieren Sie bei Bedarf die Profileinstellungen und die E-Mail-Adresse(n) und klicken Sie dann auf **Save** (Speichern).
4. Nehmen Sie bei Bedarf Änderungen an den Benachrichtigungs- und Berichtsmonitoren vor. Sie können die Monitoreinstellungen auf die Standardeinstellungen zurücksetzen, indem Sie auf die Schaltfläche **Reset to defaults** (Auf Standardeinstellungen zurücksetzen) klicken.

Entfernen eines Überwachungsprofils

Gehen Sie wie folgt vor, um ein vorhandenes Überwachungsprofil zu entfernen:

1. Navigieren Sie zu **Administration > Monitoring Defaults** (Verwaltung > Überwachungs-Standardeinstellungen).
2. Aktivieren Sie das Kontrollkästchen neben dem zu kopierenden Profil und klicken Sie auf das Symbol zum **Entfernen**.

Hinweis Wenn das Profil als Überwachungsprofil auf Organisationsebene verwendet wird, werden die entsprechende Organisation und der Gerätetyp aktualisiert, um die Konfiguration auf Systemebene zu übernehmen. Profile, die als Überwachungsprofile auf Systemebene verwendet werden, können nicht entfernt werden. Entfernen Sie das Profil von der Seite **Administration > Monitoring Defaults**(Verwaltung > Überwachungsstandards), bevor Sie es löschen.

Anzeigen von Anmeldeversuchen

Cisco Business Dashboard führt ein Protokoll aller erfolgreichen und erfolglosen Versuche, sich beim System an- und abzumelden. Um das Protokoll anzuzeigen, navigieren Sie zu **Administration** > **Login Attempts** (Verwaltung > Anmeldeversuche). Die Tabelle enthält die folgenden Informationen:

Tabelle 23: Tabelle mit Anmeldeversuchen

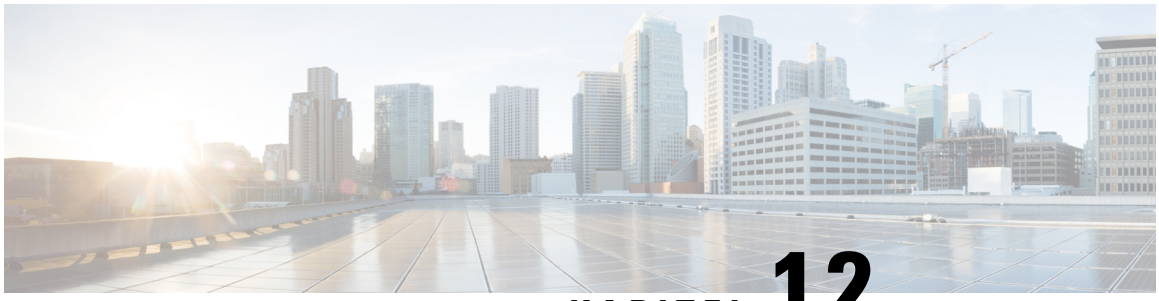
Feld	Beschreibung
Benutzername	Der dem Ereignis zugeordnete Benutzername
Anzeigename	Der Anzeigename des Benutzers
IP	Die IP-Adresse des Geräts, mit der der Benutzer sich angemeldet hat
Typ	Der Typ des Ereignisses. Gültige Werte sind LOGIN und LOGOUT.

Feld	Beschreibung
Status	Gibt an, ob der Versuch erfolgreich war oder fehlgeschlagen ist.
Zeitstempel	Datum und Uhrzeit des Ereignisses

Sie können das Suchfeld über der Tabelle verwenden, um nur Einträge mit einem bestimmten Benutzer oder einer bestimmten IP-Adresse anzuzeigen.

Verwalten der Berichtseinstellungen

Auf der Seite **Report Settings** (Berichtseinstellungen) können Sie die Zeitzone festlegen, für die Berichte generiert werden. Die Start- und Endzeiten für den Berichtszeitraum werden in der Ortszeit der ausgewählten Zeitzone angegeben.



KAPITEL 12

System

Dieses Kapitel enthält folgende Abschnitte:

Informationen zu „System“

Mit der Option „System“ in Cisco Business Dashboard können Sie den Betrieb der Plattform verwalten.

Diese Option ist in die folgenden Seiten unterteilt:

- **License** (Lizenz): Verwalten der Softwarelizenzen für das Dashboard
- **Certificate** (Zertifikat): Verwalten von Sicherheitszertifikaten im Dashboard
- **Email Settings** (E-Mail-Einstellungen): Einrichten von E-Mails
- **API Usage** (API-Nutzung): Überwachen der Nutzung der Cisco Business Dashboard-API
- **Backup** (Sichern): Sichern der Konfiguration und anderer Daten für das Dashboard
- **Restore** (Wiederherstellen): Wiederherstellen der Konfiguration und anderer Daten für das Dashboard
- **Platform Settings** (Plattformeinstellungen): Verwalten der Netzwerkkonfiguration für das Dashboard
- **Privacy Settings** (Datenschutzeinstellungen): Steuern der Daten, die mit Cisco geteilt werden können
- **Log Settings** (Protokolleinstellungen): Ändern der Protokolleinstellungen für das Dashboard
- **Local Probe** (Lokale Probe-Instanz): Verwalten einer im Dashboard gehosteten Probe-Instanz

Diese Seiten sind nur für **Administratoren**verfügbar.

Verwalten von Lizenzen

Hinweis Diese Seite ist in der gemessenen Version von Cisco Business Dashboard für AWS nicht vorhanden.

Auf der Seite **License** (Lizenz) können Sie sehen, wie viele Lizenzen für Ihr Netzwerk erforderlich sind und welche Typen von Lizenzen Sie benötigen. Außerdem können Sie das **Dashboard** über diese Seite mit dem Cisco Smart Licensing-System verbinden. Die Seite ist in zwei Informationsbereiche aufgeteilt:

- **Smart Software Licensing-Status**: In diesem Bereich finden Sie den Registrierungsstatus des Smart License-Clients sowie Informationen zum verwendeten Smart Account.
- **Smart License Usage** (Smart License-Verwendung): In diesem Bereich wird aufgeführt, wie viele Lizenzen und welche Typen von Lizenzen erforderlich sind, ausgehend vom aktuellen Netzwerkzustand. Diese Informationen werden automatisch aktualisiert, wenn Änderungen am Netzwerk vorgenommen werden. Zudem aktualisiert das Dashboard die Anzahl der über den Smart Account angeforderten Lizenzen. Im Feld „Status“ wird angezeigt, ob die benötigte Anzahl Lizenzen erfolgreich abgerufen werden konnte.

Auf dieser Seite können Sie das Dashboard auch bei Ihrem Smart Account registrieren bzw. die Registrierung aufheben.

Kann das Dashboard nicht genügend Lizenzen für das Netzwerkmanagement abrufen, wird es im Evaluierungsmodus ausgeführt und im Kopfbereich der Dashboard-Benutzeroberfläche wird eine entsprechende Meldung angezeigt. Im Evaluierungsmodus haben Sie 90 Tage Zeit, um den Fehler zu korrigieren. Falls Sie dies nicht innerhalb dieser 90-Tage-Frist tun, wird der Funktionsumfang des Dashboards eingeschränkt, bis Sie handeln (d. h. weitere Lizenzen erwerben oder die Anzahl der verwalteten Geräte reduzieren).

Registrieren des Dashboards bei einem Smart Account

Gehen Sie wie folgt vor, um das Dashboard bei Ihrem Smart Account zu registrieren:

1. Melden Sie sich unter *https://software.cisco.com* bei Ihrem Smart Account an. Klicken Sie im Abschnitt „License“ (Lizenz) auf **Smart Software Licensing**.
2. Wechseln Sie auf die Seite **Inventory** (Bestand), und wählen Sie falls nötig einen anderen Virtual Account als den standardmäßigen aus. Wechseln Sie dann auf die Registerkarte **General** (Allgemein).
3. Klicken Sie auf die Schaltfläche **New Token** (Neues Token), um ein neues **Registrierungstoken der Produktinstanz** zu erstellen. Optional können Sie auch eine Beschreibung hinzufügen und einen Wert für **Expire After** (Gültig bis) festlegen. Klicken Sie dann auf **Create Token** (Token erstellen).
4. Wählen Sie rechts neben dem Token aus dem Dropdown-Menü **Actions** (Aktionen) die Option **Copy** (Kopieren) aus, um das neu erstellte Token in die Zwischenablage zu kopieren.
5. Wechseln Sie zur Benutzeroberfläche von Cisco Business Dashboard, und klicken Sie auf **System** > **License** (System >Lizenz).
6. Klicken Sie auf die Schaltfläche **Register** (Registrieren), und fügen Sie das Token in das dafür vorgesehene Feld ein. Klicken Sie auf **OK**.

Das Dashboard wird nun bei Cisco Smart Licensing registriert und es werden genügend Lizenzen für die Anzahl verwalteter Netzwerkgeräte angefordert. Sollten nicht genügend Lizenzen verfügbar sein, wird eine entsprechende Meldung auf der Benutzeroberfläche angezeigt. Sie haben dann 90 Tage Zeit, genügend Lizenzen zu erwerben. Sollten Sie das nicht tun, wird der Funktionsumfang des Systems eingeschränkt.

Entfernen des Dashboards aus einem Smart Account

Gehen Sie wie folgt vor, um das Dashboard aus Ihrem Smart Account zu entfernen und alle zugewiesenen Lizenzen an den Pool zurückzugeben:

1. Wechseln Sie zur Benutzeroberfläche von Cisco Business Dashboard, und klicken Sie auf **System** > **License** (System >Lizenz).
2. Wählen Sie oben rechts aus der Dropdown-Liste die Option **Deregister...** (Registrierung aufheben) aus. Ein Popup-Fenster wird geöffnet. Klicken Sie dort auf **Deregister** (Registrierung aufheben), um die Aktion zu bestätigen.

Sofortiges Prüfen auf Lizenzen

Cisco Business Dashboard prüft täglich, ob noch genügend Lizenzen für das Netzwerk verfügbar sind, und führt sofort ein Update durch, falls die Anzahl benötigter Lizenzen sinkt. Werden jedoch mehr Lizenzen benötigt oder dem Pool Lizenzen hinzugefügt bzw. Lizenzen aus dem Pool entfernt, kann es bis zu einem Tag dauern, bis das Dashboard aktualisiert wird. Gehen Sie wie folgt vor, um im Dashboard eine sofortige Aktualisierung der Lizenzzuweisung zu erzwingen:

1. Wechseln Sie zur Benutzeroberfläche von Cisco Business Dashboard, und klicken Sie auf **System** > **License** (System >Lizenz).
2. Wählen Sie in der Dropdown-Liste oben rechts die Option **ReCheck License Now…** (Lizenz jetzt erneut prüfen). Cisco Business Dashboard sendet dann unmittelbar eine Anfrage an Cisco Smart Licensing, um sicherzustellen, dass genügend Lizenzen für den Betrieb des Dashboards verfügbar sind.

Autorisierung jetzt verlängern

Wenn Sie die Aktion „Renew Registration Now“ (Autorisierung jetzt verlängern) durchführen, aktualisiert das Dashboard die Zertifikate, die zur Authentifizierung der Kommunikation mit Cisco Smart Licensing verwendet werden. In der Regel ist dies nur nach Aufforderung durch den Cisco Support erforderlich, wenn ein längerer Verbindungsausfall behoben werden soll. Gehen Sie wie folgt vor, um die Autorisierung zu verlängern:

1. Wechseln Sie zur Benutzeroberfläche von Cisco Business Dashboard, und klicken Sie auf **System** > **License** (System >Lizenz).
2. Wählen Sie oben rechts aus der Dropdown-Liste die Option **Renew Authorization Now...** (Autorisierung jetzt verlängern) aus.

Sofortiges Verlängern der Registrierung

Wenn Sie die Aktion „Renew Registration Now“ (Registrierung jetzt verlängern) durchführen, aktualisiert das Dashboard die Zertifikate, die zur Authentifizierung der Kommunikation mit Cisco Smart Licensing verwendet werden. In der Regel ist dies nur nach Aufforderung durch den Cisco Support erforderlich, wenn ein längerer Verbindungsausfall behoben werden soll. Gehen Sie wie folgt vor, um die Autorisierung zu verlängern:

1. Wechseln Sie zur Benutzeroberfläche von Cisco Business Dashboard, und klicken Sie auf **System** > **License** (System >Lizenz).
2. Wählen Sie oben rechts aus der Dropdown-Liste die Option **Renew Registration Now...** (Registrierung jetzt verlängern) aus.

Übertragen des Dashboards in einen anderen Account

Wenn Sie eine Dashboard-Instanz erneut registrieren, können Sie sie in einen anderen Virtual Account verschieben. Gehen Sie wie folgt vor, um eine Dashboard-Instanz in einen anderen Account zu verschieben:

1. Wechseln Sie zur Benutzeroberfläche von Cisco Business Dashboard, und klicken Sie auf **System** > **License** (System >Lizenz).
2. Wählen Sie oben rechts aus der Dropdown-Liste die Option **Reregister...** (Erneut registrieren) aus.
3. Geben Sie das neue Registrierungstoken in das dafür vorgesehene Feld ein. Falls die Dashboard-Instanz aktuell bei einem anderen Account registriert ist, müssen Sie das Kontrollkästchen **Reregister this product instance if it is already registered** (Registrieren Sie diese Produktinstanz erneut, falls sie bereits registriert ist) aktivieren. Klicken Sie anschließend auf **OK**.

Verwalten von Zertifikaten

Cisco Business Dashboard generiert bei der Installation ein selbstsigniertes Zertifikat, um sämtliche webbasierte und sonstige Kommunikation zwischen der Software und dem Server abzusichern. Sie können dieses Zertifikat durch ein von einer vertrauenswürdigen Zertifizierungsstelle (CA, Certificate Authority) signiertes Zertifikat ersetzen. Dazu müssen Sie eine Zertifikatsignierungsanforderung (CSR, Certificate Signing Request) generieren und von der gewünschten Zertifizierungsstelle signieren lassen.

Alternativ können Sie ein Zertifikat samt zugehörigem privatem Schlüssel auch vollkommen unabhängig vom Dashboard erstellen. Dann können Sie das Zertifikat und den privaten Schlüssel vor dem Upload in einer Datei im PKCS#12-Format zusammenfassen.

Erstellen einer Zertifikatsanforderung (Certificate Signing Request, CSR)

Gehen Sie wie folgt vor, um eine Zertifikatsignierungsanforderung zu generieren:

1. Navigieren Sie zu **System** > **Certificate** (System > Zertifikat), und wählen Sie die Registerkarte **CSR** aus.
2. Ein Formular wird angezeigt. Geben Sie gültige Werte in die verschiedenen Felder ein. Anhand dieser Werte wird die CSR generiert. Sie sind auch in dem signierten Zertifikat enthalten, das Ihnen die Zertifizierungsstelle später zusendet.
3. Klicken Sie auf **Create** (Erstellen). Die CSR wird automatisch auf Ihren PC heruntergeladen. Sie können die CSR auch erst später herunterladen. Klicken Sie dann neben „CSR“ auf **Download** (Herunterladen).
4. Bei Bedarf können Sie die CSR ändern. Kehren Sie hierfür zu Schritt 2 zurück.

Hochladen eines neuen Zertifikats

Gehen Sie wie folgt vor, um ein neues Zertifikat über die Verwaltungsoberfläche hochzuladen:

1. Navigieren Sie zu **System** > **Certificate** (System > Zertifikat), und wählen Sie die Registerkarte **Update Certificate** (Zertifikat aktualisieren) aus.
2. Aktivieren Sie das Optionsfeld **Upload Cert** (Zertifikat hochladen). Sie können die Datei mit dem Zertifikat entweder in den Zielbereich ziehen oder in den Zielbereich klicken, um sie über das Dateisystem auszuwählen. Die Datei muss im PEM-Format vorliegen.

   Alternativ können Sie auch die Option **Upload PKCS12** (PKCS12 hochladen) auswählen und das Zertifikat samt dem zugehörigen privaten Schlüssel im PKCS#12-Format hochladen. Geben Sie dabei das Kennwort zum Entsperren der Datei in das dafür vorgesehene Feld ein.
3. Klicken Sie auf **Upload** (Hochladen), um die Datei hochzuladen und das aktuelle Zertifikat zu ersetzen.

Gehen Sie wie folgt vor, um ein neues Zertifikat über die Kommandozeile hochzuladen:

1. Kopieren Sie die Zertifikats- und privaten Schlüsseldateien mithilfe von SCP oder ähnlichem in das Cisco Business Dashboard-Dateisystem. Stellen Sie sicher, dass der Zugriff auf diese Dateien nur autorisierten Personen erlaubt ist, da es sich bei dem privaten Schlüssel um vertrauliche Informationen handelt.
2. Melden Sie sich über die Konsole oder über SSH beim Betriebssystem an.
3. Wenden Sie das Zertifikat mit dem folgenden Befehl auf die Dashboard-Anwendung an: **cisco-business-dashboard importcert -t pem -k <private key file> -c <certificate file>**. Das Zertifikat und der private Schlüssel werden in die Dashboard-Anwendung geladen. Sie ersetzen das aktuelle Zertifikat. Geben Sie **cisco-business-dashboard importcert -h** ein, um weitere Informationen zu diesem Befehl und seinen Optionen zu erhalten.

Hinweis Einige Browser generieren möglicherweise Zertifikatwarnungen für Zertifikate, die von einer bekannten Zertifizierungsstelle signiert wurden, während andere Browser das Zertifikat ohne Warnung akzeptieren. Auch Network Plug and Play-Clients akzeptieren das Zertifikat möglicherweise nicht. Dies liegt daran, dass die Zertifizierungsstelle das Zertifikat mit einem Zwischenzertifikat signiert hat, das nicht im Browser oder im Speicher der vertrauenswürdigen Stellen des PnP-Clients enthalten ist. Unter diesen Umständen stellt die Zertifizierungsstelle ein Bündel von Zertifikaten bereit, die vor dem Hochladen in das Dashboard mit dem Serverzertifikat verkettet werden müssen. Das Serverzertifikat muss im verketteten Paket an erster Stelle angezeigt werden.

Neugenerieren des selbstsignierten Zertifikats

Gehen Sie wie folgt vor, um das selbstsignierte Zertifikat neu zu generieren:

1. Navigieren Sie zu **System** > **Certificate** (System > Zertifikat), und wählen Sie die Registerkarte **Update Certificate** (Zertifikat aktualisieren) aus.
2. Klicken Sie auf **Renew Self-Signed Cert** (Selbstsigniertes Zertifikat verlängern). Ein Formular wird angezeigt. Geben Sie gültige Werte in die verschiedenen Felder ein. Diese Werte werden zum Erstellen des Zertifikats verwendet.
3. Klicken Sie auf **Save** (Speichern).

Anzeigen des aktuellen Zertifikats

Gehen Sie wie folgt vor, um das aktuelle Zertifikat abzurufen:

1. Navigieren Sie zu **System** > **Certificate** (System > Zertifikat), und wählen Sie die Registerkarte **Current Certificate** (Aktuelles Zertifikat) aus.
2. Das Zertifikat wird im Klartextformat im Browser angezeigt.

Herunterladen des aktuellen Zertifikats

Gehen Sie wie folgt vor, um das aktuelle Zertifikat herunterzuladen:

1. Navigieren Sie zu **System** > **Certificate** (System > Zertifikat), und wählen Sie die Registerkarte **Current Certificate** (Aktuelles Zertifikat) aus.
2. Klicken Sie unten auf der Seite auf **Download** (Herunterladen). Der Browser lädt das Zertifikat im PEM-Format herunter.

Automatisches Installieren eines Zertifikats von „Let's Encrypt“

Ab Version 2.2.1 kann Cisco Business Dashboard automatisch ein domänenvalidiertes Zertifikat von der **Zertifizierungsstelle von Let's Encrypt** (https://letsencrypt.org) anfordern und erneuern. Führen Sie dazu die folgenden Schritte aus:

1. Melden Sie sich über die Konsole oder über SSH beim Host-Betriebssystem an.
2. Führen Sie den Befehl **cisco-business-dashboard letsencrypt** aus und geben Sie mithilfe der Option **-d** einen oder mehrere vollständig qualifizierte Host-Namen an. Beispiel: **cisco-business-dashboard letsencrypt -d dashboard.example.com -d pnpserver.example.com**. Alle im Befehl aufgeführten Namen müssen in die IP-Adresse des Dashboard-Servers aufgelöst werden.
3. Befolgen Sie die Anweisungen, um ein Zertifikat auszustellen und auf die Dashboard-Anwendung anzuwenden. Das Zertifikat wird kurz vor Ablauf automatisch vom Dashboard erneuert.

Hinweis Der Dienst **Let's Encrypt** muss eine Verbindung zum Dashboard-Webserver herstellen, um die Inhaberschaft der Host-Namen zu überprüfen. Um dies zu ermöglichen, muss der Dashboard-Webserver über das Internet erreichbar sein. Unter Verwalten der Plattformeinstellungen, auf Seite 91 finden Sie weitere Informationen zum Beschränken des Zugriffs auf die Dashboard-Anwendung auf autorisierte IP-Adressen.

Verwalten der E-Mail-Einstellungen

Auf der Seite **Email Settings** (E-Mail-Einstellungen) können Sie steuern, wie E-Mails von Cisco Business Dashboard versendet werden. Auf dieser Seite können Sie folgende Parameter festlegen:

Tabelle 24: E-Mail-Einstellung

Feld	Beschreibung
SMTP-Server	Domänenname oder IP-Adresse des zu verwendenden SMTP-Servers
SMTP-Port	Zum Senden von E-Mails zu verwendender TCP-Port

Feld	Beschreibung
E-Mail-Verschlüsselung	Zu verwendende Verschlüsselungsmethode U. a. stehen folgende Optionen zur Auswahl: • Keine • TLS • SSL
Authentifizierung	Aktivieren oder Deaktivieren der E-Mail-Authentifizierung
Benutzername	Bei aktivierter Authentifizierung zu präsentierender Benutzername
Kennwort	Bei aktivierter Authentifizierung zu präsentierendes Kennwort
Von E-Mail-Adresse	Absender-E-Mail-Adresse für Nachrichten

Um die Konfiguration zu testen, klicken Sie auf **Test Connectivity** (Verbindung testen). Dadurch wird eine Ziel-E-Mail-Adresse angefordert, und es wird eine Test-E-Mail an die angegebene Adresse generiert.

Anzeigen der API-Nutzung

Auf der Seite „API Usage“ (API-Nutzung) werden Informationen zu allen externen Anwendungen angezeigt, die mit Cisco Business Dashboard integriert wurden. Der Bericht ist in die folgenden drei Abschnitte gegliedert:

- **15-minute Request Monitor** (15-Minuten-Anforderungsmonitor): Zeigt die durchschnittliche und die Spitzenanforderungsrate der letzten 15 Minuten an.
- Diagramm **Request History** (Anforderungsverlauf): Zeigt ein Diagramm der Anforderungsaktivität im zeitlichen Verlauf an. Sie können Zeiträume der letzten vier Stunden, der letzten sieben Tage oder aller verfügbaren Informationen auswählen. Sie können dann die Schieberegler unter dem Diagramm verwenden, um den Fokus des Diagramms auf einen bestimmten Zeitraum einzugrenzen.
- Tabelle **API Client Information** (API-Clientinformationen): Listet alle Clients auf, die die API mindestens einmal genutzt haben. In der folgenden Tabelle werden die in der Tabelle **API Client Information** (API-Clientinformationen) enthaltenen Informationen erläutert.

Tabelle 25: Tabelle mit API-Clientinformationen

Feld	Beschreibung
API-Version	Die Version, die vom Client beim Zugriff auf die API verwendet wird.
Kunden-ID	Der Bezeichner für eine bestimmte Instanz der Client-Anwendung
Client-IP	Die diesem Client zugeordnete IP-Adresse. Hier wird außerdem die Callback-URL angezeigt, unter der das Dashboard Ereignisbenachrichtigungen veröffentlichen soll, wenn die API-Version v1 ist und Benachrichtigungen angefordert wurden.

Feld	Beschreibung
Client-Modul	Der Typ der Anwendung, die diesem Client zugeordnet ist
Client-Version	Die Version der Anwendung, die diesem Client zugeordnet ist
Benutzername	Bei Clients, die die v1-API verwenden, wird in diesem Feld der Benutzername angezeigt, den die Anwendung bei der Authentifizierung gegenüber dem Dashboard angibt. Bei Clients, die die v2-API verwenden, werden in diesem Feld die vom Client verwendete **Zugriffsschlüssel-ID** und der Benutzername, dem der Schlüssel zugeordnet ist, angezeigt.
Zeit seit dem letzten Zugriff	Die Zeit seit der letzten Aktivität dieses Clients
Anz. abonnierte Netzwerke	Die Anzahl der Netzwerke, zu denen die Anwendung Ereignisbenachrichtigungen angefordert hat. Diese Anzahl ist ein Link, über den die Tabelle der abonnierten Netzwerke für diesen Client aufgerufen wird. Die Tabelle „Subscribed Networks“ (Abonnierte Netzwerke) wird unten erläutert.
Anz. abonnierte lizenzierte Geräte	Die Anzahl der verwalteten Geräte, für die Ereignisbenachrichtigungen an diesen Client gesendet werden.

Um Informationen zu den Netzwerken anzuzeigen, für die ein Client Benachrichtigungen angefordert hat, klicken Sie in der Tabelle **API Client Information** (API-Clientinformationen) auf den Link **Subscribed Networks** (Abonnierte Netzwerke) für den Client. Die Tabelle **Subscribed Networks** (Abonnierte Netzwerke) für den Client wird angezeigt. Diese enthält eine Liste der Netzwerke, für die der Client Benachrichtigungen angefordert hat. In der folgenden Tabelle werden die in der Tabelle **Subscribed Networks** (Abonnierte Netzwerke) enthaltenen Informationen erläutert.

Tabelle 26: Tabelle „Subscribed Networks“ (Abonnierte Netzwerke)

Feld	Beschreibung
Vermittlung	Der Name des vom Client überwachten Netzwerks
Anz. abonnierte lizenzierte Geräte	Die Anzahl der verwalteten Geräte in diesem Netzwerk, für die Ereignisbenachrichtigungen gesendet werden

Sichern und Wiederherstellen der Dashboard-Konfiguration

Die Konfiguration und andere von Cisco Business Dashboard verwendete Daten können zu Disaster-Recovery-Zwecken oder zum Vereinfachen der Dashboard-Migration zu einem neuen Host gesichert werden. Die Backups werden mit einem Kennwort verschlüsselt, um vertrauliche Daten zu schützen.

Gehen Sie wie folgt vor, um eine Sicherung durchzuführen:

1. Navigieren Sie zu **System** > **Backup** (System > Sichern).
2. Geben Sie in den Feldern **Password** (Kennwort) und **Confirm Password** (Kennwort bestätigen) ein Kennwort zur Verschlüsselung des Backups ein.

3. Klicken Sie auf **Sichern und herunterladen**. Es wird ein Popup-Fenster mit dem Fortschritt des Backups angezeigt. Bei größeren Systemen dauert das Backup möglicherweise länger. Sie können dann die Fortschrittsanzeige schließen und sie später über die Schaltfläche **View Status** (Status anzeigen) wieder aufrufen.

Nach Abschluss des Vorgangs wird die Datei mit dem Backup auf den PC heruntergeladen.

Gehen Sie wie folgt vor, um das Backup einer Konfiguration auf dem Dashboard wiederherzustellen:

1. Navigieren Sie zu **System** > **Restore** (System > Wiederherstellen).
2. Geben Sie im Feld **Password** (Kennwort) das Kennwort ein, das zum Verschlüsseln des Backups festgelegt wurde.
3. Klicken Sie auf **Upload & Restore** (Hochladen und wiederherstellen), um fortzufahren. Es wird ein Popup-Fenster angezeigt, in dem Sie eine Backupdatei vom PC für den Upload auswählen können. Sie können die Backupdatei per Drag-and-Drop in den Zielbereich ziehen oder in den Zielbereich klicken, um eine Datei im Dateisystem des PC anzugeben. Klicken Sie auf **Restore** (Wiederherstellen), um fortzufahren.

Verwalten der Plattformeinstellungen

Auf der Seite **Platform Settings** (Plattformeinstellungen) können Sie die wichtigsten Systemeinstellungen anpassen, ohne direkt auf das Betriebssystem zugreifen zu müssen. Aufgrund der unterschiedlichen Plattformen, die von Cisco Business Dashboard unterstützt werden, sind nicht alle Einstellungen auf jeder Plattform verfügbar.

Die Plattformeinstellungen sind in drei Gruppen unterteilt: Netzwerkeinstellungen, Webserver und Systemvariablen. Jede Gruppe hat eine eigene Registerkarte auf dieser Seite. In den folgenden Abschnitten werden die auf den einzelnen Registerkarten verfügbaren Einstellungen beschrieben.

Ändern des Hostnamens (Registerkarte „Network Settings“ (Netzwerkeinstellungen))

Hinweis Dies gilt nicht für Cisco Business Dashboard für AWS.

Der Hostname ist der Name, anhand dessen das Betriebssystem ein System identifiziert. Cisco Business Dashboard nutzt den Hostnamen beim Generieren von Bonjour-Bekanntmachungen als Bezeichner für das Dashboard. Gehen Sie wie folgt vor, um den Hostnamen für das Dashboard zu ändern:

1. Navigieren Sie zu **System** > **Platform Settings** (System > Plattformeinstellungen) und wählen Sie die Registerkarte **Network Settings** (Netzwerkeinstellungen) aus.
2. Geben Sie einen Hostnamen für das Dashboard in das entsprechende Feld ein.
3. Klicken Sie auf **Save** (Speichern).

Ändern der Netzwerkeinstellungen (Registerkarte „Network Settings“ (Netzwerkeinstellungen))

Hinweis Dies gilt nicht für Cisco Business Dashboard für AWS. Um die Netzwerkkonfiguration zu ändern, verwenden Sie die EC2-Konsole in AWS.

Gehen Sie wie folgt vor, um die Netzwerkkonfiguration für das Dashboard zu ändern:

1. Navigieren Sie zu **System** > **Platform Settings** (System > Plattformeinstellungen) und wählen Sie die Registerkarte **Network Settings** (Netzwerkeinstellungen) aus.
2. Wählen Sie die Methode zur IP-Adresszuweisung aus. Sie haben die Wahl zwischen DHCP (Standard) und Statische IP. Wenn Sie die Option Statische IP ausgewählt haben, geben Sie in den entsprechenden Feldern die Adresse, die Subnetzmaske, die Standardgateways und die DNS-Server an.
3. Klicken Sie auf **Save** (Speichern).

Ändern der Uhrzeiteinstellungen (Registerkarte „Network Settings“ (Netzwerkeinstellungen))

Unter **Time Settings** (Zeiteinstellungen) können Sie die Systemuhr des Dashboards verwalten. Gehen Sie wie folgt vor, um die Systemuhr einzustellen:

1. Navigieren Sie zu **System** > **Platform Settings** (System > Plattformeinstellungen) und wählen Sie die Registerkarte **Network Settings** (Netzwerkeinstellungen) aus.
2. Wählen Sie die passende Zeitzone für das Dashboard aus.
3. Wählen Sie die Methode zur Zeitsynchronisierung aus. Verfügbar sind die Optionen **NTP** (Standardeinstellung) und **Local Clock** (Lokale Uhrzeit). Wenn Sie die Option „NTP“ auswählen, können Sie optional anpassen, welche NTP-Server zur Synchronisierung verwendet werden sollen.

   Wenn Sie die Option **Local Clock** (Lokale Uhrzeit) auswählen, können Sie Datum und Uhrzeit manuell mithilfe der angezeigten Steuerelemente festlegen. Klicken Sie alternativ auf die **Uhr**, um die Uhrzeit mit Ihrem PC zu synchronisieren.
4. Klicken Sie auf **Save** (Speichern).

Ändern der Porteinstellungen (Registerkarte „Web Server“)

Unter **Port Settings** (Porteinstellungen) können Sie festlegen, auf welchen TCP-Ports die Dashboard-Benutzeroberfläche gehostet werden soll. Gehen Sie wie folgt vor, um die standardmäßigen Webserver-Ports zu ändern:

1. Navigieren Sie zu **System** > **Platform Settings** (System > Plattformeinstellungen) und wählen Sie die Registerkarte **Web Server** aus.
2. Ändern Sie die Ports, die der Webserver für die Protokolle HTTP und HTTPS verwendet.
3. Klicken Sie auf **Save** (Speichern).

Hinweis Falls das virtuelle System so konfiguriert ist, dass es die lokale Uhrzeit mit dem Hostsystem synchronisiert, werden alle auf der Seite **Plattformeinstellungen** vorgenommenen Änderungen an der lokalen Uhrzeit durch den Hypervisor überschrieben.

Wenn der verwendete Hypervisor VirtualBox ist und die VirtualBox-Gasterweiterungen auf der VM installiert sind, wird der NTP-Dienst (timesyncd) nicht ausgeführt.

Einschränken des Zugriffs auf das Dashboard (Registerkarte „Web Server“)

Sie können die IP-Adressen, die auf das Dashboard zugreifen, mithilfe der Einstellungen für die Zugriffskontrolle einschränken. Sie können verschiedene IP-Bereiche für die Dashboard-GUI, die Dashboard-API und für Verbindungen von Probes und verwalteten Geräten angeben.

Gehen Sie wie folgt vor, um den Zugriff auf das Dashboard einzuschränken:

1. Navigieren Sie zu **System** > **Platform Settings** (System > Plattformeinstellungen) und wählen Sie die Registerkarte **Web Server** aus.
2. Geben Sie ein Netzwerkpräfix und eine Maske in die dafür vorgesehenen Felder ein. Wenn für einen Abschnitt mehrere Präfixe erforderlich sind, klicken Sie auf das Pluszeichen **(+)**, um weitere Einträge hinzuzufügen. Klicken Sie auf das Papierkorbsymbol, um vorhandene Einträge zu entfernen.
3. Klicken Sie auf **Save** (Speichern).

Verwalten von Systemvariablen (Registerkarte „System Variables“ (Systemvariablen))

Cisco Business Dashboard verwendet Systemvariablen, um beim Generieren von Konfigurationsvorlagen und anderen Aufgaben bestimmte Parameter für das Dashboard bereitzustellen. Einige Systemvariablen werden möglicherweise automatisch vom Dashboard bestimmt, aber es gibt andere Variablen, die eine Benutzereingabe erfordern. Insbesondere wenn das Dashboard hinter einem Webproxy oder NAT-Gateway bereitgestellt wird, muss der Administrator externe Adressierungsinformationen für das Dashboard bereitstellen.

Gehen Sie wie folgt vor, um die externen Adressinformationen für das Dashboard zu aktualisieren:

1. Navigieren Sie zu **System** > **Platform Settings** (System > Plattformeinstellungen) und wählen Sie die Registerkarte **System Variables** (Systemvariablen) aus.
2. Geben Sie die IP-Adresse und die Portinformationen in die Parameter für die externen Systemeinstellungen ein. Wenn dieses Feld leer gelassen wird, verwendet das Dashboard die Plattformadresse und die Portinformationen für die entsprechende Systemvariable.
3. Klicken Sie auf **Save** (Speichern).

Verwalten des Datenschutzes

Einige der Funktionen von Cisco Business Dashboard erfordern die Nutzung von Online-Services, die von Cisco gehostet werden, und führen zur gemeinsamen Nutzung bestimmter Informationen mit Cisco. Die wichtigsten Dienste sind:

- **Cisco Active Advisor**: Cisco Business Dashboard kann Informationen zum Netzwerkbestand in den Cisco Active Advisor-service hochladen (*https://www.ciscoactiveadvisor.com*). Diese Funktion ist standardmäßig deaktiviert.
- **Lifecycle Reporting** (Lebenszyklusbericht): Diese Funktion deckt die Erstellung der Berichte **Lebenszyklusbericht**, **End-of-Life-Bericht und Wartungsbericht** in Cisco Business Dashboard ab. Die Funktion für Lebenszyklusberichte ist standardmäßig aktiviert.
- **Software Updates** (Software-Updates): Sie erhalten Benachrichtigungen zur Verfügbarkeit von Software-Updates für Netzwerkgeräte und die Möglichkeit, diese Updates automatisch anzuwenden. Die Funktion für Software-Updates ist standardmäßig aktiviert.
- **Product Improvement** (Produktverbesserung): Mit dieser Funktion kann Cisco Business Dashboard Informationen über die Hardware- und Softwarenutzung im Netzwerk senden, die zur Weiterentwicklung des Cisco Produktportfolios genutzt werden. Die Funktion zur Produktverbesserung ist standardmäßig aktiviert.

Alle diese Funktionen unterliegen der Cisco Datenschutzrichtlinie. Sie können sie jederzeit aktivieren oder deaktivieren. Die Seite **Privacy Settings** (Datenschutzeinstellungen) wird bei der Ersteinrichtung des Dashboards angezeigt, sodass Sie alle standardmäßig aktivierten Funktionen deaktivieren können, bevor Netzwerkdaten erfasst werden. Weitere Details zu den einzelnen Funktionen und den gemeinsam genutzten Informationen finden Sie unten.

Cisco Active Advisor

Cisco Active Advisor (CAA) ist ein Cloud-basierter Service, der wichtige Lebenszyklusinformationen zu Ihrem Netzwerkbestand bietet. Wenn diese Funktion aktiviert ist, sendet das Dashboard Informationen zum Netzwerkbestand an CAA. Sie können die Informationen zum Lebenszyklus dann im CAA-Portal anzeigen. Vertrauliche Informationen wie Benutzernamen und Kennwörter werden nicht gesendet.

Uploads können automatisch oder nach Bedarf durchgeführt werden. Gehen Sie wie folgt vor, um einen Upload nach Bedarf durchzuführen:

1. Navigieren Sie zur Seite **Network** (Netzwerk), und wählen Sie ein Netzwerk für die Anzeige aus.
2. Wählen Sie in der Dropdown-Liste **Network Actions** (Netzwerkaktionen) die Option **Upload to CAA** (In CAA hochladen) aus.
3. Wenn Sie dazu aufgefordert werden, geben Sie Ihre cisco.com-Anmeldeinformationen an.
4. Wählen Sie optional eine Beschriftung aus, die auf den Upload angewendet werden soll.
5. Klicken Sie auf **Upload** (Hochladen). Sie können auch auf **View inventory data before sending** (Bestandsdaten vor dem Senden anzeigen) klicken, um die Daten vor dem Hochladen zu überprüfen.

Hinweis Die angegebenen cisco.com-Anmeldeinformationen müssen verwendet werden, um sich mindestens einmal beim Cisco Active Advisor-Portal (*https://www.ciscoactiveadvisor.com*) anzumelden, bevor sie für den Upload verwendet werden.

Gehen Sie wie folgt vor, um automatische Uploads zu aktivieren:

1. Navigieren Sie zur Seite **Network** (Netzwerk), wählen Sie ein Netzwerk aus, und klicken Sie dann auf **More** (Mehr). Wählen Sie dann die CAA-Registerkarte aus.

2. Geben Sie in den angezeigten Feldern Ihre cisco.com-Anmeldeinformationen ein. Wählen Sie optional eine Beschriftung aus, die auf den Upload angewendet werden soll.
3. Vergewissern Sie sich, dass das Kontrollkästchen **Automatically upload newly discovered devices** (Neu erkannte Geräte automatisch hochladen) aktiviert ist.
4. Klicken Sie auf **Save** (Speichern). Sie können auch ein Beispiel für die Daten anzeigen, die hochgeladen werden sollen, indem Sie auf den Link auf dieser Seite klicken.

Gehen Sie wie folgt vor, um automatische Uploads zu deaktivieren:

1. Navigieren Sie zur Seite **Network** (Netzwerk), wählen Sie ein Netzwerk aus, und klicken Sie dann auf **More** (Mehr). Wählen Sie dann die CAA-Registerkarte aus.
2. Deaktivieren Sie das Kontrollkästchen **Automatically upload newly discovered devices** (Neu erkannte Geräte automatisch hochladen).
3. Klicken Sie auf **Save** (Speichern).

Lebenszyklusbericht

Cisco Business Dashboard enthält Informationen zum Lebenszyklusstatus der einzelnen Cisco Geräte im Netzwerk. Dazu muss das Dashboard Cisco die Produkt-ID, die Seriennummer sowie die Hardware- und Softwareversionen der einzelnen Cisco Geräte zur Verfügung stellen. Die IP-Adresse des Dashboards kann ebenfalls aufgezeichnet werden. Bei diesem Prozess werden keine anderen persönlichen oder vertraulichen Informationen absichtlich erfasst.

Gehen Sie wie folgt vor, um die Erstellung von Lebenszyklusberichten zu deaktivieren:

1. Navigieren Sie zu **System** > **Privacy Settings** (System > Datenschutzeinstellungen).
2. Deaktivieren Sie die Kontrollkästchen für die Berichte, die Sie deaktivieren möchten.
3. Klicken Sie auf **Save** (Speichern).

Produktverbesserung

Wenn Sie diese Funktion aktivieren, sendet Cisco Business Dashboard regelmäßig Nutzungsinformationen zu Hardware- und Softwareprodukten an Cisco. Die IP-Adresse des Dashboards kann ebenfalls aufgezeichnet werden. Bei diesem Prozess werden keine anderen persönlichen oder vertraulichen Informationen absichtlich erfasst.

Gehen Sie wie folgt vor, um ein Beispiel für die gesendeten Informationen anzuzeigen:

1. Navigieren Sie zu **System** > **Privacy Settings** (System > Datenschutzeinstellungen).
2. Klicken Sie neben dem Kontrollkästchen **Send product improvement data to Cisco** (Daten zur Produktverbesserung an Cisco senden) auf den Link **View a Sample** (Beispiel anzeigen). Ein Beispiel für einen Upload mit Beispieldaten wird angezeigt.

Gehen Sie wie folgt vor, um die Erstellung von Daten zur Produktverbesserung zu deaktivieren:

1. Navigieren Sie zu **System** > **Privacy Settings** (System > Datenschutzeinstellungen).
2. Deaktivieren Sie das Kontrollkästchen **Send product improvement data to Cisco** (Daten zur Produktverbesserung an Cisco senden).

3. Klicken Sie auf **Save** (Speichern).

Software-Updates

Für die Verwendung dieser Funktion muss Cisco Business Dashboard die Produkt-ID sowie Hardware- und Softwareversionsinformationen zu den einzelnen Geräten an Cisco senden. Möglicherweise wird auch Ihre lokale IP-Adresse erfasst. Bei diesem Prozess werden keine anderen persönlichen oder vertraulichen Informationen absichtlich erfasst.

Gehen Sie wie folgt vor, um die Verwendung automatischer Software-Updates zu deaktivieren:

1. Navigieren Sie zu **System** > **Privacy Settings** (System > Datenschutzeinstellungen).
2. Deaktivieren Sie die Kontrollkästchen für die Überprüfung von Geräte-Firmware und Cisco Business Dashboard-Anwendungen.
3. Klicken Sie auf **Save** (Speichern).

Verwalten der Protokolleinstellungen

Auf der Seite **Log Settings** (Protokolleinstellungen) können Sie festlegen, wie detailliert die Informationen in den Protokolldateien sein sollen, die von den unterschiedlichen Softwaremodulen angelegt werden. Die Standardprotokollierungsebene ist **Info** (Information). Durch Auswahl der Ebene **Warn** (Warnung) oder der Ebene **Error** (Fehler) können Sie die Anzahl der in den Protokollen erfassten Nachrichten reduzieren. Wenn Sie mehr Details erfassen möchten, können Sie die Ebene **Debugging** auswählen.

Gehen Sie wie folgt vor, um die Protokollierungsebenen für das Dashboard zu ändern:

1. Navigieren Sie zu **System** > **Log Settings** (System > Protokolleinstellungen).
2. Wählen Sie mithilfe der Optionsfelder jeweils die gewünschte Protokollierungsebene für die verschiedenen Softwaremodule aus.
3. Klicken Sie auf **Save** (Speichern).

Die Protokolldateien für das Dashboard finden Sie im Verzeichnis `/var/log/ciscobusiness/dashboard/` im lokalen Dateisystem. Sie können auf **Download Log File** (Protokolldatei herunterladen) klicken, um ein Archiv des Inhalts dieses Verzeichnisses herunterzuladen. Es kann einige Minuten dauern, bis alle Daten erfasst wurden.

Protokollierung bei Syslog

Ab Version 2.2.1 können Cisco Business Dashboard-Anwendungsprotokolle an den Syslog-Dienst des Hosts gesendet und von dort an externe Syslog-Server weitergeleitet werden.

Gehen Sie wie folgt vor, um das Senden von Dateien an den Host-Syslog-Dienst zu aktivieren:

1. Melden Sie sich mit SSH oder über die Konsole beim Host-Betriebssystem an und bearbeiten Sie die Datei `/etc/ciscobusiness/dashboard/cisco-business-dashboard-logger.conf`.
2. Bearbeiten Sie die Zeilen `xxx.logger`, um **file** oder **syslog** oder beides (durch Kommas getrennt) anzugeben. Die folgenden Module sind verfügbar: `redis`,`mongo` , `rabbitmq`, `nginx` und `cbd`. Wenn Sie `file` angeben, werden Protokollnachrichten an die Standardprotokolldateien im Verzeichnis

/var/log/ciscobusiness/dashboard/ weitergeleitet. Wenn **syslog** angegeben ist, werden Protokollnachrichten an den Syslog-Dienst auf dem Host weitergeleitet.

Hinweis Das mongo-Modul unterstützt nicht mehrere Protokollierungsziele. Wenn mehrere Ziele aufgeführt sind, hat der erste Eintrag Vorrang. Außerdem protokolliert das cbd-Modul immer im Dateisystem, unabhängig davon, ob das Schlüsselwort **file** in der Logger-Konfiguration vorhanden ist oder nicht.

3. Ändern Sie optional die Zeilen xxx.syslog.facility, um die Syslog-Funktion anzugeben, die für jedes der Module verwendet wird. Standardmäßig meldet sich jedes Modul bei einer separaten lokalen <*n*>-Einrichtung an, wobei <*n*> zwischen 1 und 5 liegt.
4. Starten Sie Cisco Business Dashboard neu. Geben Sie dazu den Befehl **cisco-business-dashboard stop** aus, gefolgt von **cisco-business-dashboard start**.

Sobald die Protokollkonfiguration so geändert wurde, dass Protokollnachrichten an **syslog** weitergeleitet werden, sollte die Datei /etc/rsyslog.confaktualisiert werden, um die Protokolle zu erhalten und die Dashboard-Protokollnachrichten an das gewünschte Ziel weiterzuleiten. Weitere Informationen zur Konfigurationsdatei finden Sie unter https://www.rsyslog.com/doc/v8-stable/configuration/index.html.

Führen Sie die folgenden Schritte aus:

1. Die Datei /etc/rsyslog.conf sollte aktualisiert werden, damit Protokollnachrichten über die Loopback-Schnittstelle empfangen werden können. Bearbeiten Sie die Datei und fügen Sie die folgenden Zeilen ein, um dies zu aktivieren und den Server darauf zu beschränken, *nur* die Loopback-Schnittstelle abzuhören:

```
# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514" address="::1")
input(type="imudp" port="514" address="127.0.0.1")

# provides TCP syslog reception
module(load="imtcp")
input(type="imtcp" port="514" address="::1")
input(type="imtcp" port="514" address="127.0.0.1")
```

2. Erstellen Sie eine neue Datei im Verzeichnis /etc/rsyslog.d/, die die Konfigurationsanweisungen für das Cisco Business Dashboard enthält. Der Dateiname sollte dem folgenden Format entsprechen: 40-cisco-business-dashboard-syslog.conf.
3. Bearbeiten Sie die in Schritt 2 erstellte Datei, damit sie Anweisungen zum Senden der Protokollausgabe an die gewünschten Ziele enthält. Wenn Sie beispielsweise die Standardeinrichtungen in der Datei cisco-business-dashboard-logger.conf verwenden, leitet die folgende Konfiguration die Warnmeldungen von der Dashboard-Anwendung zum Syslog-Server mit dem Namen logger.example.com weiter:

```
local2.warning  @logger.example.com
```

4. Starten Sie den rsyslog-Daemon mit dem Befehl **sudo systemctl startup rsyslog.service** neu, um die Änderungen zu übernehmen

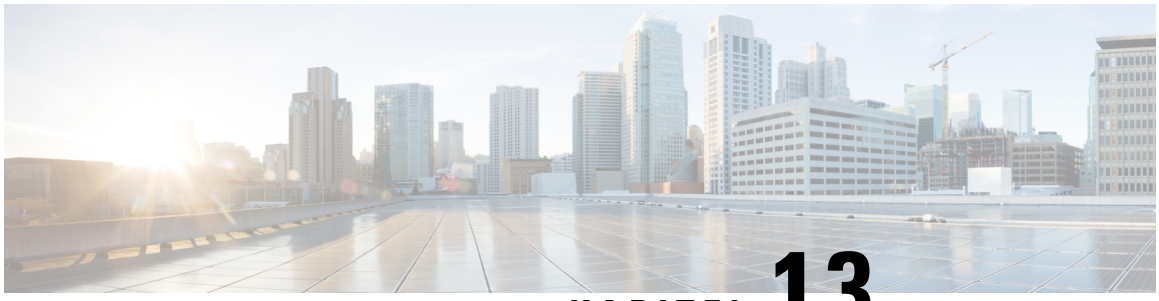
Verwalten der lokalen Network Probe-Instanz

Hinweis Diese Seite ist in Cisco Business Dashboard für AWS nicht vorhanden.

Cisco Business Dashboard Probe kann auf demselben Host installiert werden wie Cisco Business Dashboard, um Geräte im lokalen Netzwerk des Dashboards zu verwalten. Die Probe ist im von Cisco bereitgestellten VM-Image für das Dashboard enthalten. Soll das lokale Netzwerk vom Dashboard nicht verwaltet werden, können Sie die auf dem Dashboard-Host installierte Probe-Instanz wie folgt deaktivieren:

1. Navigieren Sie zu **System** > **Local Probe** (System > Lokale Probe).
2. Klicken Sie auf den Schalter, um die lokale Network Probe-Instanz zu deaktivieren.
3. Klicken Sie auf **Save** (Speichern).

Wenn Sie die Probe-Software vollständig aus Dashboard entfernen möchten: Melden Sie sich beim Betriebssystem an und führen Sie den Befehl `sudo apt-get --purge autoremove cbd-probe` aus. Dieser Befehl entfernt die Network Probe-Software samt den Konfigurationseinstellungen und allen Abhängigkeiten, die von keiner anderen Anwendung benötigt werden.



KAPITEL 13

Benachrichtigungen

Dieses Kapitel enthält folgende Abschnitte:

Allgemeines zu Benachrichtigungen

Cisco Business Dashboard generiert bei verschiedenen Ereignissen im Netzwerk Benachrichtigungen. Durch eine Benachrichtigung kann eine E-Mail oder ein in der unteren rechten Ecke des Browsers angezeigter Popup-Alarm generiert werden. Alle Benachrichtigungen werden zur späteren Prüfung protokolliert. Wenn Benachrichtigungen nicht mehr von Interesse sind, können sie bestätigt werden und erscheinen dann standardmäßig nicht mehr im **Benachrichtigungscenter**.

Unterstützte Benachrichtigungen

In der folgenden Tabelle sind die von Cisco Business Dashboard unterstützten Benachrichtigungen aufgeführt:

Tabelle 27: Unterstützte Benachrichtigungen

Ereignis	Ebene	Beschreibung	Wird automatisch gelöscht?
Gerätebenachrichtigungen			
Erreichbarkeit/Gerät erkannt	Informationen	Im Netzwerk wurde ein neues Gerät erkannt.	Ja, 5 Minuten nach Erkennung des Geräts
Erreichbarkeit/Gerät nicht erreichbar	Warnung	Ein Gerät ist durch ein Erkennungsprotokoll bekannt, ist jedoch per IP nicht zu erreichen.	Ja, sobald das Gerät wieder per IP erreichbar ist
Erreichbarkeit/Gerät offline	Alarm	Ein Gerät wird nicht mehr im Netzwerk erkannt.	Ja, nach erneuter Erkennung des Geräts

Ereignis	Ebene	Beschreibung	Wird automatisch gelöscht?
Anmeldeinformationen erforderlich/SNMP	Warnung	Network Probe kann wegen eines Authentifizierungsfehlers nicht auf das Gerät zugreifen.	Ja, bei Probe-Authentifizierung
Anmeldeinformationen erforderlich/Benutzer-ID	Warnung	Network Probe kann wegen eines Authentifizierungsfehlers nicht auf das Gerät zugreifen.	Ja, bei Probe-Authentifizierung
Geräteservice/SNMP	Warnung	SNMP ist auf dem Gerät deaktiviert.	Ja, nach Aktivierung von SNMP
Geräteservice/Webservice	Warnung	Der Webservice ist auf dem Gerät deaktiviert.	Ja, wenn der Webservice API aktiviert ist.
Integrität	Warnung/Alarm	Die Integrität des Geräts wurde in „Warnung“ oder „Alarm“ geändert.	Ja, nach Wiederherstellung der normalen Geräteintegrität
Cisco Support-Benachrichtigungen			
Firmware	Informationen	Auf cisco.com ist eine neuere Version der Firmware verfügbar.	Ja, nach Aktualisierung des Geräts auf die neueste Version
End-of-Life	Warnung/Alarm	Für das Gerät wurde ein End-of-Life-Bulletin gefunden, oder es wurde ein End-of-Life-Meilenstein erreicht.	Nein
Wartungsablauf	Warnung/Alarm	Die Garantie des Geräts ist abgelaufen, und/oder es ist kein derzeit aktiver Wartungsvertrag vorhanden.	Ja, wenn ein neuer Wartungsvertrag abgeschlossen wird
Benachrichtigungen zur Geräteintegrität			
CPU	Warnung/Alarm	Die CPU-Auslastung des Geräts überschreitet die Höchstschwellenwerte.	Ja, wenn die CPU-Auslastung wieder ein normales Niveau erreicht
Betriebszeit	Warnung/Alarm	Die Gerätebetriebszeit liegt unter den Mindestschwellenwerten.	Ja, wenn die Gerätebetriebszeit die Mindestwerte überschreitet
Verbundene Clients	Warnung/Alarm	Die Anzahl der verbundenen Clients überschreitet die Höchstschwellenwerte.	Ja, wenn die Anzahl der verbundenen Clients wieder ein akzeptables Niveau erreicht

Anzeigen und Filtern aktueller Gerätebenachrichtigungen

Gehen Sie wie folgt vor, um die aktiven Benachrichtigungen für ein bestimmtes Gerät oder alle Geräte anzuzeigen:

1. Klicken Sie im Fenster **Startseite** auf das Symbol **Benachrichtigungscenter** oben rechts in der globalen Symbolleiste. Die Zahl auf dem Symbol gibt die Gesamtzahl der nicht bestätigten ausstehenden Benachrichtigungen an, die Farbe der Zahl steht für die höchste Prioritätsstufe der ausstehenden Benachrichtigungen.

   Alle derzeit ausstehenden Benachrichtigungen sind unter den Symbolen im **Benachrichtigungscenter** aufgeführt. Die Zahl auf dem Symbol für die Prioritätsstufe gibt die Gesamtzahl der Benachrichtigungen für jede der folgenden Kategorien an:

   - Information (grüner Kreis)
   - Warnung (orangefarbenes Dreieck)
   - Alarm (rotes umgedrehtes Dreieck)

2. Im **Benachrichtigungscenter** können Sie folgende Aktionen durchführen:

   - Benachrichtigungen bestätigen – Aktivieren Sie das Kontrollkästchen einer Benachrichtigung, um sie zu bestätigen. Durch Aktivieren des Kontrollkästchens **ACK All** (ACK für alle) können Sie alle angezeigten Benachrichtigungen gleichzeitig bestätigen.
   - Angezeigte Benachrichtigungen filtern – Anweisungen dazu finden Sie im folgenden Schritt.

3. Über das Filterfeld können Sie die in der Tabelle angezeigten Benachrichtigungen einschränken. Standardmäßig werden Benachrichtigungen aller Typen und aller Schweregrade angezeigt. Um einen vorhandenen Filter zu ändern, doppelklicken Sie auf diesen Filter, um die Einstellung zu ändern. Um einen neuen Filter hinzuzufügen, klicken Sie auf die Bezeichnung „Add Filter“ (Filter hinzufügen), und wählen Sie einen Filter aus der Dropdown-Liste aus. Folgende Filter sind verfügbar:

   Tabelle 28: Verfügbare Filter

Filter	Beschreibung
Benachrichtigungstyp	Typ der anzuzeigenden Benachrichtigung. Beispiel: Wählen Sie **Device Offline** (Gerät offline) aus der Dropdown-Liste aus, wenn Sie nur Benachrichtigungen für Geräte anzeigen möchten, die offline sind.
Schweregrad	Prioritätsstufe der anzuzeigenden Benachrichtigungen. Folgende Werte sind möglich: • Info • Warnung • Alarm Aktivieren Sie das Kontrollkästchen **Higher** (Höher), wenn auch Benachrichtigungen mit höherem Schweregrad angezeigt werden sollen.

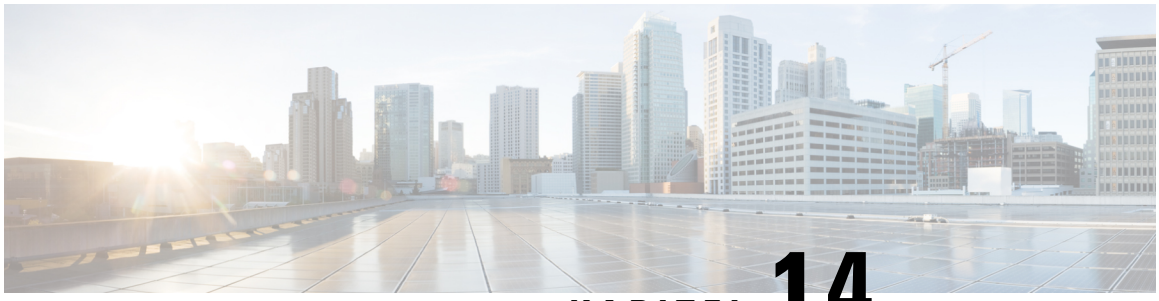
Filter	Beschreibung
Include Ack (ACK einschließen)	Bestätigte Benachrichtigungen einschließen
Netzwerk	Zeigt Benachrichtigungen für die angegebenen Netzwerke an. Wenn Sie mit der Eingabe des Filters beginnen, werden dazu passende Netzwerke in einer Dropdown-Liste angezeigt. Sie können das gewünschte Netzwerk dann per Klick auswählen. Sie können mehrere Netzwerke im Filter berücksichtigen.
Gerät	Zeigt Benachrichtigungen für die angegebenen Geräte an. Wenn Sie mit der Eingabe des Filters beginnen, werden dazu passende Geräte in einer Dropdown-Liste angezeigt. Sie können das gewünschte Gerät dann per Klick auswählen. Sie können mehrere Geräte im Filter berücksichtigen.

Hinweis Benachrichtigungen für einzelne Geräte können Sie in den Bereichen **Basic Info** (Basisinformationen) und **Detailed Info** (Detaillierte Informationen) für das jeweilige Gerät abrufen.

Um zu steuern, wie Sie Benachrichtigungen erhalten, ändern Sie die Benachrichtigungseinstellungen auf Organisations- oder Systemebene. Weitere Informationen finden Sie unter Verwalten von Organisationen oder Ändern von Überwachungsstandards, auf Seite 78.

Anzeigen und Filtern des Verlaufs der Gerätebenachrichtigungen

Das Auftreten oder die Änderung des Status einer Benachrichtigung wird als Ereignis auf dem Dashboard aufgezeichnet und kann über das Ereignisprotokoll angezeigt werden. Ein Teil des Ereignisverlaufs kann über den Bereich **Basic Info** (Basisinformationen) oder den Bereich **Device Detail** (Gerätedetails) der einzelnen Geräte abgerufen werden. Im Bereich **Basic Info** (Basisinformationen) werden nur Ereignisse angezeigt, die innerhalb der letzten 24 Stunden eingetreten sind. Im Bereich **Device Detail** (Gerätedetails) hingegen ist der gesamte gespeicherte Ereignisverlauf für das jeweilige Gerät einsehbar. Die im Bereich **Device Detail** (Gerätedetails) aufgeführten Ereignisse lassen sich filtern. So können Sie gezielt die Ereignisse aufrufen, die für Sie von Interesse sind. Weitere Informationen zum Anzeigen und Filtern des Ereignisverlaufs finden Sie unter Allgemeines zum Ereignisprotokoll (Ereignisprotokoll).



KAPITEL 14

Fehlerbehebung

Dieses Kapitel enthält folgende Abschnitte:

Erfassen von Netzwerkdiagnoseinformationen

Mit der Funktion **Network Show Tech** (Technische Netzwerkinformationen) können Sie unkompliziert Diagnoseinformationen für Ihr Netzwerk erfassen, um sie später zu analysieren oder an einen Supporttechniker zu senden. Sie können **Network Show Tech** (Technische Netzwerkinformationen) über die Dashboard-Benutzeroberfläche oder direkt über die Probe-Benutzeroberfläche generieren, falls Sie an Problemen mit der Dashboard-Probe-Verbindung arbeiten. Gehen Sie wie folgt vor, um **Network Show Tech** (Technische Netzwerkinformationen) zu erfassen:

1. Navigieren Sie zu **Network** (Netzwerk), und wählen Sie das Netzwerk aus, für das Sie Diagnoseinformationen erfassen möchten. Wählen Sie die Registerkarte **Actions** (Aktionen) aus, und klicken Sie auf **Show Tech** (Technische Informationen).

   Melden Sie sich alternativ bei der Probe-Benutzeroberfläche an, und navigieren Sie zu **Troubleshooting** > **Network Show Tech** (Fehlerbehebung > Technische Netzwerkinformationen).

2. Legen Sie mithilfe der Kontrollkästchen fest, ob Kennwörter und Zertifikate aus der Gerätekonfiguration ausgeschlossen werden sollen, und wohin die Diagnoseinformationen gesendet werden sollen. Die folgenden Optionen sind verfügbar:

   - Sie können die Diagnoseinformationen an einen bestehenden Cisco Supportfall anhängen. Geben Sie dazu die Fallnummer im entsprechenden Feld ein.
   - Sie können die Diagnoseinformationen per E-Mail versenden. Geben Sie die E-Mail-Adressen durch Kommas getrennt im entsprechenden Feld ein.
   - Sie können die Diagnoseinformationen auf Ihren PC herunterladen.

   Wenn Sie **Network Show Tech** (Technische Netzwerkinformationen) über Probe generieren, sind die Optionen zum Senden per E-Mail oder zum Anhängen an ein Support-Ticket nicht verfügbar. Sie müssen die Diagnoseinformationen auf Ihren PC herunterladen.

3. Klicken Sie auf **Gather diagnostic data** (Diagnosedaten erfassen).

Die Diagnoseinformationen werden als ZIP-Datei bereitgestellt. Sie beinhalten eine einfache Webseite zur Navigation durch die erfassten Daten. Gehen Sie wie folgt vor, um auf die Daten zuzugreifen:

1. Entpacken Sie die Diagnoseinformationen an einem für Sie praktischen Speicherort auf Ihrem PC.
2. Öffnen Sie die Datei „index.html“ aus dem erstellten Verzeichnis in einem Webbrowser.

Verwalten der Probe-Protokolleinstellungen

Sie können die **Protokolleinstellungen** für Probe über die Dashboard-Benutzeroberfläche oder direkt über die Probe-Benutzeroberfläche verwalten, falls Sie an Problemen mit der Dashboard-Probe-Verbindung arbeiten. Über die Protokolleinstellungen wird gesteuert, welche Informationen von Network Probe in den Protokolldateien gespeichert werden. Diese Informationen sind von vorrangigem Interesse für Supporttechniker, die an der Diagnose von Problemen mit Cisco Business Dashboard arbeiten.

Um die Protokolleinstellungen für ein bestimmtes Netzwerk zu ändern, navigieren Sie zu **Network** (Netzwerk), und wählen Sie das Netzwerk aus, für das Sie die Einstellungen ändern möchten. Klicken Sie auf **More** (Mehr), um den Bereich **Network Detail** (Netzwerkdetails) anzuzeigen, und wählen Sie dann die Registerkarte **Log Settings** (Protokolleinstellungen) aus. Melden Sie sich alternativ bei der Probe-Benutzeroberfläche an, und navigieren Sie dann zu **Administration** > **Log Settings** (Verwaltung > Protokolleinstellungen).

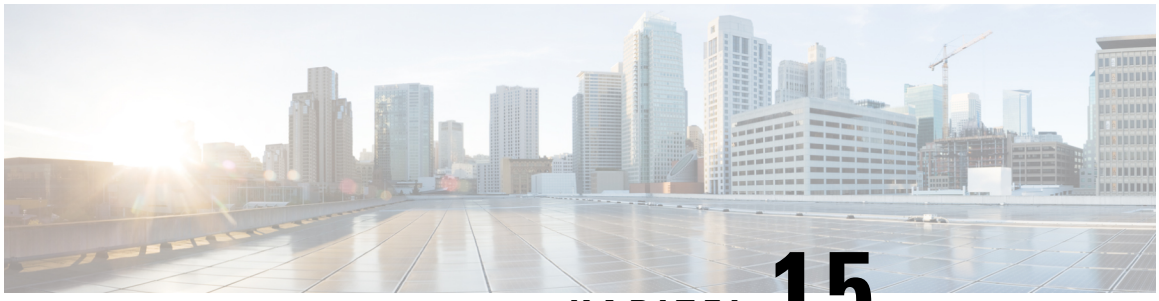
Bei den Einstellungen sind u. a. folgende Parameter verfügbar:

Tabelle 29: Protokolleinstellungen

Feld	Beschreibung
Protokollebene	Detailiertheit, mit der protokolliert werden soll. Die folgenden Optionen sind verfügbar: • **Error** (Fehler): nur Fehlermeldungen • **Warning** (Warnung): Warnungen und Fehler • **Information** (Standard): Informationsmeldungen und Meldungen höherer Stufen • **Debug**: Alle Nachrichten, inklusive Debugging-Nachrichten niedrigerer Stufen

Feld	Beschreibung
Protokollmodul	Module, für die Meldungen protokolliert werden sollen. Die folgenden Optionen sind verfügbar: • **All (default)** (Alle (Standard)): alle Module • **Call-Home-Agent**: Kommunikation zwischen Probe und dem Dashboard • **Discovry** (Erkennung): Ereignisse aus der Geräteerkennung und Topologieerkennung • **Northbound**: Kommunikation zwischen dem Dashboard und Probe • **Services**: Nachrichtenumsetzung zwischen Northbound und Southbound • **Southbound**: Low-Level-Kommunikation zwischen Probe und Geräten • **System**: Kernsystemprozesse, die nicht von anderen Modulen abgedeckt werden Sie können bei Bedarf mehrere Module auswählen.

Die Network Probe-Protokolldateien sind im Archiv **Network Show Tech** (Technische Netzwerkinformationen) enthalten. Nähere Informationen zur Option **Network Show Tech** (Technische Netzwerkinformationen) finden Sie im Abschnitt Erfassen von Netzwerkdiagnoseinformationen, auf Seite 103.



KAPITEL 15

Häufig gestellte Fragen

In diesem Kapitel finden Sie Antworten auf häufig gestellte Fragen zu den Funktionen von Cisco Business Dashboard und potenziellen Problemen. Die Themen sind in die folgenden Kategorien unterteilt:

Allgemeine häufig gestellte Fragen

Q. Welche Sprachen werden von Cisco Business Dashboard unterstützt?

A. Cisco Business Dashboard ist in den folgenden Sprachen verfügbar:

- Chinesisch
- Englisch
- Französisch
- Deutsch
- Japanisch
- Spanisch

Häufig gestellte Fragen zur Netzwerkerkennung

Q. Welche Protokolle verwendet Cisco Business Dashboard für das Management meiner Geräte?

A. Cisco Business Dashboard verwendet zur Erkennung und für das Management des Netzwerks verschiedene Protokolle. Welche Protokolle für ein bestimmtes Gerät verwendet werden, hängt vom Gerätetyp ab.

Zu den verwendeten Protokollen gehören die folgenden:

- Multicast DNS und DNS Service Discovery (d. h. *Bonjour*, siehe *RFCs 6762 bzw. 6763*)

- Cisco Discovery Protocol (CDP)
- Link Layer Discovery Protocol (siehe *Spezifikation IEEE 802.1AB*)
- Simple Network Management Protocol (SNMP)
- RESTCONF (siehe *https://datatracker.ietf.org/doc/draft-ietf-netconf-restconf/)*
- Proprietäre APIs für Webdienste

Q. Wie erkennt Cisco Business Dashboard mein Netzwerk?

A. Cisco Business Dashboard Probe erstellt durch Abhören von CDP-, LLDP- und mDNS-Bekanntmachungen eine vorläufige Liste von Geräten im Netzwerk. Network Probe stellt dann über die unterstützten Protokolle eine Verbindung zu jedem einzelnen Gerät her und fragt weitere Informationen ab, z. B. die CDP- und LLDP-Tabellen für Nachbargeräte, MAC-Adresstabellen und Listen zugeordneter Geräte. Anhand dieser Angaben werden weitere Geräte im Netzwerk identifiziert, und der Prozess wird so oft wiederholt, bis alle Geräte erfasst wurden.

Q. Führt Cisco Business Dashboard Netzwerkscans durch?

A. Cisco Business Dashboard führt nicht aktiv Netzwerkscans durch. Die Network Probe-Software scannt das IP-Subnetz, mit dem sie direkt verbunden ist, jedoch keine anderen Adressbereiche. Der Scan erfolgt auf Basis des ARP-Protokolls. Zusätzlich prüft die Network Probe-Software bei jedem erkannten Gerät, ob ein Webserver und ein SNMP-Server auf den betreffenden Standardports konfiguriert sind.

Häufig gestellte Fragen zur Konfiguration

Q. Was passiert, wenn ein neues Gerät erfasst wird? Wird die Konfiguration geändert?

A. Neue Geräte werden zur Standard-Gerätegruppe hinzugefügt. Wurden der Standard-Gerätegruppe Konfigurationsprofile zugewiesen, wird diese Konfiguration für neu erfasste Geräte übernommen.

Q. Was passiert, wenn ich ein Gerät aus einer Gerätegruppe in eine andere verschiebe?

A. VLAN- oder WLAN-Konfigurationen für Profile, die auf die Original-Gerätegruppe angewendet und nicht für die neue Gerätegruppe übernommen wurden, werden entfernt. VLAN- oder WLAN-Konfigurationen für Profile, die auf die neue Gruppe angewendet werden, aber nicht zur Originalgruppe gehören, werden zum Gerät hinzugefügt. Die Systemkonfigurationseinstellungen werden von Profilen überschrieben, die für die neue Gruppe übernommen werden. Wenn Sie für eine neue Gruppe keine Systemkonfigurationsprofile festgelegt haben, wird die Systemkonfiguration des Geräts nicht geändert.

Häufig gestellte Fragen zu Sicherheitsmaßnahmen

Q. Welche Portbereiche und Protokolle werden für Cisco Business Dashboard benötigt?

A. In der folgenden Liste sind die von Cisco Business Dashboard verwendeten Protokolle und Ports aufgeführt:

Tabelle 30: Cisco Business Dashboard Protokolle und Ports

Port	Richtung	Protokolle	Einsatzbereiche
TCP 22	Inbound	SSH	Zugriff auf das Dashboard über die Kommandozeile SSH ist im von Cisco bereitgestellten VM-Image standardmäßig deaktiviert.
TCP 80	Inbound	HTTP	Web-Zugriff auf das Dashboard Weiterleitung auf sicheren Webserver (Port 443)
TCP 443	Inbound	HTTPS Multiplex-TCP	Sicherer Web-Zugriff auf das Dashboard Kommunikation zwischen Probe und Dashboard
TCP 50000–51000	Inbound	HTTPS	Remotezugriff auf Geräte
UDP 53	Outbound	DNS	Domänennamenauflösung
UDP 123	Outbound	NTP	Zeitsynchronisation.
TCP 443	Outbound	HTTPS	Zugriff auf Cisco Webservices zum Abrufen von Informationen wie Softwareupdates, Support-Status und End-of-Life-Ankündigungen Zugriff auf die Update-Services für Betriebssysteme und Anwendungen.
UDP 5353	Outbound	mDNS	Multicast-DNS-Service-Bekanntmachungen im lokalen Netzwerk zum Bekanntmachen des Dashboards.

Q. Welche Portbereiche und Protokolle werden für Cisco Business Dashboard benötigt?

A. In der folgenden Liste sind die von Cisco Business Dashboard Probe verwendeten Protokolle und Ports aufgeführt:

Tabelle 31: Cisco Business Dashboard Protokolle und Ports

Port	Richtung	Protokolle	Einsatzbereiche
TCP 22	Inbound	SSH	Befehlszeilenzugriff auf die Probe SSH ist im von Cisco bereitgestellten VM-Image standardmäßig deaktiviert.
TCP 80	Inbound	HTTP	Web-Zugriff auf die Probe Weiterleitung auf sicheren Webserver (Port 443)
TCP 443	Inbound	HTTPS	Sicherer Web-Zugriff auf die Probe

Port	Richtung	Protokolle	Einsatzbereiche
UDP 5353	Inbound	mDNS	Multicast-DNS-Service-Bekanntmachungen im lokalen Netzwerk. Wird für die Geräteerkennung verwendet.
UDP 53	Outbound	DNS	Domänennamenauflösung
UDP 123	Outbound	NTP	Zeitsynchronisation
TCP 80	Outbound	HTTP	Gerätemanagement ohne sichere Webservices
UDP 161	Outbound	SNMP	Management von Netzwerkgeräten
TCP 443	Outbound	HTTPS Multiplex-TCP	Gerätemanagement über sichere Webservices, Zugriff auf Cisco Webservices zum Abrufen von Informationen wie Softwareupdates, Support-Status und End-of-Life-Ankündigungen Zugriff auf die Update-Services für Betriebssysteme und Anwendungen. Kommunikation zwischen Probe und Dashboard
UDP 5353	Outbound	mDNS	Multicast-DNS-Service-Bekanntmachungen im lokalen Netzwerk zum Bekanntmachen von Network Probe

Q. Wie sicher ist die Kommunikation zwischen Cisco Business Dashboard und Probe?

A. Die gesamte Kommunikation zwischen dem Dashboard und Probe wird über eine TLS1.2-Sitzung mit authentifizierten Client- und Serverzertifikaten verschlüsselt. Die Sitzung wird von Probe initiiert. Wenn die Zuordnung zwischen dem Dashboard und Probe zum ersten Mal hergestellt wurde, muss sich der Benutzer beim Dashboard über Probe anmelden.

Q. Gibt es für Cisco Business Dashboard eine „Hintertür“ für den Zugriff auf meine Geräte?

A. Nein. Wenn Cisco Business Dashboard ein unterstütztes Cisco Gerät erkennt, werden für den Zugriff die werkseitigen Standard-Anmeldeinformationen für dieses Gerät verwendet. Benutzername und Kennwort lauten dann jeweils `cisco` und die SNMP-Community lautet `public`. Wurde die Standard-Gerätekonfiguration geändert, muss der Benutzer die korrekten Anmeldeinformationen in Cisco Business Dashboard angeben.

Q. Sind die Anmeldeinformationen in Cisco Business Dashboard sicher gespeichert?

A. Die Anmeldeinformationen für den Zugriff auf Cisco Business Dashboard werden mit dem SHA512-Hash-Algorithmus verschlüsselt. Dieser Vorgang ist nicht umkehrbar. Die Anmeldeinformationen

für Geräte und andere Services, wie **Cisco Active Advisor**, werden mit dem AES-128-Algorithmus verschlüsselt. Diese Verschlüsselung ist umkehrbar.

Q. Wie kann ich ein verloren gegangenes Kennwort für die Webbenutzeroberfläche wiederherstellen?

A. Wenn Sie das Kennwort für alle Administratorkonten in der Web-Benutzeroberfläche verloren haben, können Sie es wiederherstellen, indem Sie sich bei der Konsole der Probe-Instanz anmelden und das Tool **cbdprobe recoverpassword** ausführen. Alternativ können Sie sich bei der Konsole der Dashboard-Instanz anmelden und das Tool **cisco-business-dashboard recoverpassword** ausführen. Mit diesem Tool können Sie das Kennwort für das Benutzerkonto „cisco“ auf das Standardkennwort „cisco“ zurücksetzen. Wurde das Benutzerkonto „cisco“ entfernt, können Sie das Konto mit dem Standardkennwort wiederherstellen. Nachfolgend finden Sie ein Beispiel der Befehle, mit denen Sie in diesem Tool das Kennwort wiederherstellen können.

```
cisco@cisco-business-dashboard:~$ cisco-business-dashboard recoverpassword
Are you sure? (y/n) y
Recovered the cisco account to default password
recoverpassword Cisco Business Dashboard successful!
cisco@cisco-buisness-dashboard:~$
```

Hinweis Wenn Sie Cisco Business Dashboard für AWS verwenden, ist das Kennwort die AWS-Instanz-ID.

Q. Wie lauten der Standardbenutzername und das Kennwort für den Bootloader der virtuellen Maschine?

A. Die Standard-Anmeldeinformationen für den Bootloader der virtuellen Maschine sind: Benutzername: **root**, Kennwort: **cisco**. Diese können mit dem config_vm-Tool geändert werden. Wenn Sie gefragt werden, ob Sie das Bootloader-Passwort ändern möchten, antworten Sie mit „Ja“.

Häufig gestellte Fragen zum Remote-Zugriff

Q. Verwende ich eine sichere Sitzung, wenn ich mich über Cisco Business Dashboard mit der Verwaltungsoberfläche eines Geräts verbinde?

A. Cisco Business Dashboard stellt die Remotesitzung zwischen dem Gerät und dem Benutzer per Tunneling bereit. Das zwischen Probe und dem Gerät verwendete Protokoll hängt von der Konfiguration des Endgeräts ab, aber Cisco Business Dashboard wählt immer ein sicheres Protokoll für die Sitzung, sofern verfügbar (z. B. wird HTTPS gegenüber HTTP bevorzugt). Verbindet sich der Benutzer über das Dashboard mit dem Gerät, wird die Sitzung über einen verschlüsselten Tunnel zwischen dem Dashboard und Probe abgewickelt, unabhängig von den auf dem Gerät aktivierten Protokollen. Für die Verbindung zwischen dem Webbrowser des Benutzers und dem Dashboard wird immer HTTPS genutzt.

Q. Warum wird meine Remotesitzung zu einem Gerät immer sofort unterbrochen, wenn ich eine Remotesitzung auf einem anderen Gerät starte?

A. Wenn Sie mit Cisco Business Dashboard auf ein Gerät zugreifen, registriert der Browser jede Verbindung als Kommunikation mit einem Webserver (Dashboard) und sendet Cookies von einem Gerät zum anderen. Wenn mehrere Geräte denselben Cookienamen verwenden, wird eventuell das Cookie eines Geräts von einem anderen Gerät überschrieben. Dies tritt häufig bei Sitzungscookies auf. Aus diesem Grund ist ein

Cookie immer nur für das zuletzt verwendete Gerät gültig. Alle anderen Geräte, die denselben Cookienamen verwenden, identifizieren das Cookie als ungültig und beenden die Sitzung.

Q. Warum tritt bei meiner Remotesitzung der folgende Fehler auf? **Access Error: Request Entity Too Large HTTP Header Field exceeds Supported Size** (Zugriffsfehler: Anforderungsentität zu groß – HTTP-Header-Feld übersteigt die unterstützte Größe.)

A. Nach zahlreichen Remotesitzungen zu unterschiedlichen Geräten sind im Browser viele Cookies für die Dashboard-Domäne gespeichert. Um dieses Problem zu umgehen, löschen Sie mithilfe der Browserfunktionen die Cookies für diese Domäne, und laden Sie dann die Seite erneut.

Häufig gestellte Fragen zu Softwareupdates

Q. Wie sorge ich dafür, dass das Betriebssystem des Dashboards auf dem neuesten Stand ist?

A. Das Dashboard verwendet die Ubuntu Linux-Verteilung für ein Betriebssystem Die Pakete und der Kernel lassen sich mit den Ubuntu-Standardprozessen aktualisieren. Möchten Sie beispielsweise ein manuelles Update durchführen, melden Sie sich als Benutzer „cisco“ bei der Konsole an und geben die Befehle `sudo apt-get updated` und `sudo apt-get upgrade` ein. Das System darf nicht auf eine neue Ubuntu-Version aktualisiert werden. Wir raten davon ab, zusätzliche Pakete zu installieren. Verwenden Sie nur die Pakete, die im von Cisco bereitgestellten VM-Image enthalten sind, oder die Pakete, die im Rahmen einer Minimalinstallation von Ubuntu installiert werden.

Q. Wie aktualisiere ich Java auf dem Dashboard?

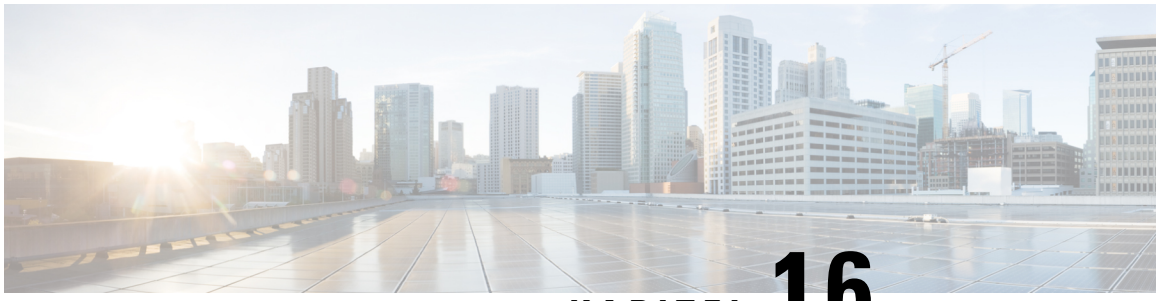
A. Cisco Business Dashboard verwendet die OpenJDK-Pakete aus den Ubuntu-Repositorys. OpenJDK wird automatisch aktualisiert, wenn das Kernbetriebssystem aktualisiert wird.

Q. Wie sorge ich dafür, dass das Betriebssystem von Network Probe auf dem neuesten Stand ist?

A. Cisco Business Dashboard verwendet die Ubuntu Linux-Verteilung für ein Betriebssystem Die Pakete und der Kernel lassen sich mit den Ubuntu-Standardprozessen aktualisieren. Möchten Sie beispielsweise ein manuelles Update durchführen, melden Sie sich als Benutzer „cisco“ bei der Konsole an und geben die Befehle `sudo apt-get updated` und `sudo apt-get upgrade` ein. Das System darf nicht auf eine neue Ubuntu-Version aktualisiert werden. Wir raten davon ab, zusätzliche Pakete zu installieren. Verwenden Sie nur die Pakete, die im von Cisco bereitgestellten VM-Image enthalten sind, oder die Pakete, die im Rahmen einer Minimalinstallation von Ubuntu installiert werden.

Q. Wie sorge ich dafür, dass das Betriebssystem von Network Probe auf dem neuesten Stand bleibt, wenn ich einen Raspberry Pi nutze?

A. Die Raspbian-Pakete und der Kernel können mit den Standardprozessen aktualisiert werden, die für Debian-basierte Linux-Distributionen verwendet werden. Möchten Sie beispielsweise ein manuelles Update durchführen, melden Sie sich als Benutzer „cisco“ bei der Konsole an und geben die Befehle `sudo apt-get updated` und `sudo apt-get upgrade` ein. Das System sollte nicht auf eine neue Raspbian-Hauptversion aktualisiert werden. Es wird empfohlen, keine Pakete außer den zur „Lite“-Version der Raspbian-Distribution gehörenden und den vom Probe-Installationsprogramm hinzugefügten Pakete zu installieren.



KAPITEL 16

Anhang A: Verwaltung von Konfigurationsvorlagen

Dieser Anhang ist in folgende Abschnitte gegliedert:

Überblick

Konfigurationsvorlagen können verwendet werden, wenn es mehrere Geräte gibt, die sehr ähnliche Konfigurationsanforderungen haben, aber eine kleine Anzahl von Parametern für jedes Gerät unterschiedlich sein müssen. So kann ein Netzwerk beispielsweise für alle Switches eine identische Konfiguration verwenden, außer dass jeder Switch einen eindeutigen Hostnamen und eine Management-IP-Adresse hat. Mit Konfigurationsvorlagen können Sie eine einzige Konfigurationsdatei erstellen, die alle gängigen Konfigurationen enthält, mit Platzhaltern für die Elemente der Konfiguration, die eindeutig sein müssen.

Eine Konfigurationsvorlage besteht aus zwei Teilen – der Konfiguration selbst und den Metadaten, die steuern, wie die Platzhalter in der Benutzeroberfläche dargestellt werden, wenn ein Gerätedatensatz erstellt wird. In den nachfolgenden Abschnitten werden diese Bestandteile detailliert beschrieben.

Konfigurationssyntax

Der Konfigurationsteil einer Konfigurationsvorlage ist ein Textdokument, das einer normalen Gerätekonfiguration sehr ähnlich ist. Tatsächlich wird bei der Erstellung einer Konfigurationsvorlage empfohlen, mit einer Sicherung der Konfiguration zu beginnen, die von einem Mustergerät stammt, das bereits mit den Funktionen und Einstellungen konfiguriert ist, die die Vorlage ermöglichen soll. Eine Konfigurationsvorlage unterscheidet sich von einer Gerätekonfiguration dadurch, dass gerätespezifische Parameter – wie z.B. ein Hostname – durch Platzhalter ersetzt werden. Wenn Sie einen neuen Gerätedatensatz erstellen, wird Ihnen ein Formular angezeigt, mit dem Sie die richtigen Werte für jeden der Platzhalter in der Konfigurationsvorlage angeben können. Diese Werte werden mit der Konfigurationsvorlage zusammengeführt, um die eigentliche Konfiguration zu erzeugen, die an das Gerät gesendet wird.

Hinweis Die Platzhalterwerte werden mit der Konfigurationsvorlage zusammengeführt, wenn die Konfiguration an das Gerät gesendet wird. Das bedeutet, dass die endgültige Gerätekonfiguration von der in der Vorschau angezeigten abweichen kann, wenn sich irgendwelche Systemvariablen ändern, bevor das Gerät mit dem Manager verbunden wird.

Konfigurationen werden als Mustache-Vorlagen erstellt – *https://mustache.github.io/*. Mustache erlaubt die Verwendung einer Vielzahl von Platzhaltern – in der Mustache-Dokumentation als Tags bezeichnet –, darunter:

- Einfache Variablen, bei denen der Platzhalter durch den im Gerätedatensatz angegebenen Wert ersetzt wird. Eine einfache Variable hat die Form **{{name}}**.
- Abschnitte, in denen der Platzhalter einen Konfigurationsblock umschließt – optional mit weiteren Platzhaltern. Der Inhalt des Abschnitts kann aus der endgültigen Konfiguration ausgeschlossen, einmal eingeschlossen oder mehrmals wiederholt werden. Das Verhalten dieser Art von Platzhaltern wird durch die Metadaten in der Vorlage und die Werte, die der Benutzer beim Erstellen eines Geräteeintrags angibt, definiert. Ein Abschnitt hat die Form **{{#name}}…{{/name}}**, wobei das erste Tag den Anfang des Blocks und das zweite Tag das Ende markiert.
- Kommentare, die zur Dokumentation der Konfigurationsvorlage verwendet werden können. Ein Kommentar hat die Form {{**! Dies ist ein Kommentar**}}.

Es folgt ein Beispiel für eine einfache Vorlage:

```
!
hostname {{hostname}}
!
{{! Insert a list of VLANs}}
{{#vlans}}
interface vlan {{vlan-id}}
 name {{vlan-name}}
!
{{/vlans}}
```

In diesem Beispiel gibt es mehrere verschiedene Platzhalter:

- **{{hostname}}** ist eine einfache Variable. Sie wird durch den für den Hostnamen im Gerätedatensatz festgelegten Wert ersetzt.
- Direkt nach der Konfiguration des Hostnamens wird ein Kommentar eingefügt. Der Kommentar wird nicht in die an das Gerät gesendete Konfiguration aufgenommen.
- **{{#vlans}}…{{/vlans}}** ist ein Abschnitt, der in diesem Beispiel verwendet wird, um eine Liste einzelner VLANs zu speichern. Für jedes im Geräteeintrag definierte VLAN wird in der Gerätekonfiguration eine Kopie des Inhalts dieses Containers erstellt.
- **{{vlan-id}}** und **{{vlan-name}}** sind einfache Variablen, aber sie sind in der Liste {{#vlans}} enthalten. Wenn der Geräteeintrag erstellt wird, können Sie mehrere Werte für **{{vlan-id}}** und **{{vlan-name}}** angeben. Diese werden zur Erzeugung der Konfiguration verwendet, die zur Erstellung jedes dieser VLANs erforderlich ist.

Weitere Einzelheiten über die Syntax von Mustache finden Sie auf der Mustache-Startseite unter *https://mustache.github.io/mustache.5.html*.

Metadaten von Vorlagen

Jede Konfigurationsvorlage enthält Metadaten, die beschreiben, wie ein bestimmter Platzhalter dem Benutzer bei der Erstellung von Gerätedatensätzen angezeigt werden soll. Diese Metadaten werden bei der Erstellung von Vorlagen mit dem Vorlageneditor erzeugt. Wenn Sie eine Konfigurationsvorlage erstellen oder bearbeiten, wird der Vorlageneditor angezeigt, wobei links die Konfiguration selbst und rechts ein Formular angezeigt wird, mit dem Sie die Metadaten für jeden Platzhalter einstellen können.

Rechts wird jeder Platzhalter in der Konfiguration angezeigt, zusammen mit den folgenden Bedienelementen:

- Ein Kontrollkästchen **Required** (Erforderlich). Dieses Steuerelement bestimmt, ob der Benutzer einen Wert für diesen Platzhalter angeben muss oder nicht.
- Eine Dropdownliste **Type** (Typ). Mit diesem Bedienelement können Sie den Typ des Platzhalters auswählen. Es steuert, wie dieser Platzhalter dem Benutzer angezeigt wird.
- Ein **Titel**. Dieses Element kann verwendet werden, um einen benutzerfreundlicheren Namen für den Parameter auf der GUI bereitzustellen. Wenn für einen Platzhalter kein Titel angegeben wird, dann wird der Platzhalter selbst angezeigt.
- Ein Symbol zum **Bearbeiten**. Bestimmte Typen verfügen über weitere Einstellungen zur Steuerung der Darstellung. So kann beispielsweise ein Zeichenfolgen-Platzhalter weiter verfeinert werden, um für eine IP-Adresse oder einen URI zu stehen, und das Eingabeformular zeigt einen Fehler an, wenn der eingegebene Text nicht das richtige Format hat. Bestimmte Typen können auch basierend auf Systeminformationen statt auf Benutzereingaben eingestellt werden. Weitere Informationen finden Sie unter „System- und dynamische Variablen“ unten.
- Steuerelemente **Nach oben/Nach unten**. Mit diesen Pfeilen können Sie die Reihenfolge ändern, in der die Platzhalter dem Benutzer angezeigt werden. Platzhalter können nach dem, was für den Benutzer am sinnvollsten ist, gruppiert werden, anstatt nach der Reihenfolge, in der sie in der Konfiguration erscheinen.

Der Vorlageneditor bietet auch eine Vorschaufunktion, mit der ein Beispiel dafür gegeben werden kann, wie das Formular für Platzhalter beim Erstellen und Bearbeiten von Geräteaufzeichnungen für den Benutzer aussehen wird.

Platzhalter-Typen

Die folgenden Platzhaltertypen stehen zur Verfügung:

- Zeichenfolge – Platzhalter dieses Typs werden in der GUI als einfaches Texteingabefeld angezeigt.
- Ganzzahl – Ganze Zahlen werden als Texteingabefeld mit Steuerelementen zum Erhöhen oder Verringern des Wertes der angezeigten Zahl angezeigt. In dieses Feld dürfen nur Zahlen eingegeben werden.
- Boolesch – Ein boolescher Platzhalter wird in der GUI als Kontrollkästchen angezeigt. Wenn das Kontrollkästchen aktiviert ist, wird der Platzhalter auf den Zeichenfolgen-Wert ‚true‘ gesetzt. Wenn das Kontrollkästchen nicht aktiviert ist, ist der Wert ‚false‘. Ein Abschnitt kann auch als boolescher Abschnitt gekennzeichnet werden. In diesem Fall wird die in dem Abschnitt enthaltene Konfiguration nur dann einbezogen, wenn das Kontrollkästchen für den Abschnitt aktiviert ist.
- Container – Der Typ „Container“ kann verwendet werden, um andere Platzhalter im Formular zu gruppieren.
- Liste – Eine Liste ist ein Container oder Abschnitt einer Konfiguration, der in einer erzeugten Konfigurationsdatei mehrfach wiederholt werden kann. Wenn für die Platzhalter innerhalb einer Liste Formularelemente erzeugt werden, werden zusätzliche Steuerelemente hinzugefügt, um Elemente in der Liste hinzuzufügen oder zu entfernen.

Zusätzlich zu den oben aufgeführten einfachen Typen können Zeichenfolgen-Variablen durch Klicken auf das Symbol zum **Bearbeiten** weiter verfeinert werden. Die verfügbaren Optionen umfassen:

- Angeben eines Standardwertes für den Platzhalter.
- Einstellung der minimalen und/oder maximalen Länge für Zeichenketten-Platzhalter.
- Festlegen einer vordefinierten Liste von Auswahlmöglichkeiten (mit der Option „Enum“ (Aufzählung)).
- Beschränken des Formats einer Zeichenfolge auf einen Hostnamen, einen URI, eine IPv4- oder eine IPv6-Adresse. Eine Zeichenfolge kann auch als Textbereich gekennzeichnet werden, wenn wahrscheinlich eine beträchtliche Menge an Inhalt eingegeben werden muss.

System- und dynamische Variablen

Platzhalter können ihre Werte nicht nur aus Benutzereingaben, sondern auch aus systemintern definierten Parametern übernehmen. Systemvariablen sind Parameter, die für den Manager selbst definiert wurden, z. B. die Manager-IP-Adresse. Durch Festlegen eines Platzhalters, der seinen Wert von einer Systemvariablen übernimmt, fügt der Manager diesen Wert ohne jeglichen Benutzereingriff in die Konfiguration ein. Einige komplexere Bereitstellungen erfordern möglicherweise Benutzereingaben, damit die Systemvariablen ordnungsgemäß funktionieren. Näheres dazu finden Sie unter Verwalten der Plattformeinstellungen, auf Seite 91.

Dynamische Variablen ähneln Systemvariablen, aber es handelt sich um Werte, die dynamisch auf der Grundlage von Informationen wie dem angemeldeten Benutzer oder der Gerätegruppe, zu der das Gerät gehört, erzeugt werden. System- und dynamische Variablen werden verwendet, um die Übertragbarkeit von Vorlagen zwischen Geräten und Systemen zu ermöglichen.

Erstellen von Konfigurationsvorlagen

Der empfohlene Ansatz zur Erstellung von Konfigurationsvorlagen besteht darin, zunächst ein Netzwerkgerät des entsprechenden Typs mit den gewünschten Einstellungen zu konfigurieren, dann eine Sicherungskopie der Gerätekonfiguration zu erstellen und diese in den Manager hochzuladen, um sie als Ausgangspunkt zu verwenden. Alternativ können Sie mit der Funktion „Save As“ (Speichern unter) eine Kopie einer bestehenden Vorlage erstellen. In jedem Fall können Sie, wenn Sie mit einer bestehenden Konfiguration beginnen, die Zeit für die Erstellung einer Vorlage reduzieren und auch die Anzahl der erforderlichen Überarbeitungen verringern, um das gewünschte Ergebnis zu erreichen. Wenn Sie eine neue Vorlage erstellen, müssen Sie eine Organisation, zu der die Vorlage gehören wird, sowie die Produkt-IDs (PIDs), mit denen die Vorlage verwendet werden darf, angeben. Die Produkt-IDs können ***** und **?** als Platzhalterzeichen enthalten.

Nachdem Sie Ihre Startkonfiguration erstellt haben, können Sie sie folgendermaßen aktualisieren:

1. Navigieren Sie zu **Network Plug and Play** > **Konfigurationen** und öffnen Sie dann Ihre Startkonfiguration im Vorlageneditor, indem Sie die Konfiguration auswählen und auf das Symbol **Bearbeiten** klicken.
2. Der Vorlageneditor wird geöffnet; die Startkonfigurationsdatei wird dabei links in einem Texteditor-Fenster angezeigt. Der Texteditor unterstützt viele gängige Bearbeitungsfunktionen, einschließlich Suchen, Ersetzen und mehrere Tastenfolgen zur Cursorsteuerung. Eine Liste finden Sie unten unter Tabelle 32: Häufige Editor-Befehle.

   Ändern Sie die Konfiguration durch Einfügen von Platzhaltern, wie unter Konfigurationssyntax beschrieben. Jedes Mal, wenn ein neuer Platzhalter eingefügt wird, wird im Formular recht ein entsprechender Eintrag hinzugefügt.

3. Ändern Sie mithilfe des Formulars auf der rechten Seite die mit jedem Platzhalter verknüpften Metadaten, um sicherzustellen, dass der Platzhalter dem Benutzer in der am besten geeigneten Weise angezeigt wird. Oben unter Vorlagen-Metadaten finden Sie weitere Einzelheiten zur Angabe von Metadaten. Sie können die Vorschaufunktion verwenden, um zu sehen, wie das Formular dem Benutzer beim Erstellen eines Gerätedatensatzes angezeigt wird.
4. Wiederholen Sie die Schritte 2 und 3, bis Sie Platzhalter für alle Konfigurationsparameter erstellt haben, die von Gerät zu Gerät unterschiedlich sein sollten.
5. Wenn die Vorlage zu Ihrer Zufriedenheit fertiggestellt ist, klicken Sie auf **Save** (Speichern).

Hinweis Jedes Mal, wenn eine Vorlage gespeichert wird, wird eine neue Version der Vorlage erstellt. Ältere Versionen von Vorlagen bleiben im Manager erhalten, es sei denn, Sie löschen sie explizit. Wenn eine Vorlage einem Gerät zugewiesen wird, wird eine bestimmte Version der Vorlage zugewiesen – standardmäßig die neueste Version. Wenn neue Versionen erstellt werden, verwenden vorhandene Geräte weiterhin die Version, die bei der Erstellung zugewiesen wurde. Eine Vorlagenversion, die derzeit einem Gerät zugeordnet ist, kann nicht gelöscht werden.

Tabelle 32: Häufige Editor-Befehle

Funktion	Beschreibung	Tastenkombination	
		PC	Mac
Alle auswählen	Gesamten Inhalt des Editors auswählen	Strg+A	Cmd+A
Rest der Zeile löschen	Löscht den Teil der Zeile nach dem Cursor. Wenn dieser nur aus Leerzeichen besteht, wird der Zeilenumbruch am Ende der Zeile ebenfalls gelöscht.		Strg+K
Zeile löschen	Löscht die gesamte Zeile unter dem Cursor, einschließlich des Zeilenumbruchs am Ende	Strg+D	Cmd+D
Rückgängig	Macht die letzte Änderung rückgängig	Strg+Z	Cmd+Z
Wiederholen	Wiederholt die letzte rückgängig gemachte Änderung	Strg+Y	Cmd+Umschalt+Z Cmd+Y
Zum Dokumentanfang	Bewegt den Cursor an den Anfang des Dokuments	Strg+Pos1	Cmd+Nach oben Cmd+Home
Zum Dokumentende	Bewegt den Cursor an das Ende des Dokuments	Strg+Ende	Cmd+Ende Cmd+Nach unten
Zum Zeilenanfang	Bewegt den Cursor an den Anfang der Zeile	Alt+Links	Strg+A
Zum Zeilenende	Bewegt den Cursor an das Ende der Zeile	Alt+Rechts	Strg+E

Funktion	Beschreibung	Tastenkombination	
		PC	Mac
Weiter einrücken	Rückt die aktuelle Zeile oder Auswahl ein	Strg+]	Cmd+]
Weniger einrücken	Rückt die aktuelle Zeile oder Auswahl aus	Strg+[	Cmd+[
Suchen		Strg+F	Cmd+F
Weitersuchen		Strg+G	Cmd+G
Nach oben suchen		Strg+Umschalt+G	Cmd+Umschalt+G
Ersetzen		Strg+Umschalt+F	Cmd+Alt+F
Alle ersetzen		Strg+Umschalt+R	Cmd+Alt+Umschalt+F