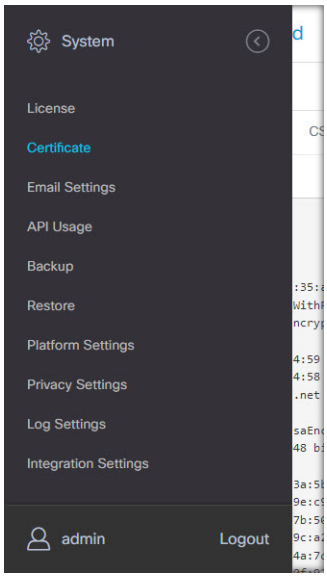
System

Dieses Kapitel enthält folgende Abschnitte:

Informationen zu „System“

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



Dieser Abschnitt ist in die folgenden Seiten unterteilt:

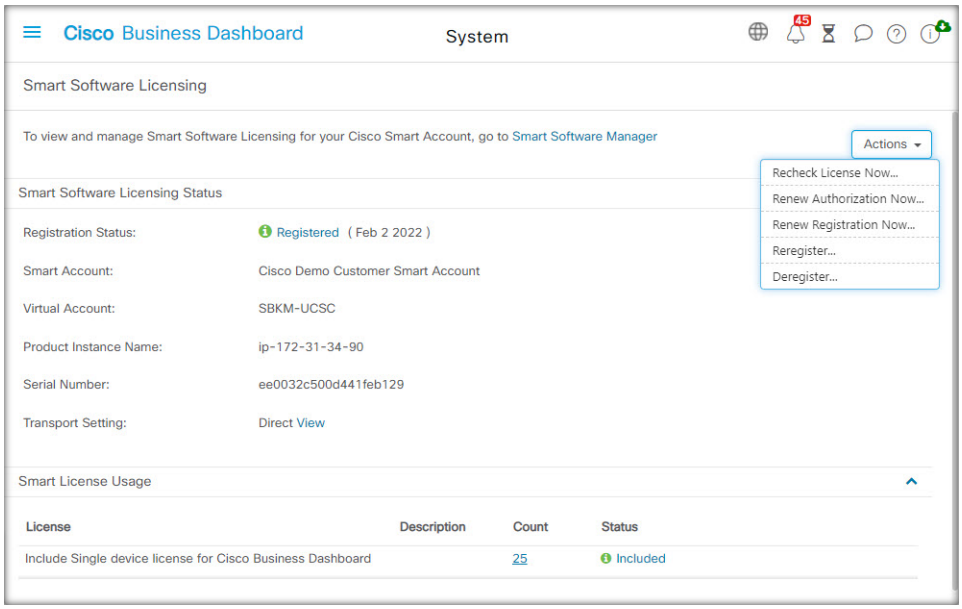
Name der Seite	Seitenfunktion
Lizenz	Verwalten der Softwarelizenzen für das Dashboard.
Zertifikat	Verwalten von Sicherheitszertifikaten im Dashboard.
E-Mail-Einstellungen	Einrichten von E-Mails ein und verwalten der Einstellungen.
API-Nutzung	Überwachen der Nutzung der Cisco Business Dashboard-API.
Backup	Sichern der Konfiguration und anderer Daten für das Dashboard.
Wiederherstellen	Wiederherstellen der Konfiguration und anderer Daten für das Dashboard.
Plattformeinstellungen	Verwalten der Netzwerkkonfiguration für das Dashboard.
Datenschutzeinstellungen	Steuern der Daten, die mit Cisco geteilt werden können.
Protokolleinstellungen	Ändern der Protokolleinstellungen für das Dashboard.
Lokaler Test	Verwalten einer im Dashboard gehosteten Probe-Instanz.
Integrationseinstellungen	Verwalten der Integration von Cisco Business Dashboard in externe Anwendungen.

Hinweis 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. Wenn Sie über bis zu 25 Geräte verfügen, ist keine zusätzliche Lizenzierung erforderlich. 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-Lizenzverwendung**

  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 Header 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).

Dashboard bei Ihrem Smart Account registrieren

Führen Sie die folgenden Schritte aus, 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.

3. Klicken Sie auf die Registerkarte **General** (Allgemein).

4. 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.
5. Klicken Sie auf **Create Token** (Token erstellen).
6. 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.
7. Wechseln Sie zur Benutzeroberfläche von Cisco Business Dashboard, und klicken Sie auf **System** > **License** (System >Lizenz).
8. Klicken Sie auf die Schaltfläche **Register** (Registrieren), und fügen Sie das Token in das dafür vorgesehene Feld ein.
9. 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.

Dashboards aus Ihrem Smart Account entfernen

Führen Sie die folgenden Schritte aus, 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. Führen Sie die folgenden Schritte aus, 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 überprüfen) aus. 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. Führen Sie die folgenden Schritte aus, 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. Führen Sie die folgenden Schritte aus, 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. Führen Sie die folgenden Schritte aus, um eine Dashboard-Instanz in ein anderes Konto zu verschieben.

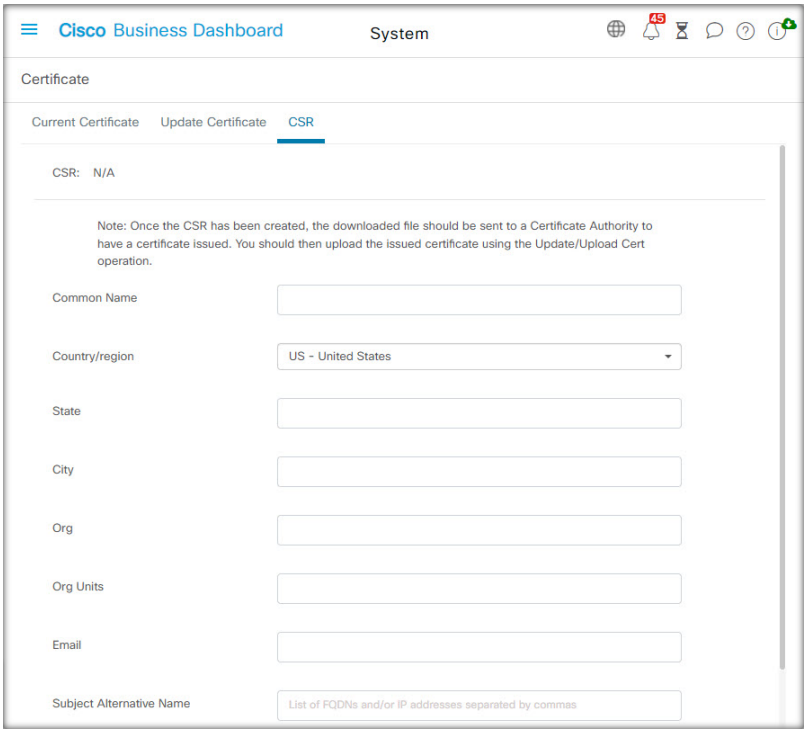
1. Wechseln Sie zur Benutzeroberfläche von Cisco Business Dashboard, und klicken Sie auf **System** > **License** (System >Lizenz).
2. Wählen Sie oben rechts aus der Dropdown-Liste die Option **Reregister...** (Erneut registrieren) aus.
3. Geben Sie das neue Registrierungstoken in das dafür vorgesehene 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.

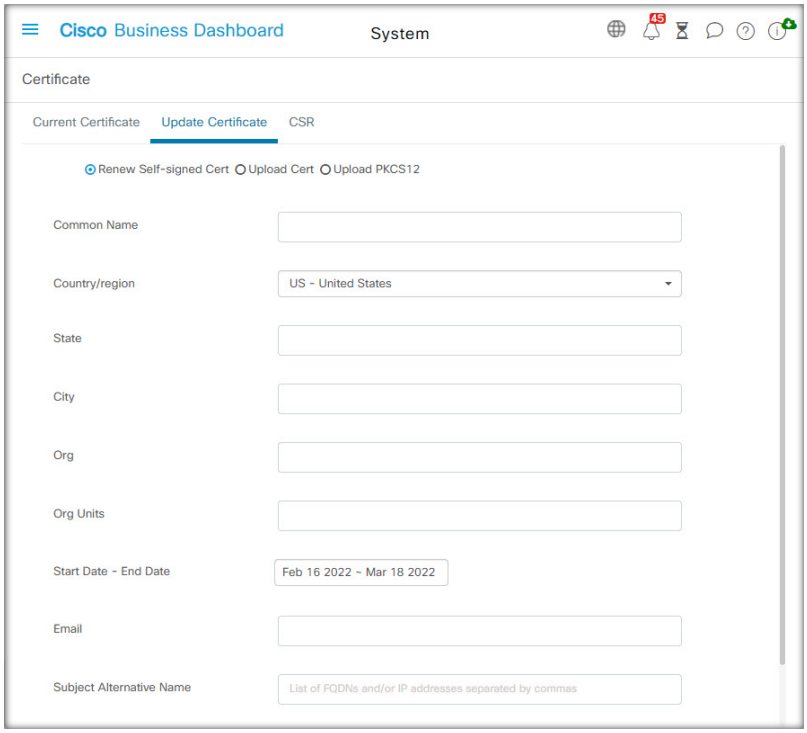
Alternativ können Sie ein Zertifikat samt zugehörigem privatem Schlüssel auch vollkommen unabhängig vom Dashboard erstellen. Dann können Sie das Zertifikat und den privaten Schlüssel vor dem Upload in einer Datei im PKCS#12-Format zusammenfassen.

Eine Zertifikatsignieranforderung (Certificate Signing Request, CSR) erstellen



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.

Ein neues Zertifikat hochladen



Führen Sie die folgenden Schritte aus, um über die Administrations-GUI ein neues Zertifikat 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.

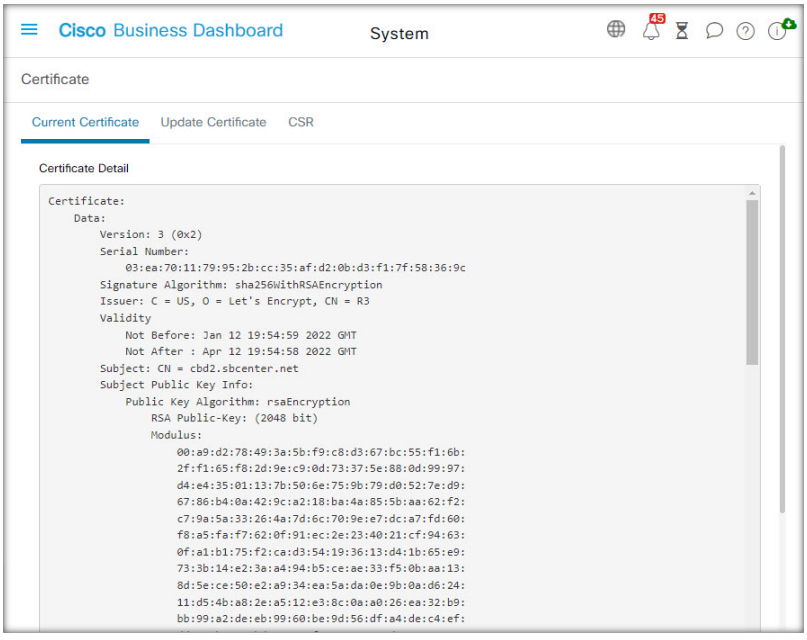
Selbstsigniertes Zertifikat neu generieren

Führen Sie die folgenden Schritte aus, 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).

Aktuelles Zertifikat anzeigen

Führen Sie die folgenden Schritte aus, um das aktuelle Zertifikat anzuzeigen.



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

Führen Sie die folgenden Schritte aus, um eine Kopie des aktuellen Zertifikats 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 Domain-validiertes Zertifikat von der **Zertifizierungsstelle von Let's Encrypt** (https://letsencrypt.org) anfordern und erneuern. In Version 2.5.0 können diese Zertifikate über die Administrationsseite gemanagt werden.

Wichtig Sie müssen über einen vollständig qualifizierten Domain-Namen und einen DNS-Eintrag verfügen, der auf die öffentliche IP-Adresse verweist. Weitere Informationen finden Sie unter Verwalten der Plattformeinstellungen, auf Seite 15.

Gehen Sie wie folgt vor, um ein Let's Encrypt-Zertifikat über die Administrations-GUI hochzuladen:

1. Navigieren Sie zu **System** > **Certificate** (System > Zertifikat), und wählen Sie die Registerkarte „Update Certificate“ (Zertifikat aktualisieren) aus.
2. Aktivieren Sie die Optionsschaltfläche *Let's Encrypt Certificate* (Let's Encrypt-Zertifikat).
3. Aktivieren Sie das Kontrollkästchen, um die Verwendung eines Let's Encrypt-Zertifikats zu aktivieren.
4. Geben Sie einen oder mehrere vollqualifizierte Domänennamen in die dafür vorgesehenen Felder ein. Die Namen müssen im Domain Name System (DNS) definiert und in die Adresse des Cisco Business Dashboard-Servers aufgelöst werden.
5. Geben Sie eine E-Mail-Adresse an, die für dringende Verlängerungs- und Sicherheitshinweise verwendet werden soll.
6. Lesen Sie die Let's Encrypt-Abonnentenvereinbarung über den bereitgestellten Link, und aktivieren Sie dann das Kontrollkästchen, um die Vereinbarung zu akzeptieren.
7. Optional können Sie das entsprechende Kontrollkästchen aktivieren, wenn die E-Mail-Adresse an die Electronic Frontier Foundation (https://www.eff.org) weitergegeben werden darf.
8. Klicken Sie auf die Schaltfläche „Get Certificate“ (Zertifikat abrufen).

Das Dashboard kontaktiert die Let's Encrypt-Zertifizierungsstelle und ruft mithilfe der HTTP-Verifizierungsmethode ein Zertifikat ab. Die Seite wird aktualisiert und zeigt die Details des Zertifikats sowie das Ablaufdatum an. Das Zertifikat wird etwa 30 Tage vor Ablauf automatisch verlängert.

Wenn Sie das Zertifikat zu einem beliebigen Zeitpunkt aktualisieren müssen, gehen Sie folgendermaßen vor:

1. Navigieren Sie zu **System** > **Certificate** (System > Zertifikat), und wählen Sie die Registerkarte **Update Certificate** (Zertifikat aktualisieren) aus.
2. Aktivieren Sie die Optionsschaltfläche **Let's Encrypt Certificate** (Let's Encrypt-Zertifikat).

3. Verwenden Sie die bereitgestellten Kontrollkästchen und Felder, um die Namen zu aktualisieren, die auf das Zertifikat angewendet werden sollen.

   Sie können die Kontaktdetails jedoch auch unten auf dem Bildschirm aktualisieren.

4. Klicken Sie auf die Schaltfläche „Get Certificate“ (Zertifikat abrufen).

Sie können auch die Neugenerierung des Zertifikats vor der normalen Verlängerungszeit erzwingen, indem Sie die Felder auf der Seite unverändert lassen und auf die Schaltfläche „Force Renewal“ (Verlängerung erzwingen) klicken.

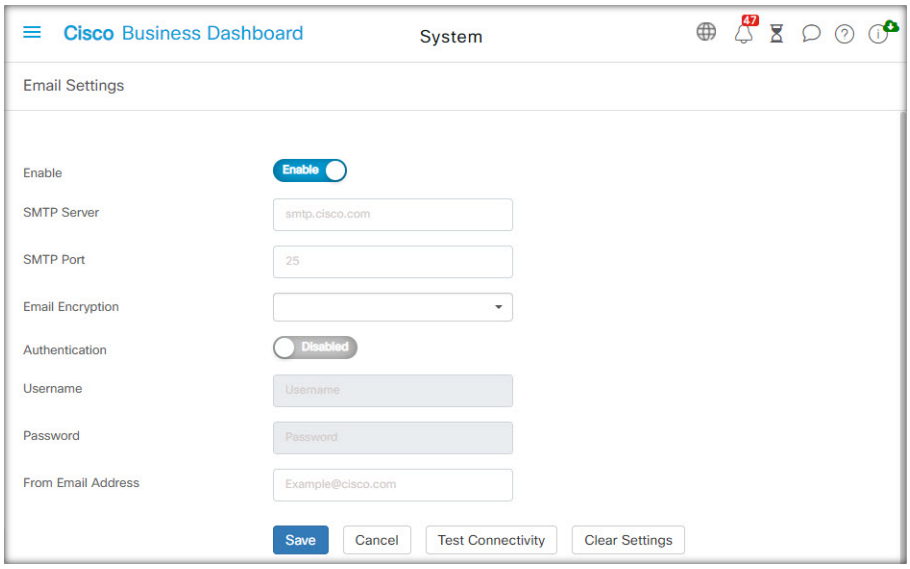
Gehen Sie wie folgt vor, um ein Let's Encrypt-Zertifikat über die Kommandozeile hochzuladen:

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 15 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.



Greifen Sie auf diese Seite zu, um folgende Parameter festzulegen.

Feld	Beschreibung
SMTP-Server	Domain-Name oder IP-Adresse des zu verwendenden SMTP-Servers
SMTP-Port	Zum Senden von E-Mails zu verwendender TCP-Port
E-Mail-Verschlüsselung	Die zu verwendende Verschlüsselungsmethode, darunter: • 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

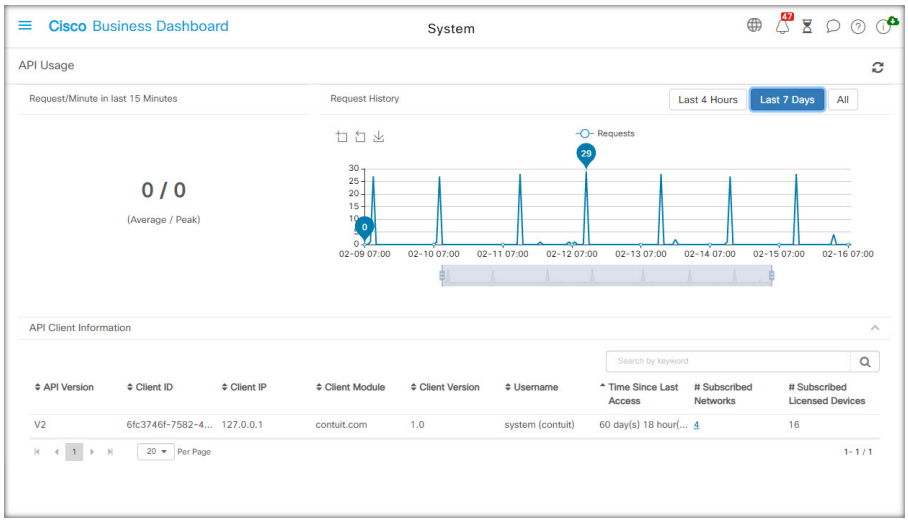
Um die Konfiguration zu testen, klicken Sie auf **Test Connectivity** (Verbindung testen). Dadurch wird eine Ziel-E-Mail-Adresse angefordert, und es wird eine Test-E-Mail an die angegebene Adresse generiert.

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.

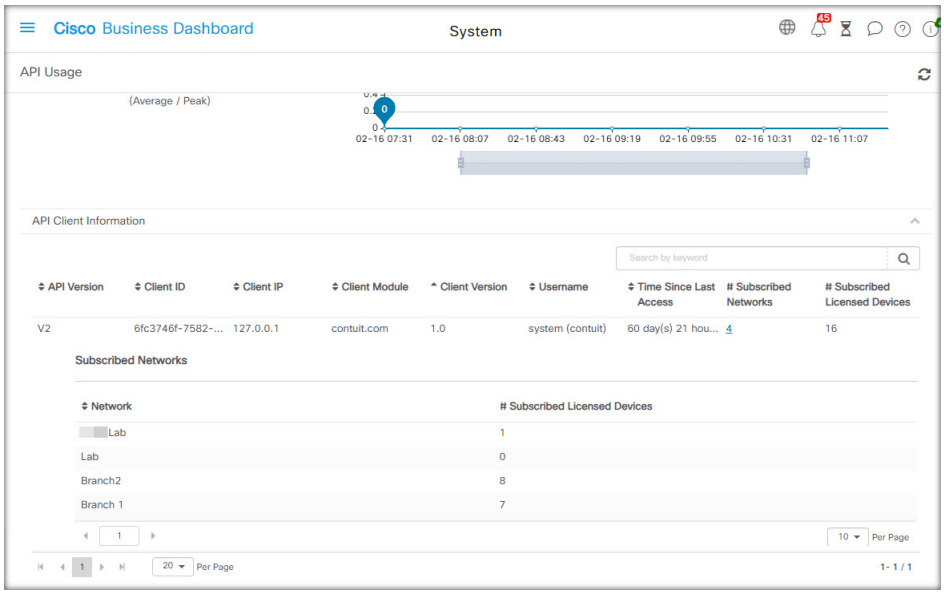
- Diagramm **Request History** (Anforderungsverlauf): Zeigt ein Diagramm der Anforderungsaktivität im zeitlichen Verlauf an. Sie können Zeiträume der letzten vier Stunden, der letzten sieben Tage oder aller verfügbaren Informationen auswählen. Sie können dann die Schieberegler unter dem Diagramm verwenden, 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.



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.
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.

Feld	Beschreibung
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.



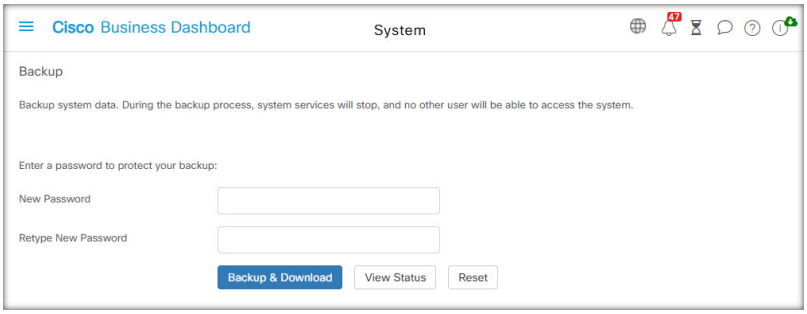
Feld	Beschreibung
Vermittlung	Der Name des vom Client überwachten Netzwerks
Anz. abonnierte lizenzierte Geräte	Die Anzahl der verwalteten Geräte in diesem Netzwerk, für die Ereignisbenachrichtigungen gesendet werden

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.

Eine Backup-Datei von Cisco Business Dashboard kann auf einem System wiederhergestellt werden, auf dem die gleiche Version wie auf dem gesicherten System ausgeführt wird oder eine Version, die um eine Nebenversion aktueller ist. So kann beispielsweise ein Backup, das von einem System mit Version 2.2.0 erstellt wurde, auf einem System mit Version 2.3.1 wiederhergestellt werden, jedoch nicht auf einem System mit Version 2.4.0.

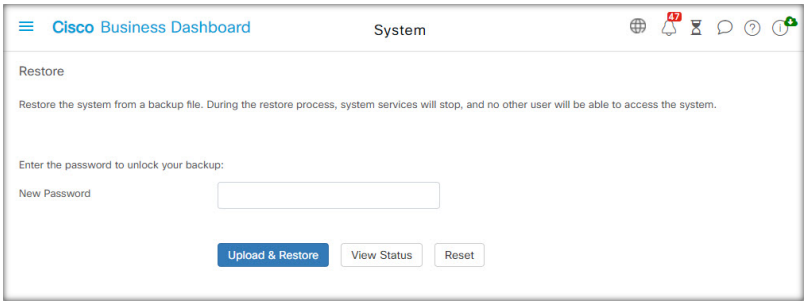
Führen Sie die folgenden Schritte aus, um ein Backup durchzuführen.



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.

Führen Sie die folgenden Schritte aus, 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 Backup-Datei per Drag-and-Drop in den Zielbereich ziehen oder in den Zielbereich klicken, um eine Datei im Dateisystem Ihres PCs anzugeben. Klicken Sie auf **Restore** (Wiederherstellen), um fortzufahren.

Wenn die Dashboard-Version 2.5.0 oder höher ist, wird die Anwendung nach Abschluss des Wiederherstellungsvorgangs neu gestartet.

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.

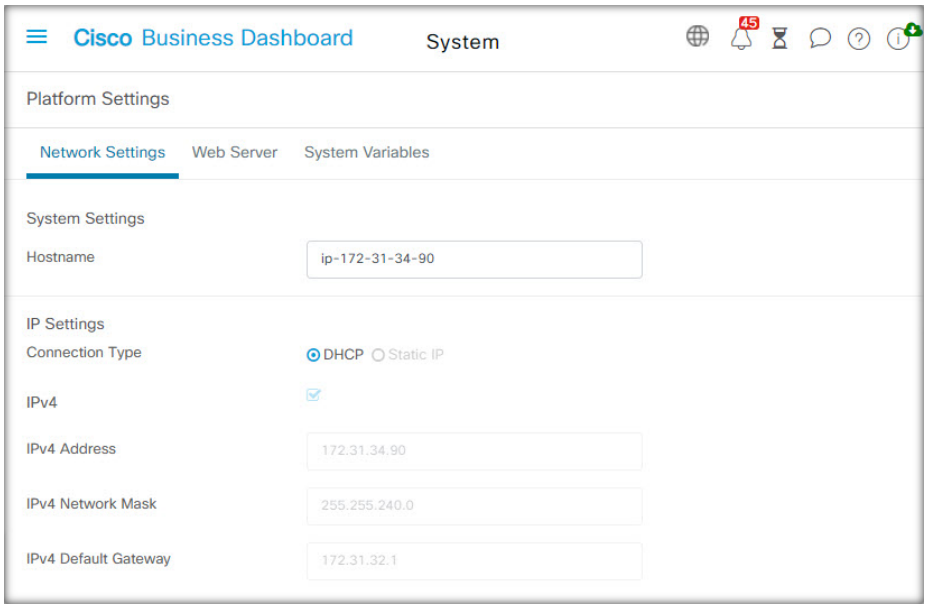
Die Plattformeinstellungen sind in drei Gruppen unterteilt

- Netzwerkeinstellungen
- Webserver
- Systemvariablen

In den folgenden Abschnitten werden die auf den einzelnen Registerkarten verfügbaren Einstellungen beschrieben.

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

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.

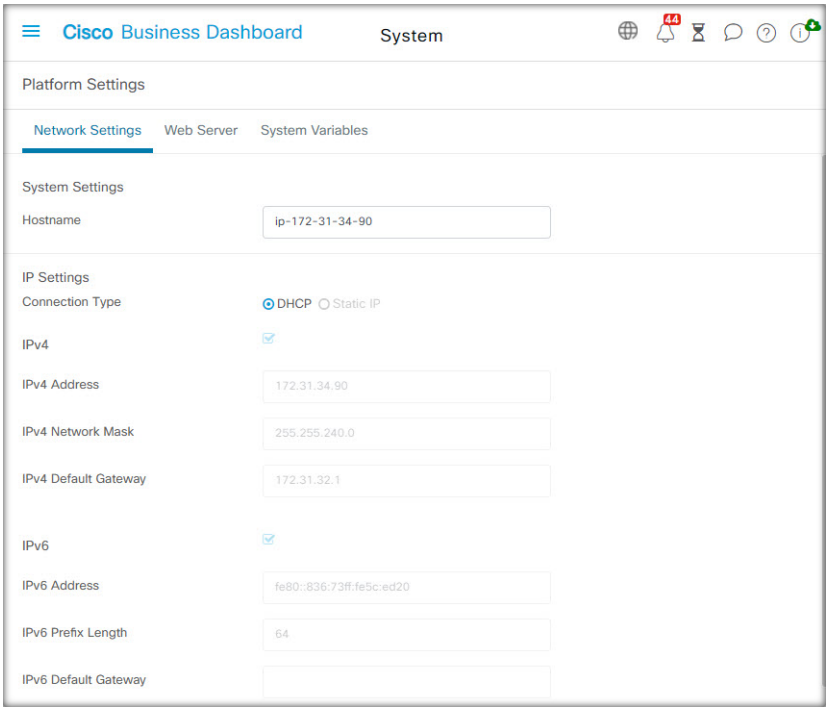


Führen Sie die folgenden Schritte aus, um den Hostnamen für das Dashboard zu ändern.

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 oder Azure. Wenn Sie die Netzwerkkonfiguration ändern möchten, verwenden Sie die EC2-Konsole in AWS für eine AWS-Instanz und das Azure-Portal für eine Azure-Instanz.

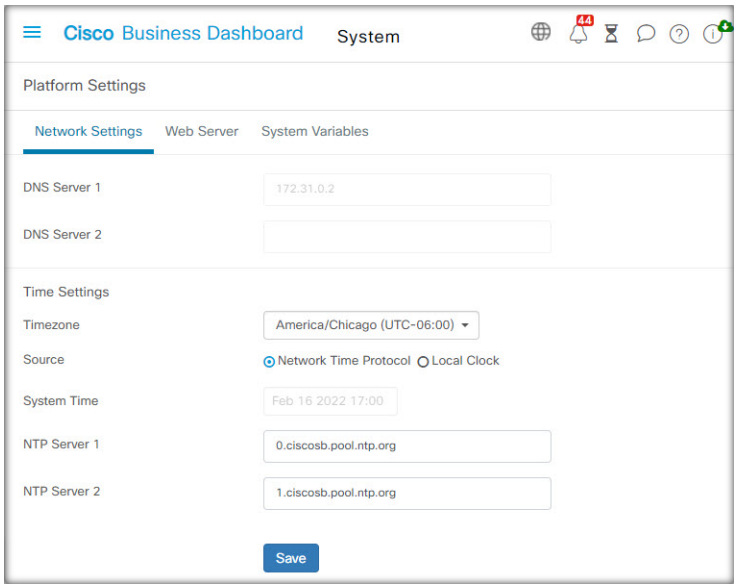


Führen Sie die folgenden Schritte aus, um die Netzwerkkonfiguration für das Dashboard zu ändern.

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. Führen Sie die folgenden Schritte aus, 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).

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.

Ändern der Porteinstellungen (Registerkarte „Web Server“)

Unter **Port Settings** (Porteinstellungen) können Sie festlegen, auf welchen TCP-Ports die Dashboard-Benutzeroberfläche gehostet werden soll. Führen Sie die folgenden Schritte aus, 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. Ändern Sie die Ports, die für den Remote-Zugriff auf Netzwerkgeräte verwendet werden, über Cisco Business Dashboard.
4. Klicken Sie auf **Save** (Speichern).

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.

Führen Sie die folgenden Schritte aus, 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))

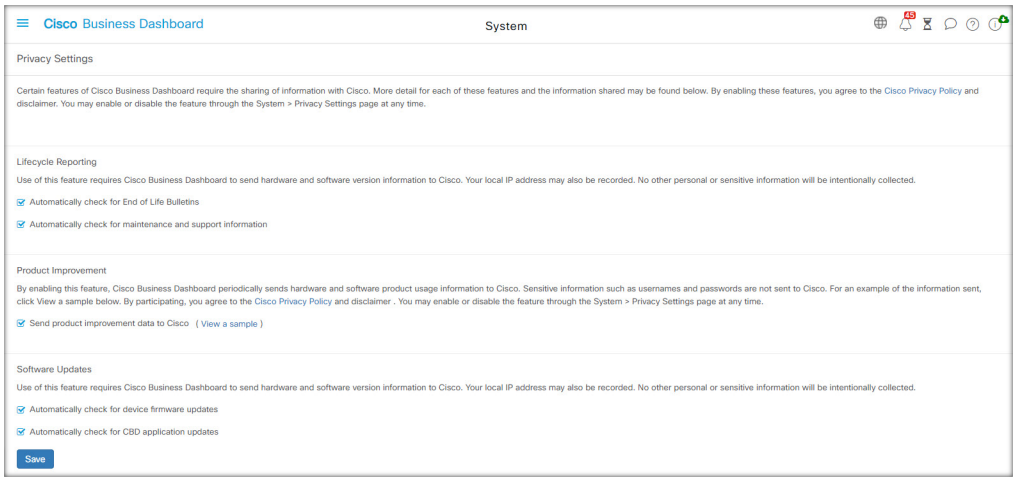
Cisco Business Dashboard verwendet Systemvariablen, um beim Generieren von Konfigurationsvorlagen und anderen Aufgaben bestimmte Parameter für das Dashboard bereitzustellen. Einige Systemvariablen werden möglicherweise automatisch vom Dashboard bestimmt, aber es gibt andere Variablen, die eine Benutzereingabe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

Führen Sie die folgenden Schritte aus, 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** (Lifecycle-Berichterstellung): Diese Funktion deckt die Erstellung der Berichte **Lifecycle-Bericht**, **End-of-Life-Bericht und Wartungsbericht** in Cisco Business Dashboard ab. Die Funktion für Lifecycle-Berichte 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 Netzwerkinventar bietet. Wenn diese Funktion aktiviert ist, sendet das Dashboard Informationen zum Netzwerkbestand an CAA. Sie können die Informationen zum Lifecycle 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 ein Label aus, das 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.

Führen Sie die folgenden Schritte aus, 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.

   Alternativ können Sie auch ein Label auswählen, das 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.

Führen Sie die folgenden Schritte aus, 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).

Lifecycle-Bericht

Cisco Business Dashboard enthält Informationen zum Lifecycle-Status 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.

Führen Sie die folgenden Schritte aus, um die Generierung von Lifecycle-Berichten zu deaktivieren.

1. Navigieren Sie zu **System** > **Privacy Settings** (System > Datenschutzeinstellungen).
2. Deaktivieren Sie bei den Berichten, die Sie deaktivieren möchten, die Kontrollkästchen.
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.

Führen Sie die folgenden Schritte aus, um ein Beispiel dafür zu sehen, welche Informationen gesendet werden.

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.

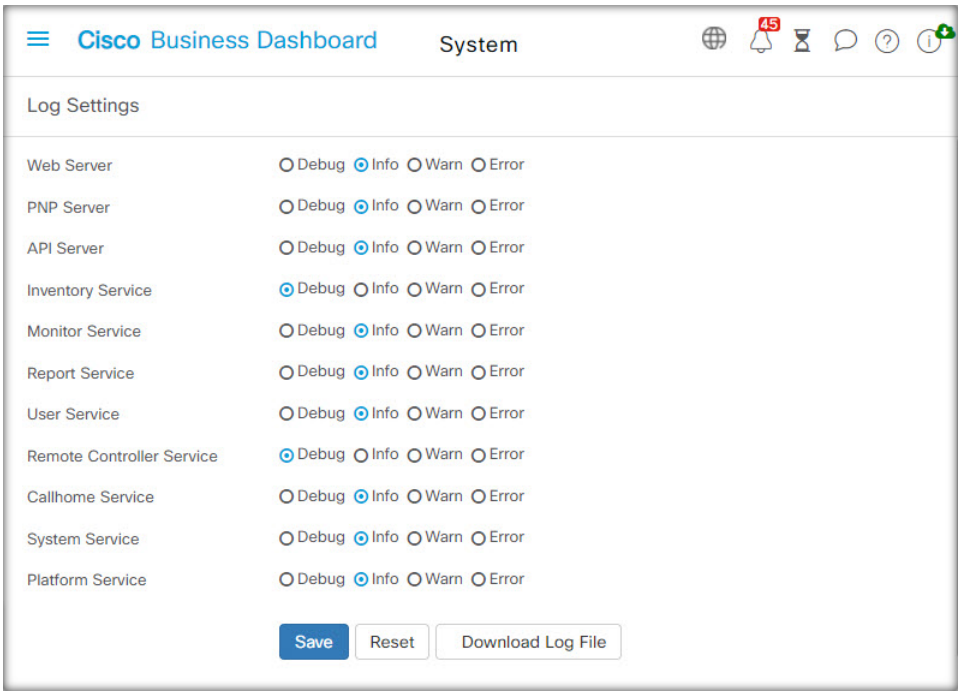
Gehen Sie wie folgt vor, um die Verwendung automatischer Software-Updates zu deaktivieren:

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.

Führen Sie die folgenden Schritte aus, um die Protokollebene für das Dashboard zu ändern:



1. Navigieren Sie zu **System** > **Log Settings** (System > Protokolleinstellungen).
2. Wählen Sie mithilfe der Optionsschaltflächen 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.

Führen Sie die folgenden Schritte aus, 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.conf`aktualisiert 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 oder Azure 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.

Verwalten von Integrationseinstellungen

Cisco Business Dashboard kann in eine Vielzahl von Anwendungen und Services von Cisco und anderen Anbietern integriert werden. Bei Integration in eine Anwendung können Daten und Ereignisse zwischen den Anwendungen ausgetauscht und Netzwerkaktionen durchgeführt werden.

Die Integration wird mit den folgenden Anwendungen und Services unterstützt:

- ConnectWise Manage
- Webex

Weitere Informationen zum Einrichten der Integration und zu den mit den einzelnen Anwendungen ausgetauschten Informationen finden Sie in den folgenden Abschnitten.

ConnectWise Manage

ConnectWise Manage ist ein Professional Services Automation-Tool (PSA), das für die Verwendung durch Anbieter von Managed Services entwickelt wurde. Es umfasst Asset-Management, Buchhaltung und Abrechnung sowie Helpdesk-Services als Teil seiner Funktionalität. Durch die Integration von Cisco Business Dashboard in ConnectWise Manage können Sie sicherstellen, dass Bestandsaufzeichnungen für Netzwerkgeräte auf dem neuesten Stand gehalten werden und Ereignisse sowie Netzwerkaktionen mit Helpdesk-Tickets verwaltet werden.

Unterstützte Funktionalität

Bei einer Integration in ConnectWise Manage bietet Cisco Business Dashboard zusätzliche Funktionen in drei Hauptbereichen: Asset-Management, Ereignismanagement und Automatisierung.

Für das Asset-Management erstellt Cisco Business Dashboard in ConnectWise Manage automatisch für jedes vom Dashboard verwaltete Netzwerkgerät Konfigurationsdatensätze und aktualisiert diese regelmäßig. Der Konfigurationsdatensatz enthält Informationen wie Gerätetyp und Modell, Seriennummer, Softwareinformationen, Ablaufdatum der Garantie und Lifecycle-Informationen. Wenn ein Gerät aus dem Dashboard-Bestand entfernt wird, wird die Konfiguration als inaktiv markiert, aber nicht aus ConnectWise Manage gelöscht.

Neben der Erstellung von Konfigurationsdatensätzen können Sie in ConnectWise Manage auch Netzwerkgerätetypen bestimmte Produkten zuordnen und Cisco Business Dashboard Vereinbarungen zu diesen Produkten mit der Anzahl der diesem Kunden zugeordneten Geräte aktualisieren lassen.

Bei der Verwaltung von Netzwerkereignissen können Sie die Cisco Business Dashboard-Überwachungsprofile so konfigurieren, dass das Dashboard Helpdesk-Tickets erstellt, wenn die ausgewählten Benachrichtigungen auftreten. Diese Benachrichtigungstickets enthalten Details zum Ereignis und sind dem Konfigurationsdatensatz für das Gerät zugeordnet, das die Benachrichtigung generiert hat. Bei Firmware-Benachrichtigungen kann das Ticket auch als Automatisierungsticket erstellt werden, um das Firmware-Update im nächsten Änderungsfenster auf das Gerät anzuwenden.

Ein Automatisierungsticket ist ein spezielles Ticket, das dazu führt, dass Cisco Business Dashboard eine Netzwerkaktion durchführt. Automatisierungstickets werden in einem dedizierten Service-Board erstellt, das vom Dashboard überwacht wird, und können zur Automatisierung der folgenden Aktionen verwendet werden:

- Sichern der Konfiguration
- Upgrade auf neueste Firmwareversion
- Neustarten des Geräts
- Speichern der aktuellen Konfiguration
- Löschen des Geräts

Automatisierungstickets können so erstellt werden, dass sie sofort oder im nächsten Änderungsfenster ausgeführt werden. Ferner kann festgelegt werden, dass vor der Ausführung eine Genehmigung erforderlich ist. Das Ticket wird während der Ausführung mit Fortschrittsinformationen und nach Abschluss mit dem Ergebnis der Aktion aktualisiert.

Voraussetzungen

Bevor Sie die ConnectWise Manage-Integration einrichten, müssen folgende Voraussetzungen erfüllt sein:

- Wenn Automatisierungstickets verwendet werden, muss die Anwendung ConnectWise Manage Verbindungen zum Cisco Business Dashboard-Webserver herstellen können. Darüber hinaus muss Cisco Business Dashboard über ein Zertifikat verfügen, dem ConnectWise Manage vertraut. In den meisten Fällen bedeutet dies, dass das Zertifikat von einer öffentlichen Zertifizierungsstelle signiert werden muss. Weitere Informationen zum Einrichten von Zertifikaten für Cisco Business Dashboard finden Sie unter Verwalten von Zertifikaten, auf Seite 5.
- Wenn sich das Dashboard hinter einem NAT-Gateway oder einer Firewall befindet, stellen Sie sicher, dass auf der Seite „System Variables“ (Systemvariablen) unter **System** > **Platform Settings**(System > Plattformeinstellungen) der Hostname und die Webserver-Ports angezeigt werden, welche die Anwendung ConnectWise Manage verwendet, um eine Verbindung zum Dashboard herzustellen.
- Eine Reihe von API-Schlüsseln muss für Cisco Business Dashboard erstellt werden und mindestens über die in der folgenden Tabelle aufgeführten Berechtigungen verfügen.

Tabelle 1: Für den API-Schlüssel erforderliche Berechtigungen

Berechtigung	Ebene hinzufügen	Ebene bearbeiten	Ebene löschen	Ebene anfragen
Unternehmen				
Wartung des Unternehmens	Keine	Keine	Keine	Alle
Konfigurationen	Alle	Alle	Alle	Alle
Finanzen				
Verträge	Keine	Alle	Keine	Alle
Beschaffung				
Produktkatalog	Keine	Keine	Keine	Alle
Service Desk				
Servicetickets	Alle	Alle	Alle	Alle
System				
Tabelleneinrichtung	Alle	Alle	Alle	Alle

- Ein für Automatisierungstickets geeignetes Service-Board muss identifiziert oder erstellt werden. Dieses Board hat eine Reihe von Einrichtungsanforderungen, die während des Integrationsprozesses gelten. Es wird empfohlen, dieses Board für den Netzwerkbetrieb zu verwenden. Im folgenden Abschnitt finden Sie weitere Informationen zur Einrichtung dieses Boards.
- Ein für Benachrichtigungstickets geeignetes Service-Board muss identifiziert oder erstellt werden. Dieses Board hat keine spezifischen Anforderungen und kann ein vorhandenes Allzweck-Board sein. Bei dem Benachrichtigungs-Board kann es sich auch um das Service-Board handeln, das für Automatisierungstickets verwendet wird.

Einrichten der ConnectWise Manage-Integration

Die Einrichtung der ConnectWise Manage-Integration umfasst mehrere Schritte.

- Stellen Sie die Kommunikation mit dem ConnectWise Manage-Service her.
- Ordnen Sie die ConnectWise-Unternehmen Cisco Business Dashboard-Organisationen zu.
- Konfigurieren Sie den Asset-Synchronisierungsprozess.
- Wählen Sie die Service-Boards für die Ereignisbenachrichtigung und Automatisierung aus.

In diesem Abschnitt wird beschrieben, wie Sie die einzelnen Schritte zur korrekten Einrichtung durchführen.

Stellen Sie die Kommunikation mit dem ConnectWise Manage-Service her.

1. Navigieren Sie zu **System** > **Integration Settings** (System > Integrationseinstellungen).

2. Suchen Sie die Kachel, welche die Integration von ConnectWise Manage darstellt, und stellen Sie sicher, dass der Schalter auf **Enabled**(Aktiviert) gesetzt ist.
3. Klicken Sie auf das Symbol **Settings** (Einstellungen), um die Seiten mit den ConnectWise Manage-Einstellungen anzuzeigen. Wählen Sie anschließend die Registerkarte **Connection** (Verbindung) aus.
4. Füllen Sie die Felder im bereitgestellten Formular aus, und klicken Sie dann auf **Save** (Speichern). In der folgenden Tabelle finden Sie Details zu den angeforderten Parametern.

Tabelle 2: Verbindungsparameter von ConnectWise Manage

Parameter	Beschreibung
API-Hostname	Das Protokoll und der Hostname des ConnectWise Manage-Service, mit dem eine Verbindung hergestellt werden soll. Der Standardwert ist https://na.connectwise.net.
Unternehmens-ID	Die ID des Unternehmens in ConnectWise Manage. Der gleiche Wert wird auch bei der Anmeldung bei der Connectwise Manage-GUI verwendet.
Öffentlicher Schlüssel	Der öffentliche Schlüssel aus dem API-Schlüssel, der in ConnectWise Manage für Cisco Business Dashboard definiert ist.
Privater Schlüssel	Der private Schlüssel aus dem API-Schlüssel, der in ConnectWise Manage für Cisco Business Dashboard definiert ist.

Nachdem Sie auf **Save** (Speichern) geklickt haben, testet Cisco Business Dashboard die Verbindung und liest dann die Informationen aus ConnectWise Manage, die später im Einrichtungsprozess benötigt werden. Diese Informationen umfassen die Liste der Unternehmen, Konfigurationstypen, Produkte, Vereinbarungstypen und Service-Boards. Wenn in ConnectWise Manage Änderungen an diesen Informationen vorgenommen werden, klicken Sie auf der Seite auf die Schaltfläche **Refresh ConnectWise Data** (ConnectWise-Daten aktualisieren), um die Daten erneut zu lesen.

ConnectWise-Unternehmen Cisco Business Dashboard-Organisationen zuordnen

Nachdem die Verbindung zwischen Cisco Business Dashboard und ConnectWise Manage hergestellt wurde, müssen Organisationen in Cisco Business Dashboard Unternehmen in ConnectWise Manage zugeordnet werden. Durch die Zuordnung von Unternehmen zu Organisationen können Netzwerkgeräte und -ereignisse in ConnectWise Manage dem richtigen Kunden zugeordnet werden. Führen Sie die folgenden Schritte aus, um die Zuordnung abzuschließen.

1. Navigieren Sie zu **System** > **Integration Settings** (System > Integrationseinstellungen).
2. Klicken Sie auf das Symbol **Settings** (Einstellungen) auf der Kachel **ConnectWise Manage** und wählen Sie dann die Registerkarte **Organization Mapping** (Organisationszuordnung) aus.
3. Klicken Sie auf die Schaltfläche **Import from ConnectWise** (Import aus ConnectWise). Dadurch wird die Liste der Unternehmen mit der Liste der Organisationen verglichen und es werden Zuordnungen erstellt, wenn entweder der Unternehmensname oder die Unternehmens-ID mit dem Organisationsnamen übereinstimmt.
4. Beliebige Zuordnungen zwischen Unternehmen und Organisationen können entweder manuell oder mithilfe von CSV-Dateien (CSV = Comma-Separated Value, kommagetrennte Werte) vorgenommen werden.

So erstellen Sie eine Zuordnung manuell:

1. Klicken Sie auf das Pluszeichen (**✚**) oberhalb der Zuordnungstabelle, um einen neuen Eintrag in der Tabelle zu erstellen.
2. Wählen Sie in den Dropdown-Listen den Namen des Unternehmens und der Organisation aus, die zugeordnet werden sollen.

Hinweis Wenn der gewünschte Unternehmensname im Dropdown-Menü nicht aufgeführt ist, kehren Sie zur Registerkarte **Connect** (Verbinden) zurück und klicken Sie auf die Schaltfläche **Refresh ConnectWise Data** (ConnectWise-Daten aktualisieren), um die Liste der Unternehmen zu aktualisieren.

3. Klicken Sie auf das Symbol zum **Speichern**.

So erstellen Sie Zuordnungen mithilfe von CSV-Dateien:

1. Erstellen Sie eine CSV-Datei mit den gewünschten Zuordnungen zwischen einem Organisations- und einem Unternehmensnamen.
2. Klicken Sie über der Zuordnungstabelle bei einer CSV-Vorlagendatei, die eine Liste der vorhandenen Zuordnungen enthält, auf das **Download**-Symbol.
3. Sobald die Vorlagendatei aktualisiert wurde, klicken Sie über der Tabelle auf die Schaltfläche **Upload** (Hochladen), um die in der Datei angegebenen neuen Zuordnungen zu erstellen.

So ändern Sie eine vorhandene Zuordnung:

1. Klicken Sie auf die Optionsschaltfläche neben der Zuordnung.
2. Klicken Sie auf das **Edit**-Symbol (Bearbeiten).
3. Nehmen Sie die erforderlichen Änderungen vor.
4. Klicken Sie auf das Symbol zum **Speichern**.

So löschen Sie eine vorhandene Zuordnung:

1. Klicken Sie auf die Optionsschaltfläche neben der Zuordnung.
2. Klicken Sie auf das Symbol **Delete** (Löschen).

Asset-Synchronisierungsprozess konfigurieren

Die Erstellung von Konfigurationsdatensätzen in ConnectWise Manage zur Darstellung der Netzwerkgeräte ist eine Voraussetzung, damit die Funktionen für das Management von Sicherheitsvorfällen und die Automatisierung funktionieren. Cisco Business Dashboard erstellt und aktualisiert automatisch Konfigurationsdatensätze für jedes Netzwerkgerät in Organisationen, die einem ConnectWise-Verwaltungsunternehmen zugeordnet sind. Führen Sie die folgenden Schritte aus, um die Synchronisierung von Assets einzurichten.

1. Navigieren Sie zu **System** > **Integration Settings** (System > Integrationseinstellungen).
2. Klicken Sie auf der Kachel **ConnectWise Manage** auf das Symbol „Settings“ (Einstellungen) und wählen Sie dann die Registerkarte **Asset Synchronization** (Asset-Synchronisierung) aus.

3. Klicken Sie auf die Schaltfläche **Create Default Configuration Types in Connectwise** (Standardkonfigurationstypen in ConnectWise erstellen).

   Dadurch werden drei Konfigurationstypen erstellt – CBD Managed Router, CBD Managed Switch und CBD Managed WAP – mit Feldern und Fragen, die für die Netzwerkgeräte geeignet sind. Wenn diese Konfigurationstypen bereits vorhanden sind, werden sie mit den Feldern und Fragen aktualisiert.

4. Klicken Sie auf das Symbol zum **Speichern**.

Täglich um Mitternacht führt Cisco Business Dashboard für jede Organisation eine Asset-Synchronisierung durch, die einem Unternehmen zugeordnet ist. Für jedes Netzwerkgerät in dieser Organisation wird ein Konfigurationsdatensatz mit Informationen zu diesem Gerät erstellt. Wenn bereits ein Konfigurationsdatensatz vorhanden ist, wird dieser mit allen Änderungen an den Geräteinformationen aktualisiert. Der Konfigurationsdatensatz, der einem Gerät zugeordnet ist und aus Cisco Business Dashboard gelöscht wurde, wird als **inaktiv** markiert.

Im Rahmen des Synchronisierungsprozesses führt Cisco Business Dashboard zudem folgende Aktionen aus:

1. Cisco Business Dashboard identifiziert für jedes Unternehmen sämtliche Vereinbarungen, die mit den von Ihnen angegebenen Vereinbarungstypen übereinstimmen.
2. Bei jeder Vereinbarung identifiziert Cisco Business Dashboard Ergänzungen, die mit den ausgewählten Produkten übereinstimmen, und ordnet sie den einzelnen Gerätetypen zu.
3. Für jede dieser Ergänzungen aktualisiert Cisco Business Dashboard die Menge basierend auf der Anzahl der Geräte mit Typen, für die das entsprechende Produkt ausgewählt ist.

Gehen Sie wie folgt vor, um dies zu ermöglichen:

1. Navigieren Sie zu **System** > **Integration Settings** (System > Integrationseinstellungen).
2. Klicken Sie auf der Kachel **ConnectWise Manage** auf das Symbol **Settings** (Einstellungen) und wählen Sie dann die Registerkarte **Asset Synchronization** (Asset-Synchronisierung) aus.
3. Klicken Sie für jeden Gerätetyp in das Feld **Product** (Produkt) und wählen Sie ein oder mehrere Produkte aus, die Geräten dieses Typs zugeordnet werden sollen.
4. Wählen Sie unter der Überschrift **Agreement Type** (Vereinbarungstyp) einen oder mehrere Vereinbarungstypen aus, um die zu aktualisierenden Vereinbarungen zu identifizieren.
5. Klicken Sie auf das Symbol zum **Speichern**.

Hinweis Wenn das gewünschte Produkt oder der gewünschte Vereinbarungstyp in den Dropdown-Menüs nicht aufgeführt wird, kehren Sie zur Registerkarte **Connect** (Verbinden) zurück und klicken Sie auf die Schaltfläche **Refresh ConnectWise Data** (ConnectWise-Daten aktualisieren), um die Listen zu aktualisieren.

Service-Boards für Ereignisbenachrichtigung und Automatisierung auswählen

Aktivieren Sie die Funktionen für das Management von Sicherheitsvorfällen und die Automatisierung, indem Sie Service-Boards angeben, die für jede dieser Funktionen verwendet werden sollen. So geben Sie die zu verwendenden Service-Boards an:

1. Navigieren Sie zu **System** > **Integration Settings** (System > Integrationseinstellungen).

2. Klicken Sie auf der Kachel **ConnectWise Manage** auf das Symbol **Settings** (Einstellungen) und wählen Sie dann die Registerkarte **Ticket Settings** (Ticket-Einstellungen) aus.
3. Wählen Sie im Dropdown-Menü **Notification Board** (Benachrichtigungsboard) das entsprechende Service-Board aus, das für Tickets verwendet werden soll, die als Reaktion auf Netzwerkereignisse erstellt werden.
4. Wählen Sie im Dropdown-Menü **Automation Board** (Automatisierungs-Board) das Service-Board aus, das auf Automatisierungstickets überwacht werden soll.

Hinweis Wenn das gewünschte Service-Board in den Dropdown-Menüs nicht aufgeführt wird, kehren Sie zur Registerkarte **Connect** (Verbinden) zurück und klicken Sie auf die Schaltfläche **Refresh ConnectWise Data** (ConnectWise-Daten aktualisieren), um die Listen dr Service-Boards zu aktualisieren.

5. Klicken Sie auf das Symbol zum **Speichern**.

   Cisco Business Dashboard aktualisiert die Einstellungen für das Automatisierungs-Board in ConnectWise Manage und enthält die entsprechenden Statuswerte, Typen und Untertypen, die zur Unterstützung der Automatisierungsfunktionen erforderlich sind. In den Tabellen 30–32 in Automatisieren von Netzwerkaktionen mit Automatisierungstickets, auf Seite 31 finden Sie Details zu den zu erstellenden Status, Typen und Untertypen.

Verwenden der ConnectWise Manage-Integration

Von den drei Integrationstypen in ConnectWise Manage erfordern das Management von Sicherheitsvorfällen und die Automatisierung, dass der Benutzer aktiv mit der Funktionalität interagiert. Die Asset-Synchronisierung erfordert im Allgemeinen keine Benutzerinteraktion. In den folgenden Abschnitten werden die einzelnen Funktionalitäten näher beschrieben.

Verwenden der Asset-Synchronisierung

Für die Asset-Synchronisierung sind über die oben beschriebene Ersteinrichtung hinaus keine besonderen Maßnahmen erforderlich. Der Bestand an Netzwerkgeräten in Cisco Business Dashboard wird automatisch mit ConnectWise Manage-Konfigurationsdatensätzen synchronisiert, welche die in der folgenden Tabelle aufgeführten Informationen enthalten. Bei allen Vereinbarungen, die mit den in den Einstellungen für die Asset-Synchronisierung festgelegten Typen übereinstimmen, werden die Mengen aller Ergänzungen, die mit den ausgewählten Produkten übereinstimmen, aktualisiert, um die Anzahl der Geräte des entsprechenden Typs zu berücksichtigen, die im Netzwerk vorhanden sind.

Der Prozess der Asset-Synchronisierung findet automatisch jeden Tag um Mitternacht statt. Falls eine sofortige Synchronisierung erforderlich ist, können Sie diese durch Klicken auf die Schaltfläche **Sync Assets** (Assets synchronisieren) auf dem Bildschirm „Asset Synchronization“ (Asset-Synchronisierung) initiieren. Dies kann auch über ein Collaboration-Tool erfolgen, wenn eines in Cisco Business Dashboard integriert wurde.

Hinweis Der Prozess der Asset-Synchronisierung dauert in der Regel mehrere Minuten und kann in größeren Netzwerken viel länger dauern.

Tabelle 3: Verwendung von Konfigurationsfeldern in ConnectWise Manage

Feld	Beschreibung
Konfigurationsname	Der Host-Name des Geräts
Konfigurationsdetails	
Typ	Der Konfigurationstyp wird basierend auf dem Gerätetyp und den auf der Seite „Asset Synchronization“ (Asset-Synchronisierung) konfigurierten Zuordnungen festgelegt.
Status	Dieses Feld ist auf **Inactive** (Inaktiv) gesetzt, wenn das Gerät aus dem Dashboard-Bestand gelöscht wurde. Andernfalls ist es auf **Active** (Aktiv) gesetzt.
Modell	Modellnummer des Geräts.
Seriennummer	Seriennummer des Geräts
Unternehmen	
Unternehmen	Das Unternehmen, das der auf der Seite **Organization Mapping** (Organisationszuordnung) definierten Organisation des Geräts entspricht.
Hinweise	
Hinweise des Anbieters	Enthält einen Hinweis, aus dem hervorgeht, dass die Konfiguration von Cisco Business Dashboard erstellt wurde, und zeigt einen Zeitstempel für die Erstellung an.
Fragen zur Konfiguration	Die Konfigurationsfragen umfassen folgende Informationen: • Die **Geräteprodukt-ID:** Dieses Feld ähnelt der Modellnummer, ist aber die Kennung, die beim Kauf eines neuen Geräts verwendet wird. • **Softwareversion:** Diese Informationen umfassen die aktuelle Version und die neueste verfügbare Version mit Versionshinweisen. • **Lifecycle-Informationen:** Dazu gehören Details zu den Enddaten der Garantie und die geltenden End-of-Life-Bulletins.
Gerätedetails	
IP-Adresse	Die Management-IP-Adresse des Geräts.
MAC-Adresse	Die MAC-Basisadresse des Geräts.

Automatisieren von Netzwerkaktionen mit Automatisierungstickets

Automatisierungstickets ermöglichen die Ausführung von Aktionen auf Netzwerkgeräten durch das Erstellen speziell formatierter Tickets.

Tickets können angeben, ob die Aktion sofort oder im nächsten Änderungsfenster erfolgen soll, und erfordern optional vor der Ausführung einen Genehmigungsschritt. Wenn alle Voraussetzungen erfüllt sind, führt Cisco Business Dashboard die im Ticket angegebene Aktion aus. Das Ticket wird dann mit dem Erfolg oder Fehlschlagen des Vorgangs aktualisiert.

Erstellen Sie zum Erstellen eines Automatisierungstickets ein neues Ticket mit den folgenden Merkmalen:

- Beim Einrichten der Integration sollte das Service-Board als Automatisierungs-Board festgelegt werden.
- Das Ticket sollte genau einer Konfiguration zugeordnet sein, die ein von Cisco Business Dashboard verwaltetes Netzwerkgerät darstellt.
- Der Typ sollte auf die gewünschte Aktion festgelegt sein. Unter Tabelle 4: Typen von Automatisierungstickets, auf Seite 33 finden Sie eine Liste der verfügbaren Aktionen.
- Der Untertyp sollte basierend auf der gewünschten Ausführungszeit und darauf, ob eine Genehmigung erforderlich ist, ausgewählt werden. Unter Tabelle 5: Untertypen von Automatisierungstickets, auf Seite 33 finden Sie eine Liste der verfügbaren Optionen.
- Der Status sollte auf **Start** gesetzt werden, um den Automatisierungsprozess zu starten. Wenn vor Beginn der Automatisierung zusätzliche Arbeiten erforderlich sind, kann der Status auf **Needs Attention** (Erfordert Aufmerksamkeit) gesetzt werden, bis die Arbeiten abgeschlossen sind. Unter Tabelle 6: Status von Automatisierungstickets, auf Seite 34 finden Sie eine vollständige Liste aller möglichen Statuswerte.

Wenn ein Automatisierungsticket erstellt wird und der Status **Start** lautet, übernimmt Cisco Business Dashboard die Kontrolle über das Ticket und führt die folgenden Schritte aus:

1. CBD überprüft das Ticket, um sicherzustellen, dass alle erforderlichen Informationen vorhanden sind. Wenn es ein Problem gibt, werden die internen Notizen aktualisiert und der Status ändert sich in **Needs Attention** (Erfordert Aufmerksamkeit).
2. Wenn das Ticket fehlerfrei ist, wird der Untertyp überprüft, um festzustellen, ob eine Genehmigung erforderlich ist. Ist dies der Fall ist, wird der Status in **Needs Approval** (Genehmigung ausstehend) geändert und es werden keine weiteren Maßnahmen ergriffen, bis der Status in **Approved** (Genehmigt) aktualisiert wird.
3. Der Untertyp wird überprüft, um festzustellen, wann die Aktion ausgeführt werden soll. Wenn das Ticket jetzt ausgeführt werden soll, führt das Dashboard die Aktion sofort aus. Wenn die Aktion so konfiguriert ist, dass sie im nächsten Änderungsfenster ausgeführt werden soll, wird ein neues Planungsprofil erstellt und der Ticketstatus aktualisiert, um anzuzeigen, dass ein Job ausstehend ist.
4. Wenn die Aktion abgeschlossen ist, aktualisiert das Dashboard die Notizen im Ticket mit dem Erfolg oder Fehlschlagen des Vorgangs. Wenn die Aktion erfolgreich abgeschlossen wurde, wird das Ticket geschlossen. Wenn die Aktion fehlgeschlagen ist, wird der Status in **Needs Attention** (Erfordert Aufmerksamkeit) aktualisiert. Wenn die Ursache für den Fehler behoben wurde, kann das Ticket erneut geplant werden, indem der Status wieder in **Start** geändert wird, oder geschlossen, wenn die Aktion nicht mehr erforderlich ist.

Die Genehmigung von Automatisierungstickets ist eine Option, mit der ein gewisses Maß an Änderungskontrolle in den Automatisierungsprozess eingefügt werden kann. Durch die Zuweisung von Automatisierungstickets zur Genehmigung wird sichergestellt, dass eine Aktion von einer Person validiert wird, bevor sie ausgeführt wird, und dass die Validierung im Ticketverlauf aufgezeichnet wird.

Die Genehmigung von Automatisierungstickets in ConnectWise Manage wird durch Statusänderungen implementiert, die anzeigen, dass eine Genehmigung erforderlich ist und erteilt wurde.

Ein genehmigungspflichtiges Ticket – eines mit dem Status „Needs Approval“ (Genehmigung ausstehend) – kann auf zwei Arten genehmigt werden:

- Der Ticketstatus kann direkt über die ConnectWise Manage-Schnittstelle aktualisiert werden. Es wird empfohlen, eine Notiz zum Ticket hinzuzufügen, während die Genehmigung aufgezeichnet wird. Die Details der Genehmigung werden jedoch auch im Prüfpfad für die Tickets aufgezeichnet.
- Das Ticket kann über ein Collaboration-Tool genehmigt werden, das in Cisco Business Dashboard integriert wurde. In diesem Fall wird dem Ticket eine Notiz hinzugefügt, welche die Genehmigung und die Identität des Genehmigenden enthält.

Hinweis Weder ConnectWise Manage noch Cisco Business Dashboard kann eine Anforderung durchsetzen, dass der Genehmiger eine andere Person als der Ersteller des Tickets sein soll. Genehmiger können nicht auf eine bestimmte Liste von Mitarbeitern beschränkt werden. Jeder Benutzer, der das Ticket bearbeiten kann oder Zugriff auf den Collaboration-Bereich hat, kann ein Ticket genehmigen. Für die Implementierung dieser Einschränkungen sind Betriebsprozesse erforderlich.

Tabelle 4: Typen von Automatisierungstickets

Typ	Beschreibung
Backup Configuration (Konfiguration sichern)	Erstellt eine Kopie der aktuellen Konfiguration für das Gerät und speichert diese in Cisco Business Dashboard.
Löschen	Entfernt ein Offline-Gerät aus dem Bestand von Cisco Business Dashboard.
Neustart	Starten Sie das Gerät neu.
Aktuelle Konfiguration speichern	Speichert die aktuelle Konfiguration auf dem Gerät, um diese beim Start zu verwenden.
Firmwareupgrade auf neueste Version	Aktualisiert die Software auf dem Gerät auf die neueste von Cisco veröffentlichte Version.

Tabelle 5: Untertypen von Automatisierungstickets

Untertyp	Beschreibung
Genehmigung ausstehend – Während des Änderungsfensters ausführen	Diese Aktion erfordert eine Genehmigung und sollte für das nächste Änderungsfenster geplant werden, nachdem das Ticket genehmigt wurde.
Genehmigung ausstehend – Jetzt ausführen	Diese Aktion erfordert eine Genehmigung und sollte sofort ausgeführt werden, sobald das Ticket genehmigt wurde.
Während des Änderungsfensters ausführen	Die Aktion sollte für das nächste Änderungsfenster geplant werden.
Jetzt ausführen	Die Aktion sollte sofort ausgeführt werden.

Tabelle 6: Status von Automatisierungstickets

Status	Beschreibung
Start	Zeigt dem Dashboard an, dass das Ticket für die Automatisierung bereit ist.
Needs Attention (Erfordert Aufmerksamkeit)	Zeigt an, dass ein manueller Eingriff erforderlich ist. Dieser Status kann manuell festgelegt werden, wenn vor dem Start der Automatisierung Arbeit erforderlich ist, und wird vom Dashboard festgelegt, falls die Automatisierungsaktion fehlschlägt.
In Bearbeitung	Das Dashboard verarbeitet das Ticket aktiv.
Genehmigung ausstehend	Gibt ein gültiges Automatisierungsticket an, das eine Genehmigung erfordert, um fortzufahren. Es ist ein manueller Eingriff erforderlich, um fortfahren zu können.
Genehmigt	Zeigt an, dass das Ticket genehmigt wurde und zur Ausführung bereit ist. Ein Ticket kann genehmigt werden, indem Sie diesen Status in der Benutzeroberfläche von ConnectWise Manage auswählen, oder durch einen Genehmigungsbefehl in einem Collaboration-Tool, das in Cisco Business Dashboard integriert wurde.
Geplant mit CBD	Ein Job wurde in Cisco Business Dashboard geplant, aber noch nicht ausgeführt. Das Ticket wird aktualisiert, sobald der Job ausgeführt wird.
Abgeschlossen (geschlossen)	Die angeforderte Aktion wurde erfolgreich abgeschlossen.

Verwalten von Netzwerkereignissen mit Benachrichtigungstickets

Um die Erstellung von Tickets als Reaktion auf Netzwerkereignisse zu ermöglichen, müssen die Cisco Business Dashboard-Überwachungsprofile aktualisiert werden, um die Aktion **Open Helpdesk Ticket** (Helpdesk-Ticket erstellen) zu einem oder mehreren Benachrichtigungsmonitoren hinzuzufügen. Weitere Informationen zum Verwalten von Überwachungsprofilen finden Sie unter Überwachungsprofile.

Hinweis Cisco empfiehlt, die Überwachungsprofile so zu konfigurieren, dass die durchschnittliche Rate von 60 Tickets und/oder Collaboration-Nachrichten pro Stunde nicht überschritten wird. Bei der Kommunikation mit externen Anwendungen können anhaltend hohe Raten zu einer Überlastung der API und zum Verlust von Ereignissen führen.

Wenn eine Benachrichtigung auftritt, die mit einem Überwachungsprofil übereinstimmt und die Aktion **Open Helpdesk Ticket** (Helpdesk-Ticket erstellen) aktiviert ist, wird ein neues Ticket im Benachrichtigungs-Board erstellt und der Konfiguration für das entsprechende Gerät zugeordnet. Der Hauptteil des Tickets wird mit relevanten Informationen zur Benachrichtigung aktualisiert.

Bei den meisten Benachrichtigungsmonitoren können nur Benachrichtigungstickets erstellt werden. Im Fall der Firmware-Benachrichtigung sind jedoch zusätzliche Optionen verfügbar. Wenn eine neue Firmware-Version für ein Gerät erkannt wird, kann das Ticket auch als Automatisierungsticket erstellt werden, um das Firmware-Update im nächsten Änderungsfenster auf das Gerät anzuwenden.

Bei der Konfiguration der Firmware-Benachrichtigung in einem Überwachungsprofil werden zwei zusätzliche Optionen bereitgestellt: **With Automation** (Mit Automatisierung) und **With Approval** (Mit Genehmigung). Wenn das Kontrollkästchen **With Automation** (Mit Automatisierung) aktiviert ist, wird anstelle eines Benachrichtigungstickets ein Automatisierungsticket erstellt. Das Ticket wird im Automatisierungs-Board erstellt, der Gerätekonfiguration zugeordnet und als Typ **Upgrade Firmware to Latest** (Firmwareupgrade auf neueste Version) festgelegt.

Schließlich wird der Untertyp so festgelegt, dass das Upgrade im nächsten Änderungsfenster geplant wird. Wenn das Kontrollkästchen **With Approval** (Mit Genehmigung) aktiviert ist, wird der Untertyp auch so festgelegt, dass eine Genehmigung erforderlich ist, bevor das Upgrade geplant wird. Unter Tabelle 5: Untertypen von Automatisierungstickets, auf Seite 33 finden Sie Details zu den verschiedenen Untertypen, die in Automatisierungstickets verwendet werden.

Webex

Webex ist eine Suite von Collaboration-Tools und -Services, die Messaging, Anrufe und Konferenzen umfassen. Durch die Integration von Cisco Business Dashboard in Webex werden Sie über kritische Netzwerkereignisse informiert und können Maßnahmen ergreifen. Sie können die Webex-Anwendung auf Ihrem Desktop oder Mobilgerät verwenden.

Unterstützte Funktionalität

In Kombination mit Webex kann Cisco Business Dashboard Benachrichtigungen an einen Collaboration-Bereich weiterleiten, um den Benutzer über Netzwerkereignisse zu informieren. Sie können die Benachrichtigungen anpassen, indem Sie die Überwachungsprofile aktualisieren und dann auswählen, welche weitergeleitet werden sollen.

Darüber hinaus wird eine eingeschränkte Kontrollschnittstelle bereitgestellt, mit der ein Benutzer bestimmte Aktionen über die Webex-Schnittstelle ausführen kann. Zu den unterstützten Maßnahmen zählen folgende:

- Anzeigen einer Liste offener, von Cisco Business Dashboard erstellter Helpdesk-Tickets.
- Anzeigen einer Liste von Automatisierungstickets, für die eine Genehmigung erforderlich ist.
- Genehmigen von Automatisierungstickets.
- Anzeigen einer Liste der Netzwerkgeräte mit verfügbaren Firmware-Updates.
- Initiieren eines Upgrades für Netzwerkgeräte.

Voraussetzungen

Bevor Sie die Webex-Integration einrichten, müssen Sie einen Webex Bot erstellen und in einen Collaboration-Bereich einladen. Gehen Sie wie folgt vor, um einen Bot einzurichten:

1. Navigieren Sie zu https://developer.webex.com/my-apps/new/bot und melden Sie sich bei Ihrem Webex-Konto an.
2. Füllen Sie das bereitgestellte Formular aus, um Ihren Bot zu erstellen. Sie müssen einen Namen, einen Benutzernamen und eine Beschreibung für Ihren Bot angeben. Sie haben auch die Möglichkeit, ein benutzerdefiniertes Symbol für Ihren Bot bereitzustellen.

Hinweis Obwohl Webex zulässt, dass der Bot-Name Leerzeichen enthält, muss der Bot-Name in Cisco Business Dashboard ein einzelnes Wort ohne Leerzeichen sein.

3. Klicken Sie auf **Add Bot** (Bot hinzufügen), um Ihren Bot zu erstellen. Notieren Sie sich das angezeigte Bot-Token, da Sie dieses bei der Einrichtung der Webex-Integration benötigen.

Beachten Das Bot-Token wird nur einmal angezeigt. Daher ist es wichtig, es zur zukünftigen Referenz an einem sicheren Ort aufzuzeichnen.

Nachdem der Bot erstellt wurde, muss er in einen Collaboration-Bereich eingeladen werden. Es kann ein dedizierter Bereich für die Interaktion mit Cisco Business Dashboard erstellt werden, aber auch ein vorhandener Bereich kann verwendet werden. Jedoch hat jedes Mitglied des Bereichs Einblick in alle Ereignisse und die Möglichkeit, alle unterstützten Befehle auszuführen. Daher sollte der Bereich nur Benutzer aufweisen, die zur Verwaltung des Netzwerks autorisiert sind.

Weitere Informationen zum Erstellen von Bereichen und zum Einladen von Benutzern finden Sie in der Webex-Dokumentation oder in der Online-Hilfe zur Webex-App.

Hinweis Der Bot sollte nur in einen einzigen Collaboration-Bereich eingeladen werden, wenn er in Cisco Business Dashboard integriert ist. Das Verhalten des Bots ist unvorhersehbar, wenn er in mehrere Bereiche eingeladen wird.

Sie sollten nicht nur einen Bot erstellen, sondern auch sicherstellen, dass die Webex-Infrastruktur Verbindungen zum Cisco Business Dashboard-Webserver herstellen kann. Wenn sich das Dashboard hinter einem NAT-Gateway oder einer Firewall befindet, stellen Sie sicher, dass auf der Seite „System Variables“ (Systemvariablen) unter **System** > **Platform Settings**(System > Plattformeinstellungen) der Hostname und die Webserver-Ports angezeigt werden, welche die Webex-Infrastruktur verwendet, um eine Verbindung zum Dashboard herzustellen.

Einrichten der Webex-Integration

Gehen Sie wie folgt vor, um die Webex-Integration einzurichten:

1. Navigieren Sie zu **System** > **Integration Settings** (System > Integrationseinstellungen).
2. Suchen Sie die Webex-Integrationskachel und stellen Sie sicher, dass der Schalter auf **Enabled** (Aktiviert) gesetzt ist.
3. Klicken Sie auf das Symbol **Settings** (Einstellungen), um die Seite **Webex Settings** (Webex-Einstellungen) anzuzeigen.
4. Kopieren Sie das Bot-Token, das Sie beim Erstellen des Bot erhalten haben, in das dafür vorgesehene Feld und klicken Sie auf das **Speichern**-Symbol.
5. Stellen Sie sicher, dass in den Statusfeldern der richtige Bot-Name und der richtige Collaboration-Bereich angezeigt werden.

Hinweis Der Bot sollte nur von einer einzelnen Instanz von Cisco Business Dashboard verwendet werden und nicht mit anderen Anwendungen. Wenn dem Bot mehrere Anwendungen zugeordnet sind, ist das Verhalten unvorhersehbar.

Sobald Cisco Business Dashboard mit den Bot-Details konfiguriert wurde, können Sie Überwachungsprofile konfigurieren, um Benachrichtigungen an den Collaboration-Bereich weiterzuleiten. Weitere Informationen zur Konfiguration von Überwachungsprofilen finden Sie unter Überwachungsprofile.

Verwenden der Webex-Integration

Die Verwendung der Webex-Integration umfasst zwei Hauptbereiche:

- Einrichten und Empfangen von Benachrichtigungen zu Netzwerkereignissen.
- Interaktion mit Cisco Business Dashboard über die eingeschränkte Kontrollschnittstelle.

In den nachfolgenden Abschnitten werden diese Aktivitäten näher beschrieben.

Verwalten von Benachrichtigungen zu Netzwerkereignissen

Um Benachrichtigungen in Webex als Reaktion auf Netzwerkereignisse zu aktivieren, müssen die Überwachungsprofile von Cisco Business Dashboard aktualisiert werden, damit die Aktion **Send To Collaboration Space** (An Collaboration-Bereich senden) an einen oder mehrere Benachrichtigungsmonitore hinzugefügt wird. Weitere Informationen zum Verwalten von Überwachungsprofilen finden Sie unter Überwachungsprofile.

Hinweis Cisco empfiehlt, die Überwachungsprofile so zu konfigurieren, dass die durchschnittliche Rate von 60 Tickets und/oder Collaboration-Nachrichten pro Stunde nicht überschritten wird. Bei der Kommunikation mit externen Anwendungen können anhaltend hohe Raten zu einer Überlastung der API und zum Verlust von Ereignissen führen.

Wenn eine Benachrichtigung auftritt, die mit einem Überwachungsprofil mit aktivierter Aktion **Send To Collaboration Space** (An Collaboration-Bereich senden) übereinstimmt, wird eine Nachricht an den Collaboration-Bereich gesendet. Die Nachricht enthält relevante Informationen zur Benachrichtigung, einschließlich Benachrichtigungsdetails, und Links zum Anzeigen des Geräts in Cisco Business Dashboard und des zugehörigen Helpdesk-Tickets in ConnectWise Manager, sofern eines für das Ereignis erstellt wurde.

Interaktion mit Cisco Business Dashboard über Webex

Wenn Cisco Business Dashboard in Webex integriert ist, bietet es eine eingeschränkte Befehlsschnittstelle, mit der das Dashboard abgefragt und Aktionen ausgeführt werden können. Die folgende Tabelle enthält eine Liste der verfügbaren Befehle und zugehörigen Aktionen.

Die Schnittstelle erfordert, dass der Benutzer den Bot erwähnt, damit ein Befehl akzeptiert wird. Während die Schnittstelle eine gewisse Flexibilität bei der Eingabe tolerieren kann, bietet sie keine Verarbeitung in natürlicher Sprache, sondern ist auf eine Reihe vordefinierter Befehle beschränkt. Bei der Schnittstelle wird auch teilweise zwischen Groß- und Kleinschreibung unterschieden, und sie erkennt gängige Verwendungen, erkennt jedoch möglicherweise keine Befehle mit ungewöhnlichen Großschreibungsmustern.

Tabelle 7: Unterstützte Collaboration-Befehle

Befehl	Beschreibung
Menühilfe?	Stellt eine Liste und Beschreibungen aller verfügbaren Befehle bereit.
Genehmigungen	Stellt eine Liste der Automatisierungstickets bereit, für die eine Genehmigung erforderlich ist. Dieser Befehl ist nur verfügbar, wenn das Dashboard in ConnectWise Manage integriert ist.
Approve <Ticket#>	Markiert das angegebene Automatisierungsticket als zur Ausführung genehmigt.
Assets	Initiiert den Asset-Synchronisierungsprozess. Dieser Befehl ist nur verfügbar, wenn das Dashboard in ConnectWise Manage integriert ist.
Firmware	Stellt eine Liste aller Netzwerkgeräte mit verfügbarem Firmware-Update bereit.
Upgrade <Serial#>	Plant die Durchführung eines Firmware-Updates für das angegebene Gerät im nächsten Änderungsfenster. Wenn das Dashboard in ConnectWise Manage integriert ist, wird für diese Aufgabe ein genehmigungspflichtiges Automatisierungsticket erstellt oder direkt in Cisco Business Dashboard geplant.

Über diese Übersetzung

Cisco kann in einigen Regionen Übersetzungen dieses Inhalts in die Landessprache bereitstellen. Bitte beachten Sie, dass diese Übersetzungen nur zu Informationszwecken zur Verfügung gestellt werden. Bei Unstimmigkeiten hat die englische Version dieses Inhalts Vorrang.