REVIEW DRAFT - CISCO CONFIDENTIAL

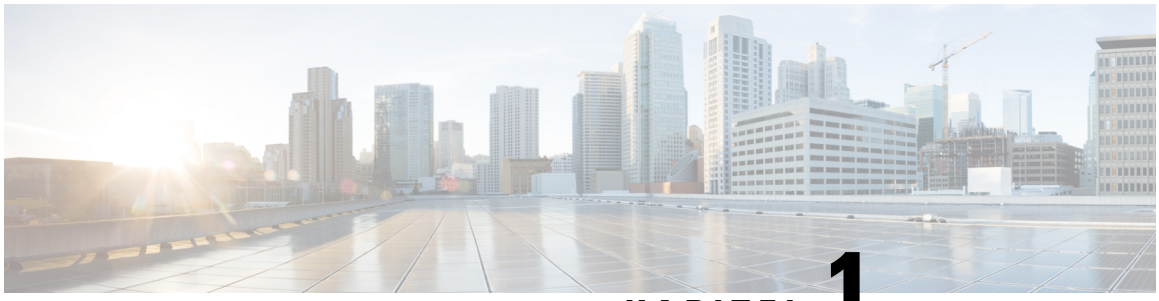
Kurzanleitung für Cisco Business Dashboard und Probe

Erste Veröffentlichung: 5 November 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:

- **Kurzanleitung (vorliegendes Dokument)**: Dieses Handbuch enthält Informationen zum Durchführen der Ersteinrichtung für Cisco Business Dashboard mit den am häufigsten ausgewählten Optionen.
- **Installationshandbücher**

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

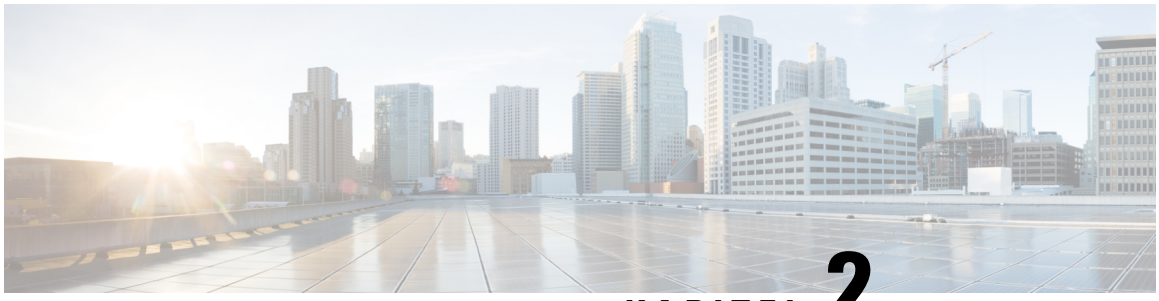
Unterstützte Plattformen	Standort
Amazon Web Services	Cisco Business Dashboard – Installationshandbuch für Amazon Web Services
Oracle VirtualBox	Cisco Business Dashboard – Installationshandbuch für Oracle VirtualBox
Microsoft Hyper-V	Cisco Business Dashboard – Installationshandbuch für Microsoft Hyper-V
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

- **Administratorhandbuch**: Dies ist ein Referenzhandbuch mit Informationen zu allen Funktionen und Optionen der Software sowie zu deren Konfiguration und Nutzung. Weitere Informationen finden Sie im Cisco Business Dashboard-Administratorhandbuch.
- **Liste der unterstützten Geräte**: Diese Liste enthält Informationen zu den von Cisco Business Dashboard unterstützten Geräte und den Funktionen, die für die jeweiligen Gerätetypen verfügbar sind. Eine Liste aller von Cisco Business Dashboard unterstützten Geräten finden Sie unter Cisco Business Dashboard − Liste der unterstützten Geräte.

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).

Begriff	Beschreibung
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
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.



KAPITEL 2

Durchführen der Ersteinrichtung für das Dashboard

Dieses Kapitel enthält folgende Abschnitte:

Durchführen der Ersteinrichtung für das Dashboard

Sie müssen einige Konfigurationsaufgaben erfüllen, um das Dashboard an Ihre Anforderungen anzupassen.

Konfigurieren der grundlegenden Systemeinstellungen im VM-Image oder der AWS-Instanz

Gehen Sie wie folgt vor, um die grundlegenden Systemeinstellungen wie die IP-Adresseinstellungen und die Uhrzeiteinstellungen für das Dashboard zu konfigurieren:

1. Wenn Sie ein virtuelles System nutzen, stellen Sie mithilfe der entsprechenden Tools für Ihren Hypervisor eine Verbindung zur Konsole des Dashboards her. Alternativ können Sie per SSH eine Verbindung zu Ihrer AWS-Instanz herstellen.
2. Wenn Sie ein virtuelles System nutzen, melden Sie sich mit dem Standardbenutzernamen und -kennwort an. Beide lauten: `cisco`. Verwenden Sie für eine AWS-Instanz das Schlüsselpaar, das Sie beim Erstellen der Instanz angegeben haben, und folgenden Benutzernamen: `cisco`.

   Unmittelbar nach der Anmeldung werden Sie aufgefordert, das Kennwort für das Cisco Konto zu ändern. Das neue Kennwort sollte ein komplexes Wort aus einem Mix verschiedener Zeichenarten sein, das in keinem Wörterbuch zu finden ist.
3. Geben Sie den Befehl `sudo config_vm` ein, um die Erstkonfiguration durchzuführen. Wenn Sie dazu aufgefordert werden, geben Sie das Kennwort für das Benutzerkonto „cisco“ ein. Vom Dienstprogramm `config_vm` werden Sie in einer Reihe von Schritten zum Ändern der Plattformeinstellungen aufgefordert.
4. Zunächst werden Sie aufgefordert, den Hostnamen für das Dashboard zu ändern. Der Hostname wird verwendet, um das Dashboard im Netzwerk zu identifizieren. Sie können einen aussagekräftigen Namen festlegen oder diesen Schritt überspringen, um den Standardhostnamen beizubehalten.

Hinweis Dieser Schritt ist bei Cisco Business Dashboard für AWS nicht verfügbar.

Durchführen der Ersteinrichtung für das Dashboard

5. Als Nächstes werden Sie aufgefordert, die Webserver-Ports zu ändern. Wenn diese Ports von den Standardwerten abweichen, müssen Sie möglicherweise auch die Firewall-Einstellungen in Ihrem Netzwerk oder die Einstellungen der Sicherheitsgruppe in AWS ändern.
6. Als Nächstes werden Sie aufgefordert, die Netzwerkschnittstelle zu konfigurieren. Sie haben die Wahl zwischen einer statischen Option und DHCP (DHCP ist der Standard). Wenn Sie sich für die statische Option entscheiden, werden Sie zum Eingeben von IP-Adressinformationen, Standardgateways und DNS-Serveradressen aufgefordert. Die Netzwerkschnittstelle wird zurückgesetzt, wenn Sie in diesem Bereich Änderungen vornehmen.

Hinweis Dieser Schritt ist bei Cisco Business Dashboard für AWS nicht verfügbar. Um die Netzwerkkonfiguration zu ändern, verwenden Sie die EC2-Konsole in AWS.

7. Anschließend werden Sie aufgefordert, die Zeiteinstellungen für das Dashboard zu konfigurieren. Sie können einen oder mehrere NTP-Server zur Zeitsynchronisierung konfigurieren (empfohlen) und werden zum Auswählen der Zeitzone aufgefordert.

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

8. Schließlich werden Sie gefragt, ob Sie das Bootloader-Passwort ändern möchten. Der Bootloader-Benutzername und das Kennwort können auf der Konsole beim Systemstart verwendet werden, um den Systemstartprozess zu ändern oder verlorene Betriebssystemkennwörter wiederherzustellen. Die Standard-Anmeldeinformationen für den Bootloader sind: Benutzername: **root**, Kennwort: **cisco**.

Sie können diese Einstellungen jederzeit ändern, indem Sie das Skript erneut ausführen oder über die Weboberfläche unter **Administration** > **Platform Settings** (Verwaltung > Plattformeinstellungen) darauf zugreifen.

Starten der Dashboard-Benutzeroberfläche

1. Öffnen Sie einen Webbrowser, beispielsweise **Google Chrome** oder **Microsoft Edge**.
2. Geben Sie im Feld **Address** (Adresse) die IP-Adresse oder den Hostnamen des Dashboards ein, und drücken Sie dann die **Eingabetaste**.
3. Geben Sie den standardmäßigen Benutzernamen (`cisco`) und das standardmäßige Kennwort (`cisco`) ein. Wenn Sie Cisco Business Dashboard für AWS verwenden, ist das Standardkennwort die Instanz-ID. Sie können die Instanz-ID in der AWS EC2-Konsole anzeigen.
4. Klicken Sie auf **Login** (Anmelden). Sie werden aufgefordert, das Kennwort für das Benutzerkonto „cisco“ zu ändern. Das neue Kennwort muss mindestens acht Zeichen lang sein und mindestens drei verschiedene Zeichenklassen enthalten.
5. Klicken Sie auf **Next** (Weiter). Sie erhalten Informationen darüber, wie Cisco Business Dashboard Ihre Daten verwendet und welche Informationen mit Cisco geteilt werden. Nehmen Sie alle erforderlichen Änderungen vor, und klicken Sie dann auf **Finish** (Fertigstellen).

Die Benutzeroberfläche von Cisco Business Dashboard wird angezeigt.

Erstellen von Organisationen (optional)

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. Die Verwendung von Organisationen ermöglicht eine detailliertere Kontrolle darüber, wer die verschiedenen Teile des Netzwerks anzeigen und verwalten kann. Eine einzelne Organisation wird standardmäßig erstellt, wenn das Dashboard installiert wird.

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 Schritte 1 bis 5 für jede Organisation, die Sie erstellen möchten.

Erstellen von Benutzern und Ändern von Kennwörtern

Im Dashboard ist zu Beginn ein einziger Standardbenutzername mit einem Standardkennwort eingerichtet.

Gehen Sie wie folgt vor, um neue Benutzer hinzuzufügen:

1. Navigieren Sie zu **Administration** > **Users** (Verwaltung > Benutzer).
2. Klicken Sie oben in der Tabelle **Users** (Benutzer) auf das Pluszeichen (✚).
3. Geben Sie im Fenster **Add User** (Benutzer hinzufügen) die Details des Benutzers ein, der erstellt werden soll. Legen Sie fest, ob der Benutzer ein Administrator, ein Org-Administrator, ein Bediener oder schreibgeschützt sein soll. Im Folgenden werden die Berechtigungen der verschiedenen Benutzertypen erläutert.
    - Administratoren haben Zugriff auf alle Funktionen, einschließlich des Systemmanagements.
    - Org-Administratoren haben Zugriff auf alle Funktionen in einer oder mehreren Organisationen, haben jedoch keinen Zugriff auf die Systemmenüs.
    - Bediener haben Zugriff auf alle Funktionen in ihren zugewiesenen Organisationen, haben jedoch nicht die Möglichkeit, Benutzer zu verwalten. Sie haben keinen Zugriff auf die Systemmenüs.
    - Schreibgeschützte Benutzer können keine Konfigurationsänderungen vornehmen, haben nur eingeschränkten Zugriff auf die Verwaltungsmenüs und keinen Zugriff auf die Systemmenüs.
4. Klicken Sie auf **Save** (Speichern), um den neuen Benutzer zu erstellen.

Auf der Seite **Users** (Benutzer) können Sie auch Vorgaben für die Kennwortkomplexität festlegen. Wählen Sie dazu die Registerkarte **User Settings** (Benutzereinstellungen) aus. Neue Kennwörter müssen diesen Vorgaben entsprechen.

Gehen Sie wie folgt vor, um Ihr Kennwort zu ändern:

Durchführen der Ersteinrichtung für das Dashboard

1. Klicken Sie in der Benutzeroberfläche oben rechts auf Ihren Benutzernamen, um das Dropdown-Menü anzuzeigen, und wählen Sie dann **My Profile** (Mein Profil) aus. Eine Seite wird angezeigt.
2. Klicken Sie auf den Link „Reset Password“ (Kennwort zurücksetzen).
3. Geben Sie in den entsprechenden Feldern Ihr aktuelles Kennwort und das neue Kennwort ein.
4. Klicken Sie auf **Save** (Speichern).

Einrichten von Lizenzen

Hinweis Dies gilt nicht für die gemessene Version von Cisco Business Dashboard für AWS.

Cisco Business Dashboard nutzt Cisco Smart Licensing zur Lizenzierung. Bei der ersten Installation wird das Dashboard in den Evaluierungsmodus geschaltet. Im Evaluierungsmodus ist das uneingeschränkte Management von bis zu 10 Netzwerkgeräten erlaubt. Falls Sie mehr als 10 Geräte verwalten, haben Sie 90 Tage Zeit, weitere Lizenzen zu erwerben. Um erworbene Lizenzen auf das System anwenden zu können, müssen Sie das Dashboard mit einem Cisco Smart Account verknüpfen, der genügend Gerätelizenzen für Ihr Netzwerk enthält.

Gehen Sie wie folgt vor, um das Dashboard mit Ihrem Smart Account zu verknüpfen:

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 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. Navigieren Sie zur Benutzeroberfläche von Cisco Business Dashboard, und klicken Sie auf **Administration** > **License** (Verwaltung > Lizenz).
6. Klicken Sie auf **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. Nähere Informationen zur Lizenzierung finden Sie im Administratorhandbuch für Cisco Business Dashboard unter *Managing Licenses* (Verwalten von Lizenzen).

Deaktivieren der in das VM-Image eingebetteten Network Probe-Instanz

Hinweis Dies gilt nicht für Cisco Business Dashboard für AWS.

Das Dashboard-VM-Image enthält die Probe-Software. Über sie können die Geräte im lokalen Netzwerk des Dashboards verwaltet werden. Soll das lokale Netzwerk nicht verwaltet werden, können Sie die eingebettete Network Probe-Instanz wie folgt deaktivieren:

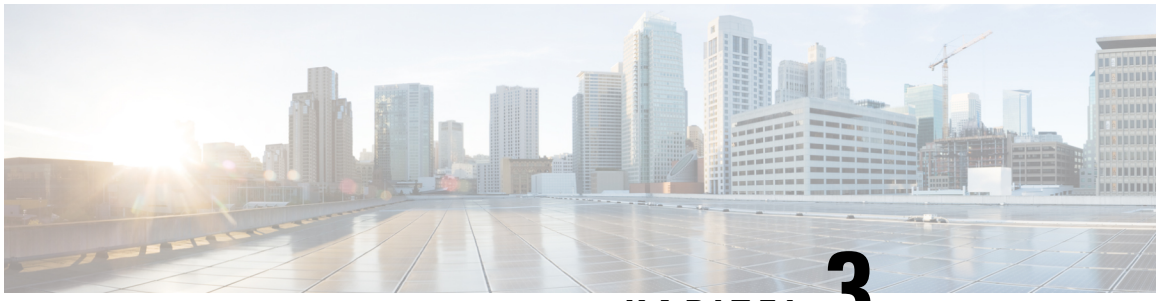
1. Navigieren Sie zu **System** > **Local Probe** (System > Lokaler Test).
2. Klicken Sie auf den Schalter, um die eingebettete Network Probe-Instanz zu deaktivieren.
3. Klicken Sie auf **Save** (Speichern).

Erstellen von Netzwerken (optional)

Im Dashboard können Sie Netzwerkdatensätze für Probes vordefinieren, die Sie dann später zuordnen. In der Regel steht jedes Netzwerk für einen separaten Standort. Dennoch können mehrere Netzwerke am gleichen Standort vorhanden sein. Gehen Sie wie folgt vor, um ein neues Netzwerk zu erstellen:

1. Navigieren Sie zu **Network** (Netzwerk).
2. Klicken Sie in der **Kartenansicht** auf **Add Network** (Netzwerk hinzufügen) bzw. in der **Listenansicht** auf das Pluszeichen (+).
3. Geben Sie einen Namen, eine Organisation und eine Standardgerätegruppe für das Netzwerk an.
4. Geben Sie die Adresse des Netzwerks in den entsprechenden Feldern ein. Wenn Sie nur eine Teiladresse eingeben, wird eine Liste passender Standorte angezeigt, aus der Sie auswählen können. Alternativ können Sie auf der Karte auf den Standort klicken.
5. Klicken Sie auf **Save** (Speichern).
6. Wiederholen Sie die Schritte 1 bis 5 für jedes Netzwerk, das Sie erstellen möchten.

Durchführen der Ersteinrichtung für das Dashboard



KAPITEL 3

Durchführen der Ersteinrichtung von Network Probe

Dieses Kapitel enthält folgende Abschnitte:

Durchführen der Ersteinrichtung von Network Probe

Sie müssen einige Konfigurationsaufgaben erfüllen, um Probe an Ihre Anforderungen anzupassen.

Ermitteln der IP-Adresse von Network Probe

Um die von Probe verwendete IP-Adresse zu finden, verwenden Sie eine der folgenden Methoden:

1. Die IP-Adresse für Network Probe wird standardmäßig per DHCP konfiguriert. Stellen Sie sicher, dass der DHCP-Server aktiv ist und erreicht werden kann. Wenn kein DHCP-Server verfügbar ist, wird die IP-Adresse standardmäßig auf 192.168.1.10 gesetzt.
2. Die Erkennung und der Zugriff auf Network Probe können über das **Cisco FindIT Network Discovery Utility** erfolgen, mit dem automatisch alle unterstützten Cisco Geräte im lokalen Netzwerksegment des Computers ermittelt werden können. Sie können eine Übersicht aller Geräte anzeigen oder das Konfigurationsprogramm starten, um die Einstellungen anzuzeigen und zu konfigurieren. Weitere Informationen finden Sie unter http://www.cisco.com/go/findit.
3. Bei Network Probe ist Bonjour aktiviert, und es erfolgt eine automatische Anzeige über das Bonjour-Protokoll. Wenn Sie über einen Bonjour-fähigen Browser verfügen, können Sie Network Probe im lokalen Netzwerk auch ohne IP-Adresse ermitteln.
4. Wenn Sie das VM-Image verwenden, können Sie die IP-Adresse von Network Probe über die VM-Konsole abrufen. Stellen Sie mithilfe der Verwaltungstools Ihres Hypervisors eine Verbindung zur Konsole des virtuellen Systems her, und melden Sie sich mit dem Standardbenutzernamen (`cisco`) und dem Standardkennwort (`cisco`) an. Unmittelbar nach der Anmeldung werden Sie aufgefordert, das Kennwort zu ändern. Das neue Kennwort sollte ein komplexes Wort aus einem Mix verschiedener Zeichenklassen sein, das in keinem Wörterbuch zu finden ist. Daraufhin wird ein Banner mit der aktuellen IP-Adresse angezeigt.

   Wenn Sie Network Probe unter einer eigenen Installation der Ubuntu oder Raspbian Linux-Distribution installiert haben, können Sie die IP-Adresse mithilfe der Betriebssystemtools ermitteln. Geben Sie hierzu

Durchführen der Ersteinrichtung von Network Probe

beispielsweise den Befehl `ifconfig` in eine Shell-Eingabeaufforderung ein. Es wird eine Liste aller Schnittstellen samt ihren Adressen zurückgegeben.

5. Ermitteln Sie die vom DHCP-Server zugewiesene IP-Adresse, indem Sie auf den Router oder DHCP-Server zugreifen. Weitere Informationen finden Sie in den Anweisungen zu Ihrem DHCP-Server.

Einrichten einer Software Probe

Eine Software Probe ist eine Probe, die in einer virtuellen Maschine oder auf einem Linux-Host ausgeführt wird, wenn kein Dashboard auf derselben VM oder demselben Host ausgeführt wird.

Gehen Sie wie folgt vor, um eine Software Probe einzurichten:

1. Öffnen Sie einen Webbrowser, beispielsweise **Google Chrome** oder **Microsoft Edge**.
2. Geben Sie im Feld **Address** (Adresse) die per DHCP zugewiesene IP-Adresse ein, und drücken Sie dann die **Eingabetaste**.
3. Geben Sie den standardmäßigen Benutzernamen (`cisco`) und das standardmäßige Kennwort (`cisco`) ein. Klicken Sie auf **Login** (Anmelden).
4. Sie werden aufgefordert, das Kennwort für das Benutzerkonto „cisco“ zu ändern. Das neue Kennwort muss mindestens acht Zeichen lang sein und mindestens drei verschiedene Zeichenklassen enthalten. Klicken Sie auf **Save** (Speichern).
5. Geben Sie die Adresse oder den Hostnamen eines Dashboards an, mit dem eine Verbindung hergestellt werden soll, und klicken Sie dann auf **Next** (Weiter).
6. Sie werden im Browser auf die Anmeldeseite des Dashboards weitergeleitet. Melden Sie sich mit den Anmeldeinformationen für das Dashboard an. Sie werden im Browser zurück zu Probe geleitet.
7. Wählen Sie in der Dropdown-Liste aus, ob Sie ein neues Netzwerk erstellen oder ein vorhandenes Netzwerk auswählen möchten. Wenn Sie ein neues Netzwerk erstellen möchten, geben Sie in den bereitgestellten Feldern einen Namen und einen Pfad für das Netzwerk an.

   Sie können die Adresse des Netzwerks in den entsprechenden Feldern eingeben. Wenn Sie nur eine Teiladresse eingeben, wird eine Liste passender Standorte angezeigt, aus der Sie auswählen können. Alternativ können Sie auf der Karte auf den Standort klicken.
8. Klicken Sie auf **Finish** (Fertigstellen).

Einrichten einer eingebetteten Network Probe-Instanz auf einem Produkt der Cisco Serie 100 bis 500

Das Zuordnen einer eingebetteten Probe zum Dashboard erfordert eine explizite Konfiguration auf dem Dashboard und der Probe, bevor eine Verbindung hergestellt werden kann. Dieser Prozess ermöglicht es, das Gerät, das die eingebettete Probe beherbergt, vor der Installation vorzukonfigurieren oder automatisch mit einem Bereitstellungsmechanismus ohne Benutzereingriffe wie Network Plug and Play zu konfigurieren.

Gehen Sie wie folgt vor, um eine eingebettete Probe-Instanz einzurichten:

1. Erstellen Sie mithilfe der Schritte unter Durchführen der Ersteinrichtung für das Dashboard, auf Seite 5 einen neuen Netzwerkdatensatz für die eingebettete Probe-Instanz. Notieren Sie sich den Namen der Organisation und des Netzwerks.
2. Rufen Sie auf der Dashboard-Benutzeroberfläche die Seite **My Profile** (Mein Profil) auf, indem Sie unten im Navigationsbereich auf Ihren Benutzernamen klicken. Verwenden Sie diese Seite, um über die

Durchführen der Ersteinrichtung von Network Probe

Schaltfläche **Generate Access Key** (Zugriffsschlüssel generieren) einen neuen **Zugriffsschlüssel** zu erstellen. Sie können auch einen vorhandenen Zugriffsschlüssel verwenden, wenn Sie dies bevorzugen.

Hinweis Der Zugriffsschlüssel, der für die Zuordnung einer eingebetteten Probe-Instanz zum Dashboard verwendet wird, muss kein langlebiger Schlüssel sein. Dieser Schlüssel muss nur zum Zeitpunkt der ersten Zuordnung gültig sein. Sobald die Probe-Instanz und das Dashboard zugeordnet sind, wird die Verbindung mit Hilfe von eingeschränktem Zugriff und kurzlebigen, für das Netzwerk eindeutigen und regelmäßig neu generierten Zugangsdaten authentifiziert.

3. Navigieren Sie mit Hilfe der Geräte-Benutzeroberfläche zur Konfigurationsseite von Probe und füllen Sie die vorgesehenen Felder aus. Sie müssen mindestens die Konfiguration für die Adresse und den Port des Dashboards, den Namen der Organisation, den Netzwerknamen sowie die ID des Zugriffsschlüssels und die geheimen Zugriffsinformationen angeben. Möglicherweise muss auch das Dashboard-Zertifikat konfiguriert werden. Weitere Informationen finden Sie unten. Optional können Sie auch weitere Änderungen vornehmen.
4. Senden Sie die Änderungen. Die Probe stellt eine Verbindung zum Dashboard her und wird dem in Schritt 1 erstellten Netzwerk zugeordnet.

Überprüfen der Identität des Dashboards

Beim Herstellen einer Verbindung zum Dashboard prüft die Probe, ob das vom Dashboard 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 als vertrauenswürdiges Zertifikat zur Gerätekonfiguration hinzugefügt werden. Einzelheiten zum Hinzufügen eines vertrauenswürdigen Zertifikats finden Sie im Handbuch zur Geräteverwaltung.
- Wenn das Dashboard als IP-Adresse konfiguriert ist, muss entweder das Feld „Common Name“ (Allgemeiner Name) oder das Feld „Subject-Alt-Name“ des Zertifikats diese IP-Adresse enthalten
- Wenn das Dashboard als Hostname konfiguriert ist, muss entweder das Feld „Common Name“ (Allgemeiner Name) oder das Feld „Subject-Alt-Name“ des Zertifikats diesen Hostnamen enthalten

Konfigurieren der grundlegenden Systemeinstellungen im VM-Image mithilfe der webbasierten Benutzeroberfläche (optional)

Gehen Sie wie folgt vor, um grundlegende Systemeinstellungen wie IP-Adressen und Uhrzeiteinstellungen für Network Probe über die Web-Benutzeroberfläche zu konfigurieren:

1. Navigieren Sie zu **Administration** > **Platform Settings** (Verwaltung > Plattformeinstellungen).
2. Geben Sie einen Hostnamen für Network Probe ein. Der Hostname wird verwendet, um die Probe im Netzwerk zu identifizieren.
3. Optional können Sie in den dafür vorgesehenen Feldern Parameter für die statische IP festlegen. Standardmäßig werden die IP-Einstellungen von Network Probe automatisch mittels DHCP festgelegt.

Durchführen der Ersteinrichtung von Network Probe

4. Alternativ können Sie Network Probe so einrichten, dass die interne Uhr als Zeitgeber verwendet wird, oder Ihre bevorzugten NTP-Server angeben. Standardmäßig wird die Uhr von Network Probe mit öffentlichen NTP-Servern synchronisiert.

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

Konfigurieren der grundlegenden Systemeinstellungen im VM-Image mithilfe der Befehlszeile (optional)

Als Alternative zum Konfigurieren der grundlegenden Systemeinstellungen über die Weboberfläche können Sie die Konfiguration mithilfe der Befehlszeile durchführen. Gehen Sie dazu wie folgt vor:

1. Stellen Sie eine Verbindung zur Konsole des virtuellen Systems her.
2. Melden Sie sich mit dem Standardbenutzernamen und -kennwort an. Beide lauten: `cisco`. Unmittelbar nach der Anmeldung werden Sie aufgefordert, das Kennwort zu ändern. Das neue Kennwort sollte ein komplexes Wort aus einem Mix verschiedener Zeichenklassen sein, das in keinem Wörterbuch zu finden ist.
3. Geben Sie den Befehl `sudo config_vm` ein, um die Erstkonfiguration durchzuführen. Vom Dienstprogramm `config_vm` werden Sie in einer Reihe von Schritten zum Ändern der Plattformeinstellungen aufgefordert.
4. Zunächst werden Sie aufgefordert, den Hostnamen für Network Probe zu ändern. Der Hostname wird verwendet, um die Probe im Netzwerk zu identifizieren. Sie können einen aussagekräftigen Namen festlegen oder diesen Schritt überspringen, um den Standardhostnamen beizubehalten.
5. Als Nächstes werden Sie aufgefordert, die Webserver-Ports zu ändern. Wenn diese Ports von den Standardwerten abweichen, müssen Sie möglicherweise auch die Firewall-Einstellungen in Ihrem Netzwerk ändern.
6. Als Nächstes werden Sie aufgefordert, die Netzwerkschnittstelle zu konfigurieren. Sie haben die Wahl zwischen einer statischen Option und DHCP (DHCP ist der Standard). Wenn Sie sich für die statische Option entscheiden, werden Sie zum Eingeben von IP-Adressinformationen, Standardgateways und DNS-Serveradressen aufgefordert. Die Netzwerkschnittstelle wird zurückgesetzt, wenn Sie in diesem Bereich Änderungen vornehmen.
7. Anschließend werden Sie aufgefordert, die Zeiteinstellungen für Probe zu konfigurieren. Sie können einen oder mehrere NTP-Server zur Zeitsynchronisierung konfigurieren (empfohlen) und werden zum Auswählen der Zeitzone aufgefordert.

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

8. Schließlich werden Sie gefragt, ob Sie das Bootloader-Passwort ändern möchten. Der Bootloader-Benutzername und das Kennwort können auf der Konsole beim Systemstart verwendet werden, um den Systemstartprozess zu ändern oder verlorene Betriebssystemkennwörter wiederherzustellen. Die Standard-Anmeldeinformationen für den Bootloader sind: Benutzername: **root**, Kennwort: **cisco**.

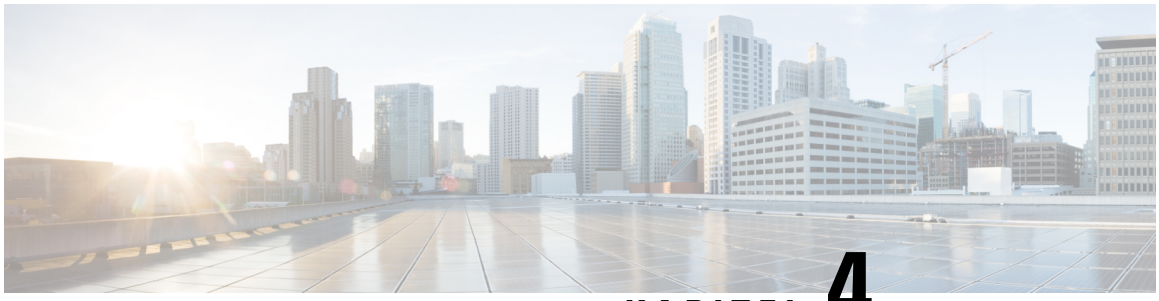
Konfigurieren der grundlegenden Systemeinstellungen, wenn die Probe in ein Cisco Business-Produkt eingebettet ist

Wenn Sie eine in ein Cisco Business-Produkt eingebettete Instanz von Probe verwenden, erfolgt der Zugriff auf die Probe-Benutzeroberfläche über die Benutzeroberfläche zur Geräteadministration. Im Administratorhandbuch zum jeweiligen Gerät finden Sie weitere Informationen zum Zuordnen der Probe zum Dashboard und zum Vornehmen von Änderungen an den Systemeinstellungen.

Konfigurieren der grundlegenden Systemeinstellungen, wenn die Probe-Instanz gemeinsam mit Cisco Business Dashboard gehostet wird

Wenn die Probe-Instanz gemeinsam mit Cisco Business Dashboard oder höher gehostet wird, gibt es keine eigene Probe-Benutzeroberfläche. Die Probe wird dann vollständig über die Dashboard-Benutzeroberfläche verwaltet.

Durchführen der Ersteinrichtung von Network Probe



KAPITEL 4

Durchführen der Ersteinrichtung von direkt verwalteten Geräten

Dieses Kapitel enthält folgende Abschnitte:

Durchführen der Ersteinrichtung von direkt verwalteten Geräten

Direkt verwaltete Geräte sind Netzwerkgeräte, die direkt einem Dashboard zugeordnet werden können und ohne Probe-Instanz im Netzwerk verwaltet werden können. Nur bestimmte Geräte unterstützen das direkte Management. Eine Liste der Geräte und Softwareversionen, die das direkte Management unterstützen, finden Sie im Cisco Business Dashboard – Liste der unterstützten Geräte. Direkt verwaltete Geräte erkennen andere Geräte im breiteren Netzwerk und fügen diese Geräte dem Dashboard-Bestand hinzu. Allerdings ist dieser Erkennungsprozess nicht so umfassend wie der, der von einer Probe-Instanz durchgeführt wird. Die resultierende Netzwerktopologie ist daher möglicherweise weniger genau.

Das Zuordnen eines direkt verwalteten Geräts zum Dashboard erfordert eine explizite Konfiguration auf dem Dashboard und dem Gerät, bevor eine Verbindung hergestellt werden kann. Dieser Prozess ermöglicht es, das Gerät vor der Installation vorzukonfigurieren oder automatisch mit einem Bereitstellungsmechanismus ohne Benutzereingriffe wie Network Plug and Play zu konfigurieren.

Gehen Sie wie folgt vor, um ein direkt verwaltetes Gerät einzurichten:

1. Erstellen Sie einen neuen Netzwerkeintrag für das Netzwerk, in dem das Gerät installiert wird, indem Sie die unter Durchführen der Ersteinrichtung für das Dashboard, auf Seite 5 beschriebenen Schritte ausführen. Notieren Sie sich den Namen der Organisation und des Netzwerks.
2. Rufen Sie auf der **Dashboard**-Benutzeroberfläche die Seite **My Profile** (Mein Profil) auf, indem Sie unten im Navigationsbereich auf Ihren Benutzernamen klicken. Verwenden Sie diese Seite, um über die Schaltfläche **Generate Access Key** (Zugriffsschlüssel generieren) einen neuen **Zugriffsschlüssel** zu erstellen. Sie können auch einen vorhandenen Zugriffsschlüssel verwenden, wenn Sie dies bevorzugen.

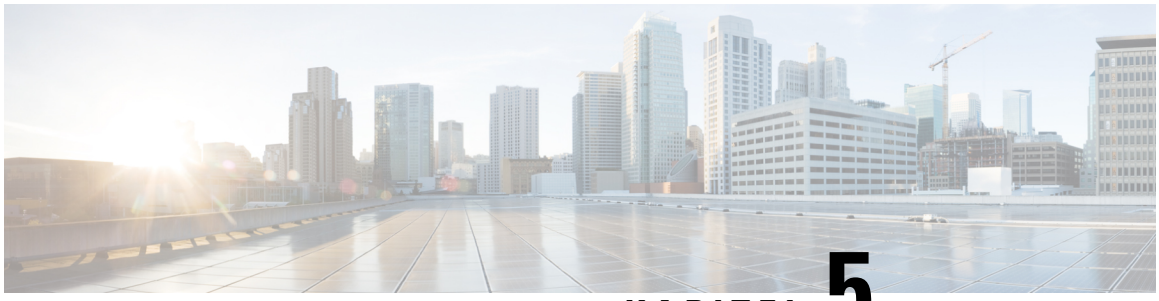
Hinweis Der Zugriffsschlüssel, der für die Zuordnung einer Probe-Instanz zum Dashboard verwendet wird, muss kein langlebiger Schlüssel sein. Dieser Schlüssel muss nur zum Zeitpunkt der ersten Zuordnung gültig sein. Sobald das Gerät und das Dashboard zugeordnet sind, wird die Verbindung mit Hilfe von eingeschränktem Zugriff und kurzlebigen, für das Gerät eindeutigen und regelmäßig neu generierten Zugangsdaten authentifiziert.

Durchführen der Ersteinrichtung von direkt verwalteten Geräten

3. Navigieren Sie mit Hilfe der Geräte-Benutzeroberfläche zur Konfigurationsseite von Cisco Business Dashboard und füllen Sie die vorgesehenen Felder aus. Sie müssen mindestens die Konfiguration für die Adresse und den Port des Dashboards, den Namen der Organisation, den Netzwerknamen sowie die ID des Zugriffsschlüssels und die geheimen Zugriffsinformationen angeben. Möglicherweise muss auch das Dashboard-Zertifikat konfiguriert werden. Weitere Informationen finden Sie unten. Ausführliche Informationen erhalten Sie im Administratorhandbuch für das Gerät.
4. Senden Sie die Änderungen. Das Gerät stellt eine Verbindung zum Dashboard her und wird dem in Schritt 1 erstellten Netzwerk zugeordnet.

Beim Herstellen einer Verbindung zum Dashboard prüft das Gerät, ob das vom Dashboard 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 als vertrauenswürdiges Zertifikat zur Gerätekonfiguration hinzugefügt werden. Einzelheiten zum Hinzufügen eines vertrauenswürdigen Zertifikats finden Sie im Handbuch zur Geräteverwaltung.
- Wenn das Dashboard als IP-Adresse konfiguriert ist, muss entweder das Feld **Common Name** (Allgemeiner Name) oder das Feld **Subject-Alt-Name** des Zertifikats diese IP-Adresse enthalten
- Wenn das Dashboard als Hostname konfiguriert ist, muss entweder das Feld **Common Name** (Allgemeiner Name) oder das Feld **Subject-Alt-Name** des Zertifikats diesen Hostnamen enthalten



KAPITEL 5

Einrichten des Netzwerks

Dieses Kapitel enthält folgende Abschnitte:

Einrichten des Netzwerks für Cisco Business Dashboard

Einrichten von Anmeldeinformationen für Geräte

Damit Cisco Business Dashboard Netzwerkgeräte verwalten kann, müssen Sie gültige Anmeldeinformationen hinterlegen, über die die Anwendung auf die betreffenden Geräte zugreifen kann.

Erkennt Network Probe ein Gerät, werden für den ersten Zugriffsversuch die Standardanmeldeinformationen verwendet. Benutzername und Kennwort lauten dann jeweils `cisco`, und die SNMP-Community lautet `public`. Wenn das Gerät jedoch andere Anmeldeinformationen verwendet, müssen Sie diese wie folgt zur Verfügung stellen:

1. Navigieren Sie zu **Administration** > **Device Credentials** (Verwaltung > Geräteanmeldeinformation). In der ersten Tabelle auf dieser Seite sind alle erkannten Geräte aufgeführt, die Anmeldeinformationen erfordern. In der zweiten Tabelle sind die erkannten Geräte aufgeführt, für die funktionierende Anmeldeinformationen bekannt sind.
2. Geben Sie in den entsprechenden Feldern eine Kombination aus einem Benutzernamen und einem Kennwort und/oder SNMP-Anmeldeinformationen ein. Wenn mehrere Sätze an Anmeldeinformationen erforderlich sind, klicken Sie auf das Plussymbol (+). So können Sie für jeden Anmeldeinformationstyp bis zu drei Angaben machen.
3. Klicken Sie auf **Apply** (Anwenden). Die Anmeldeinformationen werden von Network Probe für alle Geräte getestet, die Anmeldeinformationen erfordern. Zu jedem Gerät werden die richtigen Anmeldeinformationen gespeichert.

   Network Probe erkennt die einzelnen Netzwerke und generiert eine Topologiekarte und einen Bestand für das Netzwerk, wenn funktionierende Anmeldeinformationen zur Verfügung stehen.

Abrufen von Netzwerkinformationen

bietet einen allgemeinen Überblick über Ihr Netzwerk, wahlweise in Form einer Karte oder einer Netzwerkliste. Gehen Sie wie folgt vor, um einen Überblick alle Netzwerke anzuzeigen:

1. Stellen Sie sicher, dass Sie Ihre Probe-Instanzen dem Cisco Business Dashboard wie im vorherigen Kapitel beschrieben zugeordnet haben.
2. Klicken Sie in der Dashboard-Navigation auf **Network** (Netzwerk). Wählen Sie über die Schaltflächen entweder die **Kartenansicht** oder die **Listenansicht** aus
3. In der **Kartenansicht** können Sie die angezeigte Karte mit der Maus in die gewünschte Position ziehen und den angezeigten Kartenausschnitt mithilfe der Plusschaltfläche und der Minusschaltfläche vergrößern bzw. verkleinern. Jedes Netzwerk, in dem Cisco Business Dashboard Probe installiert ist, wird als Symbol auf der Karte angezeigt. Jedes Symbol enthält eine Zahl, die für die Anzahl der ausstehenden Benachrichtigungen zu diesem Netzwerk steht. Die Farbe des Symbols zeigt den höchsten ausstehenden Schweregrad an. Klicken Sie auf ein Symbol, um weitere Informationen über einen Standort anzuzeigen. Wenn mehrere Symbole zu eng nebeneinander liegen, um sie leicht zu unterscheiden, werden sie durch eine Clustermarkierung ersetzt, in der die Anzahl der Netzwerksymbole im jeweiligen Cluster angegeben ist. Klicken Sie auf die Clustermarkierung, um die Ansicht der Standorte in diesem Cluster zu vergrößern.

   In der **Listenansicht** können Sie auf das Symbol oben links in der Tabelle klicken, um auszuwählen, welche Spalten angezeigt werden sollen. Die Tabelleneinträge lassen sich durch Klicken auf die Spaltenüberschriften sortieren.
4. Über das Suchfeld können Sie ein bestimmtes Netzwerk lokalisieren oder herausfinden, in welchem Netzwerk sich ein bestimmtes Gerät befindet. Sie können in das Suchfeld entweder den Namen, die Adresse oder die IP-Adresse eines Netzwerks oder den Namen, die IP-Adresse, die MAC-Adresse oder die Seriennummer eines Geräts eingeben.
5. Wenn Sie auf ein Netzwerk klicken, wird der Bereich **Basic Info** (Basisinformationen) angezeigt. Hier finden Sie weitere Informationen zu dem Netzwerk. Hierzu zählen der Name und die Adresse des Netzwerks sowie ausstehende Benachrichtigungen für dieses Netzwerk.
6. Klicken Sie im Bereich **Basic Info** (Basisinformationen) auf **View** (Anzeigen), um detaillierte Informationen zum Netzwerk anzuzeigen, u. a. das Netzwerktopologiediagramm und die Etagenpläne. Wenn Sie auf **More** (Mehr) klicken, wird die Ansicht **Network Detail** (Netzwerkdetails) geöffnet, in der Sie die Einstellungen für dieses Netzwerk ändern und alle in diesem Netzwerk erkannten Geräte anzeigen können.

Sie können auch aus dem **Bestand** heraus detaillierte Informationen über alle Geräte in Ihrem Netzwerk anzeigen. Auf der Seite **Inventory** (Bestand) finden Sie eine Liste aller erkannten Geräte in tabellarischer Form. Sie können die Liste filtern, um die angezeigten Geräte einzuschränken, und auf einzelne Geräte klicken, um weitere Informationen zu diesem Gerät anzuzeigen.

Anpassen der Topologiekarte (optional)

Sobald gültige Anmeldeinformationen vorhanden sind, führt **Network Probe** die Netzwerkerkennung durch und generiert eine **Topologiekarte**. Sie können die Karte bei Bedarf anpassen.

1. Navigieren Sie zu **Network** (Netzwerk), und wählen Sie das gewünschte Netzwerk aus. Klicken Sie auf **View** (Anzeigen), um die Topologie anzuzeigen.
2. Sie können einzelne Gerätesymbole verschieben, um das Layout zu verbessern. Alle von Ihnen vorgenommenen Änderungen am Layout sind dauerhaft. Von Cisco Business Dashboard werden keine weiteren Änderungen an der Position der Symbole vorgenommen. Wenn Sie die automatische Platzierung

der Symbole wieder aktivieren möchten, klicken Sie auf **Relayout Topology** (Topologielayout aktualisieren).

3. Klicken Sie auf **Overlays**, um den Bereich **Overlays and Filters** (Overlays und Filter) zu öffnen. Legen Sie anschließend mithilfe der Kontrollkästchen fest, welche Gerätetypen im Topologiediagramm angezeigt werden sollen.

Hochladen von Etagenplänen (optional)

Sie können Etagenpläne für die einzelnen Netzwerke hochladen und Ihre Netzwerkgeräte darauf platzieren, um den genauen Standort der Geräte zu dokumentieren. Gehen Sie dazu wie folgt vor:

1. Wenn Sie das Topologiediagramm für ein Netzwerk anzeigen, klicken Sie auf **Floor Plan** (Etagenplan).
2. Geben Sie einen Namen für das Gebäude und die Etage ein, und ziehen Sie dann eine Bilddatei in den Zielbereich, oder klicken Sie in das Widget, um eine Datei von Ihren PC auszuwählen. Unterstützt werden die Bildformate `.png`, .gif und .jpg.
3. Klicken Sie auf **Save** (Speichern), um die Änderungen zu speichern.
4. Um ein Gerät auf dem Etagenplan zu platzieren, klicken Sie auf **Add Devices** (Geräte hinzufügen), und geben Sie im Suchfeld unten im Fenster den Namen oder die IP-Adresse des Geräts ein. Es werden passende Geräte angezeigt. Ausgegraute Geräte wurden bereits auf einem Etagenplan platziert.
5. Klicken Sie auf ein Gerät, und ziehen Sie es auf die richtige Position, um es dem Etagenplan hinzuzufügen.

Anpassen des Überwachungs-Dashboards

Sie können das Überwachungs-Dashboard an Ihre Anforderungen anpassen. Gehen Sie dazu wie folgt vor:

1. Wählen Sie in der Navigation links auf dem Bildschirm die Option **Dashboard** aus. Das Standard-Dashboard wird angezeigt.
2. Um einzelne Widgets innerhalb des Dashboards zu verschieben, klicken Sie auf das Zahnradsymbol oben rechts im Dashboard, und wählen Sie die Option **Edit Mode** (Bearbeitungsmodus) aus. Klicken Sie auf ein Widget, und ziehen Sie es bei gedrückter Maustaste auf die gewünschte Position. Um die Größe eines Widgets zu ändern, klicken Sie auf den Rand oder auf eine Ecke des Widgets, und halten Sie die Maustaste gedrückt.
3. Wenn Sie dem Dashboard ein neues Widget hinzufügen möchten, klicken Sie oben rechts im Dashboard auf das Zahnradsymbol, und wählen Sie die Option zum Hinzufügen eines Widgets aus. Wählen Sie das gewünschte Widget in der Liste aus. Um ein Widget aus dem Dashboard zu entfernen, klicken Sie im Bearbeitungsmodus in der oberen rechten Ecke des Dashboards auf das Symbol **Remove Widget** (Widget entfernen) (✖).
4. Wenn das Dashboard wunschgemäß angeordnet ist, klicken Sie auf das Zahnradsymbol oben rechts im Dashboard, und wählen Sie **View Mode** (Ansichtsmodus) aus, um die Änderungen zu fixieren.
5. Um das Verhalten eines Widgets zu ändern, klicken Sie oben rechts im Widget auf das Symbol **Widget-Konfiguration bearbeiten**. Wählen Sie aus den Dropdown-Menüs das vom Widget zu überwachende Gerät, die Schnittstelle oder das Netzwerk aus.

Konfigurieren der E-Mail-Einstellungen (optional)

Cisco Business Dashboard kann Ihnen eine E-Mail-Benachrichtigung senden, sobald bestimmte Ereignisse im Netzwerk eintreten. Wie Sie steuern können, bei welchen Ereignisse eine E-Mail generiert wird, ist unter Anpassen der Benachrichtigungsanzeige, auf Seite 22 beschrieben. Gehen Sie wie folgt vor, um die E-Mail-Einstellungen zu konfigurieren:

1. Navigieren Sie zu **System** > **Email Settings** (System > E-Mail-Einstellungen).
2. Auf dieser Seite können Sie den E-Mail-Server und den Port für ausgehende Nachrichten, Verschlüsselungs- und Authentifizierungseinstellungen sowie die zu verwendende E-Mail-Adresse festlegen.
3. Wenn Sie mit der Konfiguration fertig sind, klicken Sie auf **Save** (Speichern).
4. Klicken Sie auf **Test Connectivity** (Verbindung testen), um die vorgenommenen Änderungen zu testen.

Anpassen der Benachrichtigungsanzeige

Gehen Sie wie folgt vor, um das Verhalten von Benachrichtigungen anzupassen:

1. Navigieren Sie zu **Administration** > **Organizations** (Verwaltung > Organisation), und wählen Sie die Organisation aus, für die Sie das Benachrichtigungsverhalten anpassen möchten.
2. Klicken Sie auf **Notification** (Benachrichtigung).
3. Deaktivieren Sie das Kontrollkästchen **Inherit from Notification Defaults** (Übernehmen von Benachrichtigungs-Standardeinstellungen). Legen Sie mithilfe der Kontrollkästchen fest, welche Benachrichtigungen als Popup-Fenster auf der Benutzeroberfläche angezeigt werden sollen und welche Benachrichtigungen als E-Mail gesendet werden sollen. Wenn Sie E-Mail-Benachrichtigungen festlegen, achten Sie darauf, dass die E-Mail-Einstellungen richtig konfiguriert sind. Näheres dazu finden Sie unter Konfigurieren der E-Mail-Einstellungen (optional), auf Seite 22.
4. Klicken Sie auf **Save** (Speichern).

Sie können die **Benachrichtigungs-Standardeinstellungen** auch unter **Administration** > **Notification Defaults** (Verwaltung > Benachrichtigungs-Standardeinstellungen) anpassen.

Einrichten von Network Plug and Play

Cisco Business Dashboard stellt einen Cisco Network Plug and Play-Service bereit, über den Sie Firmware und Konfigurationsdateien für ausgewählte Cisco Geräte zentral verwalten können. Weitere Informationen über Network Plug and Play finden Sie in der Lösungs-Anleitung zu PnP.

Gehen Sie wie nachfolgend beschrieben vor, um Network Plug and Play einzurichten.

Hochladen von Firmware

1. Navigieren Sie zu **Network Plug and Play** > **Images**.
2. Klicken Sie auf das Plussymbol (✚).
3. Wählen Sie eine Organisation aus. Ziehen Sie dann eine Firmware-Datei 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.

4. 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. Aktivieren Sie in der Tabelle **Images** das Kontrollkästchen des Image, und klicken Sie auf **Edit** (Bearbeiten).
2. 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.
3. Klicken Sie auf **Save** (Speichern).

Hochladen von Konfigurationen (Optional)

1. Navigieren Sie zu **Network Plug and Play** > **Configurations** (Konfigurationen).
2. Klicken Sie auf das Plussymbol (✚).
3. Wählen Sie eine Organisation aus. Ziehen Sie dann 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.
4. Klicken Sie auf **Upload** (Hochladen).

Anstatt Konfigurationen hochzuladen, können Sie die im Lieferumfang der Dashboard-Anwendung enthaltenen Konfigurationsvorlagen verwenden. Bei Bedarf können Sie auf den Namen der Konfigurationsdatei klicken, um deren Inhalte zu sehen.

Einrichten der Erkennung

Damit Netzwerkgeräte **Network Plug and Play** verwenden können, müssen sie zunächst den **Network Plug and Play**-Server erkennen. Die Informationen zum Server können den Geräten mithilfe von drei Mechanismen bereitgestellt werden:

1. **DHCP**: Das Netzwerkgerät kann die Adresse des Network Plug and Play-Servers aus der DHCP-Option 43 extrahieren. Nähere Informationen zum Optionsformat finden Sie im Administratorhandbuch für Cisco Business Dashboard, im Abschnitt *Allgemeines zu Network Plug and Play*.
2. **DNS**: Kann das Netzwerkgerät die Serveradresse nicht mittels DHCP abrufen, wird ein Lookup eines bekannten Hostnamens (pnpserver) in der lokalen Domäne versucht, beispielsweise *pnpserver.example.com*. Sie können Ihre DNS-Infrastruktur so konfigurieren, dass dieser Name in die Adresse von Cisco Business Dashboard aufgelöst wird.
3. **Plug and Play Connect**: Cisco stellt mit **Plug and Play Connect** einen Weiterleitungsservice bereit, den das Gerät abfragt, falls es die Adresse des Servers auf anderem Weg nicht abrufen kann. Wie Sie den Weiterleitungsservice für Ihr Netzwerk einrichten können, erfahren Sie unter Plug and Play Connect.

Registrieren von Geräten

Gehen Sie wie folgt vor, um während der Installationsvorbereitung Geräte zu registrieren:

1. Navigieren Sie zu **Network Plug and Play** > **Enabled Devices** (Aktivierte Geräte).
2. Klicken Sie auf das Plussymbol (✚).

3. Geben Sie den Namen, die Produkt-ID (PID) und die Seriennummer des zu registrierenden Geräts ein, und wählen Sie aus den Dropdown-Listen eine Organisation, ein Netzwerk, eine Gerätegruppe und einen Gerätetyp aus.
4. Sie können ein Firmware-Image, eine Konfigurationsdatei oder beides für das Gerät auswählen. Wenn Sie als Image „Standard-Image“ auswählen, verwendet das Gerät das für den jeweiligen Gerätetyp als Standard-Image festgelegte Image, sobald es sich mit dem Server verbindet.
5. Klicken Sie auf **Save** (Speichern).

Automatisches Anfordern von Geräten

Ein Gerät, das zwar mit dem Server verbunden, jedoch nicht im Bestand vorhanden ist, wird als nicht beanspruchtes Gerät angesehen. 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 Plussymbol (✚).
3. Geben Sie die Produkt-ID (PID) ein, um das Gerät automatisch zu beanspruchen, und wählen Sie aus den Dropdown-Listen eine Organisation, ein Netzwerk, eine Gerätegruppe und einen Gerätetyp aus.
4. Sie können ein Firmware-Image, eine Konfigurationsdatei oder beides für die Produkt-ID auswählen. Wenn Sie als Image „Standard-Image“ auswählen, verwenden automatisch angeforderte Geräte das für den jeweiligen Gerätetyp als Standard-Image festgelegte Image, sobald sie sich mit dem Server verbinden.
5. Klicken Sie auf **Save** (Speichern).

Konfiguration des Netzwerks

Die Installation eines neuen Netzwerks ist eine günstige Gelegenheit, um die Erstkonfiguration des Netzwerks durchzuführen. Auch bei einem bestehenden Netzwerk bieten sich zu diesem Zeitpunkt u. U. Konfigurationsänderungen an.

Aktualisieren der Firmware von Geräten (optional)

Sie werden vom Dashboard benachrichtigt, wenn Firmware-Updates für die Geräte im Netzwerk verfügbar sind. In verschiedenen Bereichen der Benutzeroberfläche wird zudem neben dem jeweiligen Gerät das Symbol **Update Firmware** (Firmware aktualisieren) angezeigt.

Gehen Sie wie folgt vor, um die Firmware eines einzelnen Geräts zu aktualisieren:

1. Klicken Sie in der **Topologiekarte** auf ein Gerät, um den Bereich **Basic Info** (Basisinformationen) anzuzeigen.
2. Öffnen Sie den Bereich **Action** (Aktion), und klicken Sie auf die Schaltfläche **Upgrade firmware to latest** (Firmwareupgrade auf neueste Version). Das Dashboard lädt die benötigte Firmware von Cisco herunter und wendet das Update auf das Gerät an. Während des Prozesses wird das Gerät neu gestartet.

   Alternativ können Sie die Firmware über Ihren PC aktualisieren, indem Sie auf die Option **Upgrade From Local** (Upgrade aus lokaler Quelle) klicken und das Firmware-Image für den Upload angeben.

3. Um den Fortschritt des Upgrades zu verfolgen, klicken Sie oben rechts in der Benutzeroberfläche auf das Symbol **Task Status** (Aufgabenstatus).

Sie können auch mehrere Einzelgeräte über die Ansicht **Inventory** (Bestand) aktualisieren. Weitere Informationen finden Sie im Abschnitt *Anzeigen des Gerätebestands* im Cisco Business Dashboard-Administratorhandbuch.

Aktualisieren der Firmware für ein Netzwerk

Gehen Sie wie folgt vor, wenn ein ganzes Netzwerk auf die neueste Firmware aktualisiert werden soll:

1. Öffnen Sie die **Topologiekarte** für das Netzwerk, das Sie aktualisieren möchten.
2. Klicken Sie oben auf der Seite auf **Network Actions** (Netzwerkaktionen), und wählen Sie die Option **Upgrade Firmware** (Firmware aktualisieren) aus. Das Dashboard lädt für alle Geräte, für die Updates verfügbar sind, die benötigten Firmware-Dateien von Cisco herunter und wendet das Update nacheinander auf die Geräte an. Während des Prozesses werden die Geräte neu gestartet.
3. Um den Fortschritt des Upgrades zu verfolgen, klicken Sie oben rechts in der Benutzeroberfläche auf das Symbol **Task Status** (Aufgabenstatus).

Konfigurieren von Gerätegruppen

Beim Dashboard werden Gerätegruppen verwendet, damit Sie Konfigurationen auf mehrere Geräte gleichzeitig anwenden können, und um sicherzustellen, dass die Konfigurationseinstellungen im gesamten Netzwerk aufeinander abgestimmt sind. Gehen Sie wie folgt vor, um Geräte einer Gerätegruppe zuzuweisen:

1. Navigieren Sie zu **Administration** > **Device Groups** (Verwaltung > Gerätegruppen).
2. Klicken Sie auf das Plussymbol (✚), um eine neue Gruppe hinzuzufügen.
3. Geben Sie eine Organisation, einen Namen und eine Beschreibung für die Gerätegruppe an. Klicken Sie auf **Save** (Speichern).
4. Um der Gerätegruppe Geräte hinzuzufügen, klicken Sie in der Tabelle **Devices** (Geräte) auf das Pluszeichen (✚). Suchen Sie mit dem Suchfeld nach Geräten, die der Gruppe hinzugefügt werden sollen. Wählen Sie ein oder mehrere Geräte aus, die der Gruppe hinzugefügt werden sollen. Jedes Gerät kann nur zu einer einzigen Gruppe gehören. Wenn ein ausgewähltes Gerät zuvor Mitglied einer anderen Gruppe war, wird es aus dieser Gruppe entfernt. Wenn Sie ein Gerät aus der Gruppe entfernen möchten, klicken Sie neben dem Gerät auf das Symbol **Delete** (Löschen). Das Gerät wird dann in die Gerätegruppe **Default** (Standard) verschoben. Gerätegruppen können Geräte verschiedener Art enthalten.

Erstellen von Konfigurationsprofilen

Mit dem Dashboard können Sie auf einfache Weise gängige Konfigurationen auf mehrere Netzwerkgeräte übertragen. Sie können mit dem **Assistenten für die Netzwerkkonfiguration** Konfigurationsprofile für die verschiedenen Abschnitte der Konfiguration erstellen oder Einzelprofile einrichten. Gehen Sie wie folgt vor, um den **Assistenten für die Netzwerkkonfiguration** zu nutzen:

1. Navigieren Sie zu **Network Configuration** > **Wizard** (Netzwerkkonfiguration > Assistent).
2. Geben Sie einen Profilnamen für die zu erstellenden Konfigurationsprofile ein, wählen Sie eine Organisation aus, und wählen Sie dann eine oder mehrere Gerätegruppen aus, auf die die Konfiguration angewendet werden soll.

3. Klicken Sie auf **Next** (Weiter).
4. Legen Sie die Zeiteinstellungen für die Gruppe fest. Ein Profil für das **Zeitmanagement** enthält Einstellungen für die Zeitzone, für den Wechsel zwischen Sommer- und Winterzeit sowie für NTP. Wenn Sie zu dieser Gruppe kein Profil für das **Zeitmanagement** erstellen möchten, klicken Sie auf **Skip** (Überspringen). Klicken Sie anderenfalls auf **Next** (Weiter).
5. Legen Sie die **DNS-Einstellungen** für die Gruppe fest. Ein Profil für **DNS-Resolver** enthält Einstellungen für den Domänennamen und die zu verwendenden DNS-Server. Wenn Sie zu dieser Gruppe kein Profil für DNS-Resolver erstellen möchten, klicken Sie auf **Skip** (Überspringen). Klicken Sie anderenfalls auf **Next** (Weiter).
6. Legen Sie die Benutzerauthentifizierungseinstellungen für die Gruppe fest. Ein **Authentifizierungsprofil** enthält Einstellungen für die lokale Benutzerdatenbank der Geräte. Wenn Sie zu dieser Gruppe kein **Authentifizierungsprofil** erstellen möchten, klicken Sie auf **Skip** (Überspringen). Klicken Sie anderenfalls auf **Next** (Weiter).
7. Geben Sie die virtuellen LANs an, die für diese Gruppe erstellt werden sollen. Ein VLAN-Profil enthält die Details für ein oder mehrere VLANs. Wenn Sie kein VLAN-Profil erstellen möchten, klicken Sie auf **Skip** (Überspringen). Um mehrere VLANs hinzuzufügen, klicken Sie nach Fertigstellung der VLANs jeweils auf **Add Another** (Weitere hinzufügen). Klicken Sie auf **Next** (Weiter).
8. Geben Sie die Wireless LANs an, die für diese Gruppe erstellt werden sollen. Ein Wireless LAN-Profil enthält die Details für eine oder mehrere SSIDs. Wenn Sie kein Wireless LAN-Profil erstellen möchten, klicken Sie auf **Skip** (Überspringen). Um mehrere SSIDs hinzuzufügen, klicken Sie nach Fertigstellung der SSIDs jeweils auf **Add Another** (Weitere hinzufügen). Klicken Sie auf **Next** (Weiter).
9. Prüfen Sie die vorgenommenen Konfigurationseinstellungen. Wenn Sie Änderungen vornehmen möchten, klicken Sie auf **Edit** (Bearbeiten) oder auf **Back** (Zurück), um zum gewünschten Fenster zurückzukehren. Wenn die Einstellungen Ihren Wünschen entsprechen, klicken Sie auf **Finish** (Fertigstellen), um die Profile zu erstellen und sie auf die Geräte aus den ausgewählten Gerätegruppen anzuwenden.
10. Um den Fortschritt der Konfiguration zu verfolgen, klicken Sie im oberen rechten Bereich der Benutzeroberfläche auf das Symbol **Task Status** (Aufgabenstatus).

Sichern von Gerätekonfigurationen

Mit dem Dashboard können Sie die Konfigurationen Ihrer Netzwerkgeräte sichern. Gehen Sie wie folgt vor, um die Konfiguration eines einzelnen Geräts zu sichern:

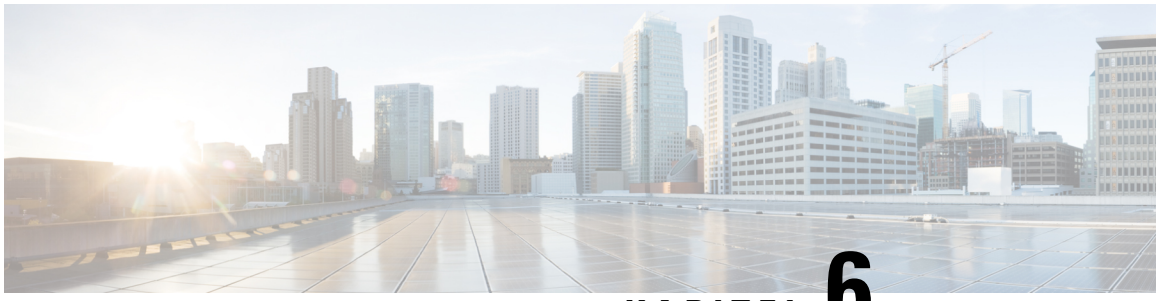
1. Klicken Sie in der **Topologiekarte** auf ein Gerät, um den Bereich **Basic Info** (Basisinformationen) anzuzeigen.
2. Öffnen Sie den Bereich **Action** (Aktion), und klicken Sie auf die Schaltfläche **Backup Configuration** (Konfiguration sichern). Optional können Sie im angezeigten Fenster einen Hinweis hinzufügen, der das Backup beschreibt. Das **Dashboard** kopiert die Konfiguration des Geräts.
3. Um den Fortschritt des Backups zu verfolgen, klicken Sie im oberen rechten Bereich der Benutzeroberfläche auf das Symbol **Task Status** (Aufgabenstatus).

Sie können Geräte auch einzeln sichern, indem Sie in der Ansicht **Inventory** (Bestand) auf die Option **Backup Configuration** (Konfiguration sichern) klicken.

Gehen Sie wie folgt vor, um die Konfigurationen des gesamten Netzwerks zu sichern:

1. Öffnen Sie die **Topologiekarte** für das Netzwerk, das Sie sichern möchten.

2. Klicken Sie oben auf der Seite auf die Schaltfläche **Actions** (Aktionen), und wählen Sie die Option **Backup Configurations** (Konfigurationen sichern) aus. Optional können Sie im angezeigten Fenster einen Hinweis hinzufügen, der das Backup beschreibt. Das Dashboard kopiert die Konfiguration der einzelnen Geräte.
3. Um den Fortschritt des Backups zu verfolgen, klicken Sie im oberen rechten Bereich der Benutzeroberfläche auf das Symbol **Task Status** (Aufgabenstatus).



KAPITEL 6

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 1: 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 2: 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.