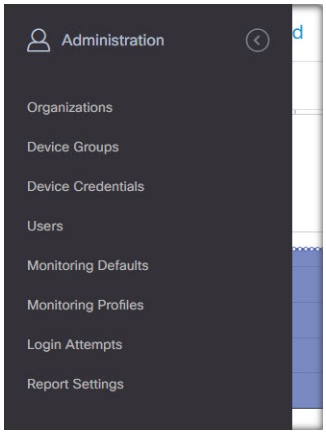
Verwaltung

Dieses Kapitel enthält folgende Abschnitte:

Über die Verwaltung

Mit der Option **Administration** (Verwaltung) in Cisco Business Dashboard können Sie den Betrieb der Anwendung auf Organisationsebene steuern.



Diese Option ist in die folgenden Seiten unterteilt:

- **Organizations** (Organisationen): Erstellen und Verwalten von Organisationen in Cisco Business Dashboard
- **Device Groups** (Gerätegruppen): Zuweisen von Netzwerkgeräten zu Gruppen für eine einfachere Verwaltung

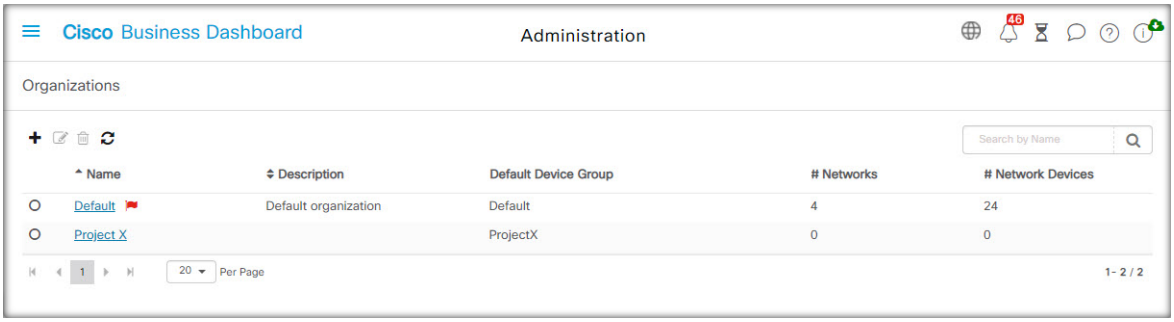
- **Device Credentials** (Anmeldeinformationen des Geräts): Eingeben der Anmeldeinformationen für den Zugriff auf Netzwerkgeräte
- **Users** (Benutzer): Definieren des Benutzerzugriffs auf Cisco Business Dashboard
- **Notification Defaults** (Benachrichtigungs-Standardeinstellungen): Ändern des Standardbenachrichtigungsverhaltens für Cisco Business Dashboard.
- **Login Attempts** (Anmeldeversuche): Protokoll des gesamten Benutzerzugriffs auf Cisco Business Dashboard
- **Report Settings** (Berichtseinstellungen): Ändern der Einstellungen, die steuern, wie Berichte generiert werden

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

Organisationen

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

Eine neue Organisation 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. Geben Sie für das Änderungsfenster der Organisation eine Startzeit und -dauer an.
6. Klicken Sie auf **Save** (Speichern).

7. Wiederholen Sie die oben genannten Schritte für jede Organisation, die Sie erstellen möchten.

Eine vorhandene Organisation ändern

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

Eine Organisation löschen

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

Überwachungsprofile für eine Organisation verwalten

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

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

1. Navigieren Sie zu **Administration** > **Organizations** (Verwaltung > Organisationen).
2. Klicken Sie auf den Namen der zu ändernden Organisation und wählen Sie die Registerkarte **Monitoring Profiles** (Überwachungsprofile) aus.
3. Verwenden Sie die Dropdown-Listen, um das entsprechende Überwachungsprofil auszuwählen, das auf Geräte des entsprechenden Typs angewendet werden soll. Weitere Informationen zum Erstellen von Überwachungsprofilen finden Sie unter Überwachungsprofile, auf Seite 11.

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

Hinweis Unter Überwachungsprofile finden Sie weitere Informationen zu den möglichen Überwachungsarten und deren Verwaltung. Weitere Informationen zum Ändern von Überwachungsprofilen auf Systemebene finden Sie unter Überwachungsstandards, auf Seite 11.

Benutzer verwalten, die einer Organisation zugeordnet sind

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

Führen Sie die folgenden Schritte aus, um der Organisation einen Benutzer zuzuordnen:

1. Navigieren Sie zu **Administration** > **Organizations** (Verwaltung > Organisationen).

2. Klicken Sie auf den Namen der zu ändernden Organisation, und wählen Sie die Registerkarte **Users** (Benutzer) aus.
3. Klicken Sie auf das Plussymbol (✚). Wählen Sie den Benutzer aus der Dropdown-Liste aus.

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

Führen Sie die folgenden Schritte aus, um einen Benutzer aus der Organisation zu entfernen:

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

Netzwerke verwalten, die einer Organisation zugeordnet sind

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

Die Zuordnung eines Netzwerks zu einer Organisation erfolgt, wenn das Netzwerk zum ersten Mal erstellt wird. Führen Sie die folgenden Schritte aus, um die Organisation zu ändern, der ein Netzwerk zugeordnet ist:

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

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

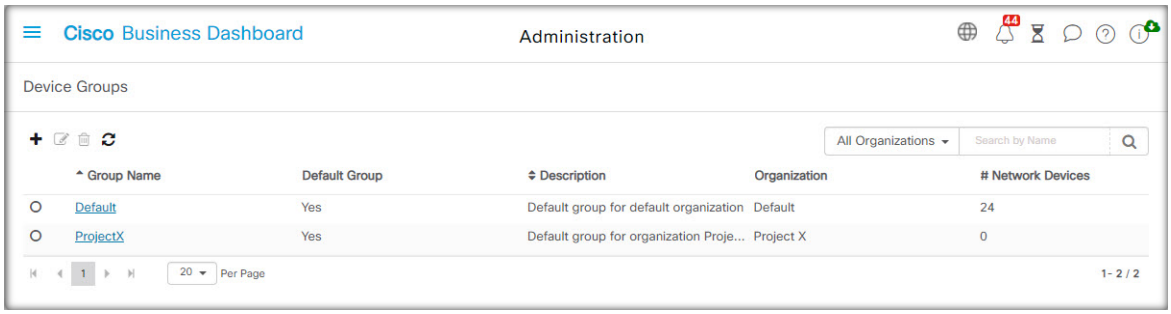
Gerätegruppen

Cisco Business Dashboard nutzt zum Ausführen der meisten Konfigurationsaufgaben Gerätegruppen. Mehrere Netzwerkgeräte werden in Gruppen zusammengefasst und können dann mit einer einzigen Aktion zusammen konfiguriert werden, wie z. B. dem Erstellen von VLANS oder WLANS für nur eine Teilmenge von Geräten.

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

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

Eine neue Gerätegruppe erstellen



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

Gerätegruppe bearbeiten

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

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

Eine Gerätegruppe löschen

1. Navigieren Sie zu **Administration** > **Device Groups** (Verwaltung > Gerätegruppen).

2. Klicken Sie auf die Optionsschaltfläche neben der zu entfernenden Gerätegruppe, und klicken Sie dann auf das Symbol **Delete** (Löschen).

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

Geräteanmeldedaten

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

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

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

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

Führen Sie die folgenden Schritte aus, um Anmeldeinformationen einzeln für ein bestimmtes Gerät einzugeben.

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

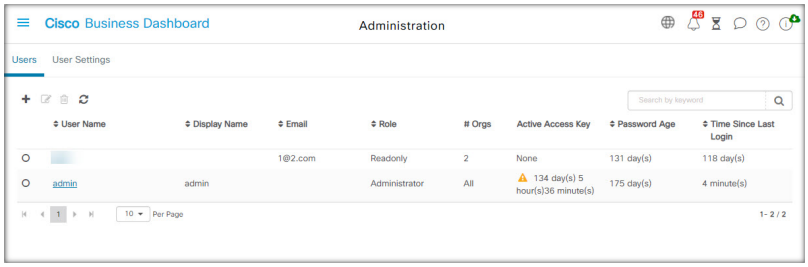
Unter dem Abschnitt **Neue Anmeldeinformationen hinzufügen** finden Sie eine Tabelle mit den Identitäten der Geräte, für die Network Probe gültige Anmeldeinformationen gespeichert hat. In dieser Tabelle ist auch das Datum angegeben, an dem die jeweiligen Anmeldeinformationen zuletzt genutzt wurden. Um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

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

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

Benutzer

Auf der Seite **User Management** (Benutzerverwaltung) können Sie steuern, welche BenutzerInnen auf Cisco Business Dashboard zugreifen dürfen. Außerdem können Sie hier die Einstellungen anpassen, die regeln, wie diese BenutzerInnen mit dem Dashboard interagieren. Darüber hinaus können Sie festlegen, ob diese BenutzerInnen auch Zugriff auf das Netzwerk erhalten sollen, wenn eine benutzerdefinierte Netzwerkauthentifizierung erfolgt. Dies ist ein nützliches Tool, wenn Sie neue Benutzer hinzufügen oder aus dem Netzwerk entfernen müssen.



Cisco Business Dashboard verfügt über Einstellungen zur Steuerung der Dashboard-Funktionen, die über die Dropdown-Liste „Dashboard Access“ (Dashboard-Zugriff) verfügbar sind, und über Einstellungen, ob BenutzerInnen beim benutzerbasierten Netzwerkzugriff auf das Netzwerk zugreifen können (Kontrollkästchen „Network Access“ (Netzwerkzugriff)). Die für diese Einstellungen verfügbaren Optionen umfassen Folgendes:

- **Administrator** (AdministratorIn): AdministratorInnen haben vollen Zugriff auf die Funktionen des Dashboards, einschließlich der Möglichkeit zur Systemwartung.
- **Organization Administrator** (OrganisationsadministratorIn): OrganisationsadministratorInnen sind auf die Verwaltung einer oder mehreren Organisationen beschränkt und können keine Änderungen am System vornehmen.
- **Operator** (BedienerIn): BedienerInnen haben ähnliche Berechtigungen wie Organisationsadministratoren, können jedoch keine BenutzerInnen managen.

- **Readonly** (Schreibgeschützt): Diese BenutzerInnen können nur die Netzwerkinformationen anzeigen. Sie können keinerlei Änderungen vornehmen.
- **No Access** (Kein Zugriff): BenutzerInnen ohne Zugriffsrechte können keine der Dashboard-Funktionen verwenden. Sie können sich jedoch beim Dashboard anmelden, um ihre Benutzerprofile zu managen.
- **Network Access** (Netzwerkzugriff): Diese Einstellung steuert, ob BenutzerInnen auf das Netzwerk zugreifen können, wenn ein benutzerbasierter Netzwerkzugriff verwendet wird. Wenn für die Einstellung „Dashboard Access“ (Dashboard-Zugriff) die Einstellung „Organization Administrator“ (OrganisationsadministratorIn) oder eine niedrigere Einstellung festgelegt ist, ist der Zugriff nur für Organisationen in der Organisationsliste von BenutzerInnen zulässig.

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

Hinweis Bei der Authentifizierung für den benutzerbasierten Netzwerkzugriff werden nur lokale BenutzerInnen überprüft.

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

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

Einen neuen Benutzers zur lokalen Benutzerdatenbank hinzufügen

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

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

Einen Benutzer ändern

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

3. Nehmen Sie die erforderlichen Änderungen vor.
4. Klicken Sie auf **Save** (Speichern).

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

Einen Benutzer löschen

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

Kennwortkomplexität ändern

Führen Sie die folgenden Schritte aus, um Anforderungen an die Kennwortkomplexität festzulegen oder diese zu ändern.

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

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

Active Directory-Authentifizierung aktivieren

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

Führen Sie die folgenden Schritte aus, um Azure Active Directory als Authentifizierungsquelle zu aktivieren.

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

4. Geben Sie die in Schritt 1 erfasste **Client-ID**, den **geheimen Client-Schlüssel** und die **Tenant-ID** in das entsprechende Feld ein.
5. Geben Sie optional eine durch Kommas getrennte Liste von Domains an, die auf das Dashboard zugreifen dürfen. Klicken Sie auf **Save** (Speichern).
6. Klicken Sie auf das Pluszeichen (✚) unter dem Header **User Group Mappings** (Benutzergruppenzuordnungen), um eine neue Gruppenzuordnung zu erstellen. Geben Sie die **Objekt-ID** für die Active Directory-Gruppe in das dafür vorgesehene Feld ein und wählen Sie dann eine Rollen- und Organisationsliste aus, die auf Benutzer in dieser Gruppe angewendet werden soll. Wiederholen Sie diesen Schritt für alle Gruppen, die zugeordnet werden müssen.

   Wenn ein/e BenutzerIn mehreren Gruppen angehört, werden die Rollen- und Organisationszuordnungen aus der ersten Übereinstimmung verwendet.
7. Notieren Sie sich die **Redirect URL** (Weiterleitungs-URL), die unter dem Kontrollkästchen **Enable** (Aktivieren) angezeigt wird. Kehren Sie zu Azure Active Directory zurück und fügen Sie die URL zur Liste der Weiterleitungs-URIs für die App-Registrierung hinzu.

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

Lokale Authentifizierung verwalten

Die Authentifizierung anhand der lokalen Benutzerdatenbank ist standardmäßig aktiviert. Führen Sie die folgenden Schritte aus, um die lokale Authentifizierung zu deaktivieren.

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

Führen Sie die folgenden Schritte aus, um die lokale Authentifizierung erneut zu aktivieren.

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

Zugriff wiederherstellen, wenn der gesamte Administratorzugriff verloren gegangen ist

Führen Sie die folgenden Schritte aus, wenn der Administratorzugriff auf die Cisco Business Dashboard-Anwendung verloren geht.

1. Melden Sie sich über die Konsole oder über SSH beim Host-Betriebssystem an.

2. Geben Sie den Befehl **cisco-business-dashboard restorepassword** ein.

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

Sitzungs-Timeouts ändern

Führen Sie die folgenden Schritte aus, um den Leerlauf-Timeout und den absoluten Timeout für Benutzersitzungen zu ändern.

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

Überwachungsstandards

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

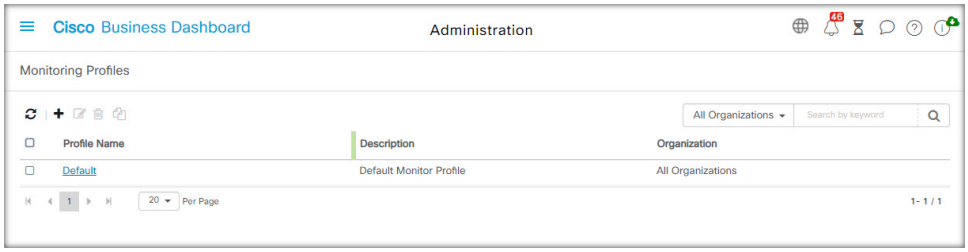
Führen Sie die folgenden Schritte aus, um die im System angewendeten **Überwachungsprofile** zu ändern.

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

Unter Überwachungsprofile finden Sie weitere Informationen zu den möglichen Überwachungsarten und deren Verwaltung. Weitere Informationen zum Ändern der Überwachungseinstellungen auf Organisationsebene finden Sie unter Organisationen, auf Seite 2.

Überwachungsprofile

Überwachungsprofile steuern die Daten, die von Geräten erfasst werden, und die Benachrichtigungen, die generiert werden.



Profile können auf verschiedene Gerätetypen innerhalb einer Organisation oder im gesamten System angewendet werden. Beispielsweise benötigen einige Geräte je nach Standort oder Sicherheitsanforderungen unterschiedliche Überwachungsanforderungen. Innerhalb eines Profils werden zwei Arten von Monitoren unterstützt: **Benachrichtigungsmonitore** und **Berichtsmonitore**.

Mit Benachrichtigungsmonitoren werden Benachrichtigungen und Warnungen generiert, in der Regel aufgrund einer Änderung des Gerätezustands oder eines Parameters, der einen Grenzwert überschreitet. Benachrichtigungen haben unterschiedliche Schweregrade – Information, Warnung und Alarm – und können über die folgenden Kanäle übermittelt werden:

- Popup-Benachrichtigungen der Web-Benutzeroberfläche.
- E-Mail. Dazu müssen die E-Mail-Einstellungen korrekt konfiguriert sein. Näheres dazu finden Sie unter Verwalten der E-Mail-Einstellungen.
- Helpdesk-Ticket. Dies erfordert die Integration in eine Anwendung, die Helpdesk-Services bereitstellt. Näheres dazu finden Sie unter Verwalten von Integrationseinstellungen.
- Collaboration-Nachricht. Dies erfordert die Integration in eine Collaboration-Anwendung. Näheres dazu finden Sie unter Verwalten von Integrationseinstellungen.

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.

Aktive Benachrichtigungen werden auch im **Benachrichtigungscenter** angezeigt und in den Ansichten mit Geräteinformationen angezeigt. Änderungen an Benachrichtigungen werden ebenfalls im **Ereignisprotokoll** aufgezeichnet.

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

Es können mehrere Überwachungsprofile erstellt und verschiedenen Gerätetypen können unterschiedliche Profile auf System- oder Organisationsebene zugewiesen werden. Weitere Informationen zum Zuweisen von Überwachungsprofilen zu Geräten finden Sie unter Organisationen, auf Seite 2 und Überwachungsstandards, auf Seite 11.

Neues Überwachungsprofil hinzufügen

1. Navigieren Sie zu **Administration** > **Monitoring Defaults**(Verwaltung > Überwachungs-Standardeinstellungen).
2. Klicken Sie auf das Plussymbol **(+)**, um ein neues Profil zu erstellen.
3. Geben Sie einen Namen für das Profil und eine Organisation an, der das Profil zugeordnet werden soll. Sie können hier auch „All Organizations“ (Alle Organisationen) angeben, sodass das Profil mit jeder Organisation oder als Standard auf Systemebene verwendet werden kann.
4. Sie können auch eine Beschreibung für das Profil und eine durch Kommas getrennte Liste mit E-Mail-Adressen angeben, um Benachrichtigungen zu erhalten.
5. Klicken Sie auf **Save** (Speichern).

6. Der Bildschirm wird aktualisiert, um die verschiedenen Benachrichtigungs- und Berichtsmonitore anzuzeigen. Sie können einzelne Monitore mithilfe der bereitgestellten Steuerelemente aktivieren und deaktivieren.
7. Die Benachrichtigungsmonitore haben zusätzliche Einstellungen, die durch Klicken auf das **Bearbeiten**-Symbol für den Monitor geändert werden können. Die Einstellungen variieren je nach Monitor, umfassen jedoch die Benachrichtigungstypen, die generiert werden sollen, den Schweregrad der Benachrichtigung und die Grenzwerte, welche die Benachrichtigung auslösen sollen.

Vorhandenes Überwachungsprofil kopieren

Führen Sie die folgenden Schritte aus, um ein vorhandenes Überwachungsprofil zu kopieren.

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

Ein Überwachungsprofil ändern

Führen Sie die folgenden Schritte aus, um ein vorhandenes Überwachungsprofil zu ändern.

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

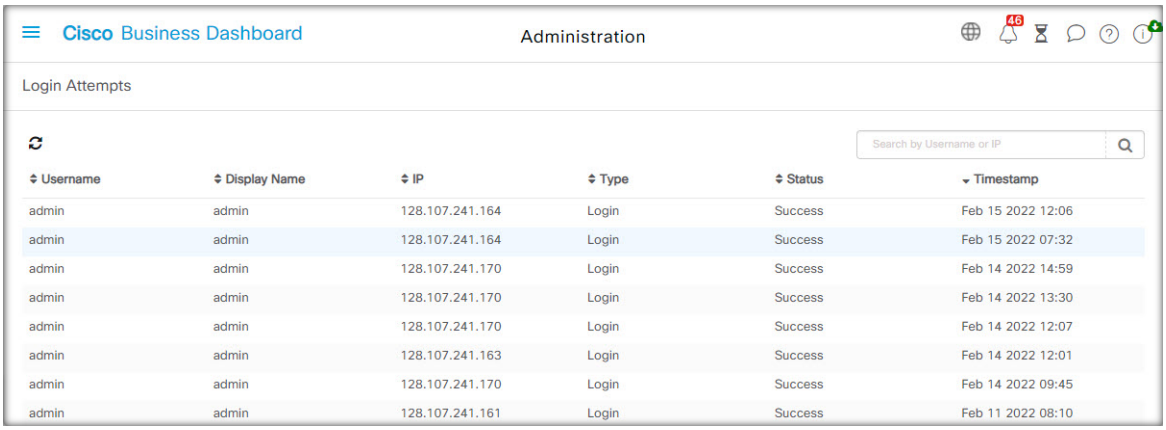
Ein Überwachungsprofil entfernen

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

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

Anzeigen von Anmeldeversuchen

Cisco Business Dashboard führt ein Protokoll aller erfolgreichen und erfolglosen Versuche, sich beim System an- und abzumelden.



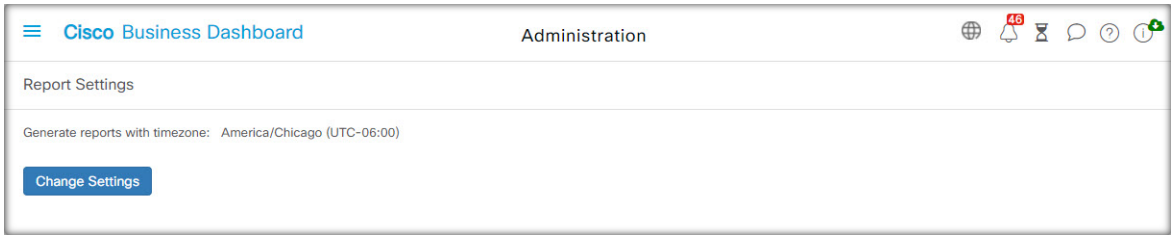
Um das Protokoll anzuzeigen, navigieren Sie zu **Administration** > **Login Attempts** (Verwaltung > Anmeldeversuche). Die Tabelle enthält die folgenden Informationen:

Feld	Beschreibung
Benutzername	Der dem Ereignis zugeordnete Benutzername
Anzeigename	Der Anzeigename des Benutzers
IP	Die IP-Adresse des Geräts, mit der der Benutzer sich angemeldet hat
Typ	Der Ereignistyp, darunter: • ANMELDEN • ABMELDEN
Status	Gibt an, ob der Versuch erfolgreich war oder fehlgeschlagen ist.
Zeitstempel	Datum und Uhrzeit des Ereignisses

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

Verwalten der Berichtseinstellungen

Auf der Seite **Report Settings** (Berichtseinstellungen) können Sie die Zeitzone festlegen, für die Berichte generiert werden.



Die Start- und Endzeiten für den Berichtszeitraum werden in der Ortszeit der ausgewählten Zeitzone angegeben.

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.