IBM Cloud Identity Portal

Administrationshandbuch

IBM Cloud Identity Portal

Administrationshandbuch

Administrationshandbuch zu Cloud Identity Portal

Inhaltsverzeichnis

Kapitel 1. IBM Cloud Identity Portal

Willkommen bei der Dokumentation zu Cloud Identity Portal. Hier finden Sie Informationen zur Verwaltung von Cloud Identity Service.

Kapitel 2. Serviceanforderungen

Die Serviceanforderungen beinhalten unterstützte Browser für Cloud Identity Service.

Browser

Unterstützte Browser für Cloud Identity Portal-Administration und Self-Service-Anwendungen.

Tabelle 1. Unterstützte Browser

Browser	Version	Betriebssystem
Microsoft Internet Explorer	Neueste Version und Version vor der neuesten Version.	Windows.
Mozilla Firefox	Neueste Version.	Windows und Mac.
Google Chrome	Neueste Version.	Windows und Mac.
Safari	Neueste Version und Version vor der neuesten Version.	Mac.

Anmerkung: Wenn die neueste Version und die Version vor der neuesten Version unterstützt werden, werden auch alle Änderungen dieser Versionen unterstützt. Wenn die neueste Version eines Browsers 24.*n* ist, werden die Versionen 24.*n* und 23.*n* unterstützt.

Anmerkung: Microsoft Edge ist derzeit der neueste MicrosoftBrowser. Microsoft Internet Explorer 11 ist derzeit die neueste Version von Internet Explorer.

Kapitel 3. Übersicht über Cloud Identity Portal

Machen Sie sich mit den Schlüsselfunktionen und -konzepten von Cloud Identity Portal vertraut.

Features und Funktionen

Bei Cloud Identity Portal handelt es sich um eine konsolidierte Verwaltungsumgebung, in der Sie alle Ihre Identity Management- und Access Management-Prozesse verwalten können.

Company Information

Die Unternehmensinformationen enthalten Informationen auf Unternehmensebene für die Personen in Ihrer Organisation, die für das Management oder die Instandhaltung von Cloud Identity Portal zuständig sind.

Directory Management

Bei Directory Management handelt es sich um das System und die Prozesse, die verwendet werden, um die Identität Ihrer Benutzer zu verwalten. Benutzer können in Gruppen zusammengefasst und über Rollen definiert werden. Sie können auch einer Reihe von Services zugeordnet werden.

Sie können Benutzer, Gruppen, Rollen, Services und Benutzerkennwortrichtlinien verwalten. Von Ihnen vorgenommene Zusätze und Änderungen haben unmittelbare Auswirkungen auf die Cloud Identity Service-Authentifizierung und -Berechtigung.

API Key Management

Verwenden Sie API Key Management zum Erstellen, Bearbeiten und Entfernen von API-Berechtigungsnachweisen, die Ihre Organisation verwenden kann, um mit der öffentlichen Cloud Identity Portal-API zu arbeiten.

Application Management

Application Management ist die Konfiguration und Anpassung von Self-Service-Anwendungen. Die Self-Service-Anwendungen beinhalten alle Anwendungen, die Benutzer zum Anfordern und Verwalten ihrer Identitätsprofile benötigen.

Zum Konfigurieren von Self-Service-Anwendungen gehört das Konfigurieren von Selbstregistrierungsoptionen, von Optionen zum Zurücksetzen des Kennworts und zur Wiederherstellung des Benutzernamens.

Zum Anpassen der Benutzerschnittstelle für Self-Service-Anwendungen gehört das Anpassen der Markenkennzeichnung und von E-Mail-Vorlagen sowie das Vergeben von Bezeichnungen für Tabellenspalten und für Benutzerprofilabschnitte.

Web Access Management

Web Access Management ist die Verwaltung von Netzverbindungen zu geschützten Webressourcen.

Sie verwalten den Webzugriff, indem Sie Netzverbindungen zu geschützten Webressourcen erstellen und verwalten. Sie steuern auch den Zugriff auf geschützte Ressourcen durch das Erstellen von Berechtigungsrichtlinien. Zu den Berechtigungsrichtlinien gehören ACLs (Access Control Lists), POPs (Protected Object Policies) und eine globale Benutzerrichtlinie.

Federated Single Sign-on

Federated Single Sign-on (SSO) ermöglicht es Benutzern, die über einen Cloud Identity Service-Account verfügen, unter Verwendung ihrer vorhandenen Identität auf Anwendungsservices von anderen Anbietern zuzugreifen. Eine Cloud Identity Service-Umgebung kann mehrere föderierte Partner unterstützen.

Vorkonfigurierte Vorlagen werden für eine Reihe der am häufigsten verwendeten Partneranwendungsservices bereitgestellt, die ein föderiertes Single-Sign-on mithilfe von SAML 2.0 unterstützen. Wenn keine Vorlage für den Partner vorhanden ist, für den Sie eine Verbindung erstellen möchten, kann eine angepasste Konfiguration verwendet werden.

Identity Provisioning

Sowohl Benutzer als auch Gruppen können über Identitätsfeeds von externen Verzeichnissen oder für externe Verzeichnisse synchronisiert oder eingerichtet werden.

Cloud Identity Service kann eine Schnittstelle mit über 70 Typen von Identitätsrepositorys, wie z. B. Active Directory, LDAP v3, relationale Datenbanken, SOAP-Services, Message Queue und SAP, herstellen.

Request Management

Wenn der normale Genehmiger nicht verfügbar ist und es keinen delegierten Genehmiger gibt, muss möglicherweise ein Cloud Identity Portal-Administrator Benutzeranforderungen für Services verwalten.

Reporting

Cloud Identity Service bietet Funktionen zur Ad-hoc-Berichterstellung für alle Auditereignisdaten innerhalb des Auditrepositorys. Sie können eine Reihe von vordefinierten Berichten verwenden und eigene Berichte definieren.

Kapitel 4. Unternehmensprofil

Die Unternehmensprofilinformationen enthalten Kontaktinformationen auf Unternehmensebene. Accountkontakte sind zuständig für die Verwaltung und Wartung von Cloud Identity Portal.

Übersicht

Die Unternehmensprofilinformationen enthalten Kontaktinformationen auf Unternehmensebene. Accountkontakte sind zuständig für die Verwaltung und Wartung von Cloud Identity Portal. Generieren Sie API-Berechtigungsnachweise, die Ihre Organisation zum Arbeiten mit der öffentlichen Cloud Identity Portal-API mit API-Schlüsselmanagement verwenden kann.

Accountverwaltungsbenutzer hinzufügen

Sie können Accountverwaltungsbenutzer hinzufügen. Accountverwaltungsbenutzer sind zuständig für die Verwaltung und Wartung von Cloud Identity Portal.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Company Profile** > **Account Management** und klicken Sie dann auf **Account Management** und **Add New Account**.
2. Geben Sie einen Benutzernamen für den Benutzer im Feld **Username** ein. Klicken Sie auf **Check Availability** (Verfügbarkeit prüfen), um zu prüfen, ob der Accountbenutzername eindeutig ist.
3. Geben Sie die verbleibenden Kontaktinformationen und -berechtigungsnachweise für den Kontakt ein.

   Anmerkung: Das Kennwort erfordert möglicherweise eine Mindestanzahl an Zeichen und Mindestanzahlen an angegebenen Zeichenarten. Verwenden Sie die Feldhilfe, um die Kennwortanforderungen zu erfahren.
4. Klicken Sie auf **Save**.

   Der Kontakt ist nun auf der Seite **Account Management** verfügbar.

API-Schlüssel verwalten

Generieren Sie API-Berechtigungsnachweise, die Ihre Organisation zum Arbeiten mit der öffentlichen Cloud Identity Portal-API verwenden kann.

Informationen zu diesem Vorgang

Erstellen, bearbeiten und entfernen Sie API-Schlüssel.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Company Profile** > **API Key Management**.
2. Verwalten Sie Ihre API-Schlüssel.

   Fügen Sie einen REST-API-Schlüssel hinzu

   a. Klicken Sie auf **+ Add New API Key**.
   b. Geben Sie die folgenden Felder an:

Tabelle 2. API-Schlüsselfelder

Feld	Beschreibung
Key Alias	Erstellen Sie einen alternativen Namen für den API-Schlüssel mit bis zu fünfzig alphanumerischen Zeichen, der leicht zu erkennen ist.
Key Description	Beschreiben Sie, wofür der Schlüssel verwendet wird und wo er sich befindet.
Access Token Validity	Geben Sie an, für wie viele Sekunden dieses Token gültig ist. Die ungefähre Anzahl an Stunden oder Tagen für den Wert, den Sie eingegeben haben, wird neben diesem Feld angezeigt. Sie erhalten ein Zugriffstoken, nachdem Sie die `client ID`, das `secret` und den `grant_type` an `URL POST https://GmaApi/oauth/token` gesendet haben. Verwenden Sie dieses Zugriffstoken, um Aufrufe an die API zu starten. **Anmerkung:** Der geheime Schlüssel wird einmalig angezeigt, nachdem Sie Ihren neuen API-Schlüssel erstellt haben. Nach dem Speichern der Änderungen für Ihren neuen API-Schlüssel wird der geheime Schlüssel nie wieder angezeigt. Fordern Sie nach Ablauf des Zugriffstokens ein neues an, indem Sie `client ID`, `secret` und `grant_type` angeben. Alternativ können Sie auch ein neues Zugriffstoken anfordern, indem Sie das Aktualisierungstoken, `client ID` und `secret` verwenden.
Refresh Token Validity	Geben Sie die Anzahl an Sekunden für die Zeit für **Refresh Token Validity** an. Dieser Wert muss höher sein als der Wert für **Access Token Validity**. Die ungefähre Anzahl an Stunden oder Tagen für den Wert, den Sie eingegeben haben, wird neben diesem Feld angezeigt.

REST-API-Schlüssel bearbeiten oder löschen

a. Zeigen Sie die Details des API-Schlüssels an, die bearbeitet oder gelöscht werden sollen, indem Sie in der Leiste **Narrow your search** suchen oder indem Sie auf den Pfeil neben dem Schlüsselnamen klicken.
b. Wählen Sie den API-Schlüsselnamen aus, den Sie bearbeiten oder löschen möchten.
c. Führen Sie eine der folgenden Aktionen aus:

- Bearbeiten und ändern Sie die Werte für einen der in Tabelle 1 beschriebenen Schlüssel.
- Klicken Sie auf **Remove Key**, um den Schlüssel dauerhaft zu entfernen.

Kapitel 5. Personen

Die Personalverwaltung besteht aus dem System und den Prozessen, die zum Verwalten der Identität Ihrer Benutzer verwendet werden. Benutzer können in Gruppen organisiert und durch Rollen definiert werden.

Übersicht zur Personalverwaltung

Zu den Tasks der Personalverwaltung gehört die Verwaltung von Benutzern, Gruppen und Services.

Sie können Benutzer, Gruppen und Services erstellen, ändern, löschen und nach ihnen suchen. Hinzufügungen und Änderungen, die Sie vornehmen, haben unmittelbare Auswirkungen auf die Authentifizierung und die Autorisierung in Cloud Identity Service. Wenn Sie z. B. einen Accountdatensatz für einen Benutzer erstellen, kann dieser Benutzer anschließend auf das Cloud Identity Service und auf Self-Service-Anwendungen zugreifen. Sie können auch einen Benutzer zu einer Gruppe hinzufügen, um ihm den Zugriff auf eine bestimmte Webanwendung zu ermöglichen. Wenn eine Genehmigung erforderlich ist, werden Servicemitgliedschaften möglicherweise nicht sofort wirksam.

Benutzer

Sie können Benutzerdatensätze hinzufügen, ändern, löschen und nach ihnen suchen. Ein Benutzerdatensatz kann als Identität oder als Account erstellt werden. Ein Account ermöglicht einem Benutzer den Anmeldungszugriff auf Self-Service-Anwendungen sowie potenziell auf andere Ressourcen, die durch Cloud Identity Service verwaltet werden. Eine Identität ist nur ein Datensatz mit Informationen zu einem Benutzer.

Ein Benutzerdatensatz setzt sich aus einer Reihe von Benutzeridentitätsattributen zusammen. Viele dieser Attribute werden in fast allen Identitätsmanagementsystemen verwendet, wie z. B. Vorname, Nachname und E-Mail-Adresse. Ihre Organisation verfügt außerdem über bestimmte Attribute, die für Ihre Gruppe von Anwendungen eindeutig sind. Attribute werden aus Datensatzquellen oder Identitätsrepositorys, die bereits in Ihrer Organisation vorhanden sind, im Verlauf der Erstkonfiguration von Cloud Identity Service für Ihre Organisation erfasst. Die meisten der bereits vorhandenen Benutzerdatensätze werden aus diesen bereits vorhandenen Identitätsrepositorys erstellt.

Gruppen

Bestimmte Richtlinienentscheidungen im Identity and Access Management werden durch die Behandlung von Benutzern als Verbund am besten durchgesetzt. Benutzer, die gemeinsame Merkmale haben, können in Gruppen zusammengefasst werden. Beispiel: Einer Gruppe von Benutzern, die in derselben Abteilung eines Unternehmens arbeiten, kann dieselbe Art von Zugriff auf eine bestimmte

Webanwendung erteilt werden. In diesem Fall wird die Gruppe der Benutzer definiert. Anschließend wird auf diese Gruppe durch eine Zugriffssteuerungsliste (Access Control List; ACL) verwiesen. Die Richtlinie erteilt (oder verweigert) einen Anwendungszugriff für alle Benutzer in dieser Gruppe.

Die Benutzermitgliedschaft in einer Gruppe kann statisch oder dynamisch definiert werden. Bei einer statischen Benutzermitgliedschaft ist es erforderlich, dass Sie jeden einzelnen Benutzer manuell zu der Gruppe hinzufügen und die Gruppenmitgliedschaft auch manuell verwalten. Bei einer dynamischen Benutzermitgliedschaft werden Benutzer automatisch für eine Mitgliedschaft ausgewählt. Die Mitgliedschaft basiert auf jeder übereinstimmenden Kombination der Identitätsattributwerte, auf anderen Gruppen- oder Servicemitgliedschaften oder auf der Zuordnung einer Managerrolle. Sie können z. B. Benutzer gruppieren, die sich in einem bestimmten Land oder an einem bestimmten Standort befinden. Sie können auch Benutzer gruppieren, deren Account innerhalb eines bestimmten Bereichs von Accountnummern liegt und die außerdem Mitglieder einer anderen angegebenen Gruppe sind.

Die dynamische Benutzermitgliedschaft wird mithilfe einer dynamischen Einrichtungsrichtlinie implementiert, in der Sie die Auswahlkriterien für die Gruppenmitgliedschaft definieren.

Schemamanagement

Sie können Ihr LDAP-Schema (Lightweight Directory Access Protocol) durch das Hinzufügen von angepassten Identitätsattributen verwalten, um die Informationshilfe in Benutzeridentitätsdatensätzen zu erweitern.

Benutzer verwalten

Sie können Benutzerdatensätze hinzufügen, ändern, löschen und nach ihnen suchen.

Übersicht zu Benutzern

Ein Benutzerdatensatz kann als Identität oder als Account erstellt werden. Ein Account ermöglicht einem Benutzer den Anmeldezugriff auf Cloud Identity Service, auf Self-Service-Anwendungen sowie auf andere Ressourcen, die von Cloud Identity Service verwaltet werden. Eine Identität ist nur ein Datensatz mit Informationen zu einem Benutzer.

Ein Benutzerdatensatz setzt sich aus einer Reihe von Benutzeridentitätsattributen zusammen. Viele dieser Attribute werden in fast jedem Identitätsmanagementsystem verwendet, wie z. B. Vorname, Nachname und E-Mail-Adresse. Ihre Organisation verfügt außerdem über bestimmte Attribute, die für Ihre Gruppe von Anwendungen eindeutig sind. Attribute werden aus Datensatzquellen oder Identitätsrepositorys, die bereits in Ihrer Organisation vorhanden sind, im Verlauf der Erstkonfiguration von Cloud Identity Service für Ihre Organisation erfasst.

Gruppen- und Servicemitgliedschaften können Benutzern zugeordnet werden. Für bestimmte Benutzer kann eine angepasste Benutzerrichtlinie erstellt werden. Benutzerrichtlinien definieren die maximale Anzahl an Anmeldefehlern, die maximale Gültigkeitsdauer des Kennworts, die Ablaufdaten für den Account und tageszeitbedingte Einschränkungen für Benutzer.

Nach Benutzern suchen

Sie können nach jedem Benutzerdatensatz in Ihrer Organisation suchen, um die Details des Benutzers anzuzeigen oder zu ändern.

Informationen zu diesem Vorgang

Sie können nach dem Namen, dem Benutzernamen oder der E-Mail-Adresse des Benutzers suchen, wenn diese Werte für den Benutzer eingegeben wurden. Sie können nur die Anfangszeichen des Namens, des Benutzernames oder der E-Mail-Adresse verwenden. Sie können keine Platzhalterzeichen verwenden. Sie müssen mindestens die ersten drei Zeichen des Namens, des Benutzernames oder der E-Mail-Adresse des Benutzers eingeben. Um nach einem Accountbenutzerdatensatz mit der E-Mail-Adresse "psmith@company.com" zu suchen, können Sie `psm` eingeben. Je mehr führende Zeichen Sie eingeben, desto genauer wird die Suche.

Wenn Sie nach einem Datensatz mithilfe des Benutzernamens suchen möchten, können Sie den Vornamen oder den Nachnamen des Benutzers verwenden. Beispiel: Um nach einem Benutzer mit dem Namen "Paul Smith" zu suchen, können Sie `pau` oder `smi` eingeben. Sie können in Ihrer Suche auch mehrere Zeichenfolgen, die durch Leerzeichen voneinander getrennt sind, eingeben, wie z. B. `pau smi`.

Eine Suche kann maximal 1000 Benutzerdatensätze zurückgeben.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **People** > **Users**.
2. Geben Sie im Feld **Begin Search** die ersten drei Zeichen des Vornamens, Nachnamens, Benutzernames oder der E-Mail-Adresse des Benutzers ein. Sie können in Ihrer Suche mehrere Zeichenfolgen eingeben, die durch Leerzeichen voneinander getrennt sind.

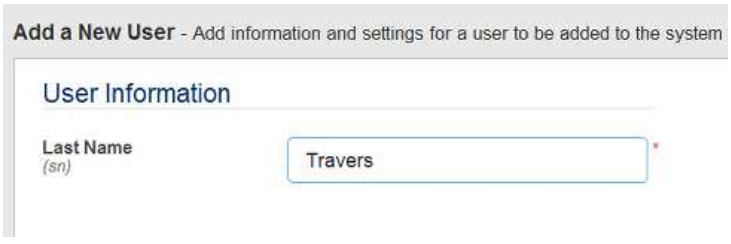
   Die Feldbezeichnung ändert sich in **Filter Results**. Die Benutzer, die mit Ihren Suchkriterien übereinstimmen, werden aufgelistet. Wählen Sie einen Benutzer zum Ändern oder Anzeigen aus.

Benutzerdatensätze hinzufügen

Sie können Datensätze für Benutzer hinzufügen. Sie können einen Datensatz als Account oder als Identität hinzufügen. Nur ein Benutzer mit einem Account kann auf Cloud Identity Service, auf geschützte Ressourcen und auf Self-Service-Anwendungen zugreifen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **People** > **Users** und dann auf **Add User**.

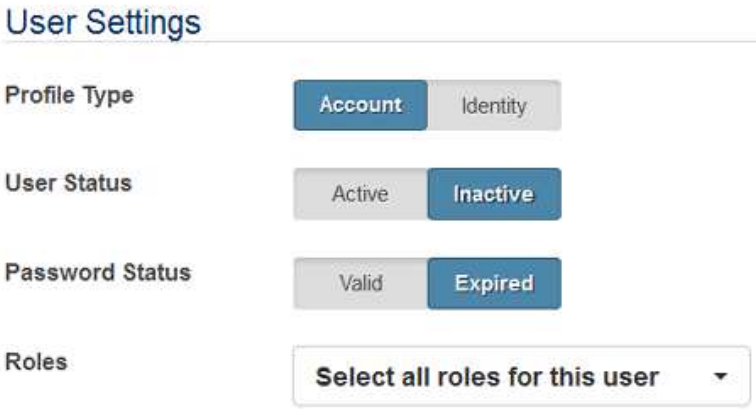


2. Geben Sie den Nachnamen des Benutzers in das Feld **Last Name** ein.
3. Wählen Sie aus, ob der Benutzertyp ein Account oder eine Identität ist.

Ein Account wird verwendet, um einem Benutzer die Anmeldung und den Zugriff auf Cloud Identity Service zu ermöglichen. Eine Identität ist nur ein Datensatz mit Informationen zu einem Benutzer.

- Um den Benutzerdatensatz nur als Identität zu erstellen, klicken Sie auf **Identity**.
- Um den Benutzerdatensatz als Account zu erstellen, klicken Sie auf **Account** und gehen Sie anschließend wie folgt vor:
  a. Geben Sie einen Benutzernamen für den Benutzer im Feld **User Name** ein. Klicken Sie auf **Check Availability** (Verfügbarkeit prüfen), um zu prüfen, ob der Benutzername eindeutig ist.

  b. Wählen Sie als Benutzerstatus **Active** oder **Inactive** aus. Ein aktiver Status ermöglicht dem Benutzer die Anmeldung beim Cloud Identity Portal.



  c. Wählen Sie als Kennwortstatus **Valid** oder **Expired** aus. Ist der Status "Expired" (Abgelaufen), wird der Benutzer gezwungen, sein Kennwort bei der nächsten erfolgreichen Anmeldung zu ändern. Ist der Status "Gültig" (Valid), kann sich der Benutzer anmelden, ohne ein Kennwort zu ändern.
  d. Wählen Sie die Rollen für den Benutzer aus. Klicken Sie auf das Menü **Roles** und markieren Sie alle Rollen, die auf den Benutzer zutreffen.

  Anmerkung: Wenn der Profiltyp ein Account ist, wird das Attribut **gtwayPrincipalName** automatisch zugeordnet, wenn der Datensatz gespeichert wird. Ein Accountdatensatz wird automatisch zum Mitglied von **gatewaywamservice**, wenn der Datensatz gespeichert wird.

4. Optional: Fügen Sie weitere Identitätsattribute für den Benutzer hinzu. Sie können beliebig viele Attribute hinzufügen. So können Sie z. B. einen zweiten Vornamen und eine Mobiltelefonnummer hinzufügen.
   a. Klicken Sie auf **Add Another Attribute**.

Suchen Sie nach dem Attribut, das Sie hinzufügen möchten, indem Sie eine Zeichenfolge in das Suchfeld eingeben. Sie können nach jeder beliebigen Zeichenfolge im Attribut suchen. Attribute werden nach ihrem Registernamen und nach ihrem Cloud Identity Service-Namen (Bezeichnung) aufgelistet, falls verfügbar. Beide Namen werden in die Suche einbezogen. Bezeichnungen werden nur dann einbezogen, wenn sie verfügbar sind. Beispiel: Um nach "User Name" zu suchen, können Sie `use` oder `ser` eingeben.

b. Geben Sie einen Wert für das Attribut ein.

Anmerkung: Das Attribut **`Password`** wird zum Zurücksetzen des Kennworts verwendet. Dieses Feld wird normalerweise während der Selbstregistrierung des Benutzers ausgefüllt. Sie können ein Benutzerkennwort nicht anzeigen.

5. Klicken Sie auf **Save Changes**, um den Datensatz zu speichern.

Gruppenmitgliedschaft zu einem Benutzer hinzufügen

Sie können manuell Gruppenmitgliedschaften zu einem Benutzer hinzufügen. Sie können eine Mitgliedschaft zu Gruppen hinzufügen, die statisch oder dynamisch verwaltet werden.

Informationen zu diesem Vorgang

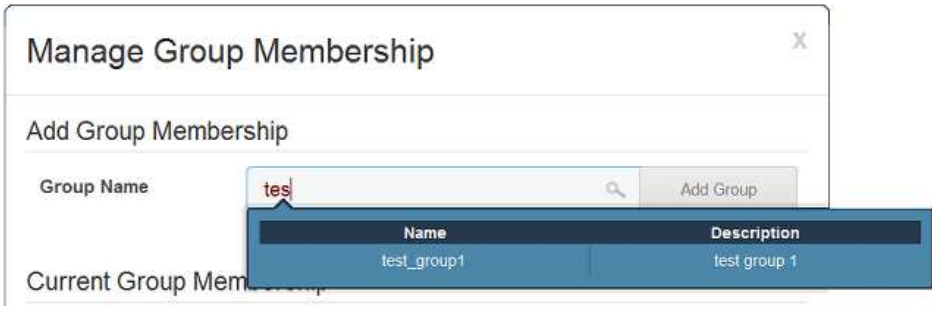
Sie können auch Benutzer zu statischen Gruppen hinzufügen, wenn Sie Gruppen manuell verwalten.

Anmerkung: Wenn Sie eine Mitgliedschaft für einen Benutzer für eine Gruppe manuell hinzufügen, die dynamisch verwaltet wird, wird die fortgesetzte Mitgliedschaft des Benutzers durch die Richtlinie der Gruppe beim nächsten Richtlinienabgleich bestimmt.

Vorgehensweise

1. Suchen Sie nach dem Benutzer und wählen Sie ihn aus.
2. Unter **User Settings** (Benutzereinstellungen):
   - Wenn es sich bei der Gruppe um die erste Gruppe handelt, zu der Sie den Benutzer hinzufügen möchten, klicken Sie auf **Add New Group**.

- Wenn der Benutzer bereits ein Mitglied von einer oder mehreren Gruppen ist, klicken Sie auf **Manage Group Membership**.



3. Suchen Sie im Feld **Group Name** nach der Gruppe, zu der Sie den Benutzer hinzufügen möchten. Um nach einer Gruppe zu suchen, geben Sie mindesten die ersten drei Zeichen des Namens der Gruppe ein.
4. Wählen Sie die Gruppe aus und klicken Sie auf **Add Group**.
5. Klicken Sie auf **Done**.

Servicemitgliedschaft zu einem Benutzer hinzufügen

Sie können manuell Servicenmitgliedschaften zu einem Benutzer hinzufügen. Das Hinzufügen von Servicemitgliedschaften zu einem Benutzer richtet sich nach den aktuell geltenden Servicegenehmigungen.

Informationen zu diesem Vorgang

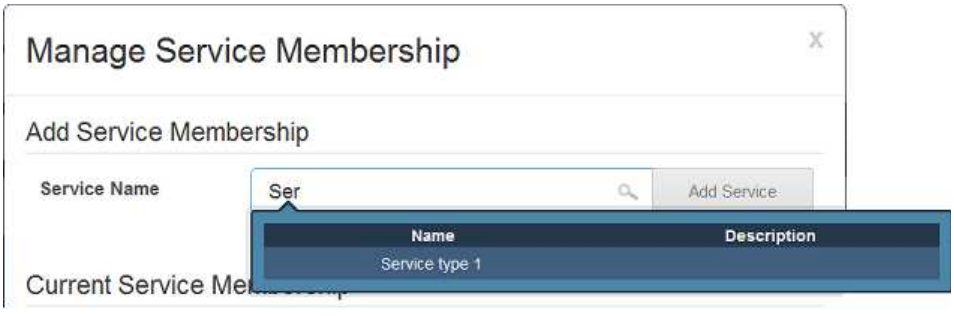
Wenn Sie eine Servicemitgliedschaft zu einem Benutzer hinzufügen und eine Genehmigungsrichtlinie für diesen Service gilt, wird der Benutzer nicht automatisch zum Service hinzugefügt. In diesem Fall wird eine Anforderung für den Benutzer generiert, damit er ein Mitglied des Service werden kann. Außerdem wird eine E-Mail-Benachrichtigung zu einer anstehenden Serviceanforderung an die Genehmiger gesendet.

Anmerkung: Wenn Sie eine Mitgliedschaft für einen Benutzer für einen Service manuell hinzufügen, die dynamisch verwaltet wird, wird die fortgesetzte Mitgliedschaft des Benutzers durch die Richtlinie des Service beim nächsten Richtlinienabgleich bestimmt.

Sie können auch Benutzer zur Servicemitgliedschaft hinzufügen, wenn Sie Services verwalten.

Vorgehensweise

1. Suchen Sie nach dem Benutzer und wählen Sie ihn aus.
2. Klicken Sie unter **User Settings** auf **Manage Service Membership** (Servicemitgliedschaft verwalten).



3. Suchen Sie im Feld **Service Name** nach dem Service, zu der Sie den Benutzer hinzufügen möchten. Um nach einem Service zu suchen, geben Sie mindesten die ersten drei Zeichen des Namens des Service ein.
4. Wählen Sie den Service aus und klicken Sie auf **Add Service**.

Benutzerrichtlinie zu einem Benutzer hinzufügen

Benutzerrichtlinien definieren bestimmte Einschränkungen für die Kennwortvalidierung, die Ablaufdaten für Accounts und Tageszeiteinschränkungen. Globale Benutzerrichtlinien werden auf alle Benutzer angewendet. Eine angepasste Benutzerrichtlinie wird auf einen bestimmten Benutzer angewendet.

Informationen zu diesem Vorgang

Richtlinieneinstellungen, die auf Benutzerebene festgelegt werden, setzen entsprechende Einstellungen in der globalen Richtlinie außer Kraft. Standardmäßig sind alle Richtlinienwerte auf Benutzerebene nicht gesetzt. Eine Richtlinieneinstellung, die auf der Benutzerebene nicht gesetzt ist, übernimmt die Einstellung von der globalen Richtlinie, falls eine vorhanden ist.

Vorgehensweise

1. Suchen Sie nach dem Benutzer und wählen Sie ihn aus.
2. Klicken Sie in **User Settings** (Benutzereinstellungen) auf **Manage User Policy** (Benutzerrichtlinie verwalten).
3. Legen Sie die gewünschten Benutzerrichtlinieneinstellungen fest.
4. Klicken Sie auf **Save**.

   Sie können dieselbe Benutzerrichtlinie auch auf andere Benutzer anwenden.
5. Klicken Sie auf **Done**.

Benutzerrichtlinieneinstellungen

Tabelle 3. Benutzerrichtlinieneinstellungen

Einstellung	Beschreibung
Maximum Login Failures	Die maximale Anzahl an fehlgeschlagenen Anmeldeversuchen, die ein Benutzer durchführen kann, bevor der Account gesperrt wird. Ist diese Option auf "0" oder "Unset" gesetzt, ist die Anzahl der fehlgeschlagenen Anmeldeversuche unbegrenzt. • **Set**. Die maximale Anzahl der fehlgeschlagenen Anmeldeversuche. Ist diese Option auf "0" gesetzt, ist die Anzahl der fehlgeschlagenen Anmeldeversuche unbegrenzt. • **Unset**. Unbegrenzte Anzahl der fehlgeschlagenen Anmeldeversuche.

Tabelle 3. Benutzerrichtlinieneinstellungen (Forts.)

Einstellung	Beschreibung
Disable Time Interval	Gibt an, ob Benutzeraccounts gesperrt werden, nachdem die Anzahl für "Max Login Failures" überschritten wurde. • **Set**. Benutzeraccounts werden gesperrt, nachdem die Anzahl für "Max Login Failures" überschritten wurde. Accounts werden dauerhaft oder vorübergehend inaktiviert. • **Unset**. Benutzeraccounts werden nie aufgrund von fehlgeschlagenen Anmeldeversuchen gesperrt. "Unset" entspricht dem Festlegen des Werts für "Max Login Failures" auf "0" oder auf "Unset". Benutzer können eine unbegrenzte Anzahl an Anmeldeversuchen durchführen. • **Disable Permanently**. Der Benutzer wird dauerhaft gesperrt, bis ein Cloud Identity Portal-Administrator den Benutzerstatus des Benutzers auf "valid" setzt. • **Disable Temporarily**. Die Zeit in Sekunden, für die ein Benutzeraccount gesperrt bleibt, nachdem die zulässige Anzahl für "Max Login Failures" überschritten wurde. Der Account wird nach Ablauf der Intervallzeit entsperrt.
Minimum Length	Die minimale Anzahl der Zeichen, die für ein gültiges Accountkennwort erforderlich sind. • **Set**. Die minimale Anzahl der Zeichen für ein Kennwort. • **Unset**. Keine Mindestlänge für das Kennwort.
Minimum Alphas	Die minimale Anzahl der alphabetischen Zeichen, die für Accountkennwörter erforderlich sind. • **Set**. Die minimale Anzahl der alphabetischen Zeichen, die das Accountkennwort enthalten muss. • **Unset**. Es gibt keinen Mindestwert.
Minimum Non-Alphas	Die minimale Anzahl der nicht alphabetischen Zeichen (Zahlen oder Sonderzeichen), die für Accountkennwörter erforderlich sind. • **Set**. Die minimale Anzahl der nicht alphabetischen Zeichen, die das Accountkennwort enthalten muss. Ist der Wert auf "0" gesetzt, gibt es keinen Mindestwert. • **Unset**. Es gibt keinen Mindestwert.
Maximum Repeated Characters	Die maximale Anzahl der aufeinanderfolgenden wiederholten Zeichen, die in einem Accountkennwort gültig sind. • **Set**. Die maximale Anzahl an wiederholten Zeichen, die gültig sind. • **Unset**. Unbegrenzte Anzahl an wiederholten Zeichen.
Spaces Allowed?	Gibt an, ob Accountkennwörter Leerzeichen enthalten können. • **Set**. Gibt an, ob Leerzeichen zulässig sind. – **Yes**. Leerzeichen sind zulässig. – **No**. Leerzeichen sind nicht zulässig. • **Unset**. Leerzeichen sind zulässig.
Password Expires?	Die Höchstdauer, für die Kennwörter nach der Erstellung gültig bleiben, bevor sie ablaufen und geändert werden müssen. • **Yes**. Die Anzahl der Tage, Stunden, Minuten und Sekunden, für die ein Kennwort gültig bleibt. Wenn alle Werte auf 0 gesetzt sind, laufen Kennwörter nie ab. • **No**. Kennwörter laufen nie ab.

Tabelle 3. Benutzerrichtlinieneinstellungen (Forts.)

Einstellung	Beschreibung
Track Password Reuse?	Gibt an, ob bei einer Kennwortzurücksetzung dasselbe Kennwort verwendet werden kann. • **Yes**. Benutzer können nicht dasselbe Kennwort verwenden, wenn sie ihr Kennwort zurücksetzen oder ändern. Geben Sie die Anzahl neuer eindeutiger Kennwörter an, die angegeben werden muss, bevor ein altes Kennwort wiederverwendet werden kann. • **No**. Benutzer können dasselbe Kennwort verwenden, wenn sie ihr Kennwort zurücksetzen.
Account Expires?	Gibt ein Ablaufdatum an, nach dem alle Accounts ungültig werden. Diese Einstellung wird normalerweise nur zum Außerkraftsetzen einzelner Benutzerrichtlinien verwendet. Wenn z. B. ein Auftragnehmer über einen begrenzten Zugriffszeitraum für eine bestimmte Ressource verfügt, kann diese Option verwendet werden, um diesen Zugriff an einem bestimmten Datum zu inaktivieren. • **Set**. Das Ablaufdatum für Accounts. Geben Sie das Datum im Format MM/TT/JJJJ ein. • **Unset**. Unbegrenzter Gültigkeitszeitraum. Die Gültigkeit von Accounts läuft nie ab.
Limit Access?	Gibt eine Einschränkung bezüglich der Tageszeit an, zu der Benutzer auf das System zugreifen dürfen. • **Yes**. Die Tage und die Tageszeit, zu der Benutzer auf das Cloud Identity Service zugreifen dürfen. Die Zeit kann als Ortszeit für den Service oder als koordinierte Weltzeit (Coordinated Universal Time, UTC) angegeben werden. • **No**. Benutzer können jederzeit auf das Cloud Identity Service zugreifen.

Benutzerkennwörter zurücksetzen

Als Administrator von Cloud Identity Portal können Sie ein Benutzerkennwort zurücksetzen.

Informationen zu diesem Vorgang

Wenn Sie ein Benutzerkennwort als Administrator im Cloud Identity Portal zurücksetzen, fügen Sie das Kennwortattribut zum Benutzeraccountdatensatz hinzu. Aus Sicherheitsgründen werden das Kennwortattribut und der Kennwortwert eines Benutzeraccountdatensatzes nicht angezeigt. Wenn Sie das Kennwortattribut hinzufügen und einen Wert eingeben, setzen Sie dadurch das Kennwort zurück. Nachdem Sie das Kennwort zurückgesetzt haben, werden das Kennwortattribut und der -wert nicht angezeigt, wenn Sie erneut auf den Benutzeraccountdatensatz zugreifen.

Wenn der Benutzer, dessen Kennwort zurückgesetzt wird, über eine E-Mail-Adresse verfügt, empfängt er eine E-Mail, die ihn darüber benachrichtigt, dass sein Kennwort zurückgesetzt wurde.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Directory Management** > **Users**.
2. Suchen Sie nach dem Benutzer und wählen Sie ihn aus.

3. Klicken Sie auf **Add Another Attribute**.

4. Suchen Sie nach dem Kennwortattribut, indem Sie eine Zeichenfolge in das Suchfeld eingeben, und wählen Sie das Kennwortattribut aus. Geben Sie z. B. `pass` ein.

   Attribute werden nach ihrem Registernamen und nach ihrem Cloud Identity Service-Namen (Bezeichnung) aufgelistet. Beide Namen werden in die Suche einbezogen.
5. Geben Sie ein Kennwort in das Feld **Password** ein. Die Zeichen, die Sie eingeben, werden durch Sterne ersetzt.
6. Klicken Sie auf **Save Changes**, um den Datensatz zu speichern.

Gruppen verwalten

Bestimmte Entscheidungen im Identity and Access Management können am besten implementiert werden, wenn Gruppen von Benutzern auf dieselbe Art behandelt werden. Sie können Gruppen erstellen, indem Sie Benutzer manuell auswählen, oder Sie können dynamische Richtlinien erstellen, die die Gruppenmitgliedschaft automatisieren.

Übersicht zu Gruppen

Gruppen von Benutzern, die gemeinsame Merkmale haben, können zusammengefasst werden, sodass sie als Verbund behandelt werden können. Beispiel: Einer Gruppe von Benutzern, die in derselben Abteilung eines Unternehmens arbeiten, kann dieselbe Art von Zugriff auf eine bestimmte Webanwendung erteilt werden.

Die Benutzermitgliedschaft in einer Gruppe kann statisch oder dynamisch definiert werden. Bei einer statischen Benutzermitgliedschaft ist es erforderlich, dass Sie jeden einzelnen Benutzer manuell zu der Gruppe hinzufügen und die Gruppenmitgliedschaft auch manuell verwalten. Bei einer dynamischen Benutzermitgliedschaft werden die Benutzer für die Mitgliedschaft automatisch auf der Grundlage einer übereinstimmenden Kombination der zugehörigen Identitätsattributwerte, anderer Gruppenmitgliedschaften, anderer Servicemitgliedschaften oder abhängig davon, ob dem Benutzer eine Rolle als Manager zugeordnet wurde, ausgewählt. Sie können z. B. Benutzer gruppieren, die sich in einem bestimmten Land oder an einem bestimmten Standort befinden. Sie können auch Benutzer gruppieren, deren Account innerhalb eines bestimmten Bereichs von Accountnummern liegt und die außerdem Mitglieder einer anderen angegebenen Gruppe sind.

Die dynamische Benutzermitgliedschaft wird mithilfe einer dynamischen Einrichtungsrichtlinie implementiert, in der Sie die Auswahlkriterien für die Gruppenmitgliedschaft definieren.

Für eine Gruppe kann eine beliebige Anzahl an Richtlinien definiert werden. Eine Richtlinie kann bei Bedarf durch Abgleichen der Richtlinie angewendet werden. Eine Richtlinie kann außerdem anhand eines Zeitplans angewendet werden. Wenn eine Richtlinie angewendet wird, werden die Auswahlkriterien ausgewertet und

die Benutzermitgliedschaft wird aktualisiert. Dabei werden nicht (mehr) übereinstimmende Benutzer entfernt und übereinstimmende Benutzer hinzugefügt.

Nach Gruppen suchen

Sie können nach jeder Gruppe in Ihrer Organisation suchen, um die Details der Gruppe anzuzeigen oder zu ändern oder um die Mitgliedschaft in der Gruppe zu verwalten.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **People** > **Groups**.
2. Geben Sie im Feld **Filter Results** mindestens die ersten drei Zeichen der Gruppe ein. Die Feldbezeichnung ändert sich in **Searching For**.

   Die Gruppen, die mit Ihren Suchkriterien übereinstimmen, werden aufgelistet. Wählen Sie eine Gruppe zum Ändern oder Anzeigen aus.

Gruppen erstellen

Sie können neue Gruppen erstellen. Nach dem Erstellen einer Gruppe können Sie Benutzer als Mitglieder der Gruppe auswählen und die Gruppe statisch oder dynamisch verwalten.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **People** > **Groups** und klicken Sie dann auf **Add Group**.
2. Geben Sie einen Namen und eine Beschreibung für die Gruppe ein. Überprüfen Sie, ob der Gruppenname bereits verwendet wird, indem Sie auf **Check Availability** (Verfügbarkeit prüfen) klicken.
3. Klicken Sie auf **Save Changes**, um die Gruppe hinzuzufügen.

Nächste Schritte

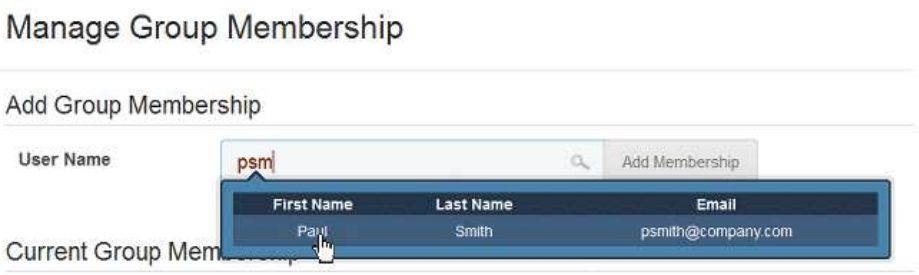
Nach dem Erstellen der Gruppe können Sie manuell oder dynamisch Mitglieder zur Gruppe hinzufügen.

Mitgliedschaft in einer Gruppe statisch verwalten

Für eine statisch definierte Benutzermitgliedschaft ist es erforderlich, dass Sie jedes Benutzermitglied manuell hinzufügen oder entfernen.

Vorgehensweise

1. Suchen Sie nach der Gruppe, zu der Sie Mitglieder hinzufügen möchten, und wählen Sie sie aus.
2. Klicken Sie auf **Manage Group Membership**.



3. Suchen Sie im Feld **User Name** nach dem Benutzer, den Sie hinzufügen möchten. Um nach einem Benutzer zu suchen, geben Sie die ersten drei Zeichen des Vornamens, Nachnamens, Benutzernames oder der E-Mail-Adresse des Benutzers ein.
4. Wählen Sie den Benutzer aus und klicken Sie auf **Add Membership**.
5. Nachdem Sie alle gewünschten Benutzer hinzugefügt haben, klicken Sie auf **Done**.

Mitgliedschaft in Gruppen dynamisch verwalten

Dynamische Einrichtungsrichtlinien ermöglichen es, dass eine Benutzermitgliedschaft in einer Gruppe auf Übereinstimmungskriterien basiert. Benutzer, die mit den Bedingungen übereinstimmen, werden automatisch für die Mitgliedschaft in der Gruppe ausgewählt.

Dynamische Einrichtungsrichtlinien erstellen

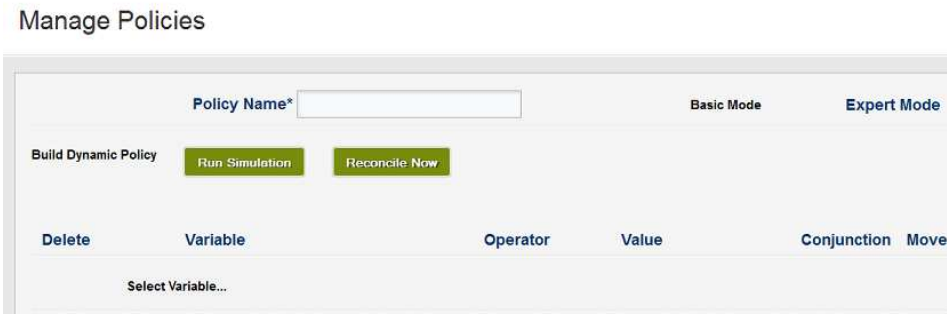
Mithilfe von dynamischen Einrichtungsrichtlinien kann die Benutzermitgliedschaft von Gruppen bestimmt werden.

Informationen zu diesem Vorgang

Die Mitgliedschaft basiert auf den Auswahlkriterien der Richtlinie. Sie können beispielsweise die Mitgliedschaft in einer Gruppe durch ein Attribut angeben, das den Arbeitsplatz bestimmt, oder durch ein Attribut, das den Arbeitsplatz und die Mitgliedschaft in einer anderen Gruppe bestimmt. Eine Gruppe kann über eine oder mehrere Richtlinien verfügen.

Vorgehensweise

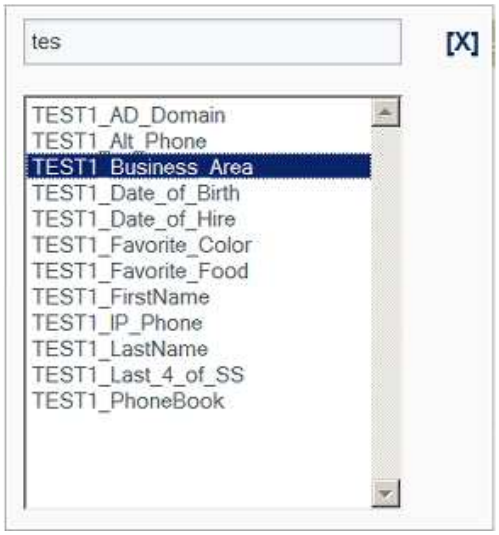
1. Suchen Sie nach der Gruppe, zu der Sie eine Richtlinie hinzufügen möchten, und wählen Sie sie aus.
2. Klicken Sie für **Dynamic Provisioning Policy** (Dynamische Einrichtungsrichtlinie) auf **Manage Policy** (Richtlinie verwalten).
3. Klicken Sie auf **Add New Policy**.



4. Geben Sie einen aussagekräftigen Namen für die Richtlinie im Feld **Policy Name** ein.
5. Wählen Sie die Variablen aus, die Sie verwenden möchten. Sie können eine oder mehrere Variablen eines beliebigen Typs auswählen, um sie in Ihrer Richtlinie zu verwenden. Sie können eine beliebige Kombination der folgenden Variablentypen auswählen:
   - **Attribute**. Sie können Benutzer auf der Grundlage eines Benutzeridentitätsattributs einbeziehen.
   - **Group**. Sie können Benutzer auf der Grundlage von anderen Gruppenmitgliedschaften einbeziehen oder ausschließen.

- **Service**. Sie können Benutzer auf der Grundlage von Servicemitgliedschaften einbeziehen oder ausschließen.
- **Manager**. Sie können Benutzer auf der Grundlage der Tatsache einbeziehen, ob ihnen die Rolle eines Managers zugeordnet wurde.

6. Gehen Sie wie folgt vor, um ein Benutzeridentitätsattribut als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Attribute**.
   b. Klicken Sie in das Feld **Filter Attributes** und geben Sie die ersten Zeichen des Attributs ein. Klicken Sie doppelt auf das Attribut, um es auszuwählen.

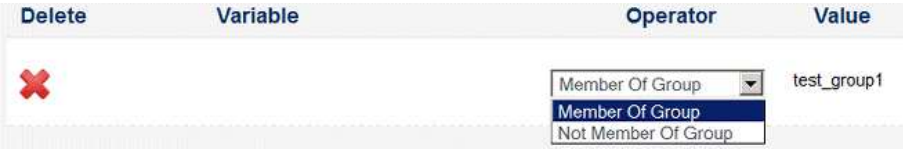


   c. Wählen Sie einen **Operator** aus und geben Sie einen Wert (**Value**) für das Attribut ein.

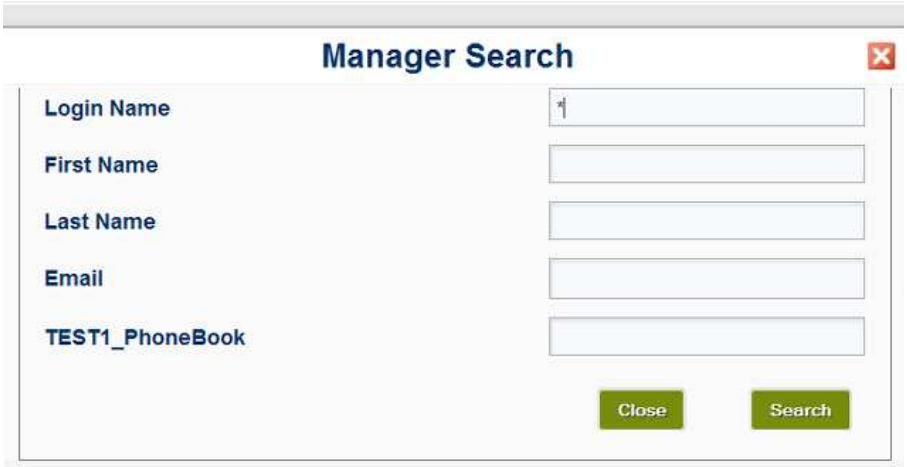
   Anmerkung: Sie können Platzhalterzeichen verwenden. Sie können z. B. "11*" eingeben, was jede Zahl darstellt, die mit "11" beginnt.

   Tipp: Wenn Ihre Organisation über Attribute verfügt, die Datumswerte verwenden, können Sie ein solches Attribut als Zeitmarke behandeln. Weitere Informationen zur Verwendung von Zeitmarken finden Sie unter „Zeitmarkenwerte” auf Seite 25. Informationen zum Suchen und Anzeigen der von Ihrer Organisation verwendeten Attribute finden Sie unter „Angepasste Attribute verwalten” auf Seite 31.

7. Gehen Sie wie folgt vor, um eine Mitgliedschaft oder eine nicht vorhandene Mitgliedschaft bei einer anderen Gruppe als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Group**.
   b. Klicken Sie in das Feld **Filter Groups** und geben Sie die ersten Zeichen der Gruppe ein. Klicken Sie doppelt auf die Gruppe, um sie auszuwählen.
   c. Wählen Sie aus, ob die Mitgliedschaft von der Mitgliedschaft in dieser anderen Gruppe abhängig ist oder ob die Mitgliedschaft von der Nichtmitgliedschaft in dieser anderen Gruppe abhängig ist.



8. Gehen Sie wie folgt vor, um eine Mitgliedschaft oder eine nicht vorhandene Mitgliedschaft bei einem Service als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Service**.
   b. Klicken Sie in das Feld **Filter Services** und geben Sie die ersten Zeichen des Service ein. Klicken Sie doppelt auf den Service, um ihn auszuwählen.
   c. Wählen Sie aus, ob die Mitgliedschaft von der Mitgliedschaft in diesem Service abhängig ist oder ob die Mitgliedschaft von der Nichtmitgliedschaft in diesem Service abhängig ist.
9. Gehen Sie wie folgt vor, um die Managerrolle als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Manager**.



   b. Suchen Sie im Fenster **Manager Search** nach dem Benutzer, indem Sie Suchkriterien in eines der Felder eingeben. Klicken Sie auf **Search**. Nur Benutzer, denen die Rolle eines Managers zugeordnet wurde und die Ihren Suchkriterien entsprechen, werden zurückgegeben.

      Anmerkung: Sie können Platzhalterzeichen in Ihrer Suche verwenden. Sie können z. B. `Joh*` eingeben, um Namen darzustellen, die mit "Joh" beginnen.
   c. Wählen Sie den Benutzer aus. Sie können die Suche wiederholen, um weitere Benutzer hinzuzufügen.
10. Verwenden Sie das Feld **Conjunction**, um eine oder mehrere Variablen zum Bestimmen der Mitgliedschaft in der Gruppe zu kombinieren. Verwenden Sie den Konjunktionswert `And` oder `Or`, um das Ergebnis eines Vergleichskriteriums mit der nächsten Zeile zu kombinieren.

    Die Gruppierung der Variablen (Bedingungen) wird von oben nach unten durchgeführt, sodass das Ergebnis der vorherigen Bedingungen mit der nachfolgenden Bedingung verbunden wird.

    Verwenden Sie die Pfeilsymbole, um Bedingungen nach oben oder unten zu verschieben. △ ▽

    Im folgenden Beispiel wird nur eine Variable zum Bestimmen der Mitgliedschaft verwendet: das Benutzeridentitätsattribut "TEST1_Business_Area". Um

ein Mitglied zu sein, muss ein Benutzer den Wert "London W4" für das Attribut "TEST1_Business_Area" aufweisen.

Im folgenden Beispiel werden zwei Variablen zum Bestimmen der Mitgliedschaft verwendet. Um ein Mitglied zu sein, muss ein Benutzer den Wert "London W4" für das Attribut "TEST1_Business_Area" aufweisen und er muss Mitglied in der Gruppe "Group1" sein.

Im folgenden Beispiel werden drei Variablen zum Bestimmen der Mitgliedschaft verwendet. Um ein Mitglied zu sein, muss ein Benutzer den Wert "London W4" für das Attribut "TEST1_Business_Area" aufweisen und er muss Mitglied in der Gruppe "Group1" oder Mitglied in der Gruppe "Group2" sein.

11. Nachdem Sie alle Bedingungen, die in Ihrer Richtlinie verwendet werden sollen, definiert haben, klicken Sie auf **Save**.

Nächste Schritte

Simulieren Sie die Richtlinie, um zu überprüfen, ob die Mitgliedschaft Ihren Erwartungen entspricht.

Zeitmarkenwerte:

Wenn Sie möchten, dass ein Attribut und ein Attributwert als Zeitmarke behandelt werden, können Sie für den Wert das Präfix `$date$` festlegen.

Das Präfix `$date$` nimmt das Standarddatumsformat JJJJ-MM-TT hh:mm:ss an. Beispiel: Sie können `$date$1970-01-01 00:00:00` angeben, um das Datum 1. Januar 1970 um Mitternacht anzugeben, oder Sie können die aktuelle Uhrzeit angeben, indem Sie `$date$now` eingeben.

Sie können auch ein vom Standard abweichendes Format für die Zeitmarke angeben, indem Sie das Format in das Präfix `$date$` einschließen, indem Sie die Option `SimpleDateFormat` verwenden. Beispiel: Für eine Z-Zeitmarke können Sie

`$date{yyyy-MM-dd HH:mm:ssZ}$1970-01-01 00:00:00-0400` eingeben, um den 1. Januar 1970 um Mitternacht in der Zeitzone 4 Stunden vor GMT/UTC anzugeben. Durch das Ändern des Standardformats wird dasselbe Format auf die Attributwerte, die abgerufen werden, angewendet. Sie müssen das Format der Werte verstehen, die Sie abrufen möchten. Das Format der abgerufenen Datumswerte muss mit dem Format konsistent sein, das Sie verwenden möchten. Weitere Informationen zu verschiedenen Datumsformatmustern finden Sie unter SimpleDateFormat.

Wenn entweder der in der Regel angegebene Wert oder der Vergleichswert nicht ohne Ausnahmebedingung analysiert werden, wird eine Warnung oder ein Fehler protokolliert. Weitere Informationen hierzu erhalten Sie bei Ihrem IBM Support-Mitarbeiter. UTC (Coordinated Universal Time) ist die Standardzeitzone.

Im folgenden Beispiel werden zwei Attributvariablen zum Bestimmen der Mitgliedschaft auf Grundlage des Einstellungsdatums verwendet. Damit der Benutzer Mitglied sein kann, muss das Einstellungsdatum für den Benutzer nach dem 1. Januar 2016 und vor dem aktuellen Datum und der aktuellen Uhrzeit liegen.

Dynamische Einrichtungsrichtlinien im Expertenmodus erstellen

In einigen Fällen können die Auswahlkriterien für die Richtlinie für eine Gruppe nicht mithilfe eines grundlegenden Attributvergleichs und mit einer anderen Gruppen- oder Servicemitgliedschaft bestimmt werden. Für die Mitgliedschaft ist möglicherweise die Überprüfung von Attributwerten (Unterzeichenfolgen) erforderlich, die auf dem Wert eines anderen Attributs basieren und die daher variieren. In diesem Fällen müssen Sie die Richtlinie im Expertenmodus definieren.

Vorbereitende Schritte

Um den Expertenmodus verwenden zu können, müssen Sie über gute Kenntnisse und fortgeschrittenes Wissen in der Codierung von JavaScript verfügen.

Informationen zu diesem Vorgang

Sie definieren Richtlinien im Expertenmodus in JavaScript.

Während der Richtlinienauswertung wird das JavaScript jeweils ein Mal für jeden Benutzer in der Registry ausgeführt. Das JavaScript prüft die Registryattribute des Benutzers und seine Mitgliedschaften und entscheidet, ob der Benutzer in die Gruppe aufgenommen wird. Das JavaScript kommuniziert diese Entscheidung an Cloud Identity Service mithilfe der Variable **`inGroup`**. Wenn das Ergebnis des JavaScript bedeutet, dass **`inGroup`** gleich "true" (wahr) ist, wird der Benutzer in die Gruppe aufgenommen, andernfalls wird er nicht aufgenommen.

Das JavaScript kann drei Methoden zum Anfordern von Cloud Identity Service-Registryattributen und Gruppeninformationen zu jedem Benutzer verwenden.

- `String isMemberOfGroup(String groupName)`
- `String[] getAttributeValues(String attributeName)`

- `String evaluateAttribute(String attributeName, int operator, String constant)`

Jede dieser Methoden kann mit einer anderen Variable **ldap** aufgerufen werden, die für das JavaScript verfügbar ist. Um beispielsweise zu bestimmen, ob der aktuelle Benutzer ein Mitglied einer Gruppe mit dem Namen **accounting** ist, kann die folgende Anweisung verwendet werden:

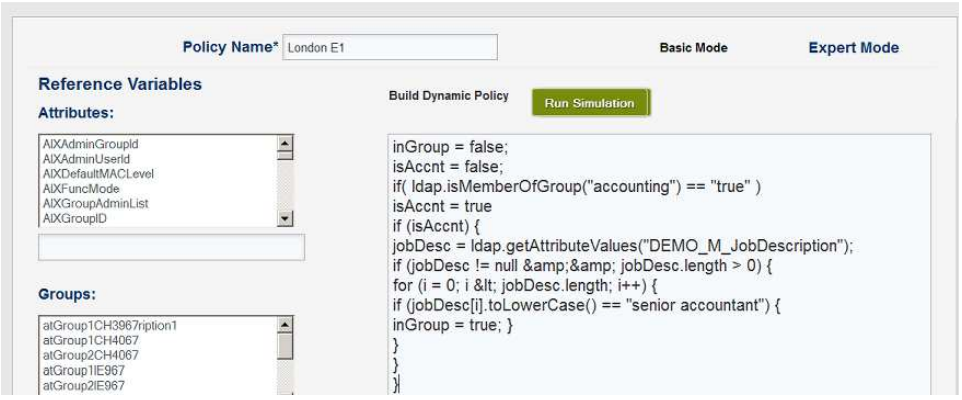
```
var isAccountant = ldap.isMemberOfGroup("accounting");
```

Im folgenden JavaScript-Beispiel wird der Benutzer in die Richtliniengruppe aufgenommen, wenn er ein Mitglied der Gruppe **accounting** ist und den Wert **senior accountant** im Attribut **DEMO_M_JobDescription** aufweist.

```
// assume user is not in group
inGroup = false;
isAccnt = false;
if( ldap.isMemberOfGroup("accounting") == "true" )
isAccnt = true
if (isAccnt) {
jobDesc = ldap.getAttributeValues("DEMO_M_JobDescription");
if (jobDesc != null && jobDesc.length > 0) {
for (i = 0; i < jobDesc.length; i++) {
if (jobDesc[i].toLowerCase() == "senior accountant") {
inGroup = true; }
}
}
}
```

Vorgehensweise

1. Suchen Sie nach der Gruppe, zu der Sie eine Richtlinie hinzufügen möchten, und wählen Sie sie aus.
2. Klicken Sie für **Dynamic Provisioning Policy** (Dynamische Einrichtungsrichtlinie) auf **Manage Policy** (Richtlinie verwalten).
3. Klicken Sie auf **Add New Policy**.
4. Klicken Sie auf **Expert Mode**.



5. Geben Sie das JavaScript ein, das Sie zum Bestimmen der Mitgliedschaft verwenden möchten.

   Attributes, **Groups** und **Services** werden in den entsprechenden Feldern als Referenz aufgelistet. Sie können nach Attributen, Gruppen und Services suchen,

indem Sie die ersten Zeichen in das Filterfeld unter dem entsprechenden Feld eingeben. Sie können ein ausgewähltes Attribut, eine Gruppe oder einen Service kopieren und einfügen.

6. Nachdem Sie alle Bedingungen, die in Ihrer Richtlinie verwendet werden sollen, definiert haben, klicken Sie auf **Save**, um die Richtlinie zu speichern.

Nächste Schritte

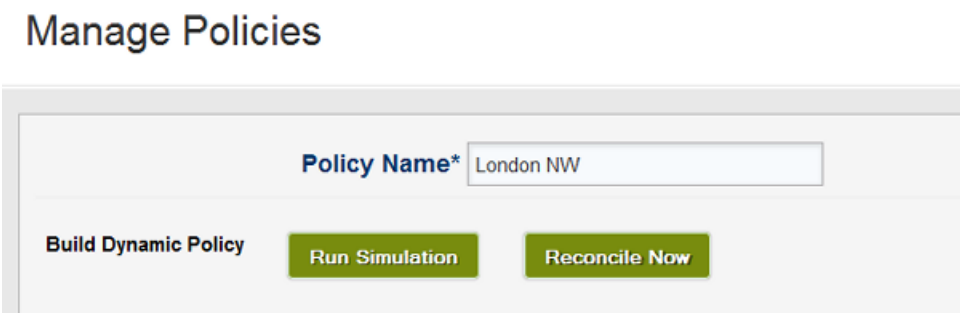
Simulieren Sie die Richtlinie, um zu überprüfen, ob die Mitgliedschaft Ihren Erwartungen entspricht.

Richtlinie simulieren

Sie können eine Richtlinie simulieren, um die Benutzermitgliedschaft in einer Gruppe auszuwerten und zu überprüfen, ob die Mitgliedschaft Ihren Erwartungen entspricht. Die Simulation ändert die Mitgliedschaft in der Gruppe nicht. Sie zeigt an, welche Benutzer die vorgeschlagene Mitgliedschaft in der Gruppe erfüllen. Die Ergebnisse können angezeigt und in einer CSV-Datei gespeichert werden.

Vorgehensweise

1. Wenn Sie die Richtlinie nicht ausgewählt haben, suchen Sie nach der Gruppe und wählen Sie sie aus. Öffnen Sie das Fenster **Manage Policies**, um die Richtlinie zu bearbeiten.
2. Klicken Sie auf **Run Simulation**.



3. Wählen Sie einen Simulationstyp für die Ausführung.
   - **Simulate all users in the directory** (Alle Benutzer im Verzeichnis simulieren). Diese Option vergleicht die Richtlinienauswahl mit allen Benutzern im Cloud Identity Service. Die Benutzer, die die Richtlinie erfüllen, werden in den Ergebnissen als "Hinzugefügt" oder als "Beibehalten" aufgelistet. Benutzer, die die Richtlinie nicht erfüllen, werden in den Ergebnissen als "Aus der Gruppe entfernt" oder als "Nicht hinzugefügt" aufgelistet.
   - **Simulate all users currently in the group** (Alle derzeit in der Gruppe enthaltenen Benutzer simulieren). Diese Option vergleicht die Richtlinienauswahlkriterien mit den Attributen aller Benutzer, die derzeit in der Gruppe enthalten sind. Jeder Benutzer in der Gruppe wird in den Ergebnissen als "Entfernt" oder "Beibehalten" aufgelistet. Es werden keine neuen Benutzer als "Hinzugefügt" aufgelistet.
   - **Simulate a single user** (Einzelnen Benutzer simulieren). Diese Option vergleicht die Richtlinienauswahlkriterien mit einem ausgewählten Benutzer. Dieser Benutzer wird in den Ergebnissen als "Beibehalten", "Entfernt", "Hinzugefügt" oder "Nicht hinzugefügt" aufgelistet. Suchen Sie anhand des Benutzernames nach dem Benutzer. Geben Sie die ersten Zeichen des Benutzernamens in das Feld **Filter Users** ein, klicken Sie auf **Search Users** und wählen Sie den Benutzer aus.

4. Klicken Sie auf **Run Simulation**.

   Die Ergebnisse der Simulation einer Einrichtungsrichtlinie für einen einzelnen Benutzer werden im Fenster **Simulate Provisioning Policy** angezeigt.

   Schließen Sie das Fenster **Simulate Policy**, um zum Fenster **Manage Policies** zurückzukehren, und klicken Sie auf **Cancel**.

5. Klicken Sie auf **Refresh** im Fenster **Manage Policies**, um die Ergebnisse der Simulationen anzuzeigen. Wenn die Simulation abgeschlossen ist, werden ein Hakensymbol und ein Link zu einer CSV-Datei angezeigt.

6. Zeigen Sie die Ergebnisse an.

   - Klicken Sie auf das Hakensymbol ✔, um das Fenster **Simulation Results** zu öffnen. Sie können auswählen, welche Ergebnisspalten Sie anzeigen möchten, indem Sie die Kontrollkästchen für die Spaltenüberschriften auswählen oder die Auswahl aufheben. Schließen Sie das Fenster **Simulation Results**, um zum Fenster **Manage Policies** zurückzukehren.

     Anmerkung: Wenn Sie auf **Clear Simulation Results** klicken, werden alle Ergebnisse im Fenster **Simulation Results** und im Fenster **Manage Policies** gelöscht.

   - Klicken Sie auf das CSV-Symbol, um die Ergebnisse in einer CSV-Datei anzuzeigen. Sie können die Datei öffnen oder speichern.

Nächste Schritte

1. Gleichen Sie die Richtlinie ab.
2. Aktivieren Sie die Richtlinie.

Dynamische Richtlinie abgleichen

Nachdem eine Richtlinie erstellt wurde, kann die Richtlinie abgeglichen werden. Wenn eine Richtlinie abgeglichen wird, wird die Benutzermitgliedschaft für die Gruppe entsprechend den Auswahlkriterien der Richtlinie implementiert.

Vorgehensweise

1. Suchen Sie nach der Gruppe und wählen Sie sie aus. Öffnen Sie das Fenster **Manage Policies**, um die Richtlinie zu bearbeiten.
2. Klicken Sie auf **Reconcile Now** (Jetzt abgleichen).

Eine Warnnachricht wird angezeigt. Klicken Sie auf **OK**, um die Richtlinie abzugleichen.

Nächste Schritte

Aktivieren Sie die Richtlinie.

Dynamische Richtlinie aktivieren und planen

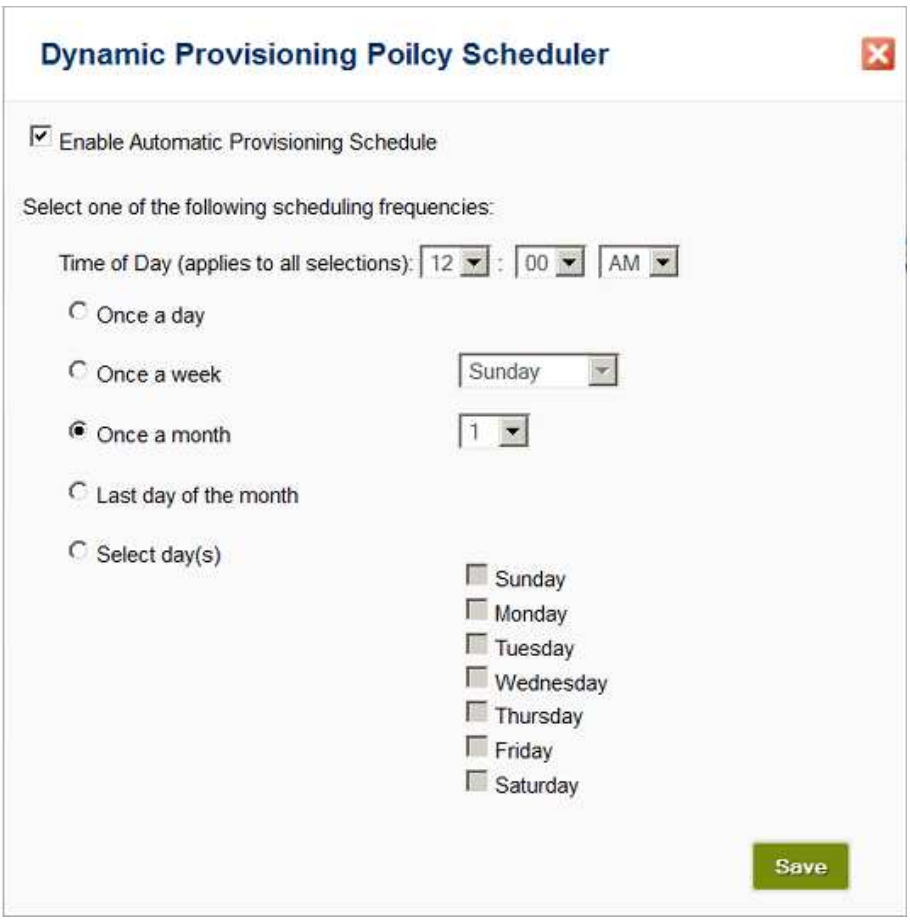
Nach dem Erstellen und Simulieren einer Richtlinie und nach dem Validieren der Simulationsergebnisse ist die Richtlinie bereit für die Aktivierung und Zeitplanung. Eine aktivierte Richtlinie wird nach einem Zeitplan ausgeführt, sodass die Mitgliedschaft einer Gruppe bei jeder Ausführung des Zeitplans bewertet und aktualisiert wird.

Vorgehensweise

1. Wenn Sie die Richtlinie nicht ausgewählt haben, suchen Sie nach der Gruppe und wählen Sie sie aus. Öffnen Sie das Fenster **Manage Policies**, um die Richtlinie zu bearbeiten.
2. Wählen Sie **Select Active** für die zu aktivierende Richtlinie aus.

Ein Warnhinweis wird angezeigt. Klicken Sie auf **OK**, um die Richtlinie zu aktivieren.

3. Klicken Sie auf das Zeitplansymbol , um das Fenster **Dynamic Provisioning Policy Scheduler** zu öffnen.



4. Aktivieren Sie das Kontrollkästchen **Enable Automatic Provisioning Schedule**.
5. Wählen Sie die Frequenz aus, mit der der Zeitplan ausgeführt werden soll:
   - **Once a day**. Wählen Sie die Tageszeit aus.
   - **Once a week**. Wählen Sie den Tag aus der Dropdown-Liste aus und wählen Sie dann die Tageszeit aus.
   - **Once a month**. Wählen Sie den Kalendertag aus der Dropdown-Liste aus und wählen Sie dann die Tageszeit aus.
   - **Last day of the month**. Wählen Sie die Tageszeit aus.
   - **Select days**. Wählen Sie die Kontrollkästchen für die Tage aus, an denen der Zeitplan ausgeführt werden soll, und wählen Sie dann die Tageszeit aus.
6. Klicken Sie auf **Save**.

Angepasste Attribute verwalten

Ein Benutzerdatensatz setzt sich aus einer Reihe von Benutzeridentitätsattributen zusammen. Sie können angepasste Attribute zu der Gruppe von Identitätsattributen hinzufügen, die für Ihre Benutzerdatensätze verwendet wird.

Übersicht über Attribute

Benutzerdatensätze setzen sich aus einer Reihe von Identitätsattributen zusammen. Die meisten Identitätsattribute werden in fast jedem Identitätsmanagementsystem verwendet, wie z. B. Vorname, Nachname und E-Mail-Adresse.

Allgemeine Attribute stammen aus einer Gruppe von LDAP-Standardattributen (Lightweight Directory Access Protocol). Ihre Organisation verfügt möglicherweise über bestimmte Attribute, die für Ihre Gruppe von Anwendungen eindeutig sind. Diese eindeutigen Attribute werden als angepasste Attribute bezeichnet. Sie können auch weitere angepasste Attribute erstellen.

Nach Attributen suchen

Sie können nach jedem in Ihren Identitätsdatensätzen verfügbaren Attribut suchen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **People** > **Schema Management**.
2. Geben Sie im Feld **Begin Search** mindestens die ersten drei Zeichen des Attributs ein. Die Feldbezeichnung ändert sich in **Searching For**.

   Die Attribute, die mit Ihren Suchkriterien übereinstimmen, werden aufgelistet. Wählen Sie ein Attribut zum Ändern oder Anzeigen aus.

   Sie können die Liste mithilfe der Kontrollkästchen **Show Default** (Standard anzeigen) und **Show User Added** (Durch Benutzer hinzugefügte anzeigen) filtern. Durch Benutzer hinzugefügte Attribute werden als angepasste Attribute bezeichnet. Sie können die Liste durch Klicken auf eine Spaltenüberschrift entsprechend der betreffenden Spalte sortieren.

Angepasste Attribute erstellen

Sie können neue angepaste Attribute erstellen, die dann in Identitätsdatensätzen verwendet werden.

Vorbereitende Schritte

Für diese Aufgabe sind grundlegende Kenntnisse von LDAP (Lightweight Directory Access Protocol), über LDAP-Schemas und über die Voraussetzungen für Identitätsdatensätze in Ihrem Unternehmen erforderlich.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **People** > **Schema Management**.
2. Klicken Sie auf **Add New Attribute**.

3. Geben Sie einen Namen und eine Beschreibung für das Attribut ein. Der Name muss eindeutig sein. Sie können überprüfen, ob der Name eindeutig ist, indem Sie auf **Check Availability** klicken.

   Anmerkung: Für den Namen können Sie die alphanumerischen Zeichen a-z, A-Z und 0-9 verwenden. Sie können die Sonderzeichen Bindestrich (-) und Unterstrich (_) verwenden. Sie können keine Leerzeichen verwenden.

   Für die Beschreibung können Sie die alphanumerischen Zeichen a-z, A-Z und 0-9 verwenden. Sie können die Sonderzeichen Bindestrich (-) und Unterstrich (_) verwenden. Sie können auch Leerzeichen verwenden.
4. Wechseln Sie zu den Attributeinstellungen.

5. Klicken Sie auf **Save Changes**, um das Attribut hinzuzufügen.

Attributeinstellungen

Zu Attributeinstellungen gehören der Typ und die Verwendung von mehreren Werten.

Tabelle 4. Attributeinstellungen

Einstellung	Beschreibung
Type	Attributtyp. • **String**. Unicode-Zeichenfolge (UTF-8). • **Boolean**. • **Integer**.
Multivalue	Gibt an, ob das Attribut viele verschiedene Werte annehmen kann. • **True**. Mehrere Werte sind zulässig. • **False**. Nur ein einziger Wert ist zulässig.

Massenimport von Benutzern verwalten

Sie können Benutzerdaten als Massendaten laden, um Benutzeridentitätsdatensätze im Cloud Identity Portal zu erstellen.

Vorbereitende Schritte

Sie benötigen ausreichende Kenntnisse von JSON und SCIM-Dateien (System for Cross-domain Identity Management) sowie grundlegende Kenntnisse von REST-APIs.

SCIM-Dateien

Sie können Benutzermassendaten durch das Hochladen von SCIM-Dateien (System for Cross-domain Identity Management) in Cloud Identity Portal laden.

SCIM-Dateien bieten ein plattformunabhängiges Schema für die Darstellung von Benutzern im JSON-Format. Weitere Informationen zu SCIM finden Sie unter SCIM (System for Cross-domain Identity Management). Die SCIM-Datei enthält einen Bereich von Operationen, von der jede die Erstellung eines Benutzerdatensatzes darstellt. Die Operationen werden über die Cloud Identity Portal-Administrations-REST-API verarbeitet. Jede erfolgreiche Operation erstellt einen neuen Benutzerdatensatz in Cloud Identity Portal. Sie können bis zu 5000 Operationen pro SCIM-Datei erstellen und so viele Dateien wie nötig hochladen. Im Folgenden sind das Format und die Inhalte einer SCIM-Beispieldatei dargestellt.

```
{
 "operations": [
  {
   "method": "POST",
   "path": "/Users",
   "bulkId": "importtest1",
   "data": {
    "userName": "userimporttest1",
    "active": true,
    "password": "core1234",
    "emails": [{
     "value": "nomail@gmail.com",
     "type": "",
     "primary": "true"
```

```
    }],
    "name": {
     "familyName": "import",
     "middleName": "mid",
     "givenName": "ctest1"
    },
    "addresses": [{
     "streetAddress": "123 oak st",
     "locality": "fort worth",
     "region": "texas",
     "postalCode": "77077",
     "country": "USA",
     "type": "home",
     "primary": "true"
    }],
    "title": "title",
    "preferredLanguage": "en-US",
    "userType": "Contractor"
   }
  },
   {
   "method": "POST",
   "path": "/Users",
   "bulkId": "importtest1",
   "data": {
    "userName": "userimporttest2",
    "active": true,
    "password": "core1234",
    "emails": [{
     "value": "nomail2@gmail.com",
     "type": "",
     "primary": "true"
    }],
    "name": {
     "familyName": "import",
     "middleName": "mid",
     "givenName": "ctest2"
    },
    "addresses": [{
     "streetAddress": "123 oak st",
     "locality": "fort worth",
     "region": "texas",
     "postalCode": "77077",
     "country": "USA",
     "type": "home",
     "primary": "true"
    }],
    "title": "title",
    "preferredLanguage": "en-US",
    "userType": "Contractor"
   }
  }
 ]
}
```

Tabelle 5. Operationsparameter

Parameter	Typ	Erforderlich	Beschreibung
method		Ja	Die Operation, die durch die Methode ausgeführt werden soll. Die Operation ist `POST`.
path	Pfad	Ja	Gibt den Pfad zu dem Objekt an, das aktualisiert werden soll. Der Pfad lautet `/Users`.
bulkId	Zeichenfolge	Ja	Eine Transaktions-ID. Jeder Transaktions-ID ist ein Antwortstatus zugeordnet.

Tabelle 5. Operationsparameter (Forts.)

Parameter	Typ	Erforderlich	Beschreibung
data	Objekt	Ja	Enthält Attribute für den Benutzer.
userName	Zeichenfolge	Ja	Gibt den Benutzernamen des Benutzers an. Der Benutzername muss eindeutig sein.
active	Boolescher Wert	Ja	Gibt an, ob der Benutzerdatensatz eine Identität oder ein Account ist. Legen Sie den Wert `true` fest, wenn der Benutzer einen Cloud Identity Service-Account erhalten soll. Benutzer können sich ohne einen Account nicht bei Cloud Identity Service authentifizieren oder auf Self-Service-Anwendungen zugreifen. Wird der Wert `false` festgelegt, wird der Benutzerdatensatz als Identität und nicht als Account erstellt.
password	Zeichenfolge	Optional	Ein Kennwort für den Zugriff auf Cloud Identity Service und auf Self-Service-Anwendungen.
emails	Objekt	Optional	Enthält E-Mail-Adressen für den Benutzer.
value	Zeichenfolge	Optional	Eine gültige E-Mail-Adresse.
type	Zeichenfolge	Optional	E-Mail-Typ, wie z. B. privat, geschäftlich oder über Social Media.
primary	Boolescher Wert	Optional	Gibt an, ob die E-Mail-Adresse die primäre E-Mail-Adresse des Benutzers ist.
name	Objekt	Ja	Enthält Namensattribute für den Benutzer.
familyName	Zeichenfolge	Ja	Der Nachname des Benutzers.
middleName	Zeichenfolge	Optional	Der zweite Vorname des Benutzers.
givenName	Zeichenfolge	Optional	Der Vorname des Benutzers.
addresses	Objekt	Optional	Enthält Postanschriften für den Benutzer.
streetAddress	Zeichenfolge	Optional	Die Standortinformationen für eine Postadresse (Straße und Hausnummer).
locality	Zeichenfolge	Optional	Der Name eines Orts, z. B. eine Stadt oder ein Bezirk.
region	Zeichenfolge	Optional	Der Name einer geografischen Region, größer als der Ort. Beispiel: Der vollständige Name eines Staates oder eines Bundeslandes.
postalCode	Zeichenfolge	Optional	Die Codes, die vom Postdienstleister zum Identifizieren von Postservicezonen verwendet werden.
country	Zeichenfolge	Optional	Der Name eines Lands.
type	Zeichenfolge	Optional	Der Adresstyp, z. B. privat oder geschäftlich.
primary	Zeichenfolge	Optional	Gibt an, ob die Adresse die primäre E-Mail-Adresse des Benutzers ist.

Tabelle 5. Operationsparameter (Forts.)

Parameter	Typ	Erforderlich	Beschreibung
title	Zeichenfolge	Optional	Ein persönlicher Titel für eine Person, etwa Herr, Frau, Dr., Prof. und Pfarrer.
preferredLanguage	Zeichenfolge	Optional	Der Sprachcode für den Benutzer. Beispiel: `en-us` oder `fr-ca`. Ist kein Sprachcode angegeben, wird die bevorzugte Sprache verwendet, die in LDAP festgelegt ist. Wenn keine bevorzugte Sprache festgelegt ist, wird die Standardsprache "Amerikanisches Englisch" verwendet.
userType	Zeichenfolge	Optional	Der Name des Benutzertyps, wie z. B. Auftragnehmer.

Benutzer importieren

Sie können SCIM-Dateien (System for Cross-domain Identity Management) importieren, um neue Benutzer im Cloud Identity Portal zu erstellen.

Vorbereitende Schritte

Sie müssen die SCIM-Dateien erstellen, die Sie hochladen möchten.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **People** > **Import Users**.
2. Klicken Sie auf **Upload SCIM**, um nach einer Datei zum Hochladen zu suchen und sie auszuwählen.

Kapitel 6. Self-Service

Self-Service Application Management ist die Konfiguration und die Anpassung von Self-Service-Anwendungen. Self-Service-Anwendungen beinhalten alle Anwendungen, die Benutzer zum Anfordern und Verwalten ihrer Identitätsprofile benötigen.

Self-Service-Anwendungen konfigurieren

Zum Konfigurieren von Self-Service-Anwendungen gehört das Konfigurieren von Optionen zur Selbstregistrierung, zum Zurücksetzen von Kennwörtern und zur Wiederherstellung von Benutzernamen sowie das Definieren von Rollen.

Übersicht über die Konfiguration

Self-Service-Anwendungen werden während der Erstkonfiguration von Cloud Identity Service für Ihre Organisation konfiguriert. Sie können eine Reihe von Einstellungen und Optionen ändern, um sie an Ihren Bedarf anzupassen.

Self-Service-Anwendungen ermöglichen es Benutzern, Aspekte ihres Accounts im Cloud Identity Service zu steuern. Benutzer können z. B. eine Selbstregistrierung für einen Account durchführen, um Zugriff auf geschützte Ressourcen zu erhalten, sie können ihr Kennwort zurücksetzen, ihren Benutzernamen wiederherstellen und ihre Profildaten verwalten. Der Zugriff auf die Self-Service-Anwendung wird von der Benutzerrolle bestimmt.

Selbstregistrierung

Die Selbstregistrierungsanwendung ermöglicht es Benutzern, einen Account in Cloud Identity Service zu übernehmen. In den meisten Fällen müssen alle Benutzer eine Selbstregistrierung durchführen, damit sie ihr Profil verwalten und Zugriff auf geschützte Ressourcen erhalten können, wie z. B. auf Webanwendungen und -server.

Sie können die Selbstregistrierungsoptionen ändern, z. B. auch, wie Accounts eingerichtet und genehmigt werden. Sie können Abschnitte und Felder im Selbstregistrierungsformular hinzufügen, entfernen und neu anordnen.

Zurücksetzen des Kennworts

Die Anwendung zum Zurücksetzen des Kennworts ist konfigurierbar, um Benutzern das Zurücksetzen eines vergessenen Kennworts zu ermöglichen. Sie können die Optionen zum Zurücksetzen des Kennworts ändern, z. B. die Anzahl der Fragen, die beantwortet werden müssen, und ob E-Mail-Überprüfung verwendet wird.

Wiederherstellung des Benutzernamens

Wenn Benutzer ihren Benutzernamen vergessen haben, können sie sich nicht anmelden oder ihr Kennwort zurücksetzen, da sie ihren Account nicht identifizieren

können. Die Anwendung zur Wiederherstellung des Benutzernamens ermöglicht Benutzern das Wiederherstellen des Benutzernamens für den Account, wenn sie diesen vergessen haben. Sie können die Optionen zur Wiederherstellung des Benutzernamens ändern, z. B., ob der Benutzername am Bildschirm angezeigt wird oder ob der Benutzername an die E-Mail-Adresse des Benutzers gesendet werden soll.

Self-Service-Profil

Die Self-Service-Profilanwendung ermöglicht es Benutzern, ihre eigenen Accountprofilinformationen zu verwalten, sobald sie sich registriert haben und sich bei Cloud Identity Service authentifizieren können. Sie können Abschnitte und Felder im Formular zur Profilkonfiguration hinzufügen, entfernen und neu anordnen.

Sicherheitsfragen

Sicherheitsfragen werden verwendet, um die Identität eines Benutzers zu überprüfen, wenn dieser sein Kennwort zurücksetzen möchte. Benutzer müssen Antworten auf Sicherheitsfragen geben, wenn sie sich selbst registrieren. Um die Identität eines Benutzers während der Kennwortzurücksetzung zu überprüfen, werden die Antworten, die bei der Selbstregistrierung gegeben wurden, mit den Antworten verglichen, die beim Zurücksetzen des Kennworts gegeben wurden.

Während der Erstkonfiguration von Cloud Identity Service für Ihre Organisation werden eine Reihe von Sicherheitsfragen definiert. Sie können neue Fragen zu den bereits definierten Fragen hinzufügen oder Fragen ausblenden. Sie können die minimale Anzahl an Fragen festlegen, die Benutzer bei der Selbstregistrierung beantworten müssen.

Rollen

Eine Rolle kann als funktionaler Titel innerhalb Ihrer Organisation betrachtet werden. Beispiele: Manager, Administrator oder Help-Desk-Ansprechpartner. Rollen definieren Benutzerverbunde. Mithilfe von Rollen wird der Zugriff auf verschiedene Self-Service-Anwendungen und -Aktionen gesteuert.

Selbstregistrierungsoptionen und -formular konfigurieren

Sie können die Einrichtungs- und Genehmigungsoptionen sowie die Felder im Selbstregistrierungsformular ändern.

Selbstregistrierungsoptionen konfigurieren

Durch die Selbstregistrierung können Benutzer einen Account in Cloud Identity Service anfordern. Die Selbstregistrierung kann für verschiedene Funktionsweisen konfiguriert werden. Sie können die Selbstregistrierungsoptionen ändern, z. B. Accounteinrichtungs- und Genehmigungsoptionen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Self-Service** > **Self Registration**.
2. Wählen Sie die gewünschten Selbstregistrierungsoptionen aus.
3. Klicken Sie auf **Save Changes**.

Selbstregistrierungsoptionen:

Selbstregistrierungsoptionen schließen Optionen zur Formatierung und Genehmigung sowie E-Mail-Optionen ein.

Tabelle 6. Einrichtungsrichtlinien und Formatierungsoptionen

Option	Beschreibung
Enable Account Claiming	Ermöglicht es Benutzern, Accounts mithilfe eines in einer E-Mail gesendeten Links zu übernehmen. • **Yes**. Benutzer können einen Account mithilfe eines Links in einer E-Mail übernehmen. Der Benutzer erhält einen Link in einer E-Mail, über den er einen Account übernehmen kann. Durch Klicken auf den Link kann der Benutzer durch erfolgreiche Selbstregistrierung einen Account übernehmen. • **No**. Benutzer können einen Account nicht mithilfe eines E-Mail-Links übernehmen.
Enable LDAP identity validation	Benutzeraccounts können basierend auf der Validierung von LDAP-Attributen eingerichtet werden. Benutzeridentitätsdatensätze müssen bereits vorhanden sein, damit Benutzer mithilfe der LDAP-Identitätsvalidierung eingerichtet werden können. Die Werte, die während der Selbstregistrierung durch einen Benutzer für Attribute eingegeben werden, werden mit Werten im bereits vorhandenen Identitätsdatensatz verglichen. Stimmen die Werte überein, kann der Benutzer eingerichtet werden. Die für die Validierung zu verwendenden LDAP-Attribute müssen für die Validierung unter Form Setup ausgewählt und aktiviert werden. • **Yes**. Werden die Informationen erfolgreich validiert, kann ein Account für den Benutzer eingerichtet werden. Die für die Validierung zu verwendenden LDAP-Attribute müssen für die Validierung unter Form Setup ausgewählt und aktiviert werden. **Wenn die Identitätsvalidierung fehlschlägt**. Wenn die Identitätsvalidierung fehlschlägt, kann eine der folgenden Optionen angewendet werden: – **Reject Registration**. Die Benutzerregistrierung wird abgelehnt. Es wird kein Account erstellt. – **Manually Provision User**. Ein Account kann manuell von einem Cloud Identity Portal-Administrator eingerichtet werden. – **Auto Provision User**. Erstellt automatisch einen Account für den Benutzer. **Wenn mehrere Identitäten gefunden werden**. Wenn mehrere Identitätsdatensätze gefunden werden, die mit den von einem Benutzer eingegebenen Registrierungsinformationen übereinstimmen, kann eine der folgenden Optionen angewendet werden: – **Reject Registration**. Die Benutzerregistrierung wird abgelehnt. Es wird kein Account erstellt. – **Manually Provision User**. Ein Account für den Benutzer muss manuell von einem Cloud Identity Portal-Administrator eingerichtet werden. – **Auto Provision User**. Erstellt automatisch einen Account für den Benutzer. • **No**. Accounts können nicht basierend auf der Validierung von LDAP-Attributen eingerichtet werden.

Tabelle 6. Einrichtungsrichtlinien und Formatierungsoptionen (Forts.)

Option	Beschreibung
Preferred username format **Alternative Formate für den Benutzernamen**	Die bevorzugten und alternativen Formate des Benutzernamens. Wenn ein Benutzer die Selbstregistrierung durchführt, kann sein Benutzername auf verschiedene Arten generiert werden. Das alternative Format des Benutzernamens wird verwendet, wenn ein Benutzername für das bevorzugte Format bereits vorhanden ist. Beide Formate müssen sich unterscheiden. • **Allow the User to select their Username**. Der Benutzer stellt einen beliebigen Benutzernamen bereit. • **User's email address**. Als Benutzername wird die vom Benutzer eingegebene E-Mail-Adresse festgelegt. • **FirstName.LastName**. Der Benutzername setzt sich aus dem Vornamen und dem Nachnamen des Benutzers (durch einen Punkt getrennt) zusammen. Beispiel: John.Smith. • **FirstInitial.LastName**. Der Benutzername setzt sich aus dem ersten Buchstaben des Vornamens und dem Nachnamen des Benutzers (durch einen Punkt getrennt) zusammen. Beispiel: J.Smith. • **LastName.FirstInitial**. Der Benutzername setzt sich aus dem Nachnamen und dem Anfangsbuchstaben des Vornamens des Benutzers (durch einen Punkt getrennt) zusammen. Beispiel: Smith.J. • **FirstName.Middle.LastName**. Der Benutzername setzt sich aus dem Vornamen, dem Anfangsbuchstaben des zweiten Vornamens und dem Nachnamen des Benutzers (durch Punkte getrennt) zusammen. Beispiel: John.A.Smith. • **Populate From**. Der Benutzername wird aus dem Wert zusammengesetzt, den der Benutzer für ein bestimmtes LDAP-Attribut eingegeben hat. Das Attribut muss unter Form Setup vorhanden sein. • **Invoke Custom Method**. Für einen Benutzernamen kann ein benutzerdefiniertes Format verwendet werden. • **User UID**.

Tabelle 7. Genehmigungs- und E-Mail-Optionen

Option	Beschreibung
Require manual approval for registrations	Ein Cloud Identity Service-Benutzer genehmigt die Benutzerregistrierung manuell. Wenn ein Benutzer über keinen vorhandenen Identitätsdatensatz verfügt, kann die manuelle Genehmigung für die Einrichtung des Accounts verwendet werden. Die manuelle Genehmigung kann auch für Benutzer mit bereits vorhandenen Identitätsdatensätzen verwendet werden. • **Yes**. Manuelle Genehmigung für Registrierungen ist erforderlich. Sie müssen einen Standardgenehmiger für das Genehmigen von Registrierungen auswählen. Wenn ein Benutzer über keinen vorhandenen Identitätsdatensatz verfügt, ist der manuelle Genehmiger der Standardgenehmiger. Wenn ein Benutzer über einen vorhandenen Identitätsdatensatz verfügt, kann ein Manager die Registrierung genehmigen. – **Require manager approval (when possible)**. Ein Manager genehmigt Registrierungen. Ein Manager kann Registrierungen nur für Benutzer genehmigen, für die bereits Identitätsdatensätze vorhanden sind. Ist kein Manager zuständig, genehmigt der Standardgenehmiger die Registrierung. Suchen Sie im Feld **Default approver** nach dem Benutzer. Geben Sie die ersten drei Zeichen des Vornamens, des Nachnamens oder der E-Mail-Adresse des Benutzers ein, der die Registrierungen genehmigen soll. Wählen Sie den Benutzer aus. • **No**. Manuelle Genehmigung ist nicht erforderlich.
Require user to accept a policy agreement	Eine Richtlinienvereinbarung muss für die Registrierung akzeptiert werden. • **Yes**. Der Benutzer muss eine Richtlinienvereinbarung akzeptieren. • **No**. Der Benutzer muss keine Richtlinienvereinbarung akzeptieren.
Require identity verification questions	Fragen zur Identitätsverifizierung werden verwendet, um einen Benutzer zu überprüfen, wenn dieser ein Kennwort zurücksetzt. Die Antworten auf diese Fragen werden normalerweise von Benutzern bei der Registrierung bereitgestellt. • **Yes**. Der Benutzer muss Antworten auf Fragen zur Identitätsverifizierung bereitstellen. • **No**. Der Benutzer muss keine Antworten auf Fragen zur Identitätsverifizierung bei der Registrierung bereitstellen.
Send email when registration is pending	E-Mail an den Benutzer senden, **Yes** oder **No**.
Send email when a registration rejected	E-Mail an den Benutzer senden, **Yes** oder **No**.
Send email when a registration succeeds	E-Mail an den Benutzer senden, **Yes** oder **No**.

Selbstregistrierungsformular konfigurieren

Das Selbstregistrierungsformular dient zur Selbstregistrierung. Das Formular enthält mehrere Felder, die Benutzer bei der Registrierung ausfüllen. Sie können die Felder und Abschnitte umordnen, neue Abschnitte hinzufügen und Felder hinzufügen oder entfernen.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Self-Service** > **Self Registration** und klicken Sie dann auf **Form Setup**.

2. Fügen Sie ein Feld hinzu:
   a. Klicken Sie auf **Add New** > **Add New Field**.
   b. Wählen Sie die Attribut- und Feldoptionen aus, um das Feld zu definieren.
   c. Klicken Sie auf **Save Changes**, um das Feld hinzuzufügen.
3. Optional: Fügen Sie einen Abschnitt hinzu:
   a. Klicken Sie auf **Add New** > **Add New Section**.
   b. Geben Sie für den Abschnitt **Label** (Bezeichnung), **Subheading** (Unterüberschrift) und **Header** (Überschrift) ein. Bezeichnung, Unterüberschrift und Überschrift dienen zum Identifizieren des Abschnitts auf dem Formular.
   c. Klicken Sie auf **Add New Field**, um ein neues Feld in den Abschnitt einzugeben, und wählen Sie die Attribut- und Feldoptionen aus, um das Feld zu definieren.
   d. Klicken Sie auf **Save Changes**, um den neuen Abschnitt zu speichern. Im Hauptfenster **Self Registration Form Setup** können Sie weitere Felder zum Abschnitt hinzufügen.
4. Um die Reihenfolge in einem Formular zu ändern und einen Abschnitt oder ein Feld an eine neue Position zu verschieben, klicken Sie auf das Feld oder den Abschnitt und ziehen Sie es oder ihn an die neue Position.

5. Klicken Sie auf **Save Changes**, um das Formular zu speichern.

Formularoptionen:

Formularoptionen werden verwendet, um die Eigenschaften von Feldern festzulegen, die in Self-Service-Anwendungen verwendet werden.

Je nach definiertem Formular sind möglicherweise nicht alle Optionen verfügbar.

Tabelle 8. Formularfeldoptionen

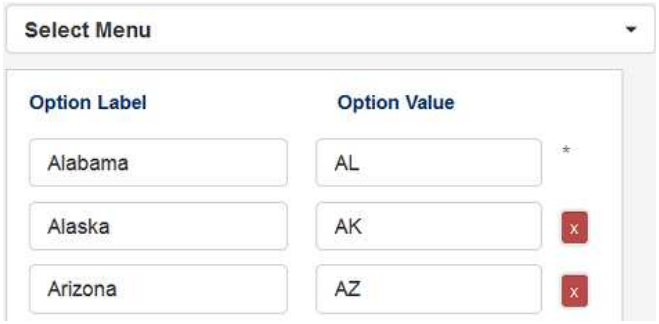
Option	Beschreibung
LDAP attribute	Als Feld zu verwendendes LDAP-Attribut. Wenn ein Attribut ausgewählt wird, für das ein anderer Benutzer als Wert eingegeben werden muss, wird ein Suchtool zum Feld hinzugefügt. Beispiel: Für ein Managerattribut muss möglicherweise ein anderer Benutzer eingegeben werden. Je nach definiertem Feld oder Formular können nicht alle Attribute ausgewählt werden.
Default Value	Ein Standardwert für das Feld. Ist das Feld bearbeitbar, können Benutzer den Standardwert ersetzen.
Field Label	Bezeichnung, die zum Identifizieren des Felds verwendet wird.
Field Type	• **Checkboxes**. Benutzer können eine oder mehrere Optionen als Eingabe für das Feld auswählen. • **Password Field**. Kennwortfelder sind ausgeblendet. • **Radio Buttons**. Benutzer können eine von mehreren Optionen als Eingabe für das Feld auswählen. • **Select Menu**. Benutzer können eine von mehreren Optionen als Eingabe für das Feld auswählen. • **Text Field**. Benutzer geben einen Wert in das Feld als eingegebenen Text ein. • **Text Area**. Unformatiertes Textfeld. Fügen Sie für **Checkboxes**, **Radio Buttons** und **Select Menu** die Optionen für das Feld hinzu. • **Option Label**. Bezeichnung, die zum Identifizieren der Option verwendet wird. • **Option Value**. Wert der Option. In diesem Beispiel verfügt ein Auswahlmenü über eine Reihe von Optionen für verschiedene Status. 
Placeholder	Bezeichnung für Platzhalter.
Tool Tip	Feldhilfetext.

Tabelle 8. Formularfeldoptionen (Forts.)

Option	Beschreibung
Editable	• **Yes**. Benutzer können einen Wert in das Feld eingeben. • **No**. Benutzer können keinen Wert in das Feld eingeben. Einige Felder werden mit vorhandenen Daten gefüllt. Während einer Selbstregistrierung kann ein Benutzer z. B. einen Account aus einem vorhandenen Identitätsdatensatz übernehmen. In diesem Fall kann ein Feldwert aus dem Identitätsdatensatz verwendet werden.
Required	• **Yes**. Das Feld ist ein Pflichtfeld. – Selbstregistrierungsformular. Benutzer können die Selbstregistrierung nur durch Eingabe eines Werts für das Feld abschließen. – Self-Service-Profilformular. Benutzer werden aufgefordert, Werte für nicht ausgefüllte Pflichtfelder einzugeben. • **No**. Das Feld ist optional.
Require current password match	Nur für ein LDAP-Kennwort-Attribut. • **Yes**. Benutzer müssen das Kennwort zweimal in separate Felder eingeben. Die in die einzelnen Felder eingegebenen Werte müssen übereinstimmen, um zu bestätigen, dass das Kennwort richtig ist. • **No**. Das Kennwort wird nur einmal in ein Feld eingegeben.
Masked	**Yes**. Das Feld ist ausgeblendet und der eingegebene Wert wird am Bildschirm nicht angezeigt. Die einzelnen eingegebenen Zeichen werden am Bildschirm durch einen Stern ersetzt.
Require a matching field	• **Yes**. Benutzer müssen den Wert zweimal in separate Felder eingeben. Die in die einzelnen Felder eingegebenen Werte müssen übereinstimmen, um zu bestätigen, dass der Wert richtig ist. Wenn ein Benutzer z. B. eine E-Mail-Adresse eingibt, können Sie von ihm verlangen, die Adresse zweimal einzugeben. • **No**. Der Wert wird nur einmal in ein Feld eingegeben.

Tabelle 8. Formularfeldoptionen (Forts.)

Option	Beschreibung
Validation	Validierungsregeln: • **Yes**. Der eingegebene Wert muss bestimmte Validierungsregeln erfüllen. Ein Datum muss z. B. möglicherweise einer Formatvalidierungsregel entsprechen, wie z. B. mm/tt/jjjj. • **No**. Die eingegebenen Werte werden nicht validiert. Validierungstypen: • **Date**. Die Werte müssen einem bestimmten Datumsformat entsprechen. Beispiel: mm/tt/jjjj. • **Email Address**. Die Werte müssen den E-Mail-Adress-Formaten entsprechen. Beispiel: *Textzeichenfolge@Textzeichenfolge*.com. • **Letters**. Die Werte dürfen nur alphabetische Zeichen enthalten. • **Maximum Character Length**. Die Werte dürfen nur eine bestimmte Anzahl an Zeichen enthalten. • **Minimum Character Length**. Die Werte müssen mindestens eine bestimmte Anzahl an Zeichen enthalten. • **Number**. Die Werte dürfen nur numerische Zeichen enthalten. • **Password Strength**. Ein Kennwortfeld muss allgemeinen, standardmäßigen oder starken Validierungsregeln entsprechen. Die Regeln basieren auf der Anzahl und dem Typ der Zeichen, die eingegeben werden müssen. • **US Phone Number**. Die Werte müssen dem in den USA üblichen Format für Telefonnummern entsprechen. Benutzerdefinierte reguläre Ausdrücke. Ein regulärer Ausdruck, der mit dem eingegebenen Wert verglichen wird. Wenn eine Übereinstimmung erkannt wird ("true"), ist der Wert gültig. • **Pattern**. Ein regulärer Ausdruck. Um z. B. Registrierungen auf Adressen im US-Bundesstaat North Carolina zu beschränken, verwenden Sie den regulären Ausdruck `^NC$` für das Bundesstaatsattribut, wobei NC als optionaler Wert für den Bundesstaat definiert ist. • **Error Message**. Fehlernachricht, die Benutzern angezeigt wird, wenn ein eingegebener Wert nicht gültig ist.

Tabelle 9. Formularabschnittsoptionen

Option	Beschreibung
Label	Abschnittsbezeichnung.
Subheading	Bezeichnung für Unterüberschrift.
Header	Überschrift.

Beispiel für ein Selbstregistrierungsformular:

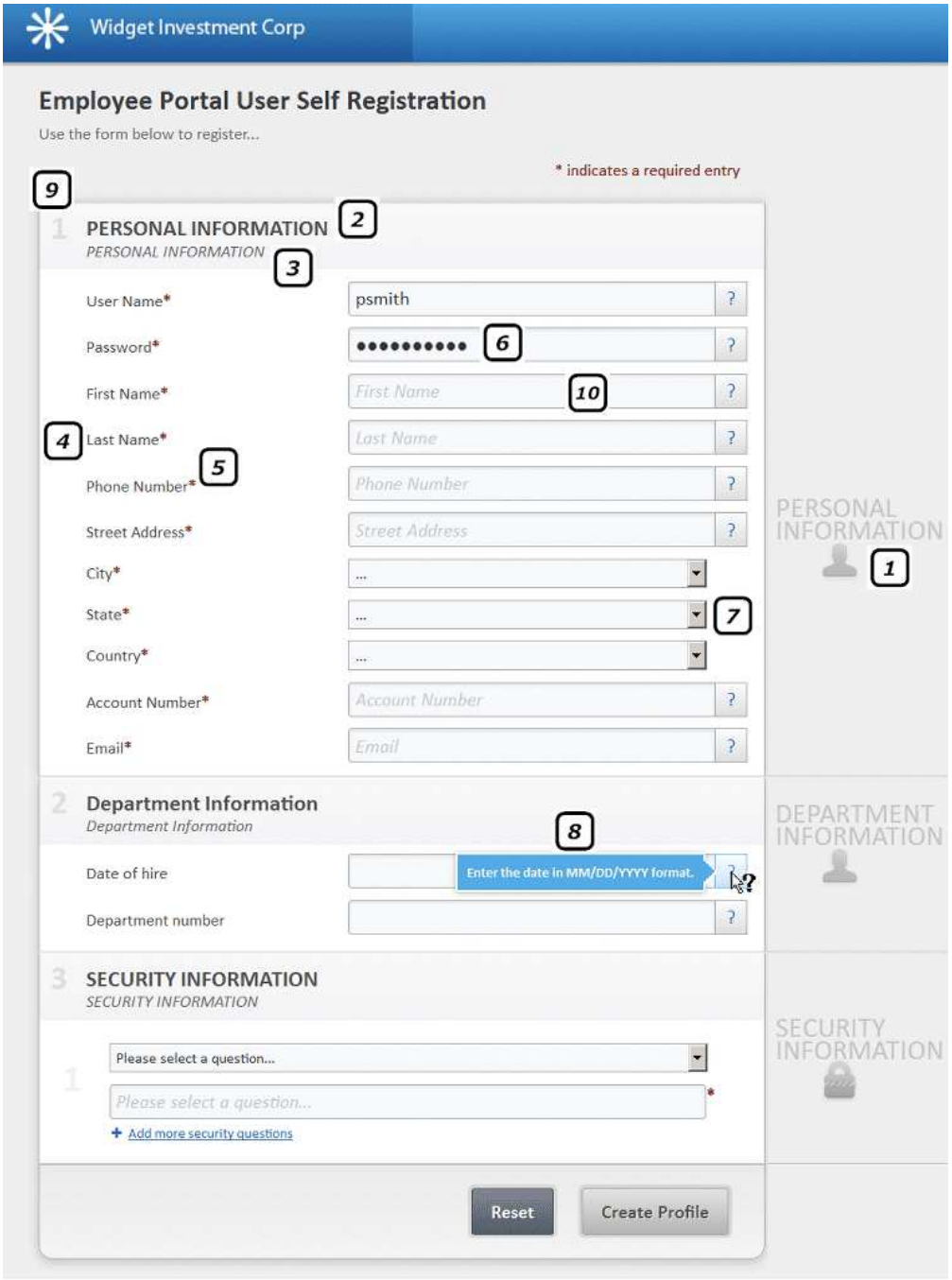


Tabelle 10. Feld- und Abschnittselemente für Selbstregistrierungsformular

Nummer	Beschreibung
1	Abschnittsbezeichnung.
2	Bezeichnung für Abschnittsüberschrift.
3	Bezeichnung für Abschnittsunterüberschrift.

Tabelle 10. Feld- und Abschnittselemente für Selbstregistrierungsformular (Forts.)

Nummer	Beschreibung
4	Feldbezeichnung.
5	Pflichtfeld, durch einen Stern angegeben.
6	Ausgeblendetes Feld. Kennwortfelder sind immer ausgeblendet.
7	Menüauswahlfeld.
8	Hilfetext für QuickInfo-Feld.
9	Abschnittsnummer.
10	Textfeld.

Optionen zum Zurücksetzen des Kennworts konfigurieren

Sie können die Optionen zum Zurücksetzen des Kennworts ändern, einschließlich der Anzahl der Sicherheitsfragen, die beantwortet werden müssen, und ob E-Mail-Überprüfung verwendet werden soll.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Self-Service** > **Password Reset**.
2. Wählen Sie die gewünschten Optionen zum Zurücksetzen des Kennworts aus.
3. Klicken Sie auf **Save Changes**.

Optionen zum Zurücksetzen des Kennworts

Tabelle 11. Optionen zum Zurücksetzen des Kennworts

Option	Beschreibung
Required security questions	Gilt nur, wenn **Use multi-factor authentication** auf **No** gesetzt ist. Die Mindestanzahl an Sicherheitsfragen, die ein Benutzer zum Zurücksetzen des Kennworts beantworten muss.
Maximum failed attempts	Gilt nur, wenn **Use multi-factor authentication** auf **No** gesetzt ist. Die Gesamtzahl an falschen Antworten, die auf alle Fragen gegeben werden kann. Benutzer werden gesperrt, wenn die maximale Anzahl überschritten wird.

Tabelle 11. Optionen zum Zurücksetzen des Kennworts (Forts.)

Option	Beschreibung
Require email verification	Gilt nur, wenn **Use multi-factor authentication** auf **No** gesetzt ist. Bei der E-Mail-Überprüfung muss der Benutzer auf einen Link klicken, der ihm per E-Mail gesendet wurde, nachdem er das Zurücksetzen des Kennworts angefordert hat. • **Yes**. Die E-Mail-Überprüfung ist erforderlich. Geben Sie die Zeit in Minuten ein, für die der Link gültig ist. Der Link muss innerhalb eines bestimmten Zeitlimits verwendet werden. Über den Link gelangt der Benutzer zum Fenster für das Zurücksetzen des Kennworts.  • **No**. Es wird keine E-Mail gesendet.
Send email upon successful reset	• **Yes**. Eine E-Mail wird an den Benutzer gesendet, um ihn zu informieren, dass das Kennwort erfolgreich zurückgesetzt wurde. • **No**. Es wird keine E-Mail gesendet.

Wiederherstellungsoptionen und -formular für Benutzernamen konfigurieren

Sie können die Wiederherstellungsoptionen und -felder für Benutzernamen ändern.

Wiederherstellungsoptionen für Benutzernamen konfigurieren

Sie können die Wiederherstellungsoptionen für Benutzernamen konfigurieren, z. B. ob der Benutzername auf dem Bildschirm angezeigt werden soll oder ob der Benutzername an die E-Mail-Adresse des Benutzers gesendet werden soll.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Self-Service** > **Username Recovery**.

2. Wählen Sie die gewünschten Wiederherstellungsoptionen für Benutzernamen aus.
3. Klicken Sie auf **Save Changes**.

Optionen zur Wiederherstellung des Benutzernamens:

Tabelle 12. Optionen zur Wiederherstellung des Benutzernamens

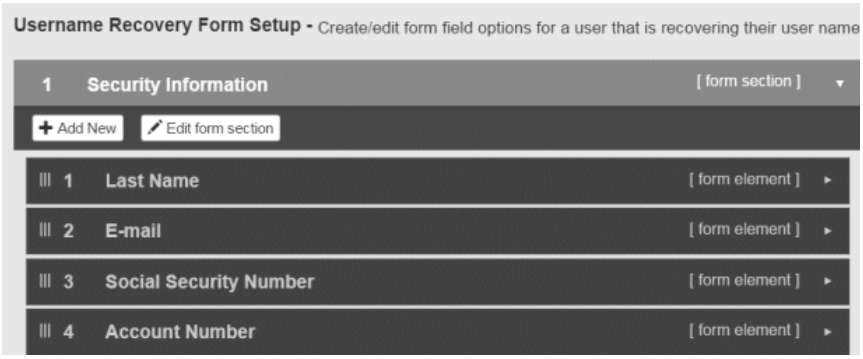
Option	Beschreibung
Enable Username Recovery	• **Yes**. Benutzernamen können mithilfe der Self-Service-Anwendung zum Wiederherstellen des Benutzernamens wiederhergestellt werden. • **No**. Benutzer können ihre Benutzernamen nicht mithife der Self-Service-Anwendung zum Wiederherstellen des Benutzernamens wiederherstellen.
Show username on screen	• **Yes**. Der Benutzername wird auf dem Bildschirm in der Self-Service-Anwendung zum Wiederherstellen des Benutzernamens angezeigt. • **No**. Der Benutzername wird während der Wiederherstellung des Benutzernamens nicht am Bildschirm angezeigt.
Send username to the user's email address	• **Yes**. Der Benutzername wird an den Benutzer gesendet. • **No**. Es wird keine E-Mail gesendet.

Formular zur Wiederherstellung des Benutzernamens konfigurieren

Das Formular zur Wiederherstellung des Benutzernamens dient zur Wiederherstellung eines Benutzernamens. Das Formular enthält mehrere Felder, die Benutzer bei der Wiederherstellung eines Benutzernamens ausfüllen. Sie können die Felder und die Auswahl umordnen, neue Abschnitte hinzufügen und Felder hinzufügen oder entfernen.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Self-Service** > **Username Recovery** und klicken Sie dann auf **Form Setup**.



2. So fügen Sie ein Feld hinzu:
   a. Klicken Sie auf **Add New** > **Add New Field**.
   b. Wählen Sie die Attribut- und Feldoptionen aus, um das Feld zu definieren.
   c. Klicken Sie auf **Save Changes**, um das Feld hinzuzufügen.
3. Optional: So fügen Sie einen Abschnitt hinzu:
   a. Klicken Sie auf **Add New** > **Add New Section**.
   b. Geben Sie für den Abschnitt **Label** (Bezeichnung), **Subheading** (Unterüberschrift) und **Header** (Überschrift) ein. Bezeichnung, Unterüberschrift und Überschrift dienen zum Identifizieren des Abschnitts auf dem Formular.
   c. Klicken Sie auf **Add New Field**, um ein neues Feld in den Abschnitt einzugeben, und wählen Sie die Attribut- und Feldoptionen aus, um das Feld zu definieren.
   d. Klicken Sie auf **Save Changes**, um den neuen Abschnitt zu speichern. Im Hauptfenster **Username Recovery Form Setup** können Sie weitere Felder zum Abschnitt hinzufügen.
4. Um die Reihenfolge in einem Formular zu ändern und einen Abschnitt oder ein Feld an eine neue Position zu verschieben, klicken Sie auf das Feld oder den Abschnitt und ziehen Sie es oder ihn an die neue Position.

5. Klicken Sie auf **Save Changes**, um das Formular zu speichern.

Formularoptionen:

Formularoptionen werden verwendet, um die Eigenschaften von Feldern festzulegen, die in Self-Service-Anwendungen verwendet werden.

Je nach definiertem Formular sind möglicherweise nicht alle Optionen verfügbar.

Tabelle 13. Formularfeldoptionen

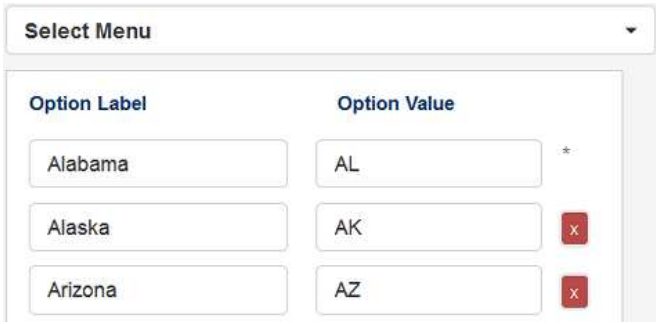
Option	Beschreibung
LDAP attribute	Als Feld zu verwendendes LDAP-Attribut. Wenn ein Attribut ausgewählt wird, für das ein anderer Benutzer als Wert eingegeben werden muss, wird ein Suchtool zum Feld hinzugefügt. Beispiel: Für ein Managerattribut muss möglicherweise ein anderer Benutzer eingegeben werden. Je nach definiertem Feld oder Formular können nicht alle Attribute ausgewählt werden.
Default Value	Ein Standardwert für das Feld. Ist das Feld bearbeitbar, können Benutzer den Standardwert ersetzen.
Field Label	Bezeichnung, die zum Identifizieren des Felds verwendet wird.
Field Type	• **Checkboxes**. Benutzer können eine oder mehrere Optionen als Eingabe für das Feld auswählen. • **Password Field**. Kennwortfelder sind ausgeblendet. • **Radio Buttons**. Benutzer können eine von mehreren Optionen als Eingabe für das Feld auswählen. • **Select Menu**. Benutzer können eine von mehreren Optionen als Eingabe für das Feld auswählen. • **Text Field**. Benutzer geben einen Wert in das Feld als eingegebenen Text ein. • **Text Area**. Unformatiertes Textfeld. Fügen Sie für **Checkboxes**, **Radio Buttons** und **Select Menu** die Optionen für das Feld hinzu. • **Option Label**. Bezeichnung, die zum Identifizieren der Option verwendet wird. • **Option Value**. Wert der Option. In diesem Beispiel verfügt ein Auswahlmenü über eine Reihe von Optionen für verschiedene Status. 
Placeholder	Bezeichnung für Platzhalter.
Tool Tip	Feldhilfetext.
Editable	• **Yes**. Benutzer können einen Wert in das Feld eingeben. • **No**. Benutzer können keinen Wert in das Feld eingeben. Einige Felder werden mit vorhandenen Daten gefüllt. Während einer Selbstregistrierung kann ein Benutzer z. B. einen Account aus einem vorhandenen Identitätsdatensatz übernehmen. In diesem Fall kann ein Feldwert aus dem Identitätsdatensatz verwendet werden.

Tabelle 13. Formularfeldoptionen (Forts.)

Option	Beschreibung
Required	• **Yes**. Das Feld ist ein Pflichtfeld. – Selbstregistrierungsformular. Benutzer können die Selbstregistrierung nur durch Eingabe eines Werts für das Feld abschließen. – Self-Service-Profilformular. Benutzer werden aufgefordert, Werte für nicht ausgefüllte Pflichtfelder einzugeben. • **No**. Das Feld ist optional.
Require current password match	Nur für ein LDAP-Kennwort-Attribut. • **Yes**. Benutzer müssen das Kennwort zweimal in separate Felder eingeben. Die in die einzelnen Felder eingegebenen Werte müssen übereinstimmen, um zu bestätigen, dass das Kennwort richtig ist. • **No**. Das Kennwort wird nur einmal in ein Feld eingegeben.
Masked	**Yes**. Das Feld ist ausgeblendet und der eingegebene Wert wird am Bildschirm nicht angezeigt. Die einzelnen eingegebenen Zeichen werden am Bildschirm durch einen Stern ersetzt.
Require a matching field	• **Yes**. Benutzer müssen den Wert zweimal in separate Felder eingeben. Die in die einzelnen Felder eingegebenen Werte müssen übereinstimmen, um zu bestätigen, dass der Wert richtig ist. Wenn ein Benutzer z. B. eine E-Mail-Adresse eingibt, können Sie von ihm verlangen, die Adresse zweimal einzugeben. • **No**. Der Wert wird nur einmal in ein Feld eingegeben.

Tabelle 13. Formularfeldoptionen (Forts.)

Option	Beschreibung
Validation	Validierungsregeln: • **Yes**. Der eingegebene Wert muss bestimmte Validierungsregeln erfüllen. Ein Datum muss z. B. möglicherweise einer Formatvalidierungsregel entsprechen, wie z. B. mm/tt/jjjj. • **No**. Die eingegebenen Werte werden nicht validiert. Validierungstypen: • **Date**. Die Werte müssen einem bestimmten Datumsformat entsprechen. Beispiel: mm/tt/jjjj. • **Email Address**. Die Werte müssen den E-Mail-Adress-Formaten entsprechen. Beispiel: *Textzeichenfolge@Textzeichenfolge*.com. • **Letters**. Die Werte dürfen nur alphabetische Zeichen enthalten. • **Maximum Character Length**. Die Werte dürfen nur eine bestimmte Anzahl an Zeichen enthalten. • **Minimum Character Length**. Die Werte müssen mindestens eine bestimmte Anzahl an Zeichen enthalten. • **Number**. Die Werte dürfen nur numerische Zeichen enthalten. • **Password Strength**. Ein Kennwortfeld muss allgemeinen, standardmäßigen oder starken Validierungsregeln entsprechen. Die Regeln basieren auf der Anzahl und dem Typ der Zeichen, die eingegeben werden müssen. • **US Phone Number**. Die Werte müssen dem in den USA üblichen Format für Telefonnummern entsprechen. Benutzerdefinierte reguläre Ausdrücke. Ein regulärer Ausdruck, der mit dem eingegebenen Wert verglichen wird. Wenn eine Übereinstimmung erkannt wird ("true"), ist der Wert gültig. • **Pattern**. Ein regulärer Ausdruck. Um z. B. Registrierungen auf Adressen im US-Bundesstaat North Carolina zu beschränken, verwenden Sie den regulären Ausdruck `^NC$` für das Bundesstaatsattribut, wobei NC als optionaler Wert für den Bundesstaat definiert ist. • **Error Message**. Fehlernachricht, die Benutzern angezeigt wird, wenn ein eingegebener Wert nicht gültig ist.

Tabelle 14. Formularabschnittsoptionen

Option	Beschreibung
Label	Abschnittsbezeichnung.
Subheading	Bezeichnung für Unterüberschrift.
Header	Überschrift.

Beispiel für ein Formular zur Wiederherstellung des Benutzernamens:

Tabelle 15. Feld- und Abschnittselemente für Benutzernamensformular

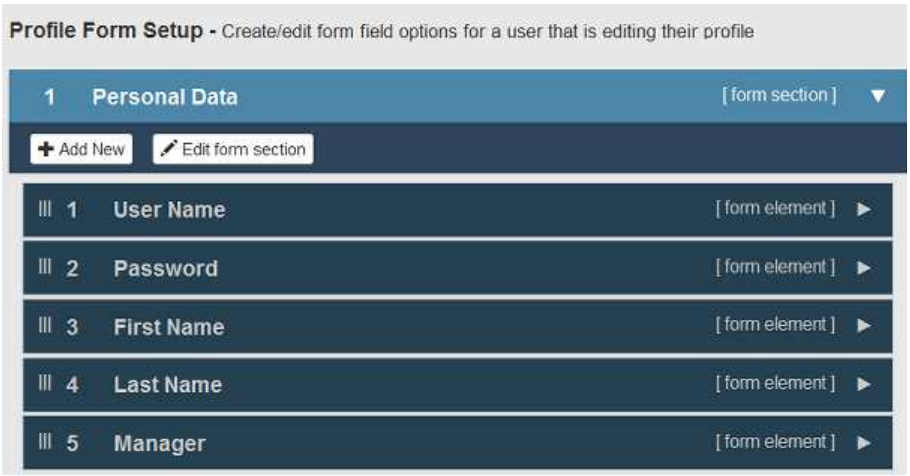
Nummer	Beschreibung
1	Abschnittsnummer.
2	Abschnittsbezeichnung.
3	Pflichtfeld, durch einen Stern angegeben.
4	Ausgeblendetes Feld.
5	Feldbezeichnung.

Self-Service-Profilformular konfigurieren

Das Self-Service-Profilformular enthält mehrere Felder, die das Profil eines Benutzers in der Self-Service-Profilanwendung enthalten. Sie können die Felder und Abschnitte umordnen, neue Abschnitte hinzufügen und Felder hinzufügen oder entfernen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Self-Service** > **Self Service Portal**.



2. So fügen Sie ein Feld hinzu:
   a. Klicken Sie auf **Add New** > **Add New Field**.
   b. Wählen Sie die Attribut- und Feldoptionen aus, um das Feld zu definieren.
   c. Klicken Sie auf **Save Changes**, um das Feld hinzuzufügen.
3. So fügen Sie einen Abschnitt hinzu:
   a. Klicken Sie auf **Add New** > **Add New Section**.
   b. Geben Sie für den Abschnitt **Label** (Bezeichnung), **Subheading** (Unterüberschrift) und **Header** (Überschrift) ein. Bezeichnung, Unterüberschrift und Überschrift dienen zum Identifizieren des Abschnitts auf dem Formular.
   c. Klicken Sie auf **Add New Field**, um ein neues Feld in den Abschnitt einzugeben, und wählen Sie die Attribut- und Feldoptionen aus, um das Feld zu definieren.
   d. Klicken Sie auf **Save Changes**, um den neuen Abschnitt zu speichern. Im Hauptfenster **Profile Form Setup** können Sie weitere Felder zum Abschnitt hinzufügen.
4. Um die Reihenfolge in einem Formular zu ändern und einen Abschnitt oder ein Feld an eine neue Position zu verschieben, klicken Sie auf das Feld oder den Abschnitt und ziehen Sie es oder ihn an die neue Position.

5. Klicken Sie auf **Save Changes**, um das Formular zu speichern.

Formularoptionen

Formularoptionen werden verwendet, um die Eigenschaften von Feldern festzulegen, die in Self-Service-Anwendungen verwendet werden.

Je nach definiertem Formular sind möglicherweise nicht alle Optionen verfügbar.

Tabelle 16. Formularfeldoptionen

Option	Beschreibung
LDAP attribute	Als Feld zu verwendendes LDAP-Attribut. Wenn ein Attribut ausgewählt wird, für das ein anderer Benutzer als Wert eingegeben werden muss, wird ein Suchtool zum Feld hinzugefügt. Beispiel: Für ein Managerattribut muss möglicherweise ein anderer Benutzer eingegeben werden. Je nach definiertem Feld oder Formular können nicht alle Attribute ausgewählt werden.
Default Value	Ein Standardwert für das Feld. Ist das Feld bearbeitbar, können Benutzer den Standardwert ersetzen.
Field Label	Bezeichnung, die zum Identifizieren des Felds verwendet wird.

Tabelle 16. Formularfeldoptionen (Forts.)

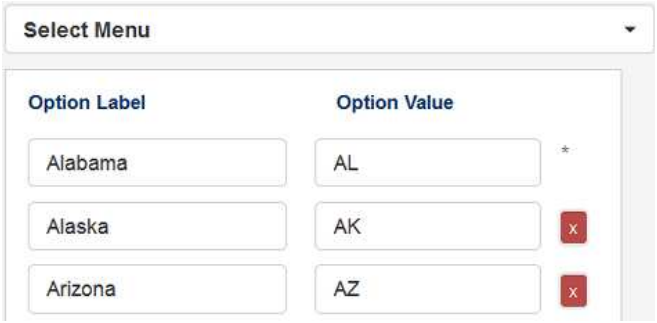
Option	Beschreibung
Field Type	• **Checkboxes**. Benutzer können eine oder mehrere Optionen als Eingabe für das Feld auswählen. • **Password Field**. Kennwortfelder sind ausgeblendet. • **Radio Buttons**. Benutzer können eine von mehreren Optionen als Eingabe für das Feld auswählen. • **Select Menu**. Benutzer können eine von mehreren Optionen als Eingabe für das Feld auswählen. • **Text Field**. Benutzer geben einen Wert in das Feld als eingegebenen Text ein. • **Text Area**. Unformatiertes Textfeld. Fügen Sie für **Checkboxes**, **Radio Buttons** und **Select Menu** die Optionen für das Feld hinzu. • **Option Label**. Bezeichnung, die zum Identifizieren der Option verwendet wird. • **Option Value**. Wert der Option. In diesem Beispiel verfügt ein Auswahlmenü über eine Reihe von Optionen für verschiedene Status. 
Placeholder	Bezeichnung für Platzhalter.
Tool Tip	Feldhilfetext.
Editable	• **Yes**. Benutzer können einen Wert in das Feld eingeben. • **No**. Benutzer können keinen Wert in das Feld eingeben. Einige Felder werden mit vorhandenen Daten gefüllt. Während einer Selbstregistrierung kann ein Benutzer z. B. einen Account aus einem vorhandenen Identitätsdatensatz übernehmen. In diesem Fall kann ein Feldwert aus dem Identitätsdatensatz verwendet werden.
Required	• **Yes**. Das Feld ist ein Pflichtfeld. – Selbstregistrierungsformular. Benutzer können die Selbstregistrierung nur durch Eingabe eines Werts für das Feld abschließen. – Self-Service-Profilformular. Benutzer werden aufgefordert, Werte für nicht ausgefüllte Pflichtfelder einzugeben. • **No**. Das Feld ist optional.

Tabelle 16. Formularfeldoptionen (Forts.)

Option	Beschreibung
Require current password match	Nur für ein LDAP-Kennwort-Attribut. • **Yes**. Benutzer müssen das Kennwort zweimal in separate Felder eingeben. Die in die einzelnen Felder eingegebenen Werte müssen übereinstimmen, um zu bestätigen, dass das Kennwort richtig ist. • **No**. Das Kennwort wird nur einmal in ein Feld eingegeben.
Masked	**Yes**. Das Feld ist ausgeblendet und der eingegebene Wert wird am Bildschirm nicht angezeigt. Die einzelnen eingegebenen Zeichen werden am Bildschirm durch einen Stern ersetzt.
Require a matching field	• **Yes**. Benutzer müssen den Wert zweimal in separate Felder eingeben. Die in die einzelnen Felder eingegebenen Werte müssen übereinstimmen, um zu bestätigen, dass der Wert richtig ist. Wenn ein Benutzer z. B. eine E-Mail-Adresse eingibt, können Sie von ihm verlangen, die Adresse zweimal einzugeben. • **No**. Der Wert wird nur einmal in ein Feld eingegeben.

Tabelle 16. Formularfeldoptionen (Forts.)

Option	Beschreibung
Validation	Validierungsregeln: • **Yes**. Der eingegebene Wert muss bestimmte Validierungsregeln erfüllen. Ein Datum muss z. B. möglicherweise einer Formatvalidierungsregel entsprechen, wie z. B. mm/tt/jjjj. • **No**. Die eingegebenen Werte werden nicht validiert. Validierungstypen: • **Date**. Die Werte müssen einem bestimmten Datumsformat entsprechen. Beispiel: mm/tt/jjjj. • **Email Address**. Die Werte müssen den E-Mail-Adress-Formaten entsprechen. Beispiel: *Textzeichenfolge*@*Textzeichenfolge*.com. • **Letters**. Die Werte dürfen nur alphabetische Zeichen enthalten. • **Maximum Character Length**. Die Werte dürfen nur eine bestimmte Anzahl an Zeichen enthalten. • **Minimum Character Length**. Die Werte müssen mindestens eine bestimmte Anzahl an Zeichen enthalten. • **Number**. Die Werte dürfen nur numerische Zeichen enthalten. • **Password Strength**. Ein Kennwortfeld muss allgemeinen, standardmäßigen oder starken Validierungsregeln entsprechen. Die Regeln basieren auf der Anzahl und dem Typ der Zeichen, die eingegeben werden müssen. • **US Phone Number**. Die Werte müssen dem in den USA üblichen Format für Telefonnummern entsprechen. Benutzerdefinierte reguläre Ausdrücke. Ein regulärer Ausdruck, der mit dem eingegebenen Wert verglichen wird. Wenn eine Übereinstimmung erkannt wird ("true"), ist der Wert gültig. • **Pattern**. Ein regulärer Ausdruck. Um z. B. Registrierungen auf Adressen im US-Bundesstaat North Carolina zu beschränken, verwenden Sie den regulären Ausdruck `^NC$` für das Bundesstaatsattribut, wobei NC als optionaler Wert für den Bundesstaat definiert ist. • **Error Message**. Fehlernachricht, die Benutzern angezeigt wird, wenn ein eingegebener Wert nicht gültig ist.

Tabelle 17. Formularabschnittsoptionen

Option	Beschreibung
Label	Abschnittsbezeichnung.
Subheading	Bezeichnung für Unterüberschrift.
Header	Überschrift.

Beispiel für ein Portalprofilformular

Tabelle 18. Feld- und Abschnittselemente für Selbstregistrierungsformular

Nummer	Beschreibung
1	Abschnittsbezeichnung.
2	Feldbezeichnung.
3	Pflichtfeld, durch einen Stern angegeben.
4	Textfeld.
5	Textfeld mit Tool für die Benutzersuche.
6	Ausgeblendetes Feld. Kennwortfelder sind immer ausgeblendet.

Optionen zum Ändern der Sicherheitsfrage

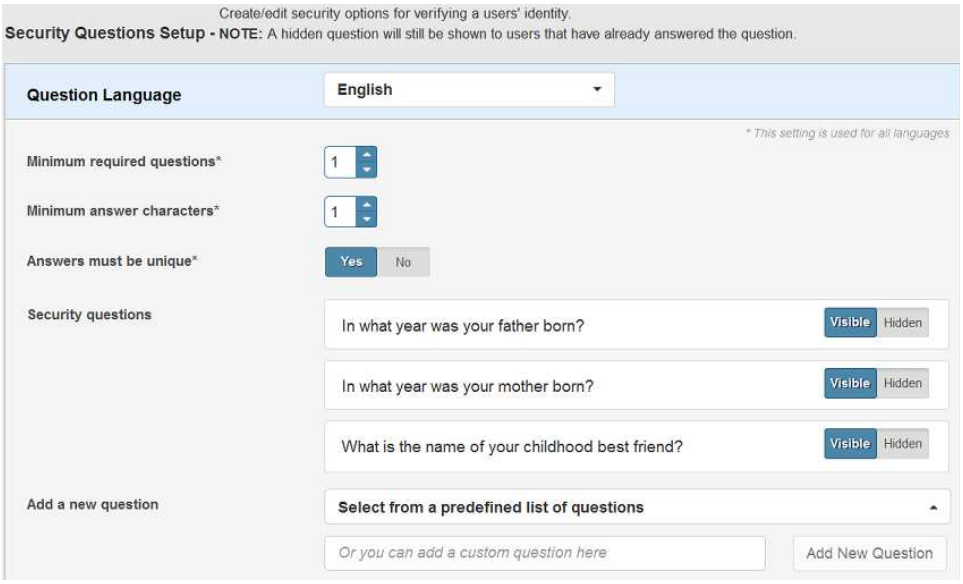
Während der Erstkonfiguration von Cloud Identity Service für Ihre Organisation werden eine Reihe von Sicherheitsfragen definiert. Die Antworten auf Sicherheitsfragen dienen zur Überprüfung von Benutzern, wenn diese versuchen, ihr Kennwort zurückzusetzen. Sie können neue Sicherheitsfragen hinzufügen.

Informationen zu diesem Vorgang

Benutzer müssen bei der Selbstregistrierung Antworten auf Sicherheitsfragen angeben. Benutzer können die Fragen, auf die sie Antworten angeben möchten, aus einem Pool von Fragen auswählen. Sie können neue Fragen hinzufügen und die Mindestanzahl von Fragen festlegen, auf die Benutzer bei der Selbstregistrierung Antworten angeben müssen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Self-Service** > **Security Questions**.



2. Optional: Wählen Sie in der Dropdown-Liste **Question Language** eine Sprache aus, für die Sie Unterstützung in der Landessprache der Benutzer bereitstellen möchten.

   Die Sprachen, die Sie auswählen können, werden bei der Erstkonfiguration von Cloud Identity Service für Ihre Organisation definiert. Sie fügen Übersetzungen für Fragen hinzu, die in der Standardsprache bereits definiert sind.

   a. Klicken Sie auf **Choose a question to translate** und wählen Sie eine Frage aus der Liste aus.

      Die verfügbaren Fragen sind diejenigen, die in der Standardsprache bereits definiert sind. Die Standardsprache ist Englisch.

   b. Geben Sie die Übersetzung im Textfeld ein und klicken Sie auf **Add Translation**.

3. Legen Sie die gewünschten Optionen zur Einrichtung von Sicherheitsfragen fest.
4. Klicken Sie auf **Save Changes**.

Optionen für Sicherheitsfragen

Zu den Optionen für Sicherheitsfragen zählen die Mindestanzahl an Sicherheitsfragen, die Eindeutigkeit der Fragen und die Mindestlänge der Antworten.

Tabelle 19. Optionen für Sicherheitsfragen

Option	Beschreibung
Enable salting and hashing of answers	Gibt an, ob für Antworten auf Sicherheitsfragen Salting und Hashing verwendet werden soll. Hashing codiert eine Antwort in eine Zeichenfolge fester Länge, sodass die Antwort besser gegen Erkennung gesichert ist. Salting randomisiert Hashwerte willkürlich durch das Hinzufügen einer zufälligen Zeichenfolge, sodass Antworten schwieriger zu decodieren sind. **Wichtig:** Wenn Salting und Hashing aktiviert sind, können diese Funktionen nicht inaktiviert werden.
Minimum required questions	Die minimale Anzahl an Sicherheitsfragen, die ein Benutzer bei der Registrierung beantworten muss. Diese Option bezieht sich nicht auf die Anzahl der Fragen, die beim Zurücksetzen des Kennworts beantwortet werden muss. Ein Benutzer kann z. B. Antworten auf 5 Fragen geben, während des Zurücksetzens des Kennworts sind aber nur 3 Antworten erforderlich. In diesem Fall werden 3 Fragen nach dem Zufallsprinzip aus den 5 während der Registrierung beantworteten Fragen ausgewählt.
Minimum answer characters	Die minimale Anzahl an Zeichen, die als Antwort eingegeben werden müssen.
Answers must be unique	• **Yes**. Benutzer dürfen nicht dieselbe Antwort auf verschiedene Fragen eingeben. • **No**. Antworten auf verschiedene Fragen dürfen gleich sein.
Make default tab in profile on error	Gibt bei der Anmeldung beim Self-Service-Portal an, ob dem Benutzer zuerst die Registerkarte mit Sicherheitsfragen angezeigt wird, wenn Sicherheitsfragenfehler vorliegen.
Security questions	Sicherheitsfragen können ausgeblendet oder sichtbar sein. • **Visible**. Die Frage ist für den Benutzer verfügbar, damit er während der Registrierung eine Antwort geben kann. • **Hidden**. Die Frage ist für den Benutzer während der Registrierung nicht verfügbar und er kann keine Antwort auf die Frage geben.
Add a new question	Sie können eine Frage auf zwei Arten hinzufügen. • **Select from a predefined list of questions**. Treffen Sie eine Auswahl aus einer Liste mit Fragen. • **Add a custom question**. Geben Sie die Frage in das Textfeld ein und klicken Sie auf **Add New Question**. **Wichtig:** Neue Sicherheitsfragen können nur entfernt werden, wenn sie noch nicht gespeichert wurden. Nach dem Hinzufügen einer Frage und dem Speichern der Änderungen kann die Frage nur durch Öffnen eines Support-Tickets entfernt werden.

Rollen verwalten

Sie können Rollen hinzufügen und ändern, aber nicht löschen.

Übersicht über Rollen

Eine Rolle kann als funktionaler Titel innerhalb Ihrer Organisation betrachtet werden, Beispiele: Manager, Administrator oder Help-Desk-Ansprechpartner. Rollen werden z. B. verwendet, um den Zugriff auf die verschiedenen Self-Service-Anwendungen und -Aktionen sowie auf verschiedene Abschnitte in der Self-Service-Profilanwendung zu steuern.

Rollen hinzufügen

Eine Rolle kann als Funktionsbezeichnung in Ihrer Organisation betrachtet werden. Beispiele: Manager, Administrator oder Help-Desk-Ansprechpartner. Rollen werden Benutzern zugewiesen. Mithilfe von Rollen wird der Zugriff auf verschiedene Self-Service-Anwendungen und -Tasks kontrolliert.

Informationen zu diesem Vorgang

Rollen können verschiedenen Instanzen zugewiesen werden. Eine Instanz ist eine Gruppe von Konfigurationen, Optionen und Markenkennzeichnungen für Self-Service-Anwendungen. Eine Instanz kann z. B. eine Gruppe von Farbschemata, Textübersetzungen, Formularlayouts und Selbstregistrierungsoptionen definieren. Ferner kann für jede definierte Rolle eine Instanz ausgewählt werden. Einer Help-Desk-Rolle und einer Rolle für Managementaufgaben können z. B. verschiedene Instanzen zugewiesen werden. Eine Rolle kann nur einer einzigen Instanz zugewiesen werden, eine Einzelinstanz kann jedoch mehreren Rollen zugewiesen sein.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Self-Service** > **Self-ServiceRoles**.
2. Klicken Sie auf **Add a new Role**.
3. Geben Sie im Feld **Role Name** einen Namen für die Rolle ein.
4. Optional: Wählen Sie die Instanz der Self-Service-Anwendungen aus der Dropdown-Liste **Instance** aus.

   Self-Service-Anwendungen können über verschiedene Instanzen verfügen. Eine Instanz definiert die Fenster, Felder, Beschriftungen und andere Elemente der Benutzerschnittstelle in Self-Service-Anwendungen. Verschiedene Instanzen können entworfen werden, um die Anforderungen verschiedener Rollen zu erfüllen. Die Cloud Identity Service-Standardinstanz ist ausgewählt. Eine Rolle kann nur einer einzigen Instanz zugewiesen werden.
5. Wählen Sie unter role settings die gewünschten Rolleneinstellungen aus.
6. Klicken Sie auf **Save Changes**, um die Rolle zu speichern.

Rolleneinstellungen:

Rolleneinstellungen steuern den Zugriff auf unterschiedliche Self-Service-Anwendungen und -Aktionen für Benutzer, die dieser Rolle zugewiesen sind. Zu den Rolleneinstellungen gehören Profilverwaltung, Zurücksetzen des Kennworts, Suche nach dem Benutzernamen, Optionen zur Selbstregistrierung, Suchoptionen und Berechtigungen zum Anzeigen und Bearbeiten von Profilen.

Tabelle 20. Rolleneinstellungen

Einstellung	Beschreibung
Self Service Portal	Zugriff für Benutzer zum Verwalten ihrer eigenen Profile mit Benutzerinformationen.

Tabelle 20. Rolleneinstellungen (Forts.)

Einstellung	Beschreibung
Section Access	Unterschiedliche Abschnitte in Self-Service-Portal und -Profilanwendungen. • **Launchpad**. Zugriff auf Launchpad. Launchpad stellt einen einzigen Standort im Self-Service-Portal bereit, über den Benutzer auf verbundene Webanwendungen und Webanwendungen föderierter Partner zugreifen können. • **Profile**. Zugriff für Benutzer zur Verwaltung ihrer eigenen Profildaten. – **Show profile as a page**. Gibt an, ob Profildaten als Seite oder als Dropdown-Header angezeigt werden sollen. • **Direct Reports**. Zugriff zur Verwaltung der Profile von direkt unterstellten Mitarbeitern. – **Allow new user creation**. Kann neue Benutzer erstellen. – **Can demote accounts**. Kann Accounts auf Benutzeridentitäten herabstufen. – **Can toggle user status**. Kann einen Benutzeraccount aktivieren oder inaktivieren. Wenn ein Account inaktiviert wird, kann sich ein Benutzer nicht bei Self-Service anmelden. – **Can expire password**. Kann Benutzerkennwörter ablaufen lassen. • **Requests**. Zugriff zur Verwaltung von anstehenden Genehmigungsanforderungen und Anforderungen zur erneuten Zertifizierung. • **Services**. Zugriff zum Anzeigen einer Liste von Services, denen der Benutzer angehört, und die Möglichkeit, Services anzufordern. • **User Control**. Zugriff zum Anzeigen von Profilinformationen anderer Benutzer auf der Seite **User Control**. – **Allow new user creation**. Kann neue Benutzer erstellen. – **Can demote accounts**. Kann Accounts auf Benutzeridentitäten herabstufen. – **Can toggle user status**. Kann einen Benutzeraccount aktivieren oder inaktivieren. Wenn ein Account inaktiviert wird, kann sich ein Benutzer nicht bei Self-Service anmelden. – **Can expire password**. Kann Benutzerkennwörter ablaufen lassen.
Section Settings	• **Show Check Username button**. Kann überprüfen, ob ein Benutzername vorhanden ist, wenn ein neuer Benutzer erstellt wird.
Password Reset	Zugriff für Benutzer auf die Anwendung zum Zurücksetzen des Kennworts für das Zurücksetzen des eigenen Kennworts. Für die Anwendung ist keine Authentifizierung erforderlich.
Username Recovery	Zugriff für Benutzer auf die Anwendung zur Wiederherstellung des Benutzernamens für die Wiederherstellung des eigenen Benutzernamens. Für die Anwendung ist keine Authentifizierung erforderlich.

Tabelle 20. Rolleneinstellungen (Forts.)

Einstellung	Beschreibung
Self Registration	Zugriff auf die Selbstregistrierungsanwendung zur Selbstregistrierung. Für die Anwendung ist keine Authentifizierung erforderlich.
User Search Settings **Service Search Settings**	Die Priorität, nach der Attribute sortiert und angezeigt werden, wenn eine Suche nach einem Benutzer oder einem Service in Self-Service-Anwendungen durchgeführt wird. • **Search Results Priority**. Bei Suchergebnissen wird ein Attribut mit höherer Priorität vor einem Attribut mit geringerer Priorität angezeigt. Um ein Attribut zu den Suchergebnissen hinzuzufügen, wählen Sie ein Attribut aus der Liste **Add New Attribute** aus und klicken Sie auf . Klicken Sie auf ein Attribut und ziehen Sie es an eine neue Position, um seine Priorität zu ändern. • **Search Results Filter**. Attributfilterregeln können angewendet werden, um Benutzer oder Services aus einer Suche auszuschließen. Sie können z. B. Benutzer mit einer bestimmten Rolle ausschließen. Klicken Sie zum Hinzufügen eines Ausschlussfilters auf **Add Exclusion Filter**. Wählen Sie das Attribut, auf dem der Ausschluss basieren soll, aus der Liste **When Attribute** aus. Geben Sie den auszuschließenden Attributwert in das Feld **Is Equal To** ein.

Tabelle 20. Rolleneinstellungen (Forts.)

Einstellung	Beschreibung
View Permissions	Berechtigungen für Benutzerprofile anzeigen und bearbeiten. Sie können angeben, dass Identitätsattribute für Profile in Self-Service-Anwendungen anzeigbar und bearbeitbar sind. • **Any Users Profile**. Profile aller Benutzer. • **Users Own Profile**. Eigenes Profil des Benutzers. • **Direct Reports Profile**. Profile von direkt unterstellten Mitarbeitern eines Benutzers. • **Group Members Profile**. Profile von Benutzern mit einer bestimmten Gruppenmitgliedschaft. • **Service Members Profile**. Profile von Benutzern mit einer bestimmten Servicemitgliedschaft. • **Role Members Profile**. Profile von Benutzern mit einer bestimmten Rolle. Gehen Sie wie folgt vor, um Berechtigungen zum Anzeigen und Bearbeiten von Attributen hinzuzufügen: 1. Klicken Sie auf **Add View Permissions Filter**. 2. Wählen Sie die Benutzerprofile, auf die Sie Berechtigungen zum Anzeigen und Bearbeiten von Attributen anwenden möchten, aus der Liste **Applies when viewing** aus. Wählen Sie für "Role Members Profile" die entsprechende Rolle aus der Liste **who belongs to** aus. Suchen Sie für "Group Members Profile" und "Service Members Profile" nach der Gruppe oder dem Service und wählen Sie sie/ihn aus der Liste **who belongs to** aus. Um nach einer Gruppe oder einem Service zu suchen, geben Sie mindestens die ersten 3 Zeichen des Gruppen- oder Servicenamens ein. 3. Wählen Sie das Attribut, auf das Sie Berechtigungen anwenden möchten, aus dem Menü **Add Attribute** aus und klicken Sie auf . Sie können beliebig viele Attribute hinzufügen. Geben Sie an, ob das Attribut anzeigbar und bearbeitbar sein soll, indem Sie auf **Yes** oder **No** klicken. 4. Klicken Sie auf **Save Changes**.

Benutzerschnittstelle für Self-Service-Anwendungen anpassen

Zum Anpassen der Benutzerschnittstelle für Self-Service-Anwendungen gehört das Anpassen der Markenkennzeichnung sowie der Beschriftungen von Textschlüsseln und E-Mail-Vorlagen, der Beschriftungen in der Self-Service-Profilanwendung und der Beschriftungen für Seiten der Self-Service-Anwendungssuite.

Übersicht über Anpassung der Self-Service-Benutzerschnittstelle

Self-Service-Anwendungen werden während der Erstkonfiguration von Cloud Identity Service für Ihre Organisation konfiguriert. Sie können die Markenkennzeichnung von Self-Service-Anwendungen anpassen. Sie können den Inhalt von E-Mails, die an Benutzer gesendet werden, ändern und Sie können Spaltenbezeichnungen der Benutzerschnittstelle und weitere Textelemente ändern.

Markenkennzeichnung

Sie können die Markenkennzeichnung (Branding) von Self-Service-Anwendungen steuern. Die Markenkennzeichnung beinhaltet das Farbschema, das Logo, die Symbole und die visuelle Präsentation von Formularelementen in Anwendungen.

Textschlüssel

Textschlüssel werden verwendet, um Standardtexte für Anwendungsüberschriften und -fußzeilen, Fehlernachrichten, Schaltflächenbeschriftungen, Attributbezeichnungen und Formularabschnittsbezeichnungen bereitzustellen. Sie können den Text für Textschlüssel ändern.

E-Mail-Vorlagen

E-Mail-Vorlagen werden verwendet, um den Inhalt für E-Mail-Nachrichten bereitzustellen, die als Antwort auf ein Ereignis an Benutzer gesendet werden. Beispiel: Der Inhalt von Nachrichten, die gesendet werden, wenn eine Registrierungsanforderung genehmigt wird oder wenn ein Kennwort zurückgesetzt wird. Sie können den Inhalt von Nachrichten ändern. Sie können Aspekte der verwendeten Schriftart und der verwendeten Absatzstile ändern.

Portal

Das Self-Service-Profilportal oder die entsprechende Anwendung ermöglichen es Benutzern, ihre eigenen Accountprofilinformationen zu verwalten, sobald sie sich registriert haben und sich bei Cloud Identity Service authentifizieren können. Sie können den Text, der zum Bezeichnen von Tabellenspaltenüberschriften verwendet wird, und den Text, der für andere Elemente der Benutzerschnittstelle verwendet wird, ändern.

Suiteseiten

Suiteseiten sind die einzelnen Seiten der Self-Service-Anwendung, auf die Benutzer zugreifen, um Aspekte ihrer Cloud Identity Service-Identität oder ihres Accounts zu verwalten. Zu den Suiteseiten gehören die Selbstregistrierung, das Zurücksetzen des Kennworts, die Wiederherstellung des Benutzernamens und die Verzeichnissuche. Sie können den Text ändern, der zur Bezeichnung von Abschnitten und Überschriften auf Suiteseiten verwendet wird.

Markenkennzeichnung anpassen

Sie können die Markenkennzeichnung anpassen, indem Sie die Farben, Logos, Symbole und Bilder ändern, die in Self-Service-Anwendungen verwendet werden.

Basismotivfarbe auswählen

Sie können eine Farbe auswählen, die als Basishintergrundfarbe für alle Self-Service-Anwendungen verwendet wird.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Self Service** > **Branding** und klicken Sie dann auf **Themes**.

2. Wählen Sie die Basismotivfarbe aus. Eine Vorschau wird angezeigt.
3. Klicken Sie auf **Save**.

Motivfarben auswählen

Sie können bestimmte Grundfarben für eine Reihe von Elementen der Benutzerschnittstelle für Self-Service auswählen. Sie können ferner Farben auswählen, die für Nachrichten und Schaltflächen verwendet werden.

Informationen zu diesem Vorgang

Die ausgewählten Farben setzen die Basismotivfarbe außer Kraft.

Vorgehensweise

1. Klicken Sie im Navigationsfenster im Navigationsmenü auf **Self Service** > **Branding** und klicken Sie dann auf **Colors**.

2. Ändern Sie die Farbe eines Elements durch eine der folgenden Methoden.
   - Klicken Sie in das Quadrat zur Farbauswahl.
   - Geben Sie den HTML-Farbcode ein.

   Sie können Farben für die folgenden Elemente der Benutzerschnittstelle von Self-Service auswählen.
   - Basisversion des Programms
     - Header
     - Tabelle

- Profil
- Link
- Fehler

- Schaltfläche
  - Primär
  - Sekundär
  - Alternierend
- Nachricht
  - Allgemein
  - Erfolg
  - Wird geladen
  - Feedback
  - Alert
  - Fehler

3. Klicken Sie auf **Save**.

Bilder auswählen

Sie können die Bilder, Logos und Symbole ersetzen, die in Self-Service-Anwendungen verwendet werden.

Informationen zu diesem Vorgang

Sie können Bilder ändern, indem Sie Dateien hochladen, um aktuell verwendete Bilddateien zu ersetzen.

Anmerkung: Eine Ersatzdatei überschreibt eine aktuelle Datei. Wenn eine aktuelle Datei nicht die ursprüngliche Datei ist, können Sie die aktuelle Version der Datei speichern, bevor Sie sie ersetzen. Ursprüngliche Dateien sind jederzeit zum Download und zur Wiederverwendung verfügbar. Bilddateien haben eine maximale Größe von 50 KB.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Self Service** > **Branding** und klicken Sie dann auf **Images**.
2. Optional: Um eine aktuell verwendete Datei herunterzuladen, klicken Sie auf **Download Current File**.
3. Um eine Ersatzdatei hochzuladen, klicken Sie auf **Select New File**.

Bilddateien:

Bilddateien werden für Self-Service-Symbole, -Bilder und -Logos verwendet.

Tabelle 21. Bilddateien

Datei	Beschreibung
Logobild	Headerlogo. Dieses Logo wirkt am besten vor einem transparenten Hintergrund. Die Größe kann nicht geändert werden. Bei einem Überschreiten der aktuellen Höhe oder Breite kann es zu einer Verzerrung des Bilds kommen.

Tabelle 21. Bilddateien (Forts.)

Datei	Beschreibung
Fehlersymbol	Bild für fehlgeschlagene Operation oder Fehler. Dieses Logo wirkt am besten vor einem transparenten Hintergrund. Die Größe kann nicht geändert werden. Bei einem Überschreiten der aktuellen Höhe oder Breite kann es zu einer Verzerrung des Bilds kommen.
Favoritensymbol	Im Browser angezeigtes Favoritensymbol. Das Symbol muss die Maße 16 x 16 Pixel aufweisen, damit es ordnungsgemäß als Lesezeichensymbol im Browser angezeigt wird.
Formularelemente	Bilder für Kontrollkästchen und Optionsfelder. Dieses Bild-Sprite enthält alle Bilder für jeden Status des Formularelements in einer einzigen Datei. Die einzelnen Bilder dürfen die Höhe oder Breite des Standardbilds nicht überschreiten. Andernfalls wird das Bild beim Laden in den Browser abgeschnitten (getrimmt).
Seitenhintergrund	Nebeneinander angeordnetes Hintergrundbild für die Profilverwaltung. Dieses Bild wird vertikal nebeneinander angeordnet (wiederholt) und beim Laden der Seite links ausgerichtet.
Datenladeanzeige	Bild für Laden der Daten. Sie können ein statisches oder ein animiertes Bild verwenden. Die Abmessungen dürfen nicht geändert werden.
Ladebild	Bild für das Laden des Abschnitts. Sie können ein statisches oder ein animiertes Bild verwenden. Die Abmessungen dürfen nicht geändert werden.
Suchfeldsymbol	Bild für Eingabefeld, das automatisches Ausfüllen oder die Suchfunktion unterstützt. Sie müssen ein statisches Bild verwenden. Die Abmessungen dürfen nicht geändert werden.
Suchsymbol	Bild für Ausführung der Suche. Sie können ein statisches oder ein animiertes Bild verwenden. Die Abmessungen dürfen nicht geändert werden.
Erfolgssymbol	Symbol für erfolgreiche Operation. Dieses Symbol wirkt am besten vor einem transparenten Hintergrund. Die Größe kann nicht geändert werden. Bei einem Überschreiten der aktuellen Höhe oder Breite kann es zu einer Verzerrung des Bilds kommen.
Seitensymbol	Seitensymbole auf Self-Service-Anzeigen. Dieses Bild-Sprite enthält alle Bilder für jeden Abschnitt der Benutzertoolseiten in einer einzigen Datei. Die einzelnen Bilder dürfen die Höhe oder Breite des Standardbilds nicht überschreiten. Andernfalls wird das Bild beim Laden in den Browser abgeschnitten (getrimmt).

Anmelde- und Fehlerseiten anpassen

Sie können das Style-Sheet, das Logo und den Seitentitel ersetzen, die für die Cloud Identity Service-Anmeldeseite und die Fehlerseiten verwendet werden. Sie können auch Textelemente ändern und hinzufügen, die am Seitenende angezeigt werden.

Vorbereitende Schritte

Zum Ersetzen der Style-Sheet-Datei sollten Sie gut mit CSS vertraut sein. Das Style-Sheet wird verwendet, um die Dimensionierung, die Positionierung und das Design von Elementen der Benutzerschnittstelle auf der Seite zu steuern.

Informationen zu diesem Vorgang

Sie können das Logo oder das Style-Sheet ändern, indem Sie Dateien hochladen, um die derzeit verwendeten Logo- oder Style-Sheet-Dateien zu ersetzen. Sie geben Text ein, um den Seitentitel und Textelemente zu ändern. Textelemente werden am Ende der Seite angezeigt. Sie können auch Unterstützung für die Landessprache für Textelemente bereitstellen.

Anmerkung: Die ursprünglichen Dateien stellen nützliche Beispiele für die Anpassung von Anmelde- und Fehlerseiten bereit.

Anmerkung: Die Ersatz-Style-Sheet- oder -Logo-Datei überschreibt die aktuelle Datei. Wenn eine aktuelle Datei nicht die ursprüngliche Datei ist, können Sie die aktuelle Version der Datei herunterladen und speichern, bevor Sie sie ersetzen. Ursprüngliche Dateien sind jederzeit zum Download und zur Wiederverwendung verfügbar. Bilddateien haben eine maximale Größe von 50 KB.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Self Service** > **Branding** und klicken Sie dann auf **Global**.
2. Optional: Laden Sie eine neue Style-Sheet-Datei hoch, indem Sie auf **Upload Stylesheet** klicken.
3. Optional: Geben Sie einen neuen Seitentitel in das Feld **Page Title** ein.
4. Optional: Laden Sie eine neue Logo-Datei hoch, indem Sie auf **Upload Logo** klicken.
5. Optional: Geben Sie neuen Text für ein Textelement in das Feld **Text Element** ein.

   Anmerkung: Sie können übersetzte Versionen von Textelementen hinzufügen, um Unterstützung für die Landessprache in einer beliebigen Sprache bereitzustellen, die für Ihre Konfiguration von Cloud Identity Service verfügbar ist.
6. Optional: Klicken Sie auf **Add New Text Element**, um ein neues Textelement einzugeben.

   Anmerkung: Neue Textelemente werden in einer bestimmten Reihenfolge, unter dem vorherigen Element, angezeigt.

   Anmerkung: Sie können eine Vorschau der von Ihnen vorgenommenen Änderungen anzeigen, indem Sie auf **Preview Changes** klicken.
7. Klicken Sie auf **Save Changes**.

Allgemeine Self-Service-UI-Textschlüssel anpassen

Sie können Text hinzufügen und den Text für allgemeine Textschlüssel ändern, die für die Beschriftung von Schaltflächen, Feldern, Spalten, LDAP-Attributen und anderen Elementen in allen Self-Service-Anwendungen verwendet werden.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Self-Service** > **Content Management** und klicken Sie dann auf **General**.
2. Wählen Sie die Textschlüssel, die Sie anpassen möchten, in der Dropdown-Liste **Text Keys** aus. Für die folgenden allgemeinen Textschlüssel können Sie Text hinzufügen und die Textschlüssel ändern:

- **Autocomplete**. Textschlüssel zum automatischen Ausfüllen, die in den Suchtabellen "Service" und "User" verwendet werden.
- **Button Labels**. Schaltflächenbeschriftungen, die in allen Self-Service-Anwendungen verwendet werden.
- **Error Messaging**. Allgemeine Fehlernachrichten, die oben auf dem Bildschirm angezeigt werden.
- **Footer Text**. Fußzeilentext, der unten in Self-Service-Anwendungen angezeigt wird.
- **Form Labels**. In Formularen verwendete Beschriftungen.
- **Form Field Placeholder Text**. In Formularen verwendeter Platzhaltertext.
- **Form Field Tooltip Text**. Formularfeld-QuickInfos.
- **Header Text**. Oben in Self-Service-Anwendungen angezeigter Text.
- **LDAP Attributes**. LDAP-Attributnamen. Textschlüssel für LDAP-Attribute können in Suchen nach LDAP-Attributen verwendet werden.
- **User Profile Layout**. Header des Profilabschnittlayouts.
- **Validation Messaging (Custom)**. Angepasste Validierungsnachrichten. Wird verwendet zur Validierung von durch den Kunden bereitgestellten regulären Ausdrücken.
- **Validation Messaging (Standard)**. Standardvalidierungsnachrichten.

3. Ändern Sie die gewünschten Textschlüssel und klicken Sie auf **Save Changes**.

E-Mail-Vorlagen konfigurieren

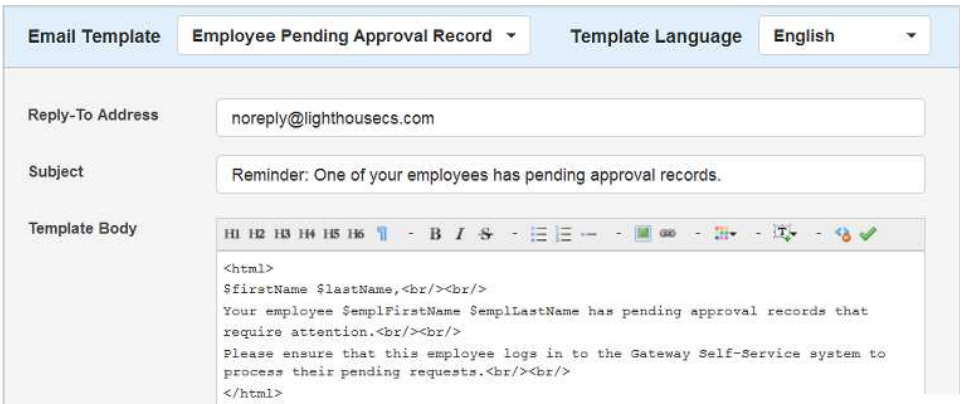
E-Mail-Vorlagen stellen den Inhalt bereit, der verwendet wird, wenn E-Mail-Nachrichten an Benutzer gesendet werden. Sie können den Inhalt und das Format von E-Mail-Vorlagen ändern.

Vorbereitende Schritte

Zur Bearbeitung des Vorlagenhauptteils sind Grundkenntnisse und eine fließende Beherrschung von HTML erforderlich.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Self-Service** > **Content Management** und klicken Sie dann auf **Email Templates**.



2. Wählen Sie aus dem Menü **Email Template** die Vorlage aus, die Sie konfigurieren möchten.
3. Sie können die folgenden Headerdetails ändern:
   - **Reply-To Address**. Die Adresse des Absenders.

- **Subject**. Eine Beschreibung des Zwecks der E-Mail.

4. Geben Sie im Vorlagenhauptteil den Nachrichtentext ein oder ändern Sie ihn.

   Verwenden Sie die Menüleiste **Template Body**, um Text zu formatieren oder Absätze, Bilder, Links und Attribute einzufügen. Durch jedes Symbol werden die entsprechenden HTML-Tags oder Attribute im Hauptteil der Vorlage eingefügt. Heben Sie Text hervor positionieren Sie den Cursor an dem Punkt, an dem Sie die Formatierung anwenden oder ein Attribut, einen Link oder ein Bild einfügen möchten.

5. Klicken Sie auf **Save Changes**.

Optionen zur Formatierung und zum Inhalt von E-Mail-Vorlagen

Tabelle 22. Optionen für Hauptteil, Format und Inhalt von E-Mail-Vorlagen

Optionen für Format und Inhalt	Beschreibung
	Fügt Überschriften 1-6 ein. Schriftartgrößen von Überschrift 1-6 sind 36, 30, 24, 18, 14 und 12 Pixel.
	Fügt einen Absatz ein.
	Textformatierung für Fett, Kursiv und Durchstreichung.
	Listenformatierung für Liste mit Aufzählungszeichen, nummerierte Liste und Listenelement.
	Fügt ein Bild ein. Geben Sie eine URL an, die einen Link zu einem Bild enthält. Sie können alternativen Text für ein Bild angeben. Alternativer Text wird verwendet, um Anforderungen für die barrierefreie Bedienung zu erfüllen. Sie können auch angeben, ob verhindert werden soll, dass der Link zusätzliche Dialogfenster erstellt. Zusätzliche Dialogfenster sind Popup-Fenster.
	Fügen Sie einen Link zu einer Webseite ein. Geben Sie eine URL an, die einen Link zu einer Seite enthält. Ein Bereich im Ankertag ist hervorgehoben, in den Sie Ihren Linktext einfügen können: **Your text to link**. Geben Sie den Text ein, auf den der E-Mail-Empfänger klicken muss, um auf die verlinkte Seite zuzugreifen.
	Textfarbe.

Tabelle 22. Optionen für Hauptteil, Format und Inhalt von E-Mail-Vorlagen (Forts.)

Optionen für Format und Inhalt	**Beschreibung**
	Gibt ein Attribut ein. Eine Reihe von Attributen ist verfügbar. • Approval Create Time. Das Datum und die Uhrzeit, zu der der Service angefordert wird. • Approval Grace Period. Die Zeitdauer, die für das Genehmigen der Serviceanforderung gewährt wird. • Approver First Name. Der Vorname des Administrators, der für das Genehmigen oder Ablehnen der Anforderung zuständig ist. • Approver Last Name. Der Nachname des Administrators, der für das Genehmigen oder Ablehnen der Anforderung zuständig ist. • Client Name. Der Name Ihrer Organisation. • Client Web Presence Name. Der Webauftrittsname für Ihre Organisation, der während des Erstkonfigurationsprozesses definiert wird. • Connection Name. Der Name der sicheren Verbindung zu Cloud Identity Service. • Deprovisioning Instructions. Anweisungen zum Löschen eines Accounts. • Email Address. Die E-Mail-Adresse des Benutzers. • Email Minutes. Die Zeit, für die ein Link zum Zurücksetzen des Kennworts gültig ist. • Employee First Name. Der Vorname des Mitarbeiters mit anstehenden Anforderungen. • Employee Last Name. Der Nachname des Mitarbeiters mit anstehenden Anforderungen. • First Name. Der Vorname des Benutzers. • Last Name. Der Nachname des Benutzers. • Password Minutes. Die zum Ändern eines Kennworts verfügbare Zeit, nachdem ein Benutzer auf den Link zum Zurücksetzen geklickt hat. • Password Reset URL. Ein Link zum Zurücksetzen eines Kennworts. • Provisioning Instructions. Anweisungen zum Erstellen eines Accounts. • Reason. Der Grund für das Ausführen oder Anfordern einer Aktion. • Requester First Name. Der Vorname des Benutzers, der die Serviceanforderung übergibt. • Requester Last Name. Der Nachname des Benutzers, der die Serviceanforderung übergibt. • Service Description. Eine zusammenfassende Beschreibung eines Service. • Service Name. Der Name des angeforderten Service. • Username. Der Benutzername des Benutzers.
	Entfernt die Formatierung des ausgewählten Texts.

Tabelle 22. Optionen für Hauptteil, Format und Inhalt von E-Mail-Vorlagen (Forts.)

Optionen für Format und Inhalt	Beschreibung
	Zeigt eine Vorschau der E-Mail an.

Self-Service-Profilanwendung anpassen

Sie können die Self-Service-Portalprofilanwendung anpassen. Sie können die zum Beschriften von Spalten verwendeten Textschlüssel und andere Elemente des Portals ändern.

Informationen zu diesem Vorgang

Mit der Self-Service-Profilanwendung können -Benutzer ihre eigenen Accountprofilinformationen verwalten und Services anzeigen und anfordern. Mit dem Self-Service-Portal können außerdem direkt unterstellte Mitarbeiter, Serviceanforderungen und delegierte Benutzer verwaltet werden.

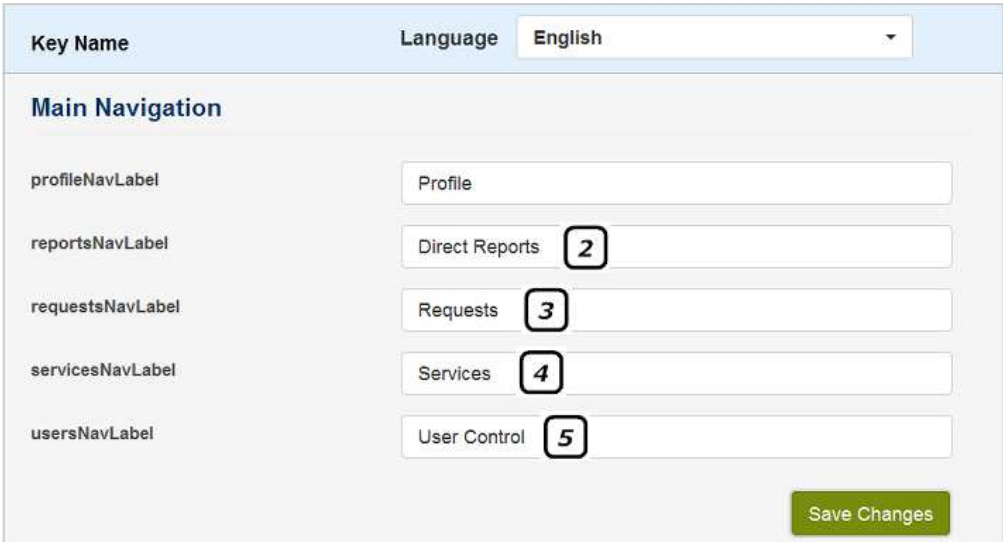
Sie können den für Tabellenspaltenüberschriften im gesamten Portal verwendeten Text sowie den Text für andere Elemente der Benutzerschnittstelle ändern.

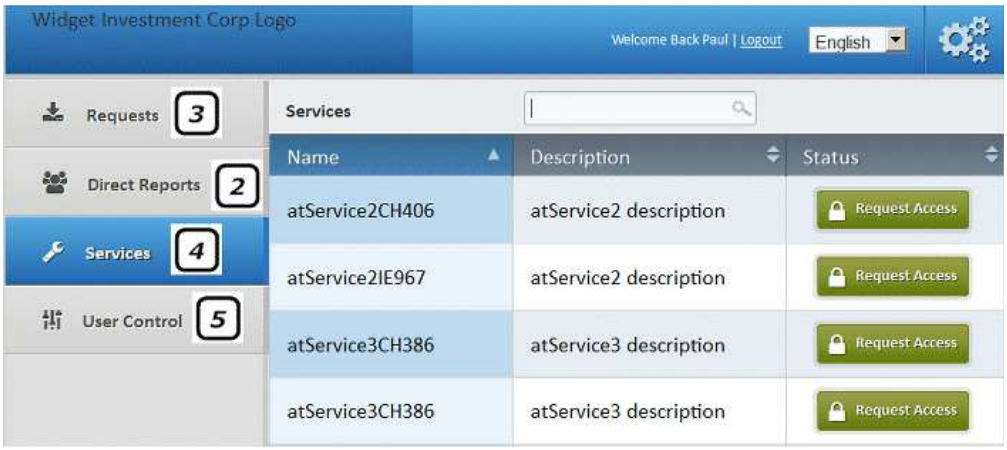
Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Self-Service** > **Content Management** und klicken Sie dann auf **Portal**.
2. Wählen Sie den UI-Abschnitt, den Sie anpassen möchten, in der Dropdown-Liste **Text Keys** aus. Für die folgenden UI-Bereiche können Sie die Textschlüssel ändern:
   - **Main Navigation** (Hauptnavigation).
   - **Service Table Columns** (Servicetabellenspalten).
   - **Direct Reports Table Columns** (Tabellenspalten zu direkt unterstellten Mitarbeitern).
   - **Requests Table Columns** (Anforderungstabellenspalten).
   - **User Control Table Columns** (Tabellenspalten zu Steuerelementen).
   - **Table labels** (Tabellenbeschriftungen).
   - **Search Labels** (Suchbeschriftungen).
3. Nehmen Sie die gewünschten Änderungen bei Beschriftungen und Text vor und klicken Sie auf **Save Changes**.

Navigationsschlüsselnamen und Bezeichnungen zu "Main Portal"

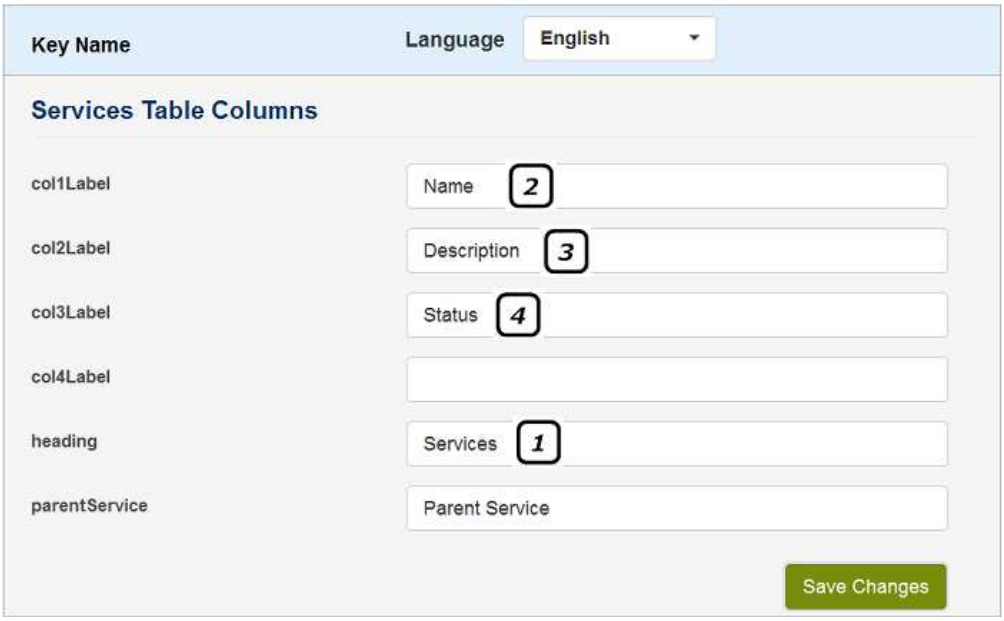
Navigationsschlüsselnamen für "Main Portal" werden verwendet, um die Hauptabschnitte auf der Hauptseite des Self-Service-Portals zu bezeichnen.





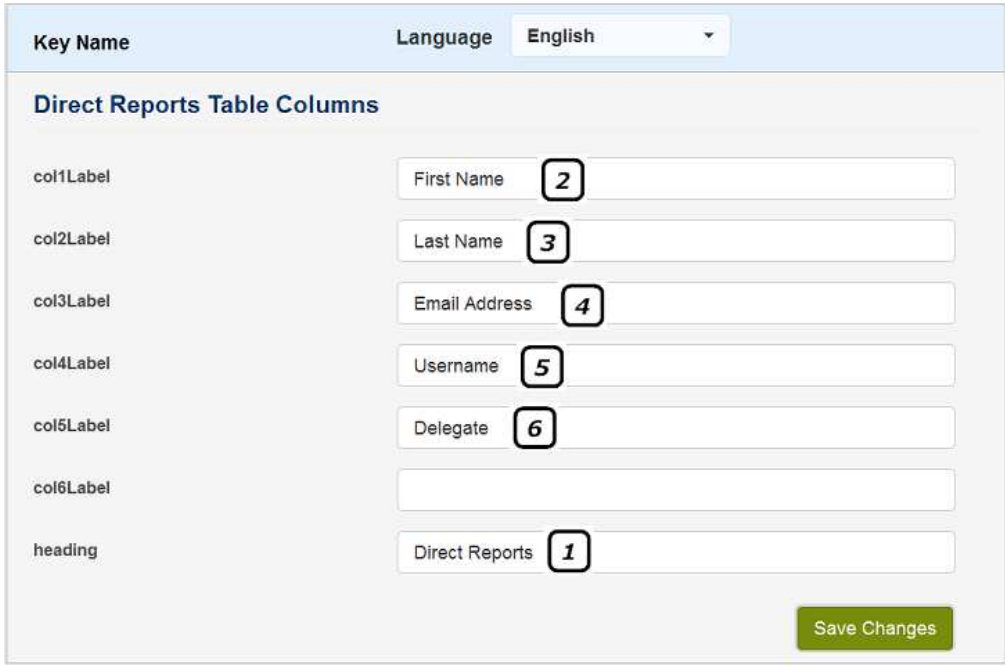
Schlüsselnamen und Bezeichnungen der Seite "Services"

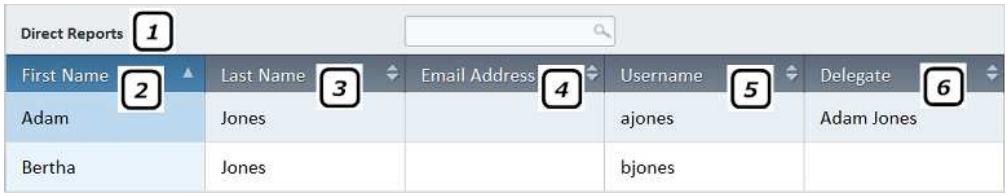
Schlüsselnamen der Seite "Services" werden verwendet, um die Überschrift und die Tabellenspalten der Seite **Services** zu bezeichnen.



Schlüsselnamen und Bezeichnungen der Seite "Direct Reports"

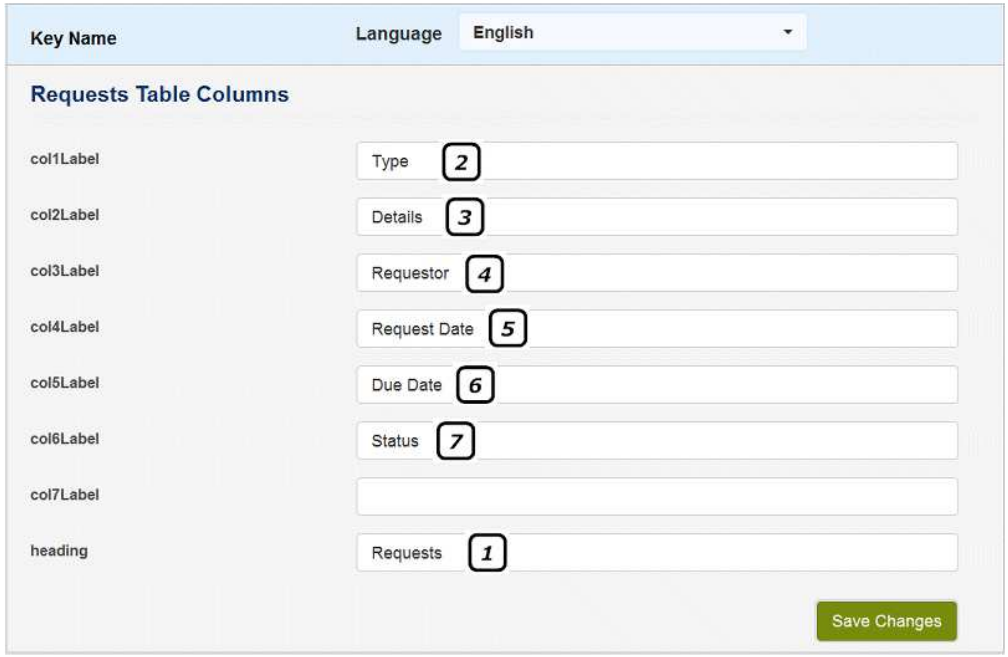
Schlüsselnamen für "Direct Reports" werden verwendet, um die Überschrift und die Tabellenspalten der Seite **Direct Reports** zu bezeichnen.





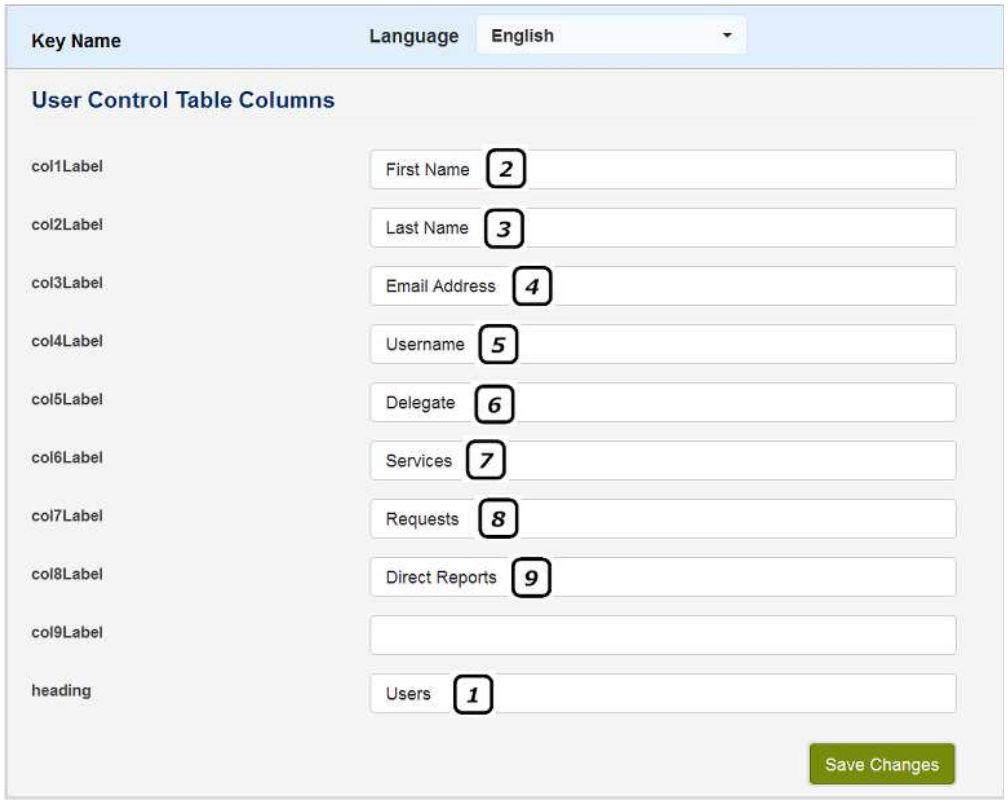
Schlüsselnamen und Bezeichnungen der Seite "Requests"

Schlüsselnamen der Seite "Requests" werden verwendet, um die Überschrift und die Tabellenspalten der Seite **Requests** zu bezeichnen.



Schlüsselnamen und Bezeichnungen der Seite "User Control"

Schlüsselnamen der Seite "User Control" werden verwendet, um die Überschrift und die Tabellenspalten der Seite **User Control** zu bezeichnen.



Benutzerschnittstelle für Seiten der Self-Service-Suite anpassen

Sie können die Seiten der Self-Service-Anwendungssuite anpassen. Sie können die für Überschriften, Felder und andere Elemente der Self-Service-Anwendungen verwendeten Textschlüssel ändern.

Informationen zu diesem Vorgang

Mit den Self-Service-Anwendungen können Benutzer mehrere Self-Service-Tasks steuern, einschließlich Selbstregistrierung, Zurücksetzen des Kennworts und Wie-

derherstellung des Benutzernamens. Sie können den für Felder und Überschriften in allen Self-Service-Anwendungen verwendeten Text ändern.

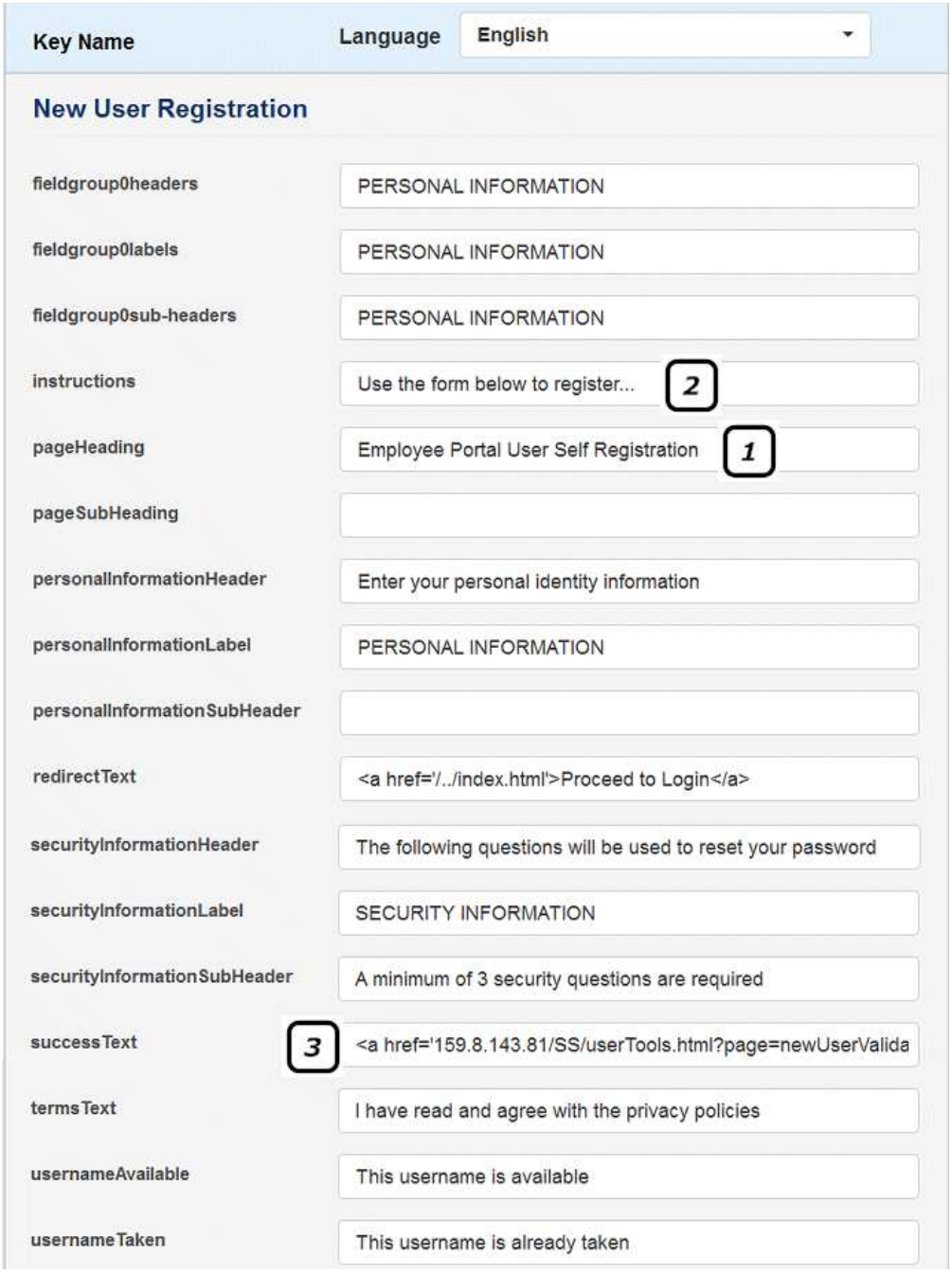
Welche Textelemente Sie ändern können, hängt davon ab, welche Optionen für Ihre Self-Service-Anwendungen konfiguriert sind.

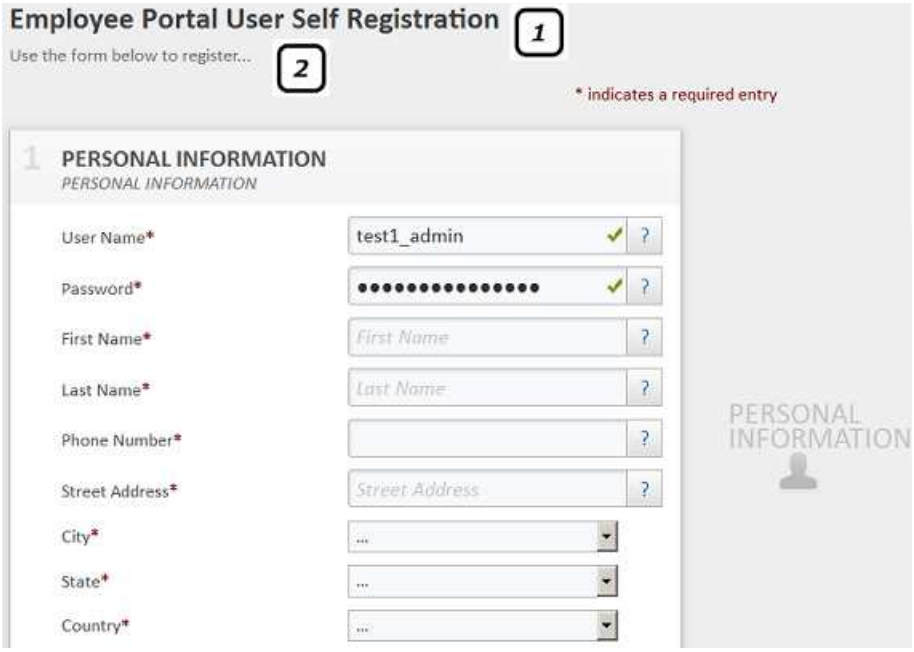
Vorgehensweise

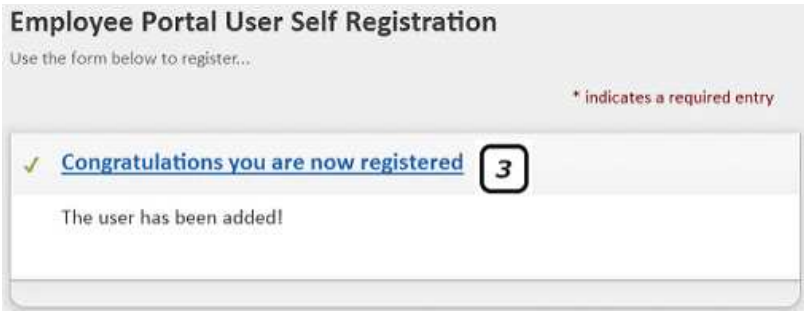
1. Klicken Sie im Navigationsmenü auf **Self-Service** > **Content Management** und klicken Sie dann auf **Suite Pages**.
2. Wählen Sie die Self-Service-Anwendung, die Sie anpassen möchten, aus dem Menü **Text Keys** aus. Für die folgenden Self-Service-Anwendungen können Sie die Textschlüssel ändern:
   - **New User Registration** (Registrierung für Erstbenutzer).
   - **Password Reset** (Zurücksetzen des Kennworts).
   - **Password Reset Verification** (Überprüfung des Zurücksetzens des Kennworts).
   - **Username Recovery** (Wiederherstellung von Benutzernamen).
   - **Directory Lookup Text** (Text für Verzeichnissuche).
3. Ändern Sie die gewünschten Textschlüssel und klicken Sie auf **Save Changes**.

Schlüsselnamen für "User Registration"

Schlüsselnamen für "User Registration" werden verwendet, um Überschriften und Felder auf der Seite "Self-Service User Registration" zu bezeichnen.

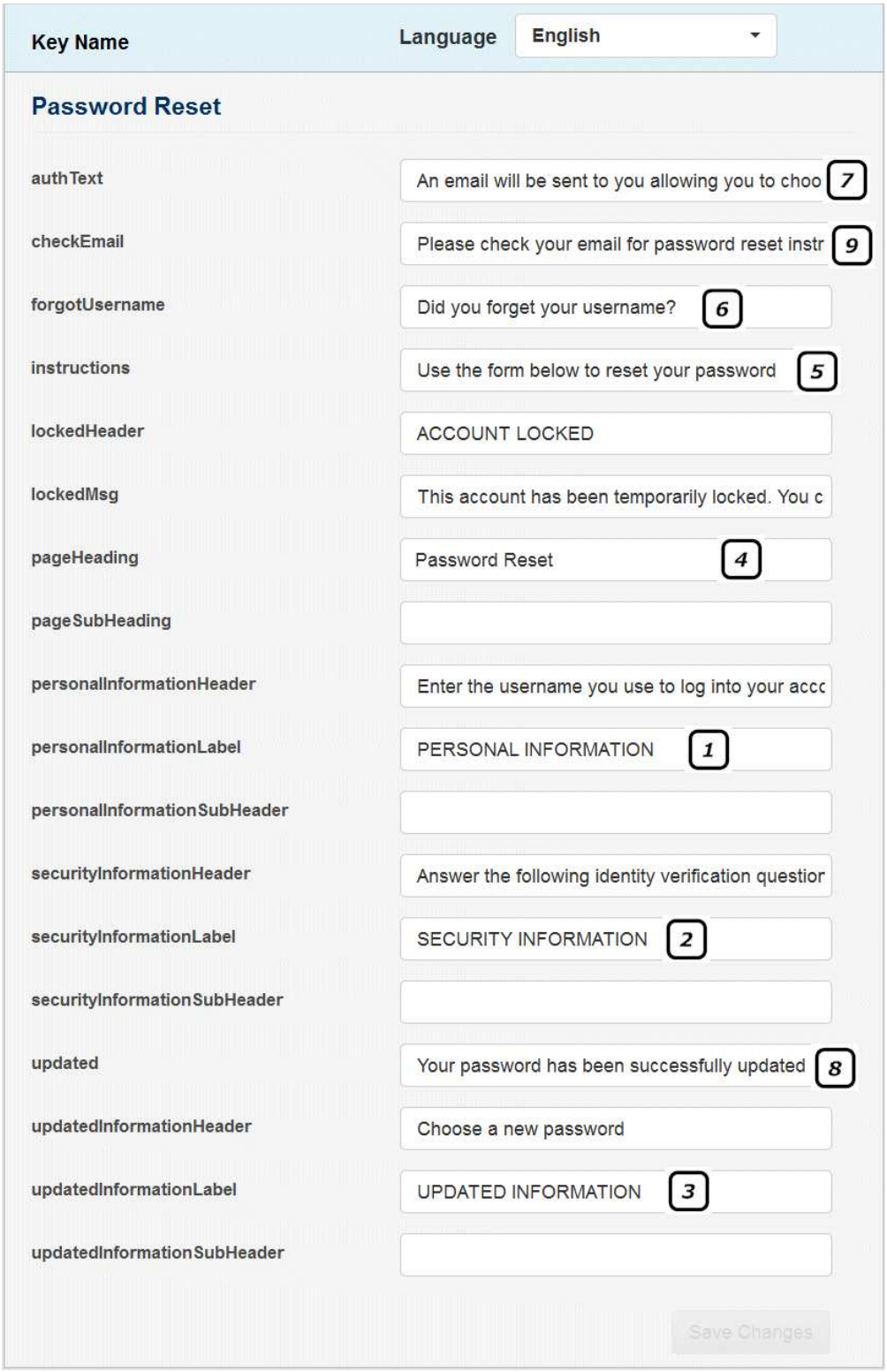

Key Name
Language
English
New User Registration
fieldgroup0headers
PERSONAL INFORMATION
fieldgroup0labels
PERSONAL INFORMATION
fieldgroup0sub-headers
PERSONAL INFORMATION
instructions
Use the form below to register...
2
pageHeading
Employee Portal User Self Registration
1
pageSubHeading
personalInformationHeader
Enter your personal identity information
personalInformationLabel
PERSONAL INFORMATION
personalInformationSubHeader
redirectText
Proceed to Login
securityInformationHeader
The following questions will be used to reset your password
securityInformationLabel
SECURITY INFORMATION
securityInformationSubHeader
A minimum of 3 security questions are required
successText
3
<a href='159.8.143.81/SS/userTools.html?page=newUserValida
termsText
I have read and agree with the privacy policies
usernameAvailable
This username is available
usernameTaken
This username is already taken

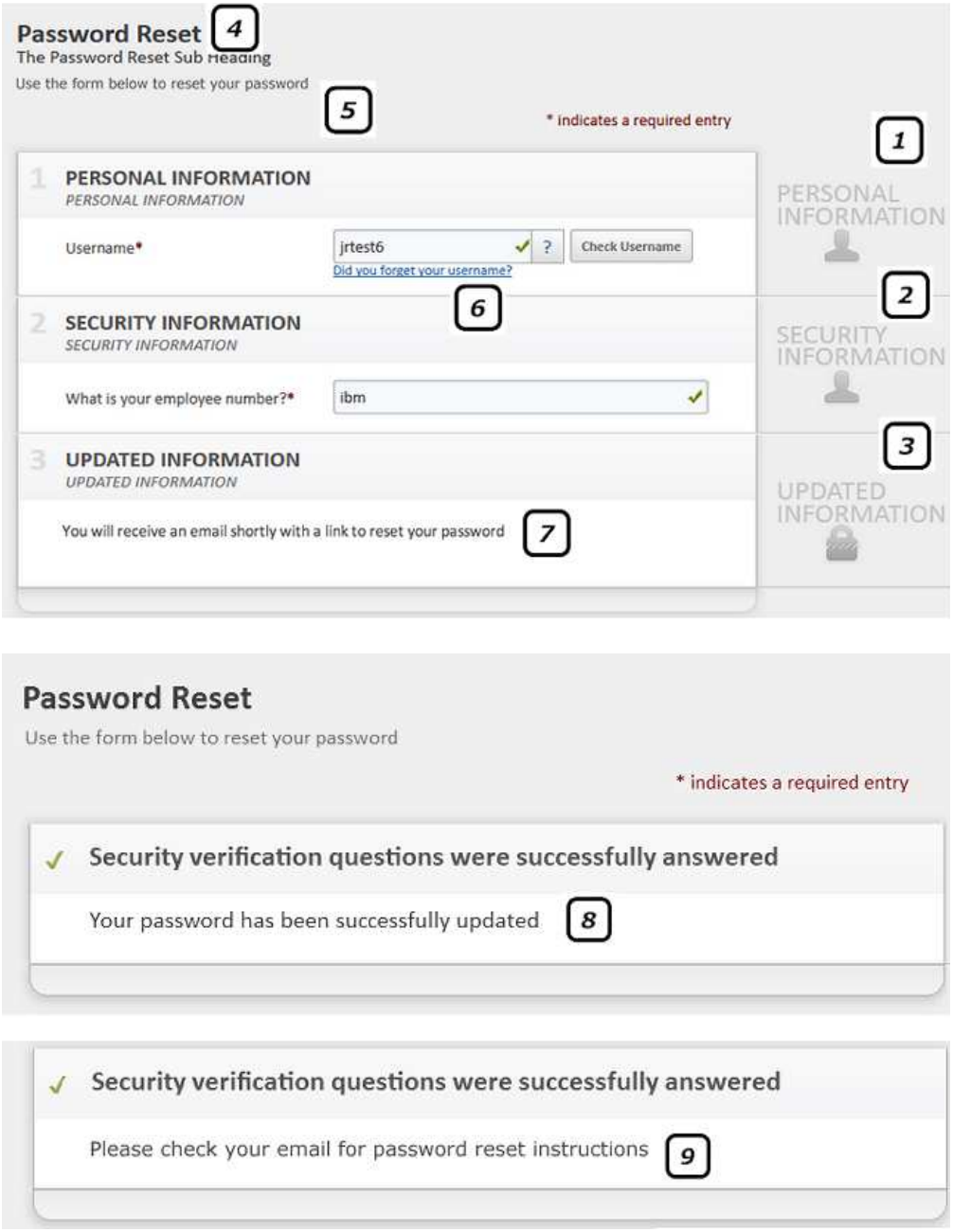




Schlüsselnamen für "Password Reset"

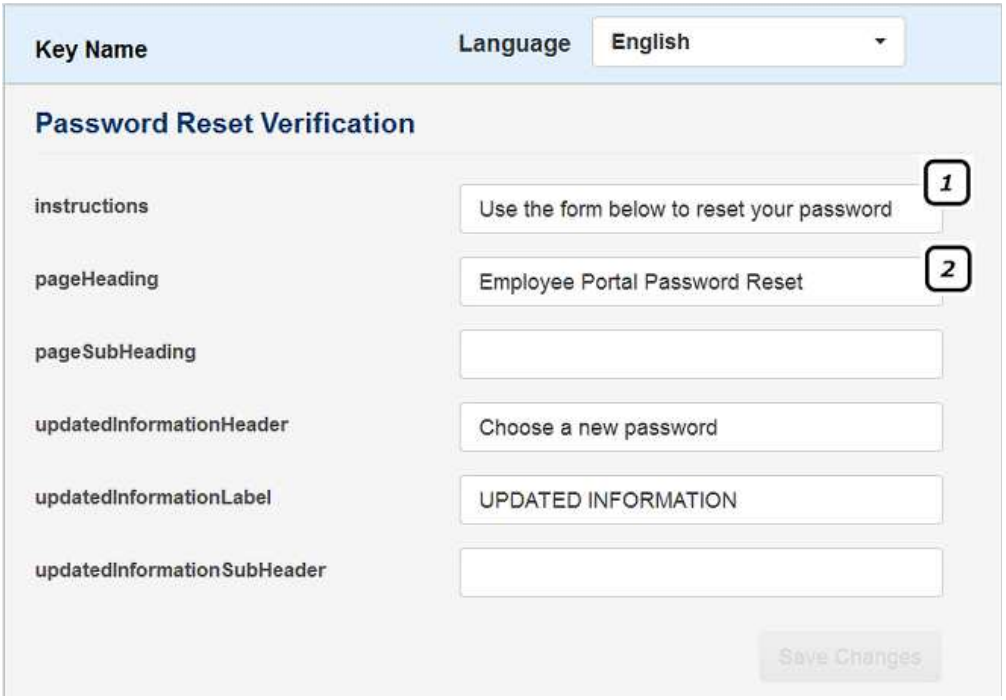
Schlüsselnamen für "Password Reset" werden verwendet, um Überschriften, Abschnitte und Felder in der Self-Service-Anwendung von Password Reset zu bezeichnen.

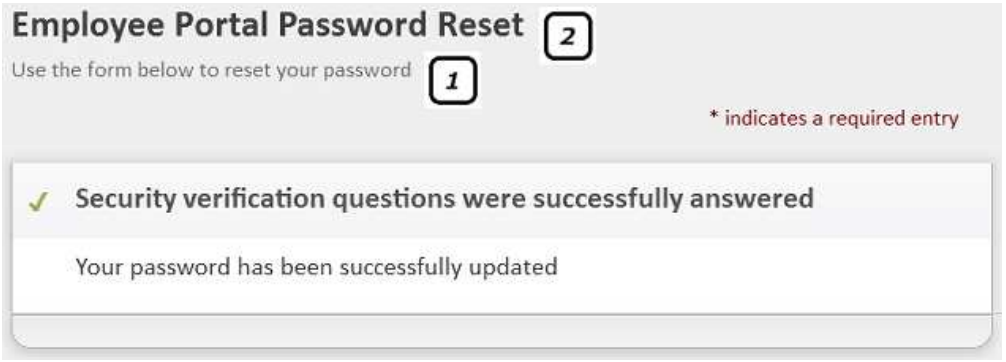

Key Name
Language
English
Password Reset
authText
An email will be sent to you allowing you to choo
7
checkEmail
Please check your email for password reset instr
9
forgotUsername
Did you forget your username?
6
instructions
Use the form below to reset your password
5
lockedHeader
ACCOUNT LOCKED
lockedMsg
This account has been temporarily locked. You c
pageHeading
Password Reset
4
pageSubHeading
personalInformationHeader
Enter the username you use to log into your accc
personalInformationLabel
PERSONAL INFORMATION
1
personalInformationSubHeader
securityInformationHeader
Answer the following identity verification questior
securityInformationLabel
SECURITY INFORMATION
2
securityInformationSubHeader
updated
Your password has been successfully updated
8
updatedInformationHeader
Choose a new password
updatedInformationLabel
UPDATED INFORMATION
3
updatedInformationSubHeader
Save Changes



Schlüsselnamen für "Password Reset Verification"

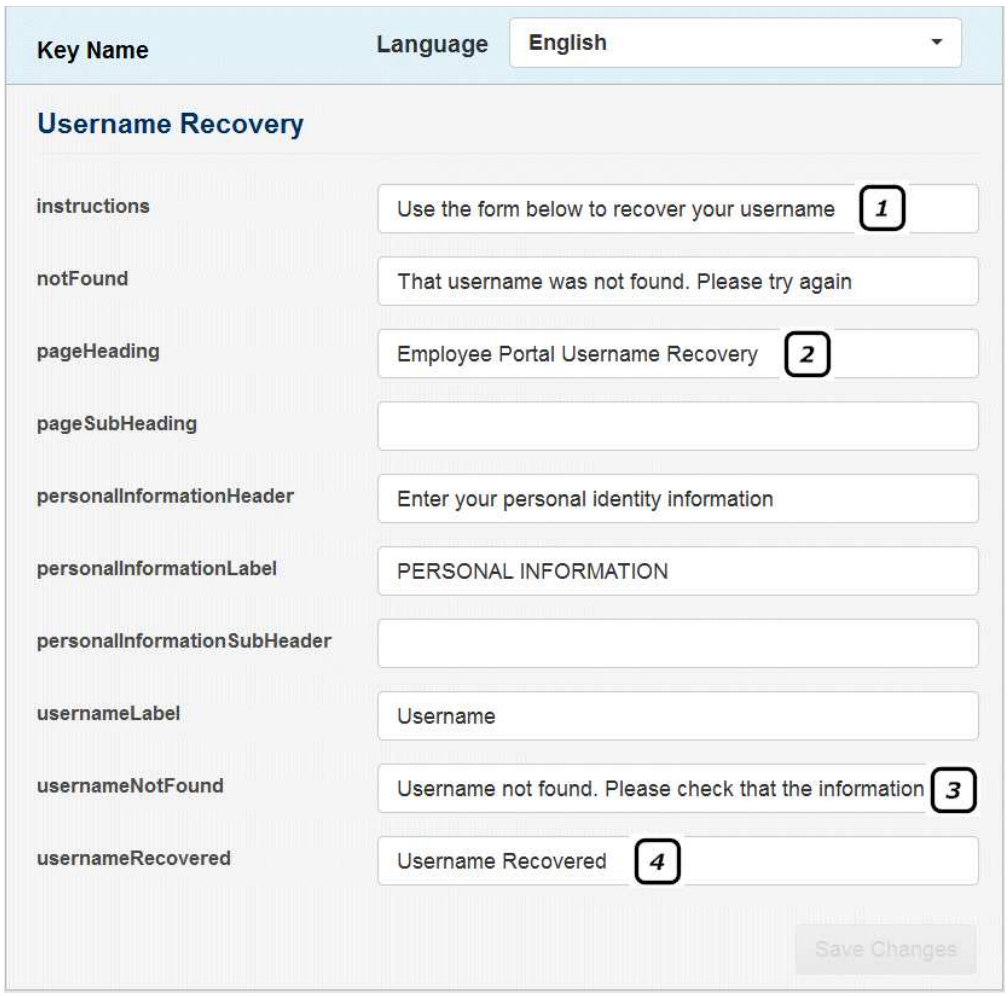
Schlüsselnamen für "Password Reset Verification" werden verwendet, um Überschriften und Felder auf der Seite "Self-Service Password Reset verification" zu bezeichnen.

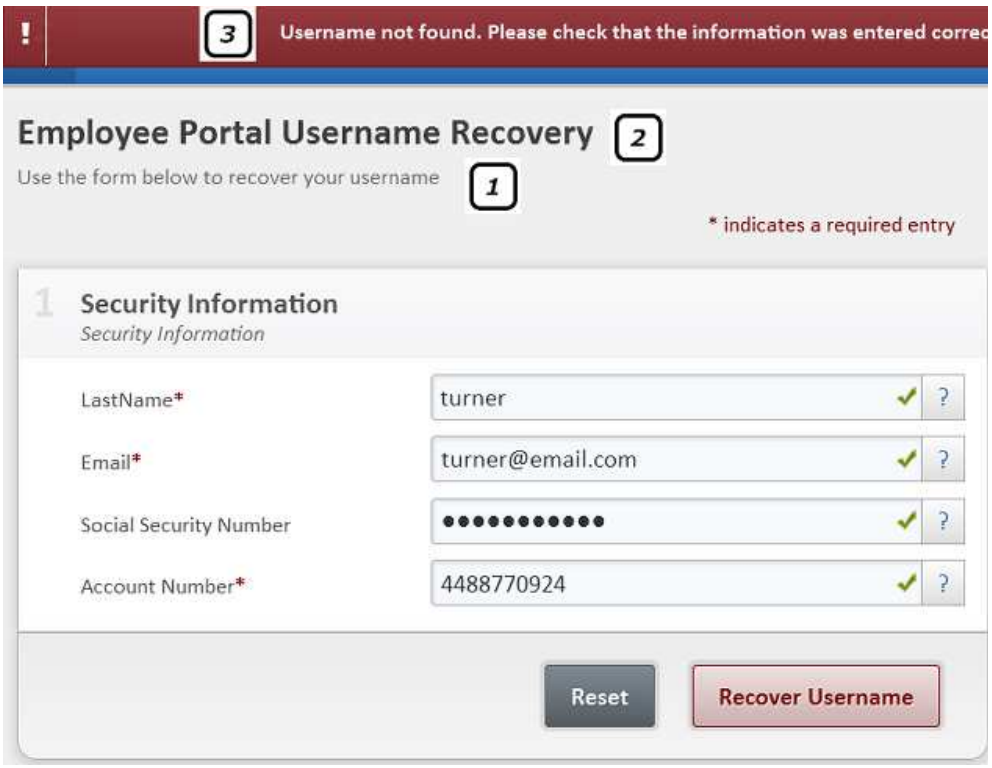


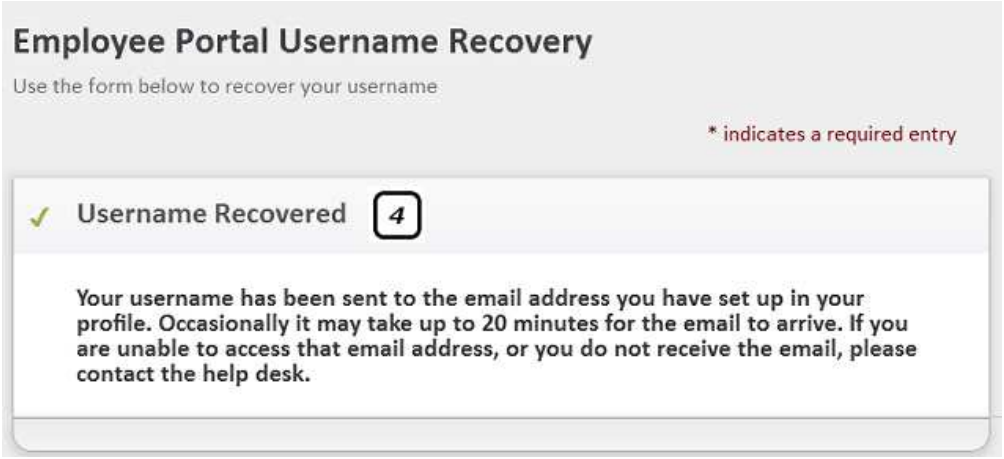


Schlüsselname für "Username Recovery"

Schlüsselnamen für "Username Recovery" werden verwendet, um Überschriften und Felder auf den Seiten von "Self-Service Username Recovery" zu bezeichnen.

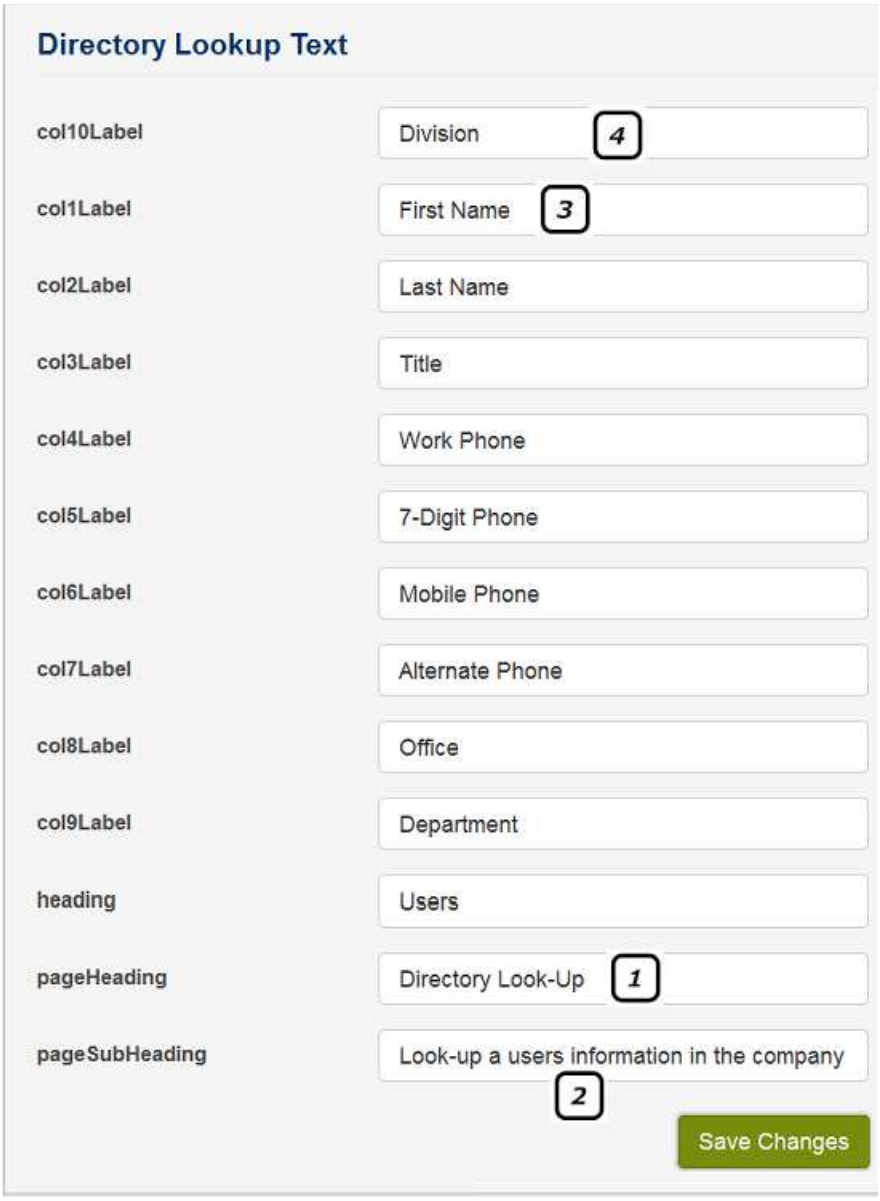

Key Name
Language
English
Username Recovery
instructions
Use the form below to recover your username
1
notFound
That username was not found. Please try again
pageHeading
Employee Portal Username Recovery
2
pageSubHeading
personalInformationHeader
Enter your personal identity information
personalInformationLabel
PERSONAL INFORMATION
personalInformationSubHeader
usernameLabel
Username
usernameNotFound
Username not found. Please check that the information
3
usernameRecovered
Username Recovered
4
Save Changes

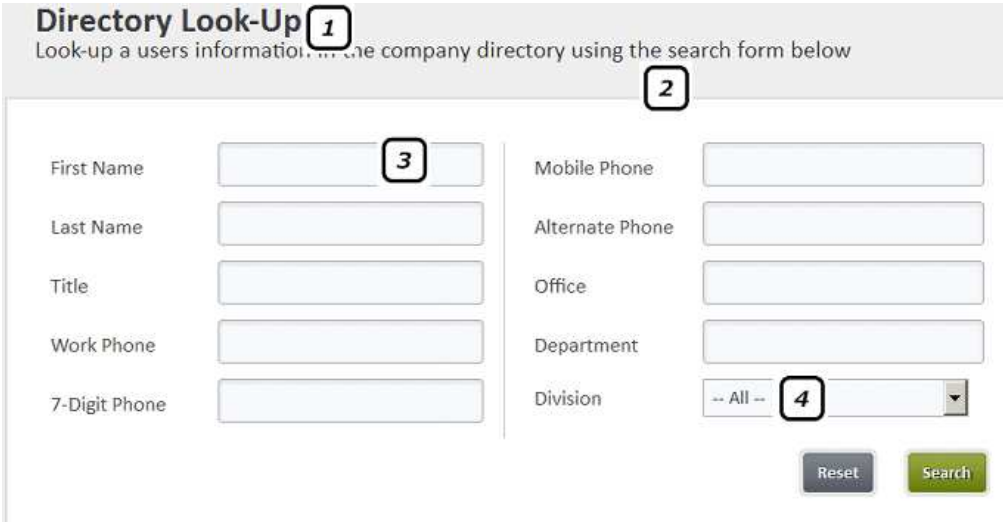




Schlüsselnamen für "Directory Lookup"

Schlüsselnamen für "Directory Lookup" werden verwendet, um Überschriften und Felder auf der Seite "Self-Service Directory Look-up" zu bezeichnen.


Directory Lookup Text
col10Label
Division
4
col1Label
First Name
3
col2Label
Last Name
col3Label
Title
col4Label
Work Phone
col5Label
7-Digit Phone
col6Label
Mobile Phone
col7Label
Alternate Phone
col8Label
Office
col9Label
Department
heading
Users
pageHeading
Directory Look-Up
1
pageSubHeading
Look-up a users information in the company
2
Save Changes


Directory Look-Up
1
Look-up a users information in the company directory using the search form below
2
First Name
3
Last Name
Title
Work Phone
7-Digit Phone
Mobile Phone
Alternate Phone
Office
Department
Division
-- All --
4
Reset
Search

Instanzen hinzufügen

Sie können eine Reihe von Instanzen hinzufügen, die von verschiedenen Rollen in Ihrer Organisation verwendet werden sollen.

Informationen zu diesem Vorgang

Bei einer Instanz handelt es sich um eine Gruppierung von Konfigurationen und Optionen für Self-Service-Anwendungen. Eine Instanz kann z. B. Textübersetzungen, Formularlayouts, Selbstregistrierungsoptionen und weitere Self-Service-Anwendungsoptionen definieren. Für jede definierte Rolle kann eine Instanz ausgewählt werden. Die Rolle "help desk" und die Rolle "manager" können verschiedenen Instanzen zugewiesen werden, um ihnen Zugriff auf verschiedene Self-Service-Anwendungsoptionen zu geben. Eine Rolle kann nur einer Instanz zugewiesen werden. Eine einzige Instanz kann von vielen Rollen verwendet werden.

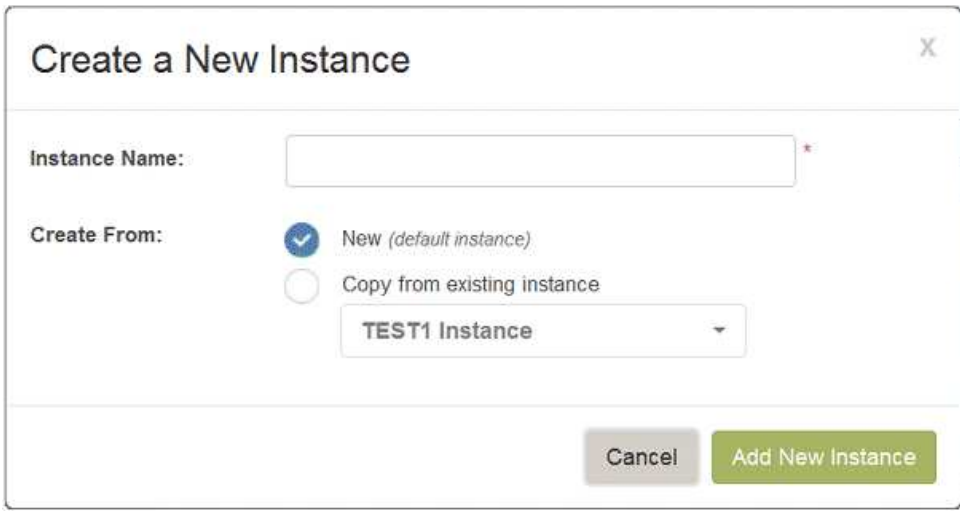
Sie können eine Instanz für die folgenden Aktionen auswählen:

- Konfigurieren von Self-Service-Anwendungen
- Anpassen der Benutzerschnittstelle für Self-Service-Anwendungen

Instanzen können über die meisten der Self-Service-Konfigurations- und Anpassungstasks erstellt werden, sobald sie benötigt werden. Im folgenden Beispiel wird eine Instanz von **Self-Service** > **Content Management** aus erstellt.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Content Management**.
2. Klicken Sie auf **Add a new instance**.



3. Geben Sie einen Namen für die Instanz in das Feld **Instance Name** ein.
4. Wählen Sie aus, ob die Instanz auf der Standardinstanz oder auf einer anderen Instanz basieren soll.
   - **New**. Die Instanz basiert auf den Konfigurationsoptionen, die für die Standardinstanz erstellt werden.
   - **Copy from existing instance**. Die Instanz basiert auf den Konfigurationsoptionen, die für die ausgewählte Instanz erstellt werden.
5. Klicken Sie auf **Add New Instance**.

Unterstützung für Landessprache hinzufügen

Sie können Unterstützung für Ihre Landessprache hinzufügen, sodass Text in Self-Service-Anwendungen, Nachrichten und E-Mails in der gewählten Sprache angezeigt werden.

Sprachen hinzufügen

Sie können unterstützte Sprachen zu Cloud Identity Portal hinzufügen. Hinzugefügte Sprachen können verwendet werden, um Text in Ihrer gewählten Sprache in Self-Service-Anwendungen zur Verfügung zu stellen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Self-Service** > **Content Management**.
2. Wählen Sie im Menü **Add a new language** eine Sprache aus, die hinzugefügt werden soll. Im Menü wird eine Liste aller unterstützten Sprachen angezeigt.
3. Klicken Sie auf **Add New Language**.

Übersetzten Text bereitstellen

Sie können übersetzten Text angeben, um Unterstützung in Landessprache für Benutzer der Self-Service-Anwendungen bereitzustellen.

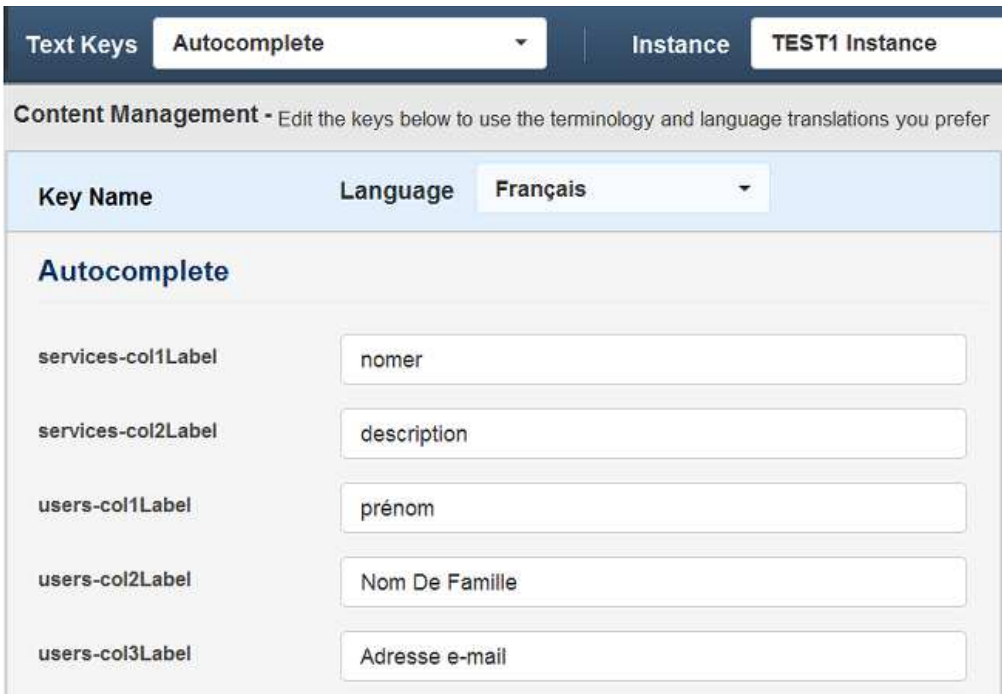
Informationen zu diesem Vorgang

Sie können Text für viele Aspekte von Self-Service-Anwendungen bereitstellen, einschließlich E-Mail-Vorlagen und Sicherheitsfragen. Sie können aus einer Reihe von unterstützten Sprachen auswählen.

Sie können für Folgendes eine Landessprache auswählen, in der Sie Text bereitstellen möchten:

- Sicherheitsfragen
- UI-Text für Self-Service-Anwendungen
- E-Mail-Vorlagen
- Self-Service-Profilportal
- Seiten der Self-Service-Anwendungssuite, einschließlich Selbstregistrierung, Zurücksetzen des Kennworts, Wiederherstellung des Benutzernamens und Verzeichnissuche

Im folgenden Beispiel werden Textschlüssel zum automatischen Ausfüllen ins Französische übersetzt.


Text Keys
Autocomplete
Instance
TEST1 Instance
Content Management - Edit the keys below to use the terminology and language translations you prefer
Key Name
Language
Français
Autocomplete
services-col1Label
nomer
services-col2Label
description
users-col1Label
prénom
users-col2Label
Nom De Famille
users-col3Label
Adresse e-mail

Kapitel 7. Anwendungen

Das Anwendungsmanagement umfasst das Management von Netzverbindungen zu geschützten Webressourcen des Unternehmens und zu föderierten Webanwendungen anderer Anbieter sowie das Management der Benutzereinrichtung und der Services.

Services verwalten

Ein Service stellte zusätzliche Features zu den Features einer Rolle oder Gruppe bereit. Allgemein werden Services zum Bereitstellen einer Verbindung zwischen Benutzeridentitäten und den zu Cloud Identity Service externen Systemen verwendet.

Übersicht über Services

Allgemein werden Services zum Bereitstellen einer Verbindung zwischen Benutzeridentitäten und den zu Cloud Identity Service externen Systemen verwendet, für die Benutzer möglicherweise eingerichtet werden müssen.

Sie können Services, einschließlich der Servicemitgliedschaft, mithilfe von Cloud Identity Service verwalten. Die Servicemitgliedschaft kann manuell oder mithilfe einer dynamischen Einrichtungsrichtlinie verwaltet werden. Jeder Service muss über einen Serviceeigner verfügen. Ein Serviceeigner ist ein Benutzer, der üblicherweise als der Eigner oder Administrator des externen Systems definiert ist, zu dem der Service eine Verbindung herstellt. Servicekategorien können verwendet werden, um zusammengehörige Services zu gruppieren und Self-Service-Benutzern das Verwalten ihrer Services zu erleichtern.

Die Benutzermitgliedschaft in einem Service kann statisch oder dynamisch definiert werden. Bei einer statischen Benutzermitgliedschaft ist es erforderlich, dass Sie jeden einzelnen Benutzer manuell zum Service hinzufügen und die Mitgliedschaft auch manuell verwalten. Bei einer dynamischen Benutzermitgliedschaft werden die Benutzer für die Mitgliedschaft automatisch auf der Grundlage einer übereinstimmenden Kombination der zugehörigen Identitätsattributwerte, anderer Gruppenmitgliedschaften, anderer Servicemitgliedschaften oder abhängig davon, ob dem Benutzer eine Rolle als Manager zugeordnet wurde, ausgewählt.

Die dynamische Benutzermitgliedschaft wird mithilfe einer dynamischen Einrichtungsrichtlinie implementiert, in der Sie die Auswahlkriterien für die Mitgliedschaft definieren.

Für einen Service kann eine beliebige Anzahl von dynamischen Richtlinien definiert werden. Eine Richtlinie kann bei Bedarf durch Abgleichen der Richtlinie angewendet werden. Eine Richtlinie kann außerdem anhand eines Zeitplans angewendet werden. Wenn eine Richtlinie angewendet wird, werden die Auswahlkriterien ausgewertet und die Benutzermitgliedschaft wird aktualisiert. Dabei werden nicht (mehr) übereinstimmende Benutzer entfernt und übereinstimmende Benutzer hinzugefügt.

Services beziehen Optionen zum Erstellen von Abhängigkeiten zwischen Services mit ein, einschließlich von Beziehungen zwischen über- und untergeordneten Elementen sowie Containerzuordnungen. Eine Beziehung zwischen über- und untergeordneten Elementen dient dazu, die Mitgliedschaft zum übergeordneten Service durchzusetzen, bevor die Mitgliedschaft zu untergeordneten Services durchgesetzt wird. Containerzuordnungen dienen zum Definieren von Services, die die Mitgliedschaft eines Benutzers zu jedem enthaltenen Service direkt anfordern, wenn die Mitgliedschaft zu dem Container erreicht ist.

Es werden Benachrichtigungen verwendet, um Benachrichtigungs-E-Mails an verschiedene Empfänger zu senden. Benachrichtigungen können servicespezifische Informationen zur Einrichtung und zum Aufheben von Einrichtungen einbeziehen.

Die erneute Zertifizierung dient zur Steuerung der Mitgliedschaft zu einem Service über einen bestimmten Zeitraum. Richtlinien für die erneute Zertifizierung werden auf dieselbe Art wie dynamische Einrichtungsrichtlinien definiert. Je nachdem, wie der Service definiert ist, sendet jedes Mitglied, das die Bedingungen einer Richtlinie für die erneute Zertifizierung erfüllt, eine Anforderung zur erneuten Zertifizierung an den jeweiligen Manager oder den Eigner oder an beide. Der Manager oder der Serviceeigner zertifiziert, ob der Benutzer noch zu dem Service gehört. Eine erneute Zertifizierung kann für richtlinienbasierte Servicemitgliedschaften und für manuell gesteuerte Servicemitgliedschaften erforderlich sein. Richtlinien für die erneute Zertifizierung können zeitlich geplant werden, sodass die erneute Zertifizierung in bestimmten, regelmäßigen Abständen durchgeführt wird.

Genehmigungen dienen dazu, das Erhalten einer Mitgliedschaft für einen Service zu steuern. Eine Genehmigung kann für dynamisch gesteuerte und für manuell gesteuerte Mitgliedschaften erforderlich sein. Für eine Genehmigung ist möglicherweise eine Aktion eines Managers, eines Serviceeigners oder beider Personen erforderlich. Genehmigungen können auf Mitgliedschaftsprozesse und auf Prozesse zur erneuten Zertifizierung angewendet werden.

Nach Services suchen

Sie können nach jedem Service in Ihrer Organisation suchen, um die Details des Service anzuzeigen oder zu ändern oder um die Mitgliedschaft bei einem Service zu verwalten.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Applications** > **Services** und dann auf **General**.
2. Geben Sie im Feld **Filter Results** mindestens die ersten drei Zeichen des Service ein. Die Feldbeschriftung ändert sich in **Searching For**.

   Die Services, die mit Ihren Suchkriterien übereinstimmen, werden aufgelistet. Wählen Sie einen Service zum Ändern oder Anzeigen aus.

Servicekategorien suchen

Sie können nach jeder Kategorie suchen, um Details der Kategorie anzuzeigen oder zu ändern und um Services zu verwalten, die unter der Kategorie gruppiert sind.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Applications** > **Services** und dann auf **Category Management**.
2. Geben Sie im Feld **Filter Results** mindestens die ersten drei Zeichen der Servicekategorie ein. Die Feldbeschriftung ändert sich in **Searching For**.

Ihren Suchkriterien entsprechende Kategorien werden aufgelistet. Wählen Sie eine Kategorie zum Ändern oder Anzeigen aus.

Services erstellen

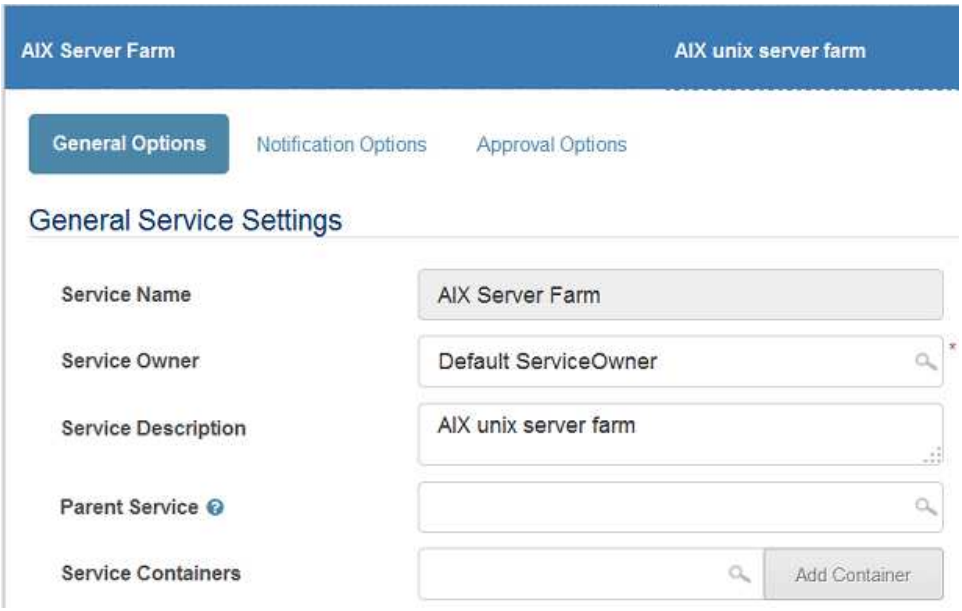
Sie können neue Services hinzufügen. Nach dem Hinzufügen eines Service können Sie Benutzer als Mitglieder des Service auswählen und den Service statisch oder dynamisch verwalten.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Applications** > **Services** und klicken Sie dann auf **Add Service**.
2. Geben Sie einen Namen, den Serviceeigner und eine Beschreibung für den Service ein.

   Der Servicename muss eindeutig sein. Überprüfen Sie, ob der Servicename bereits verwendet wird, indem Sie auf **Check Availability** (Verfügbarkeit prüfen) klicken.

   Um einen Benutzer als Serviceeigner zu suchen und ihn auszuwählen, geben Sie mindestens die ersten drei Stellen Ihrer Suchkriterien in das Feld **Service Owner** ein. Sie können nach dem Vornamen, dem Nachnamen oder der E-Mail-Adresse des Benutzers suchen. Wählen Sie den Benutzer aus der zurückgegebenen Liste aus.
3. Klicken Sie auf **Save Changes**, um den Service hinzuzufügen. Der Service wird gespeichert. Sie kehren zur Liste der Services zurück.
4. Suchen Sie nach dem Service und wählen Sie ihn aus, um die **General Options** (Allgemeine Optionen), **Notification Options** (Benachrichtigungsoptionen), **Approval Options** (Genehmigungsoptionen) und **Form Options** (Formularoptione) einzugeben.



Nächste Schritte

Nach dem Erstellen des Service können Sie manuell oder dynamisch Mitglieder zum Service hinzufügen und Sie können Richtlinien für die erneute Zertifizierung erstellen.

Serviceeinstellungen

Zu den Serviceeinstellungen zählen allgemeine Optionen, Benachrichtigungs- und Genehmigungsoptionen.

Tabelle 23. Allgemeine Optionen

Einstellung	Beschreibung
Service Name	Der Servicename.
Service Owner	Der Benutzername des Serviceeigners.
Service Description	Beschreibung für den Service.
Parent Service	Gibt an, ob die Mitgliedschaft bei einem übergeordneten Service für die Mitgliedschaft beim Service erforderlich ist. Vor dem Erlangen der Mitgliedschaft beim übergeordneten Service sind Benutzer für eine Mitgliedschaft nicht auswählbar. Um nach dem übergeordneten Service zu suchen und ihn auszuwählen, geben Sie mindestens die ersten 3 Zeichen des Servicenamens ein.
Contained Services	Gibt einen enthaltenen Service an. Containerzuordnungen werden verwendet, um Services zu definieren, die direkt die Mitgliedschaft eines Benutzers in jedem enthaltenen Service anfordern, wenn die Mitgliedschaft beim Container erlangt wird. Um nach einem enthaltenen Service zu suchen und ihn auszuwählen, geben Sie mindestens die ersten 3 Zeichen des Servicenamens ein, wählen Sie den Service aus und klicken Sie auf **Add Service**.
Request Instructions	Anweisungen, die Benutzern angezeigt werden, wenn sie den Service anfordern.
SOD Callout Required	Trennung von Aufgaben. Gibt an, ob ein Workflow erforderlich ist, bevor der Genehmigungsprozess ausgelöst wird, um Serviceanforderungsgenehmigungen auf einem externen System aufzuzeichnen.
Hide Service From Self-Service UI	Gibt an, ob der Service in der Self-Service-Profilanwendung angezeigt werden soll.
Allow repeated membership requests	Gibt an, ob wiederholte Mitgliedschaftsanforderungen zugelassen werden sollen. • **On**. Der Service darf keine permanenten Mitglieder enthalten. Die Benutzermitgliedschaft läuft automatisch ab. Die Mitgliedschaft muss erneut angefordert werden. • **Off**. Die Benutzermitgliedschaft läuft nicht automatisch ab.
Dynamic Provisioning Policy	Verwaltung von Richtlinien. Verwaltet die Mitgliedschaft beim Service mithilfe von dynamischen Einrichtungsrichtlinien.
Recertification Policies	Verwaltung von Richtlinien. Verwaltet die erneute Zertifizierung des Service mithilfe von Richtlinien für die erneute Zertifizierung.
Service Members	Verwaltet die Mitgliedschaft beim Service statisch (manuell).

Tabelle 23. Allgemeine Optionen (Forts.)

Einstellung	Beschreibung
Assign To Categories	Sie können einen Service einer oder mehreren Servicekategorien zuordnen. Dienstleistungskategorien werden verwendet, um zusammengehörige Services zusammen zu gruppieren, wodurch es für Benutzer einfacher wird, ihre Services in Self-Service-Anwendungen zu verwalten. Klicken Sie auf **Manage Categories**, um das Fenster **Assign Service to Categories** zu öffnen. Um eine Kategorie zu suchen und auszuwählen, geben Sie mindestens die ersten 3 Ziffern des Kategorienamens in das Feld **Category Name** ein. Wählen Sie die Kategorie aus der zurückgegebenen Liste aus und klicken Sie auf **Add Category**. Fügen Sie den Service zu so vielen Gruppen hinzu, wie Sie möchten, und klicken Sie auf **Done**.

Tabelle 24. Benachrichtigungsoptionen

Einstellung	Beschreibung
Recipient Type	Gruppe, Service oder Benutzer. Benachrichtigungs-E-Mails werden an alle Mitglieder einer Gruppe oder eines Service oder an einen Benutzer gesendet. Benachrichtigungen werden beim Auftreten eines Ereignisses gesendet, z.B. wenn ein Benutzer zu einem Service hinzugefügt wird.
Recipient Name	Der Name der Gruppe, des Service oder des Benutzers, an die oder den die Benachrichtigung gesendet werden soll. Um nach einer Gruppe oder einem Service zu suchen und sie oder ihn auszuwählen, geben Sie mindestens die ersten 3 Zeichen des Gruppen- oder Servicenamens ein. Wählen Sie die Gruppe oder den Service aus der zurückgegebenen Liste aus. Um nach einem Benutzer zu suchen und ihn auszuwählen, geben Sie mindestens die ersten 3 Zeichen Ihres Suchkriteriums ein. Sie können nach dem Vornamen, nach dem Nachnamen oder nach der E-Mail-Adresse des Benutzers suchen. Wählen Sie den Benutzer aus der zurückgegebenen Liste aus.
Provisioning Instructions	Anweisungen, die von Benutzern befolgt werden müssen, wenn sie zum Service hinzugefügt werden.
Deprovisioning Instructions	Anweisungen, die von Benutzern befolgt werden müssen, wenn sie vom Service entfernt werden.
Notify members of assignment/revocation	Gibt an, ob eine Benachrichtigung an Benutzer gesendet wird, wenn sie zum Service hinzugefügt oder vom Service entfernt werden.
Notify managers of assignment/revocation	Gibt an, ob eine Benachrichtigung an die für Benutzer zuständigen Manager gesendet wird, wenn Benutzer zum Service hinzugefügt oder vom Service entfernt werden.

Tabelle 25. Genehmigungsoptionen und Optionen für die erneute Zertifizierung

Einstellung		Beschreibung
Approval Requirements	**Delinquency Action**	Die Aktion, die ausgeführt werden soll, wenn eine Servicegenehmigungsanforderung bis zum Fälligkeitsdatum nicht genehmigt wurde (Rückstandsaktion).
	Action Due Within	Anzahl der Tage, bis die Rückstandsaktion fällig wird.
	Manager Approval	Gibt an, ob die für Benutzer zuständigen Manager die Genehmigung erteilen müssen, damit die Benutzer die Mitgliedschaft beim Service erhalten können. • **Dynamic** – Das Kontrollkästchen ist aktiviert: Wenn eine dynamische Richtlinie aktiv ist, werden automatisch Benachrichtigungs-E-Mails zur Serviceanforderungsgenehmigung generiert, die die Manager über anstehende Serviceanforderungen benachrichtigen, die sie manuell genehmigen müssen. – Das Kontrollkästchen ist inaktiviert: Genehmigungen werden im Auftrag des Managers automatisch erteilt. • **Request**. Das Kontrollkästchen ist aktiviert: Anforderungen werden an die für die Benutzer zuständigen Manager gesendet, die den Service angefordert haben. Anforderungen müssen für die Benutzer genehmigt werden, damit diese Mitglieder des Service werden.
	Service Owner	Gibt an, ob Serviceeigner die Genehmigung erteilen müssen, damit die Benutzer die Mitgliedschaft beim Service erhalten können. • **Dynamic** – Das Kontrollkästchen ist aktiviert: Wenn eine dynamische Richtlinie aktiv ist, werden automatisch Benachrichtigungs-E-Mails zur Serviceanforderungsgenehmigung generiert, die den Serviceeigner über anstehende Serviceanforderungen benachrichtigen, die er manuell genehmigen muss. – Das Kontrollkästchen ist inaktiviert: Genehmigungen werden im Auftrag des Serviceeigners automatisch erteilt. • **Request**. Das Kontrollkästchen ist aktiviert: Anforderungen werden an die für die Benutzer zuständigen Serviceeigner gesendet, die den Service angefordert haben. Anforderungen müssen für die Benutzer genehmigt werden, damit diese Mitglieder des Service werden.

Tabelle 25. Genehmigungsoptionen und Optionen für die erneute Zertifizierung (Forts.)

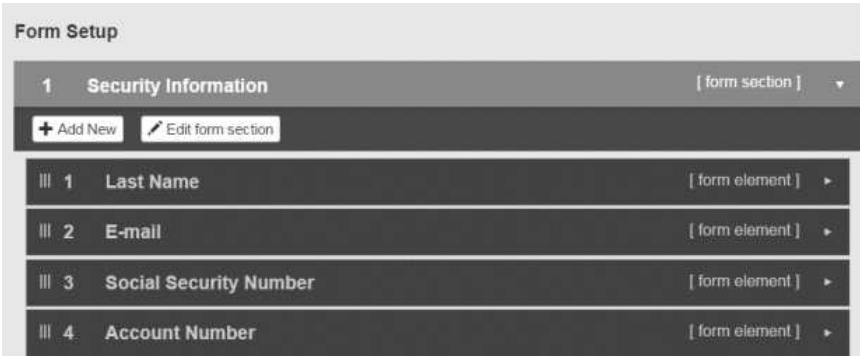
Einstellung		Beschreibung
Recertification Settings	**Delinquency Action**	Die Aktion, die ausgeführt werden soll, wenn die Servicemitgliedschaft bis zum Fälligkeitsdatum nicht erneut zertifiziert wurde. Das Fälligkeitsdatum ist das Datum, das im Zeitplan für die erneute Zertifizierung festgelegt wurde.
	Action Due Within	Anzahl der Tage, bis die Rückstandsaktion fällig wird.
	Manager Approval	Gibt an, ob die für Benutzer zuständigen Manager die Genehmigung erteilen müssen, damit Benutzer erneut zertifiziert werden können. • **Dynamic** – Das Kontrollkästchen ist aktiviert: Benachrichtigungs-E-Mails zur Genehmigung der erneuten Zertifizierung werden automatisch generiert, die den Manager über anstehende Anforderungen zur erneuten Zertifizierung benachrichtigen, die sie manuell genehmigen müssen. – Das Kontrollkästchen ist inaktiviert: Genehmigungen werden im Auftrag des Managers automatisch erteilt. • **Request**. Das Kontrollkästchen ist aktiviert: Anforderungen werden an den Manager gesendet. Anforderungen müssen für die Benutzer genehmigt werden, damit diese erneut zertifiziert werden können.
	Service Owner	Gibt an, ob der Serviceeigner die Genehmigung erteilen muss, damit Benutzer erneut zertifiziert werden können. • **Dynamic** – Das Kontrollkästchen ist aktiviert: Benachrichtigungs-E-Mails zur Genehmigung der erneuten Zertifizierung werden automatisch generiert, die den Serviceeigner über anstehende Anforderungen zur erneuten Zertifizierung benachrichtigen, die sie manuell genehmigen müssen. – Das Kontrollkästchen ist inaktiviert: Genehmigungen werden im Auftrag des Serviceeigners automatisch erteilt. • **Request**. Das Kontrollkästchen ist aktiviert: Anforderungen werden an den Serviceeigner gesendet. Anforderungen müssen für die Benutzer genehmigt werden, damit diese erneut zertifiziert werden können.

Serviceformulare konfigurieren

Benutzer oder Serviceeigner müssen ein Formular ausfüllen, wenn sie einen Servicezugriff anfordern oder widerrufen möchten. Jedes Formular enthält eine Anzahl von Feldern, die Benutzer oder Serviceeigner müssen ausfüllen müssen, wenn sie einen Servicezugriff anfordern oder widerrufen möchten. Sie können die Felder und Abschnitte neu anordnen, neue Abschnitte hinzufügen und Felder hinzufügen oder entfernen.

Vorgehensweise

1. Klicken Sie auf **Edit Form** für das Formular, das Sie bearbeiten möchten. Sie können die folgenden Formulare bearbeiten:
   - **Request Access Form** (Formular zum Anfordern von Zugriff). Wird von einem Benutzer ausgefüllt, wenn der Benutzer Zugriff auf den Service anfordert.
   - **Revoke Access Form** (Formular zum Widerrufen von Zugriff). Wird von einem Serviceeigner ausgefüllt, wenn der Serviceeigner den Zugriff eines Benutzers auf den Service entfernen möchte.



2. Fügen Sie ein Feld hinzu:
   a. Klicken Sie auf **Add New** > **Add New Field**.
   b. Wählen Sie die Attribut- und Feldoptionen aus, um das Feld zu definieren.
   c. Klicken Sie auf **Save Changes**, um das Feld hinzuzufügen.
3. Fügen Sie einen Abschnitt hinzu:
   a. Klicken Sie auf **Add New** > **Add New Section**.
   b. Geben Sie eine Bezeichnung (**Label**), eine Unterüberschrift (**Subheading**) und eine Überschrift (**Header**) für den Abschnitt ein. Die Beschriftung, die Unterüberschrift und die Überschrift werden zum Identifizieren des Abschnitts im Formular verwendet.
   c. Klicken Sie auf **Add New Field**, um ein neues Feld im Abschnitt einzugeben. Wählen Sie die Attribut- und Feldoptionen aus, um das Feld zu definieren.
   d. Klicken Sie auf **Save Changes**, um den neuen Abschnitt zu speichern. Im Hauptfenster **Form Setup** (Formularkonfiguration) können Sie weitere Felder zum Abschnitt hinzufügen.
4. Um die Reihenfolge eines Formulars zu ändern und einen Abschnitt oder ein Feld in eine neue Position zu verschieben, klicken Sie auf das Feld oder den Abschnitt und ziehen Sie es oder ihn auf die neue Position.

5. Klicken Sie auf **Save Changes**, um das Formular zu speichern.

Formularoptionen:

Formularoptionen werden verwendet, um die Eigenschaften von Feldern festzulegen, die in Self-Service-Anwendungen verwendet werden.

Je nach definiertem Formular sind möglicherweise nicht alle Optionen verfügbar.

Tabelle 26. Formularfeldoptionen

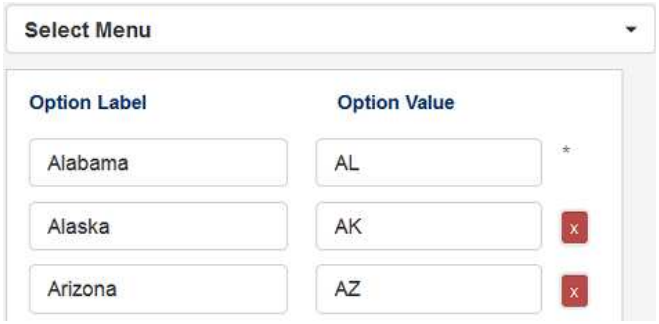
Option	Beschreibung
LDAP attribute	Als Feld zu verwendendes LDAP-Attribut. Wenn ein Attribut ausgewählt wird, für das ein anderer Benutzer als Wert eingegeben werden muss, wird ein Suchtool zum Feld hinzugefügt. Beispiel: Für ein Managerattribut muss möglicherweise ein anderer Benutzer eingegeben werden. Je nach definiertem Feld oder Formular können nicht alle Attribute ausgewählt werden.
Default Value	Ein Standardwert für das Feld. Ist das Feld bearbeitbar, können Benutzer den Standardwert ersetzen.
Field Label	Bezeichnung, die zum Identifizieren des Felds verwendet wird.
Field Type	• **Checkboxes**. Benutzer können eine oder mehrere Optionen als Eingabe für das Feld auswählen. • **Password Field**. Kennwortfelder sind ausgeblendet. • **Radio Buttons**. Benutzer können eine von mehreren Optionen als Eingabe für das Feld auswählen. • **Select Menu**. Benutzer können eine von mehreren Optionen als Eingabe für das Feld auswählen. • **Text Field**. Benutzer geben einen Wert in das Feld als eingegebenen Text ein. • **Text Area**. Unformatiertes Textfeld. Fügen Sie für **Checkboxes**, **Radio Buttons** und **Select Menu** die Optionen für das Feld hinzu. • **Option Label**. Bezeichnung, die zum Identifizieren der Option verwendet wird. • **Option Value**. Wert der Option. In diesem Beispiel verfügt ein Auswahlmenü über eine Reihe von Optionen für verschiedene Status. 
Placeholder	Bezeichnung für Platzhalter.
Tool Tip	Feldhilfetext.

Tabelle 26. Formularfeldoptionen (Forts.)

Option	Beschreibung
Editable	• **Yes**. Benutzer können einen Wert in das Feld eingeben. • **No**. Benutzer können keinen Wert in das Feld eingeben. Einige Felder werden mit vorhandenen Daten gefüllt. Während einer Selbstregistrierung kann ein Benutzer z. B. einen Account aus einem vorhandenen Identitätsdatensatz übernehmen. In diesem Fall kann ein Feldwert aus dem Identitätsdatensatz verwendet werden.
Required	• **Yes**. Das Feld ist ein Pflichtfeld. – Selbstregistrierungsformular. Benutzer können die Selbstregistrierung nur durch Eingabe eines Werts für das Feld abschließen. – Self-Service-Profilformular. Benutzer werden aufgefordert, Werte für nicht ausgefüllte Pflichtfelder einzugeben. • **No**. Das Feld ist optional.
Require current password match	Nur für ein LDAP-Kennwort-Attribut. • **Yes**. Benutzer müssen das Kennwort zweimal in separate Felder eingeben. Die in die einzelnen Felder eingegebenen Werte müssen übereinstimmen, um zu bestätigen, dass das Kennwort richtig ist. • **No**. Das Kennwort wird nur einmal in ein Feld eingegeben.
Masked	**Yes**. Das Feld ist ausgeblendet und der eingegebene Wert wird am Bildschirm nicht angezeigt. Die einzelnen eingegebenen Zeichen werden am Bildschirm durch einen Stern ersetzt.
Require a matching field	• **Yes**. Benutzer müssen den Wert zweimal in separate Felder eingeben. Die in die einzelnen Felder eingegebenen Werte müssen übereinstimmen, um zu bestätigen, dass der Wert richtig ist. Wenn ein Benutzer z. B. eine E-Mail-Adresse eingibt, können Sie von ihm verlangen, die Adresse zweimal einzugeben. • **No**. Der Wert wird nur einmal in ein Feld eingegeben.

Tabelle 26. Formularfeldoptionen (Forts.)

Option	Beschreibung
Validation	Validierungsregeln: • **Yes**. Der eingegebene Wert muss bestimmte Validierungsregeln erfüllen. Ein Datum muss z. B. möglicherweise einer Formatvalidierungsregel entsprechen, wie z. B. mm/tt/jjjj. • **No**. Die eingegebenen Werte werden nicht validiert. Validierungstypen: • **Date**. Die Werte müssen einem bestimmten Datumsformat entsprechen. Beispiel: mm/tt/jjjj. • **Email Address**. Die Werte müssen den E-Mail-Adress-Formaten entsprechen. Beispiel: *Textzeichenfolge@Textzeichenfolge*.com. • **Letters**. Die Werte dürfen nur alphabetische Zeichen enthalten. • **Maximum Character Length**. Die Werte dürfen nur eine bestimmte Anzahl an Zeichen enthalten. • **Minimum Character Length**. Die Werte müssen mindestens eine bestimmte Anzahl an Zeichen enthalten. • **Number**. Die Werte dürfen nur numerische Zeichen enthalten. • **Password Strength**. Ein Kennwortfeld muss allgemeinen, standardmäßigen oder starken Validierungsregeln entsprechen. Die Regeln basieren auf der Anzahl und dem Typ der Zeichen, die eingegeben werden müssen. • **US Phone Number**. Die Werte müssen dem in den USA üblichen Format für Telefonnummern entsprechen. Benutzerdefinierte reguläre Ausdrücke. Ein regulärer Ausdruck, der mit dem eingegebenen Wert verglichen wird. Wenn eine Übereinstimmung erkannt wird ("true"), ist der Wert gültig. • **Pattern**. Ein regulärer Ausdruck. Um z. B. Registrierungen auf Adressen im US-Bundesstaat North Carolina zu beschränken, verwenden Sie den regulären Ausdruck `^NC$` für das Bundesstaatsattribut, wobei NC als optionaler Wert für den Bundesstaat definiert ist. • **Error Message**. Fehlernachricht, die Benutzern angezeigt wird, wenn ein eingegebener Wert nicht gültig ist.

Tabelle 27. Formularabschnittsoptionen

Option	Beschreibung
Label	Abschnittsbezeichnung.
Subheading	Bezeichnung für Unterüberschrift.
Header	Überschrift.

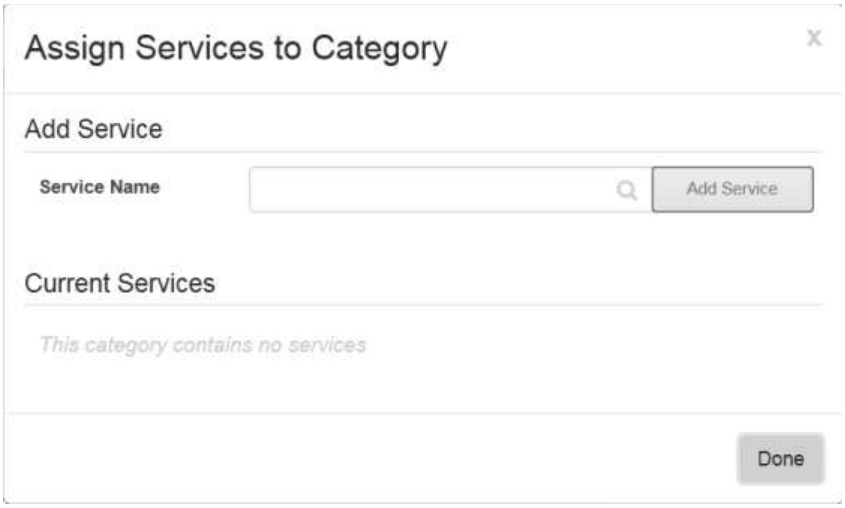
Servicekategorien erstellen

Sie können Servicekategorien erstellen, um zusammengehörige Services zu gruppieren. Servicegruppen machen es für Benutzer einfacher, ihre Services in Self-Service-Anwendungen zu verwalten.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Applications** > **Services** und klicken Sie dann auf **Category Management** und **Add a New Category**.
2. Geben Sie einen Namen und eine Beschreibung ein und wählen Sie ein Symbol für die Kategorie aus.

   Der Kategoriename muss eindeutig sein. Sie können ein Symbol suchen, indem Sie eine Zeichenfolge in das Suchfeld **Choose one of the following** eingeben.
3. Klicken Sie auf **Add Category**, um die Servicekategorie hinzuzufügen. Die Kategorie wird gespeichert. Sie werden zur Liste der Servicekategorien zurückgeleitet.
4. Suchen Sie die Kategorie und wählen Sie sie aus, um ihr Services hinzuzufügen.
5. Klicken Sie auf **Manage Services**, um das Fenster **Assign Services to Category** zu öffnen.



   Um einen Service zu suchen und auszuwählen, geben Sie mindestens die ersten 3 Ziffern des Servicenamens in das Feld **Service Name** ein. Wählen Sie den Service aus der zurückgegebenen Liste aus und klicken Sie auf **Add Service**.

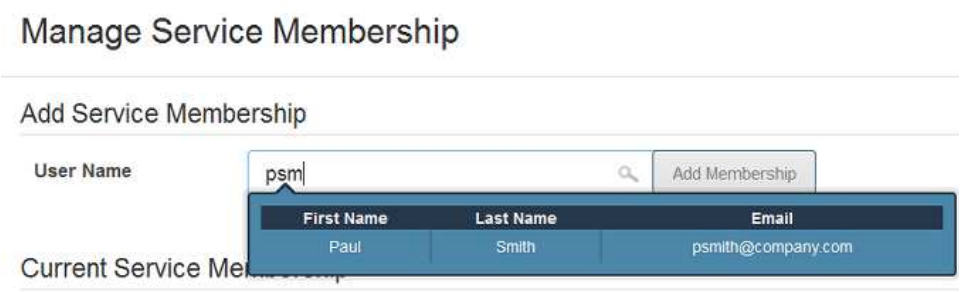
   Fügen Sie alle gewünschten Services hinzu und klicken Sie auf **Done**.

Mitgliedschaft bei einem Service statisch verwalten

Für eine statisch definierte Benutzermitgliedschaft ist es erforderlich, dass Sie jedes Benutzermitglied manuell hinzufügen oder entfernen.

Vorgehensweise

1. Suchen Sie nach dem Service, zu dem Sie Mitglieder hinzufügen möchten, und wählen Sie ihn aus.
2. Klicken Sie auf **Manage Service Membership**.



3. Suchen Sie im Feld **User Name** nach dem Benutzer, den Sie hinzufügen möchten. Um nach einem Benutzer zu suchen, geben Sie die ersten drei Zeichen des Vornamens, Nachnamens, Benutzernames oder der E-Mail-Adresse des Benutzers ein.
4. Wählen Sie den Benutzer aus und klicken Sie auf **Add Membership**.
5. Nachdem Sie alle gewünschten Benutzer hinzugefügt haben, klicken Sie auf **Done**.

Mitgliedschaft bei Services dynamisch verwalten

Dynamische Einrichtungsrichtlinien ermöglichen es, dass eine Benutzermitgliedschaft bei einem Service auf Übereinstimmungskriterien basiert. Benutzer, die mit den Bedingungen übereinstimmen, werden automatisch für die Mitgliedschaft beim Service ausgewählt.

Dynamische Einrichtungsrichtlinien erstellen

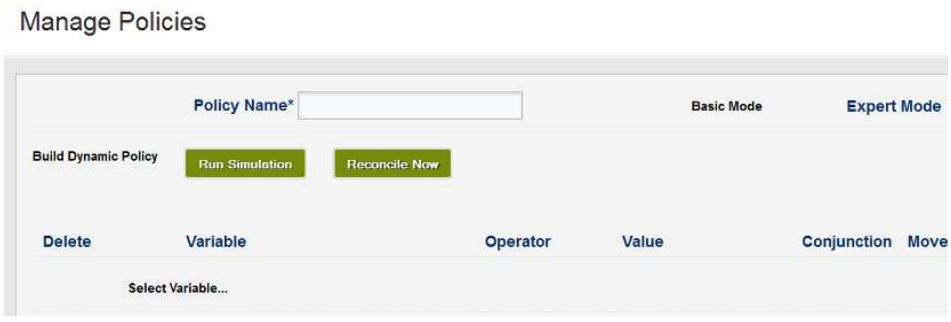
Mithilfe von dynamischen Einrichtungsrichtlinien kann die Benutzermitgliedschaft in einem Service bestimmt werden.

Informationen zu diesem Vorgang

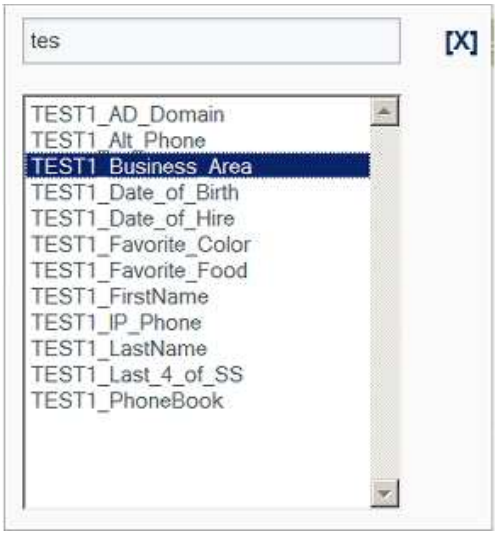
Die Mitgliedschaft basiert auf den Auswahlkriterien der Richtlinie. Sie können beispielsweise die Mitgliedschaft in einem Service durch ein Attribut angeben, das den Arbeitsplatz bestimmt, oder durch ein Attribut, das den Arbeitsplatz und die Mitgliedschaft in einer Gruppe bestimmt. Ein Service kann über eine oder mehrere Richtlinien verfügen.

Vorgehensweise

1. Suchen Sie nach der Gruppe, zu der Sie die Richtlinie hinzufügen möchten, und wählen Sie sie aus.
2. Klicken Sie für **Dynamic Provisioning Policy** (Dynamische Einrichtungsrichtlinie) auf **Manage Policy** (Richtlinie verwalten).
3. Klicken Sie auf **Add New Policy**.



4. Geben Sie einen aussagekräftigen Namen für die Richtlinie im Feld **Policy Name** ein.
5. Wählen Sie die Variablen aus, die Sie verwenden möchten. Sie können eine oder mehrere Variablen eines beliebigen Typs auswählen, um sie in Ihrer Richtlinie zu verwenden. Sie können eine beliebige Kombination der folgenden Variablentypen auswählen:
   - **Attribute**. Sie können Benutzer auf der Grundlage eines Benutzeridentitätsattributs einbeziehen.
   - **Group**. Sie können Benutzer auf der Grundlage von Gruppenmitgliedschaften einbeziehen oder ausschließen.
   - **Service**. Sie können Benutzer auf der Grundlage von anderen Servicemitgliedschaften einbeziehen oder ausschließen.
   - **Manager**. Sie können Benutzer auf der Grundlage der Tatsache einbeziehen, ob ihnen die Rolle eines Managers zugeordnet wurde.
6. Gehen Sie wie folgt vor, um ein Benutzeridentitätsattribut als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Attribute**.
   b. Klicken Sie in das Feld **Filter Attributes** und geben Sie die ersten Zeichen des Attributs ein. Klicken Sie doppelt auf das Attribut, um es auszuwählen.



   c. Wählen Sie einen **Operator** aus und geben Sie einen Wert (**Value**) für das Attribut ein.

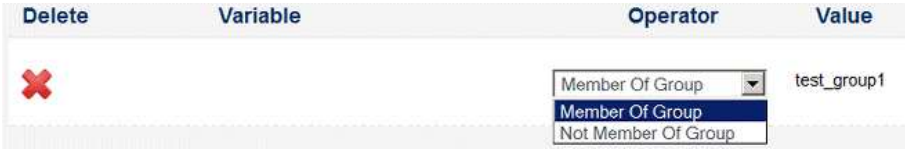
Anmerkung: Sie können Platzhalterzeichen verwenden. Sie können z. B. "11*" eingeben, was jede Zahl darstellt, die mit "11" beginnt.

Tipp: Wenn Sie möchten, dass ein Attribut oder ein Attributwert als Zeitmarke behandelt wird, können Sie dem Wert `$date$` als Präfix voranstellen. Dieses Präfix nimmt das Standarddatumsformat JJJJ-MM-TT HH:mm:ss an. Sie können z. B. `$date$1970-01-01 00:00:00` eingeben, um den 1. Januar 1970 um Mitternacht anzugeben.

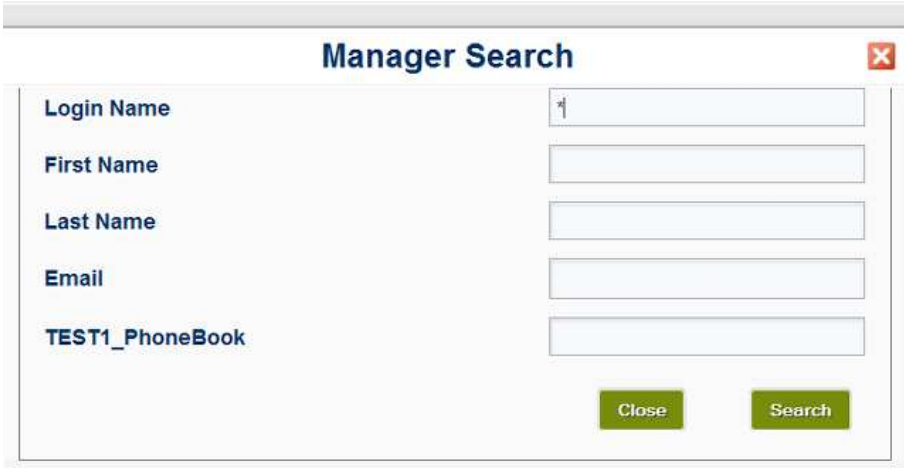
Sie können auch ein vom Standard abweichendes Format für die Zeitmarke angeben, indem Sie das Format mithilfe von `SimpleDateFormat`in das Präfix `$date$` einschließen. Für eine Z-Zeitmarke können Sie z. B. `$date{yyyy-MM-dd HH:mm:ssZ}$1970-01-01 00:00:00-0400` für den 1. Januar 1970 um Mitternacht in der Zeitzone 4 Stunden vor GMT/UTC anzugeben. Das Ändern des Standardformats bewirkt, dass dasselbe Format auf die Attributwerte angewendet wird, die abgerufen werden. Sie müssen das Format der Werte kennen, die Sie abrufen möchten, und Sie müssen wissen, dass sie mit dem Format konsistent sind, das Sie verwenden möchten. Weitere Informationen zu unterschiedlichen Formatmustern finden Sie unter SimpleDateFormat.

Wenn entweder der in der Regel angegebene Wert oder der Wert, mit dem dieser verglichen wird, nicht ohne Ausnahme analysiert wird, wird eine Warnung oder ein Fehler protokolliert. Wenn Sie weitere Informationen benötigen, wenden Sie sich an Ihren IBM Supportmitarbeiter. Die koordinierte Weltzeit (UTC, Coordinated Universal Time) ist die Standardzeitzone.

7. Gehen Sie wie folgt vor, um eine Mitgliedschaft oder eine nicht vorhandene Mitgliedschaft in einer Gruppe als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Group**.
   b. Klicken Sie in das Feld **Filter Groups** und geben Sie die ersten Zeichen der Gruppe ein. Klicken Sie doppelt auf die Gruppe, um sie auszuwählen.
   c. Wählen Sie aus, ob die Mitgliedschaft von der Mitgliedschaft in dieser anderen Gruppe abhängig ist oder ob die Mitgliedschaft von der Nichtmitgliedschaft in dieser Gruppe abhängig ist.



8. Gehen Sie wie folgt vor, um eine Mitgliedschaft oder eine nicht vorhandene Mitgliedschaft in einem anderen Service als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Service**.
   b. Klicken Sie in das Feld **Filter Services** und geben Sie die ersten Zeichen des Service ein. Klicken Sie doppelt auf den Service, um ihn auszuwählen.
   c. Wählen Sie aus, ob die Mitgliedschaft von der Mitgliedschaft in diesem anderen Service abhängig ist oder ob die Mitgliedschaft von der Nichtmitgliedschaft in diesem anderen Service abhängig ist.
9. Gehen Sie wie folgt vor, um die Managerrolle als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Manager**.



b. Suchen Sie im Fenster **Manager Search** nach dem Benutzer, indem Sie Suchkriterien in eines der Felder eingeben. Klicken Sie auf **Search**. Nur Benutzer, denen die Rolle eines Managers zugeordnet wurde und die Ihren Suchkriterien entsprechen, werden zurückgegeben.

   Anmerkung: Sie können Platzhalterzeichen in Ihrer Suche verwenden. Sie können z. B. `Joh*` eingeben, um Namen darzustellen, die mit "Joh" beginnen.

c. Wählen Sie den Benutzer aus. Sie können die Suche wiederholen, um weitere Benutzer hinzuzufügen.

10. Verwenden Sie das Feld **Conjunction**, um eine oder mehrere Variablen zum Bestimmen der Mitgliedschaft im Service zu kombinieren. Verwenden Sie den Konjunktionswert `And` oder `Or`, um das Ergebnis eines Vergleichskriteriums mit der nächsten Zeile zu kombinieren.

    Die Gruppierung der Variablen (Bedingungen) wird von oben nach unten durchgeführt, sodass das Ergebnis der vorherigen Bedingungen mit der nachfolgenden Bedingung verbunden wird.

    Verwenden Sie die Pfeilsymbole, um Bedingungen nach oben oder unten zu verschieben. 

    Im folgenden Beispiel wird nur eine Variable zum Bestimmen der Mitgliedschaft verwendet: das Benutzeridentitätsattribut "TEST1_Business_Area". Um ein Mitglied zu sein, muss ein Benutzer den Wert "London W4" für das Attribut "TEST1_Business_Area" aufweisen.

    Im folgenden Beispiel werden zwei Variablen zum Bestimmen der Mitgliedschaft verwendet. Um ein Mitglied zu sein, muss ein Benutzer den Wert "London W4" für das Attribut "TEST1_Business_Area" aufweisen und er muss Mitglied in der Gruppe "Group1" sein.

Im folgenden Beispiel werden drei Variablen zum Bestimmen der Mitgliedschaft verwendet. Um ein Mitglied zu sein, muss ein Benutzer den Wert "London W4" für das Attribut "TEST1_Business_Area" aufweisen und er muss Mitglied in der Gruppe "Group1" oder Mitglied in der Gruppe "Group2" sein.

11. Nachdem Sie alle Bedingungen, die in Ihrer Richtlinie verwendet werden sollen, definiert haben, klicken Sie auf **Save**.

Nächste Schritte

Simulieren Sie die Richtlinie, um zu überprüfen, ob die Mitgliedschaft Ihren Erwartungen entspricht.

Dynamische Einrichtungsrichtlinien im Expertenmodus erstellen

In einigen Fällen können die Auswahlkriterien für die Richtlinie für einen Service nicht mithilfe eines grundlegenden Attributvergleichs und mit einer anderen Service- oder Gruppenmitgliedschaft bestimmt werden. Für die Mitgliedschaft ist möglicherweise die Überprüfung von Attributwerten (Unterzeichenfolgen) erforderlich, die auf dem Wert eines anderen Attributs basieren und die daher variieren. In diesem Fällen müssen Sie die Richtlinie im Expertenmodus definieren.

Vorbereitende Schritte

Um den Expertenmodus verwenden zu können, müssen Sie über gute Kenntnisse und fortgeschrittenes Wissen in der Codierung von JavaScript verfügen.

Informationen zu diesem Vorgang

Sie definieren Richtlinien im Expertenmodus in JavaScript.

Während der Richtlinienauswertung wird das JavaScript jeweils ein Mal für jeden Benutzer in der Registry ausgeführt. Das JavaScript prüft die Registryattribute des Benutzers und seine Mitgliedschaften und entscheidet, ob der Benutzer in den Service aufgenommen wird. Das JavaScript kommuniziert diese Entscheidung an Cloud Identity Service mithilfe der Variable **`inGroup`**. Wenn das Ergebnis des JavaScript bedeutet, dass **`inGroup`** gleich "true" (wahr) ist, wird der Benutzer in den Service aufgenommen, andernfalls wird er nicht aufgenommen.

Das JavaScript kann drei Methoden zum Anfordern von Cloud Identity Service-Registryattributen und Gruppeninformationen zu jedem Benutzer verwenden.

- `String isMemberOfGroup(String groupName)`
- `String[] getAttributeValues(String attributeName)`
- `String evaluateAttribute(String attributeName, int operator, String constant)`

Jede dieser Methoden kann mit einer anderen Variable **`ldap`** aufgerufen werden, die für das JavaScript verfügbar ist. Um beispielsweise zu bestimmen, ob der aktuelle Benutzer ein Mitglied einer Gruppe mit dem Namen **`accounting`** ist, kann die folgende Anweisung verwendet werden:

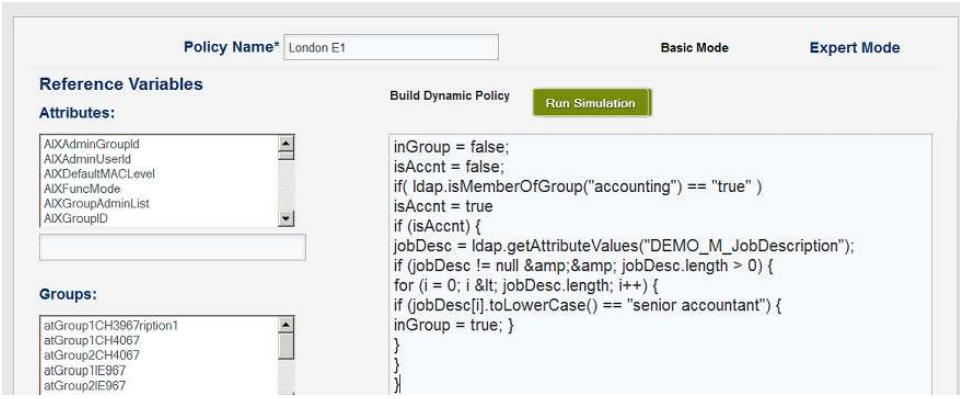
```
var isAccountant = ldap.isMemberOfGroup("accounting");
```

Im folgenden JavaScript-Beispiel wird der Benutzer in die Richtlinie aufgenommen, wenn er ein Mitglied der Gruppe **`accounting`** ist und den Wert **`senior accountant`** im Attribut **`DEMO_M_JobDescription`** aufweist.

```
// assume user is not in group
inGroup = false;
isAccnt = false;
if( ldap.isMemberOfGroup("accounting") == "true" )
isAccnt = true
if (isAccnt) {
jobDesc = ldap.getAttributeValues("DEMO_M_JobDescription");
if (jobDesc != null && jobDesc.length > 0) {
for (i = 0; i < jobDesc.length; i++) {
if (jobDesc[i].toLowerCase() == "senior accountant") {
inGroup = true; }
}
}
}
```

Vorgehensweise

1. Suchen Sie nach der Gruppe, zu der Sie die Richtlinie hinzufügen möchten, und wählen Sie sie aus.
2. Klicken Sie für **Dynamic Provisioning Policy** (Dynamische Einrichtungsrichtlinie) auf **Manage Policy** (Richtlinie verwalten).
3. Klicken Sie auf **Add New Policy**.
4. Klicken Sie auf **Expert Mode**.



5. Geben Sie das JavaScript ein, das Sie zum Bestimmen der Mitgliedschaft verwenden möchten.

   Attributes, **Groups** und **Services** werden in den entsprechenden Feldern als Referenz aufgelistet. Sie können nach Attributen, Gruppen und Services suchen, indem Sie die ersten Zeichen in das Filterfeld unter dem entsprechenden Feld eingeben. Sie können ein ausgewähltes Attribut, eine Gruppe oder einen Service kopieren und einfügen.
6. Nachdem Sie alle Bedingungen, die in Ihrer Richtlinie verwendet werden sollen, definiert haben, klicken Sie auf **Save**, um die Richtlinie zu speichern.

Nächste Schritte

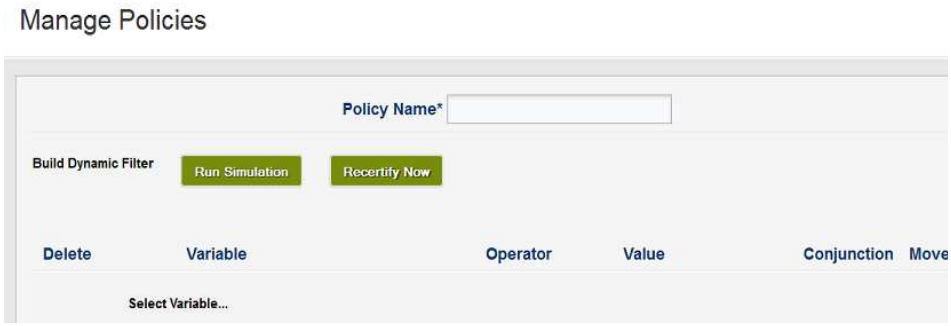
Simulieren Sie die Richtlinie, um zu überprüfen, ob die Mitgliedschaft Ihren Erwartungen entspricht.

Richtlinien für erneute Zertifizierung erstellen

Mithilfe von Richtlinien für erneute Zertifizierung kann bestimmt werden, welche Benutzer Mitglieder in einem Service bleiben. Richtlinien für die erneute Zertifizierung werden auf dieselbe Art wie dynamische Einrichtungsrichtlinien definiert. Das Fortsetzen der Mitgliedschaft basiert auf den Benutzeridentitätsattributwerten, auf anderen Gruppen- und Servicemitgliedschaften und auf der Managerrolle. Ein Service kann über eine oder mehrere Richtlinien für die erneute Zertifizierung verfügen.

Vorgehensweise

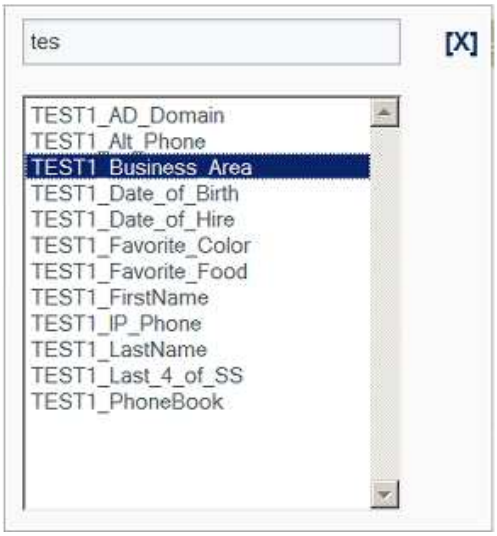
1. Suchen Sie nach der Gruppe, zu der Sie die Richtlinien für erneute Zertifizierung hinzufügen möchten, und wählen Sie sie aus.
2. Klicken Sie für **Recertification Policies** (Richtlinien für erneute Zertifizierung) auf **Manage Policy** (Richtlinie verwalten).
3. Klicken Sie auf **Add New Policy**.



4. Geben Sie einen aussagekräftigen Namen für die Richtlinie im Feld **Policy Name** ein.
5. Wählen Sie die Variablen aus, die Sie verwenden möchten. Sie können eine oder mehrere Variablen eines beliebigen Typs auswählen, um sie in Ihrer Richtlinie zu verwenden. Sie können eine beliebige Kombination der folgenden Variablentypen auswählen:
   - **Attribute**. Sie können Benutzer auf der Grundlage eines Benutzeridentitätsattributs einbeziehen.
   - **Group**. Sie können Benutzer auf der Grundlage von anderen Gruppenmitgliedschaften einbeziehen oder ausschließen.
   - **Service**. Sie können Benutzer auf der Grundlage von anderen Servicemitgliedschaften einbeziehen oder ausschließen.

- **Manager**. Sie können Benutzer auf der Grundlage der Tatsache einbeziehen, ob ihnen die Rolle eines Managers zugeordnet wurde.

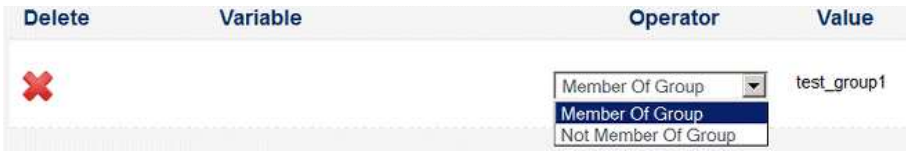
6. Gehen Sie wie folgt vor, um ein Benutzeridentitätsattribut als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Attribute**.
   b. Klicken Sie in das Feld **Filter Attributes** und geben Sie die ersten Zeichen des Attributs ein. Klicken Sie doppelt auf das Attribut, um es auszuwählen.



   c. Wählen Sie einen **Operator** aus und geben Sie einen Wert (**Value**) für das Attribut ein.

   Anmerkung: Sie können Platzhalterzeichen verwenden. Sie können z. B. "11*" eingeben, was jede Zahl darstellt, die mit "11" beginnt.

7. Gehen Sie wie folgt vor, um eine Mitgliedschaft oder eine nicht vorhandene Mitgliedschaft in einer Gruppe als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Group**.
   b. Klicken Sie in das Feld **Filter Groups** und geben Sie die ersten Zeichen der Gruppe ein. Klicken Sie doppelt auf die Gruppe, um sie auszuwählen.
   c. Wählen Sie aus, ob die Mitgliedschaft von der Mitgliedschaft in dieser Gruppe abhängig ist oder ob die Mitgliedschaft von der Nichtmitgliedschaft in dieser Gruppe abhängig ist.



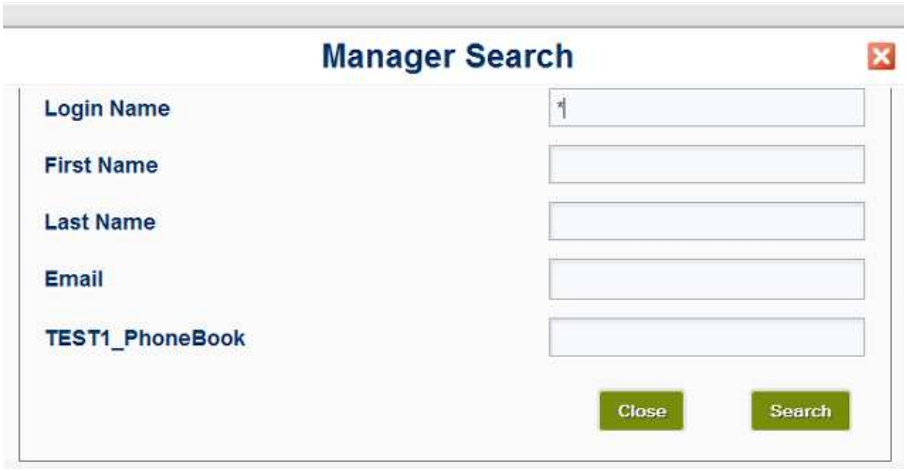
8. Gehen Sie wie folgt vor, um eine Mitgliedschaft oder eine nicht vorhandene Mitgliedschaft in einem anderen Service als Variable zu verwenden:
   a. Klicken Sie auf **Select Variable** und klicken Sie auf **Service**.

b. Klicken Sie in das Feld **Filter Services** und geben Sie die ersten Zeichen des Service ein. Klicken Sie doppelt auf den Service, um ihn auszuwählen.

c. Wählen Sie aus, ob die Mitgliedschaft von der Mitgliedschaft in diesem anderen Service abhängig ist oder ob die Mitgliedschaft von der Nichtmitgliedschaft in diesem anderen Service abhängig ist.

9. Gehen Sie wie folgt vor, um die Managerrolle als Variable zu verwenden:

a. Klicken Sie auf **Select Variable** und klicken Sie auf **Manager**.



b. Suchen Sie im Fenster **Manager Search** nach dem Benutzer, indem Sie Suchkriterien in eines der Felder eingeben. Klicken Sie auf **Search**. Nur Benutzer, denen die Rolle eines Managers zugeordnet wurde und die Ihren Suchkriterien entsprechen, werden zurückgegeben.

Anmerkung: Sie können Platzhalterzeichen in Ihrer Suche verwenden. Sie können z. B. `Joh*` eingeben, um Namen darzustellen, die mit "Joh" beginnen.

c. Wählen Sie den Benutzer aus. Sie können die Suche wiederholen, um weitere Benutzer hinzuzufügen.

10. Verwenden Sie das Feld **Conjunction**, um eine oder mehrere Variablen zum Bestimmen der forgesetzten Mitgliedschaft im Service zu kombinieren. Verwenden Sie den Konjunktionswert `And` oder `Or`, um das Ergebnis eines Vergleichskriteriums mit der nächsten Zeile zu kombinieren.

Die Gruppierung der Variablen (Bedingungen) wird von oben nach unten durchgeführt, sodass das Ergebnis der vorherigen Bedingungen mit der nachfolgenden Bedingung verbunden wird.

Verwenden Sie die Pfeilsymbole, um Bedingungen nach oben oder unten zu verschieben. 

Im folgenden Beispiel wird nur eine Variable zum Bestimmen der fortgesetzten Mitgliedschaft verwendet: das Benutzeridentitätsattribut "TEST1_Business_Area". Um ein Mitglied zu sein, muss ein Benutzer den Wert "London W4" für das Attribut "TEST1_Business_Area" aufweisen.

Im folgenden Beispiel werden zwei Variablen zum Bestimmen der fortgesetzten Mitgliedschaft verwendet. Um ein Mitglied zu sein, muss ein Benutzer

den Wert "London W4" für das Attribut "TEST1_Business_Area" aufweisen und er muss Mitglied in der Gruppe "Group1" sein.

Im folgenden Beispiel werden drei Variablen zum Bestimmen der fortgesetzten Mitgliedschaft verwendet. Um ein Mitglied zu sein, muss ein Benutzer den Wert "London W4" für das Attribut "TEST1_Business_Area" aufweisen und er muss Mitglied in der Gruppe "Group1" oder Mitglied in der Gruppe "Group2" sein.

11. Nachdem Sie alle Bedingungen, die in Ihrer Richtlinie verwendet werden sollen, definiert haben, klicken Sie auf **Save**.

Nächste Schritte

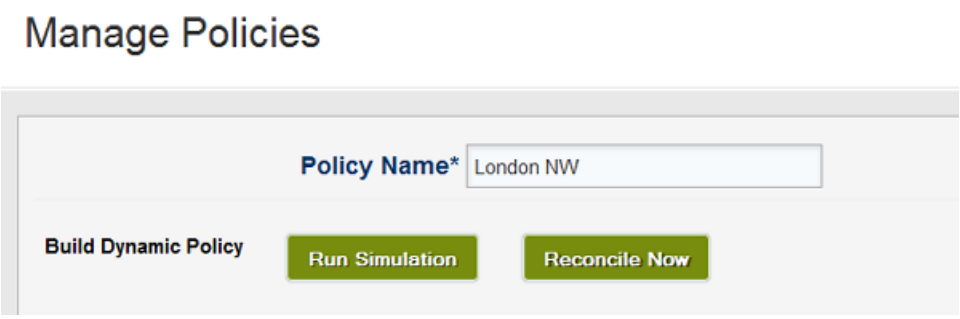
Simulieren Sie die Richtlinie, um zu überprüfen, ob die fortgesetzte Mitgliedschaft Ihren Erwartungen entspricht.

Richtlinie simulieren

Sie können eine Richtlinie simulieren, um die Benutzermitgliedschaft in einem Service auszuwerten und zu überprüfen, ob die Mitgliedschaft Ihren Erwartungen entspricht. Sie können dynamische Einrichtungsrichtlinien und Richtlinien für erneute Zertifizierung simulieren. Die Simulation ändert die Mitgliedschaft im Service nicht. Sie zeigt an, welche Benutzer die vorgeschlagene Mitgliedschaft im Service erfüllen. Die Ergebnisse können angezeigt und in einer CSV-Datei gespeichert werden.

Vorgehensweise

1. Wenn Sie die Richtlinie nicht ausgewählt haben, suchen Sie nach dem Service und wählen Sie ihn aus. Öffnen Sie das Fenster **Manage Policies**, um die Richtlinie zu bearbeiten.
2. Klicken Sie auf **Run Simulation**.



3. Wählen Sie einen Simulationstyp für die Ausführung.
   - Dynamische Einrichtungsrichtlinien.
     - **Simulate all users in the directory** (Alle Benutzer im Verzeichnis simulieren). Diese Option vergleicht die Richtlinienauswahl mit allen Benutzern im Cloud Identity Service. Die Benutzer, die die Richtlinie erfüllen, werden in den Ergebnissen als "Hinzugefügt" oder als "Beibehalten" aufgelistet. Benutzer, die die Richtlinie nicht erfüllen, werden in den Ergebnissen als "Aus dem Service entfernt" oder als "Nicht hinzugefügt" aufgelistet.
     - **Simulate all users currently in the group** (Alle derzeit in der Gruppe enthaltenen Benutzer simulieren). Diese Option vergleicht die Richtlinienauswahlkriterien mit den Attributen aller Benutzer, die derzeit im Service enthalten sind. Jeder Benutzer im Service wird in den Ergebnissen als "Entfernt" oder "Beibehalten" aufgelistet. Es werden keine neuen Benutzer als "Hinzugefügt" aufgelistet.
     - **Simulate a single user** (Einzelnen Benutzer simulieren). Diese Option vergleicht die Richtlinienauswahlkriterien mit einem ausgewählten Benutzer. Dieser Benutzer wird in den Ergebnissen als "Beibehalten", "Entfernt", "Hinzugefügt" oder "Nicht hinzugefügt" aufgelistet. Suchen Sie anhand des Benutzernames nach dem Benutzer. Geben Sie die ersten Zeichen des Benutzernamens in das Feld **Filter Users** ein, klicken Sie auf **Search Users** und wählen Sie den Benutzer aus.

   - Richtlinien für erneute Zertifizierung.
     - **Simulate all current service members** (Alle aktuellen Servicemitglieder simulieren). Diese Option vergleicht die Richtlinienauswahlkriterien mit den Attributen aller Benutzer, die derzeit im Service enthalten sind. Jeder Benutzer im Service wird in den Ergebnissen als "Einbezogen" oder "Ausgeschlossen" aufgelistet. Es werden keine neuen Benutzer als "Hinzugefügt" aufgelistet.
     - **Simulate a single service member** (Einzelnes Servicemitglied simulieren). Diese Option vergleicht die Richtlinienauswahlkriterien mit einem ausgewählten Benutzer. Dieser Benutzer wird in den Ergebnissen als "Einbezogen", "Ausgeschlossen", "Hinzugefügt" oder "Nicht hinzugefügt" aufgelis-

tet. Suchen Sie anhand des Benutzernames nach dem Benutzer. Geben Sie die ersten Zeichen des Benutzernamens in das Feld **Filter Users** ein, klicken Sie auf **Search Users** und wählen Sie den Benutzer aus.

4. Klicken Sie auf **Run Simulation**.
   - Die Ergebnisse der Simulation einer Einrichtungsrichtlinie für einen einzelnen Benutzer werden im Fenster **Simulate Provisioning Policy** angezeigt.
   - Die Ergebnisse der Simulation einer Richtlinie für erneute Zertifizierung für einen einzelnen Benutzer werden im Fenster **Simulate Recertification Policy** angezeigt.

   Schließen Sie das Fenster **Simulate Policy**, um zum Fenster **Manage Policies** zurückzukehren, und klicken Sie auf **Cancel**.
5. Klicken Sie auf **Refresh** im Fenster **Manage Policies**, um die Ergebnisse der Simulationen anzuzeigen. Wenn die Simulation abgeschlossen ist, werden ein Hakensymbol und ein Link zu einer CSV-Datei angezeigt.

6. Zeigen Sie die Ergebnisse an.
   - Klicken Sie auf das Hakensymbol ✔, um das Fenster **Simulation Results** zu öffnen. Sie können auswählen, welche Ergebnisspalten Sie anzeigen möchten, indem Sie die Kontrollkästchen für die Spaltenüberschriften auswählen oder die Auswahl aufheben. Schließen Sie das Fenster **Simulation Results**, um zum Fenster **Manage Policies** zurückzukehren.

     Anmerkung: Wenn Sie auf **Clear Simulation Results** klicken, werden alle Ergebnisse im Fenster **Simulation Results** und im Fenster **Manage Policies** gelöscht.

   - Klicken Sie auf das CSV-Symbol, um die Ergebnisse in einer CSV-Datei anzuzeigen. Sie können die Datei öffnen oder speichern.

Nächste Schritte

- Für eine dynamische Einrichtungsrichtlinie gleichen Sie die Richtlinie ab und aktivieren Sie die Richtlinie.
- Für eine Richtlinie für erneute Zertifizierung zertifizieren Sie die Richtlinie erneut und aktivieren Sie die Richtlinie.

Dynamische Richtlinie abgleichen

Nachdem eine Richtlinie erstellt wurde, kann die Richtlinie abgeglichen werden. Wenn eine Richtlinie abgeglichen wird, wird die Benutzermitgliedschaft für den Service entsprechend den Auswahlkriterien der Richtlinie implementiert.

Vorgehensweise

1. Suchen Sie nach dem Service und wählen Sie ihn aus. Öffnen Sie das Fenster **Manage Policies**, um die Richtlinie zu bearbeiten.
2. Klicken Sie auf **Reconcile Now** (Jetzt abgleichen).

Eine Warnnachricht wird angezeigt. Klicken Sie auf **OK**, um die Richtlinie abzugleichen.

Nächste Schritte

Aktivieren Sie die Richtlinie.

Dynamische Richtlinie aktivieren und planen

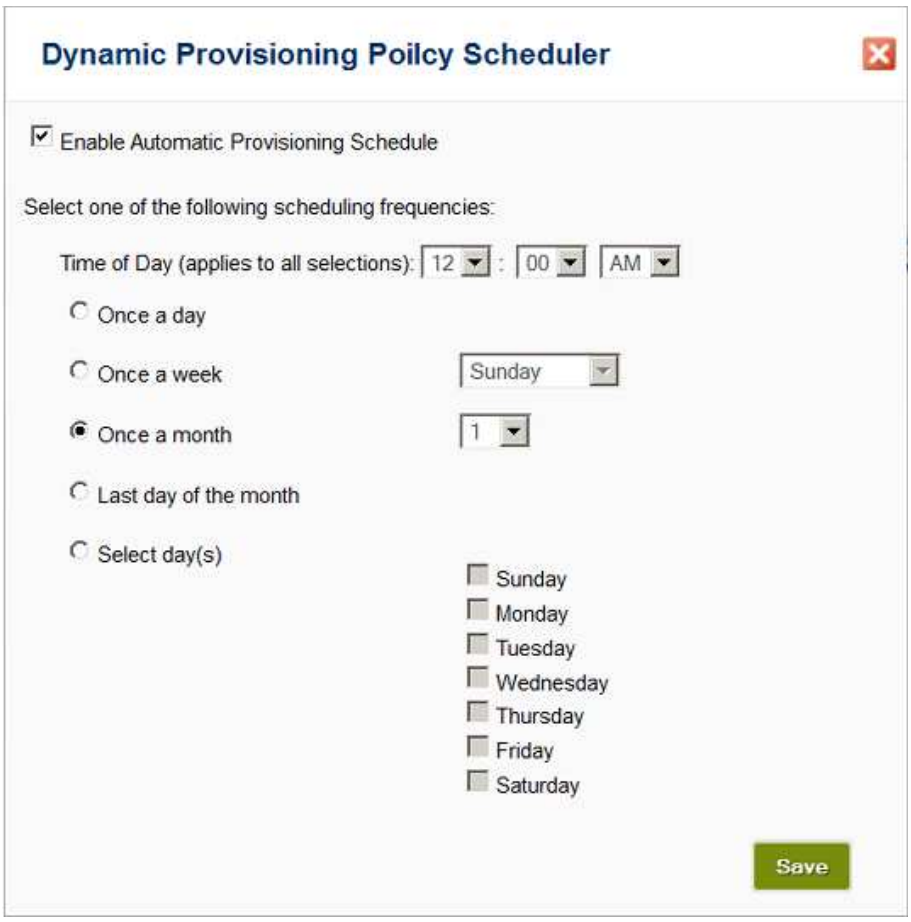
Nach dem Erstellen und Simulieren einer Richtlinie und nach dem Validieren der Simulationsergebnisse ist die Richtlinie bereit für die Aktivierung und Zeitplanung. Eine aktivierte Richtlinie wird nach einem Zeitplan ausgeführt, sodass die Mitgliedschaft eines Service bei jeder Ausführung des Zeitplans bewertet und aktualisiert wird.

Vorgehensweise

1. Wenn Sie die Richtlinie nicht ausgewählt haben, suchen Sie nach dem Service und wählen Sie ihn aus. Öffnen Sie das Fenster **Manage Policies**, um die Richtlinie zu bearbeiten.
2. Wählen Sie **Select Active** für die zu aktivierende Richtlinie aus.

Ein Warnhinweis wird angezeigt. Klicken Sie auf **OK**, um die Richtlinie zu aktivieren.

3. Klicken Sie auf das Zeitplansymbol , um das Fenster **Dynamic Provisioning Policy Scheduler** zu öffnen.



4. Aktivieren Sie das Kontrollkästchen **Enable Automatic Provisioning Schedule**.
5. Wählen Sie die Frequenz aus, mit der der Zeitplan ausgeführt werden soll:
   - **Once a day**. Wählen Sie die Tageszeit aus.
   - **Once a week**. Wählen Sie den Tag aus der Dropdown-Liste aus und wählen Sie dann die Tageszeit aus.
   - **Once a month**. Wählen Sie den Kalendertag aus der Dropdown-Liste aus und wählen Sie dann die Tageszeit aus.
   - **Last day of the month**. Wählen Sie die Tageszeit aus.
   - **Select days**. Wählen Sie die Kontrollkästchen für die Tage aus, an denen der Zeitplan ausgeführt werden soll, und wählen Sie dann die Tageszeit aus.
6. Klicken Sie auf **Save**.

Richtlinie erneut zertifizieren

Nachdem eine Richtlinie für erneute Zertifizierung erstellt wurde, kann die Richtlinie erneut zertifiziert werden. Wenn eine Richtlinie erneut zertifiziert wird, wird die Benutzermitgliedschaft für den Service entsprechend den Auswahlkriterien der Richtlinie für erneute Zertifizierung implementiert. Das Ausführen eines Abgleichs generiert sofort Genehmigungsanforderungen für eine erneute Zertifizierung, die nicht zurückgezogen werden können.

Vorgehensweise

1. Suchen Sie nach dem Service und wählen Sie ihn aus. Öffnen Sie das Fenster **Manage Policies**, um die Richtlinie zu bearbeiten.
2. Klicken Sie auf **Recertify Now** (Jetzt erneut zertifizieren).

Eine Warnnachricht wird angezeigt.

3. Klicken Sie auf **OK**, um die Richtlinie erneut zu zertifizieren.

Nächste Schritte

Aktivieren Sie die Richtlinie.

Richtlinie für die erneute Zertifizierung aktivieren und planen

Nach dem Erstellen und Simulieren einer Richtlinie und nach dem Validieren der Simulationsergebnisse ist die Richtlinie bereit für die Aktivierung und Zeitplanung. Eine aktivierte Richtlinie wird nach einem Zeitplan ausgeführt, sodass die erneute Zertifizierung des Service für Benutzer bei jedem Ausführen des Zeitplans angefordert wird.

Vorgehensweise

1. Wenn Sie die Richtlinie nicht ausgewählt haben, suchen Sie nach dem Service und wählen Sie ihn aus. Öffnen Sie das Fenster **Manage Policies**, um die Richtlinie zu bearbeiten.
2. Wählen Sie **Select Active** für die zu aktivierende Richtlinie aus.

Ein Warnhinweis wird angezeigt. Klicken Sie auf **OK**, um die Richtlinie zu aktivieren.

3. Klicken Sie auf das Zeitplansymbol , um das Fenster **Recertification Schedule** zu öffnen.

4. Aktivieren Sie das Kontrollkästchen **Enable Scheduled Execution**.
5. Wählen Sie die Tageszeit, zu der die Richtlinie ausgeführt werden soll, in **Daily Start Time** aus.
6. Wählen Sie den Zeitplantyp aus:
   - **Static Schedule**.
     a. Wählen Sie das Datum, an dem die Richtlinie starten soll, in **Start Date** aus. Die Daten werden im Format MM/TT/JJJJ eingegeben.
     b. Wählen Sie die Frequenz, mit der die Richtlinie ausgeführt werden soll, unter **Repetition Interval** aus.
   - **Rolling Schedule**.
     a. Geben Sie die Intervallfrequenz in Tagen in **Repetition Interval** ein. Die Richtlinie wird, beginnend mit dem ersten Intervall, jeweils nach der von Ihnen eingegebenen Anzahl an Tagen ausgeführt. Wenn Sie z. B. 30 eingeben, wird die Richtlinie vom aktuellen Datum an nach 30 Tagen, dann nach 60 Tagen, dann nach 90 Tagen usw. ausgeführt.
7. Klicken Sie auf **Save Changes**.

Webzugriff verwalten

Das Management des Webzugriffs umfasst das Management von Netzverbindungen zu geschützten Webressourcen in Ihrem Unternehmen.

Überblick über den Webzugriff

Sie verwalten den Webzugriff durch das Erstellen und Verwalten von Netzverbindungen zu geschützten Webressourcen. Sie kontrollieren außerdem den Zugriff auf geschützte Ressourcen durch das Erstellen von Berechtigungsrichtlinien. Die Berechtigungsrichtlinien umfassen Zugriffssteuerungslisten (Access Control Lists, ACLs), Richtlinien für geschützte Objekte (Protected Object Policies, POPs) und eine globale Benutzerrichtlinie.

Geschützte Ressourcen

Geschützte Ressourcen sind Webanwendungen und Server, die Sie durch Cloud Identity Service schützen möchten. Gängige Beispiele für geschützte Ressourcen sind Webportale, Anwendungsserver der Java™ Platform, Enterprise Edition, unter IIS ausgeführte Microsoft .NET-Webanwendungen und Server für statische HTML-Inhalte.

Nach der Authentifizierung eines Benutzers durchlaufen Anforderungen von diesem Benutzer Cloud Identity Service hin zu Ihren geschützten Ressourcen. Jede Anforderung wird von Cloud Identity Service überprüft und mit Ihren Berechtigungsrichtlinien verglichen. Ob ein Benutzer zum Zugriff auf eine Ressource oder zur Ausführung einer Transaktion berechtigt ist, hängt von zahlreichen Faktoren wie Rollen-, Gruppen- und Servicemitgliedschaft, Uhrzeit und Netz-IP ab.

Über die Webanwendungsschnittstelle können Sie Verbindungen zu Clientanwendungsservern definieren und verwalten. Außerdem können Sie die Richtlinien verwalten, die mit Verbindungen verknüpft sind, sowie geschützte Pfadobjekte, die den Verbindungsobjektbereich auf den einzelnen Clientanwendungsservern darstellen.

Berechtigungsrichtlinien

Zugriffssteuerungslisten (ACLs) definieren, welche Benutzer auf welche geschützten Ressourcen zugreifen und was sie mit den Ressourcen, auf die sie Zugriff haben, ausführen können. Richtlinien für geschützte Objekte (POPs) schränken den Zugriff auf Ressourcen ein, indem sie Uhrzeitbedingungen und Bedingungen für IP-Adressbereiche festlegen. Eine Richtlinie wird durchgesetzt, indem sie an eine Junction oder an ein Pfadobjekt angehängt wird. Wenn eine Richtlinie an eine Verbindung angehängt wird, wird sie auf diese Verbindung sowie alle untergeordneten Objekte angewandt. Eine geerbte Richtlinie wird außer Kraft gesetzt, wenn andere Richtlinien auf einer niedrigeren Ebene angehängt werden.

Verbindungen zu Webanwendungen suchen

Sie können nach Netzverbindungen zu geschützten Webanwendungen suchen, um eine Verbindung anzuzeigen, zu ändern oder zu löschen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Applications** > **Connection Management** und dann auf **Web Applications**.
2. Geben Sie im Feld **Search** mindestens die ersten drei Zeichen der Verbindung ein. Die Feldbeschriftung ändert sich in **Searching For**.

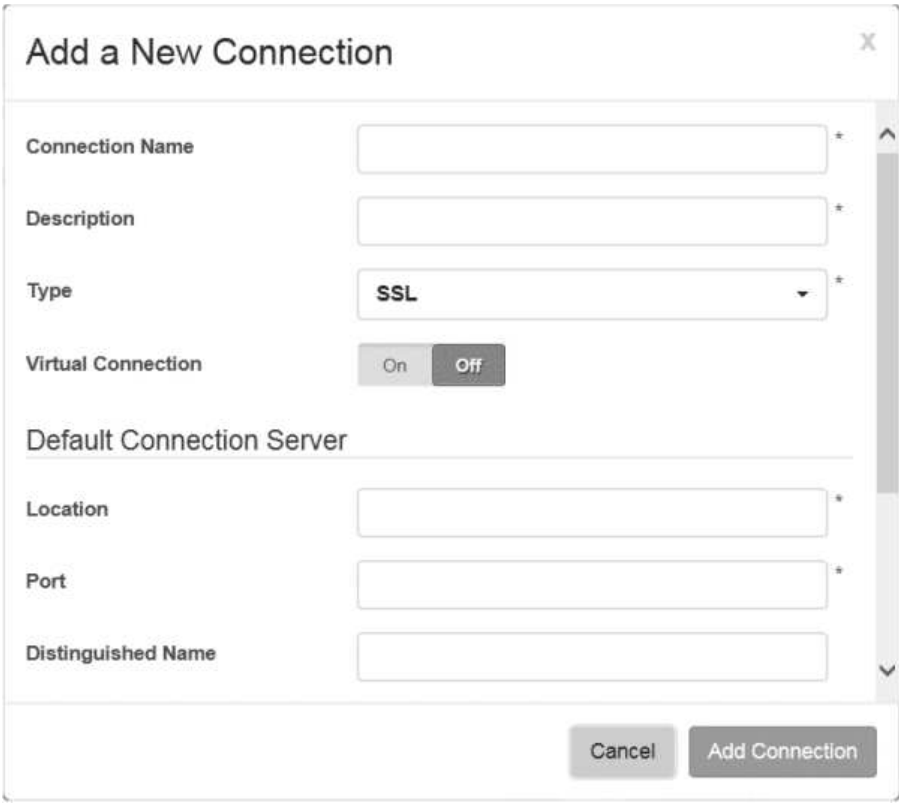
   Die Ihren Suchkriterien entsprechenden Verbindungen werden aufgelistet. Wählen Sie eine Verbindung aus, die Sie ändern oder anzeigen möchten.

Webverbindungen einrichten

Eine Verbindung stellt die logische Verbindung von einem Cloud Identity Service-Web-Proxy-Server zu Endpunkten auf einem oder mehreren Clientanwendungsservern dar. Einer Verbindung können mehrere Serververbindungen hinzugefügt werden.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Applications** > **Connection Management** und dann auf **Web Applications**.



2. Geben Sie den Verbindungsnamen und andere grundlegende Verbindungseinstellungen ein.
3. Geben Sie die Einstellungen für einen Standardverbindungsserver ein. Sie können mehrere Serververbindungen hinzufügen.
4. Klicken Sie auf **Add Connection**.
5. Optional: Geben Sie optionale Einstellungen ein.
6. Optional: Wählen Sie eine Zugriffssteuerungsliste aus oder fügen Sie sie hinzu.
7. Optional: Wählen Sie eine Richtlinie für geschützte Objekte aus oder fügen Sie sie hinzu.
8. Optional: Erstellen Sie geschützte Objekte.
9. Klicken Sie auf **Save**.

Verbindungseinstellungen

Verbindungseinstellungen umfassen den Verbindungstyp und -namen, die Server-Host-Informationen und optionale Einstellungen.

Grundlegende Einstellungen

Tabelle 28. Grundlegende Verbindungseinstellungen

Einstellung	Beschreibung
Connection Name	Der Name der Verbindung. Der Name der Verbindung bestimmt den URL-Pfad, der verwendet wird, um auf den Anwendungsserver zuzugreifen, der über diese Verbindung angeschlossen ist. Wenn z. B. die Verbindung den Namen `webapp_1` hat, lautet die URL für den Root des Anwendungsservers `https://`*`Cloud_Identity_Portal-Adresse_des_Clients`*`/webapp_1/`.

Tabelle 28. Grundlegende Verbindungseinstellungen (Forts.)

Einstellung	Beschreibung
Description	Verbindungsbeschreibung.
Type	Verbindungsprotokoll, TCP oder SSL.
Virtuelle Verbindung	Virtuelle Verbindungen kommunizieren mit virtuellen Hosts. HTTP-Host-Header werden in Clientanforderungen verwendet, um diese Anforderungen zur richtigen Speicherposition auf verbundenen Servern zu leiten. Ein Benutzer kann mithilfe des Hostnamens des verbundenen Servers direkt auf Ressourcen zugreifen (`http://`*`geschützter_Server`*`/resource`), anstatt indirekt mithilfe des Hostnamens des WebSEAL-Servers und eines möglicherweise geänderten Ressourcenpfads (`http://`*`WebSEAL/Verbindung/`*`resource`). Für den direkten Zugriff auf die Ressource mithilfe des Hostnamens des verbundenen Servers ist keine URL-Filterung nötig.
Connection Servers	Wird beim Einrichten einer neuer Verbindung nicht verwendet. Die für die Verbindung einzurichtenden Serveradressen, -pfade und -ports. Klicken Sie auf **Add Server**, um eine Serververbindung hinzuzufügen. Weitere Informationen zum Hinzufügen eines Servers finden Sie unter „Verbindungsserver hinzufügen" auf Seite 132.

Verbindungsrichtlinien und -regeln

Tabelle 29. Verbindungszugriffsrichtlinien und -regeln

Einstellung	Beschreibung
Access Control List (ACL)	Beschränkung des Zugriffs auf die Ressource durch eine Zugriffssteuerungsliste. Wählen Sie in der Liste **Add a new list** aus, um eine Zugriffssteuerungsliste zu erstellen. Siehe „Zugriffssteuerungslisten erstellen" auf Seite 137.
Protected Object Policy (POP)	Beschränkung des Zugriffs auf die Ressource durch eine Richtlinie für geschützte Objekte (POP). Wählen Sie in der Liste **Add a new policy** aus, um eine Richtlinie für geschützte Objekte hinzuzufügen. Siehe „Richtlinien für geschützte Objekte erstellen" auf Seite 134.

Verbindungsobjektbereich

Der Verbindungsobjektbereich stellt die logischen Pfade zu geschützten Objekten unter der Verbindung dar. Zum Beispiel Pfade zu Verzeichnissen, Dateien, Programmen oder Speicherpositionen. Sie können so viele geschützte Objekte zu einer Verbindung hinzufügen, wie nötig.

Tabelle 30. Verbindungsobjektbereich

Einstellung	Beschreibung
Object Name	Objektname. Das geschützte Objekt muss nach dem Objekt benannt werden, das es darstellt. Wenn das Objekt z. B. eine Seite mit dem Namen `page1.jsp` darstellt, die sich am Stamm der Junction befindet, muss das Pfadobjekt mit dem Namen `page1.jsp` erstellt werden.
ACL	Die auf das Objekt angewendete Zugriffssteuerungsliste.

Tabelle 30. Verbindungsobjektbereich (Forts.)

Einstellung	Beschreibung
POP	Die auf die Verbindung angewendete Richtlinie für geschützte Objekte.
Children	Untergeordnete Objekte.

Optionale Einstellungen

Tabelle 31. Optionale Einstellungen

Einstellung	Beschreibung
Stateful Connection	Gibt an, dass die Verbindung statusabhängige Anwendungen unterstützt. Standardmäßig sind Verbindungen nicht statusabhängig.
Boolean Rule	Ermöglicht, dass verweigerte Anforderungen und Informationen zu Fehlerursachen von Berechtigungsregeln im Header für boolesche Regeln (AM_AZN_FAILURE) über die gesamte Verbindung hinweg gesendet werden.
Thread Limit	Definiert die variablen und festen Grenzwerte für die Nutzung von Worker-Threads.

Tabelle 31. Optionale Einstellungen (Forts.)

Einstellung	Beschreibung
HTTP Basic Authentication Header	Definiert, wie der WebSEAL-Reverse-Proxy-Server Informationen zur Clientidentität in HTTP-Basisauthentifizierungsheadern an die Webanwendungsserver übergibt. Optionen für die Handhabung von Clientidentitätsinformationen. • **Filter**. Standardoption. Diese Option wird verwendet, wenn WebSEAL-Authentifizierung für die Verwendung von Basisauthentifizierungsheader-Informationen eingestellt ist. Der WebSEAL-Basisauthentifizierungsheader wird für alle nachfolgenden HTTP-Transaktionen verwendet. Für den Back-End-Server erscheint WebSEAL als immer angemeldet. WebSEAL-Authentifizierung mithilfe eines Clientzertifikats ist mit dieser Option zulässig. Wenn der Back-End-Server eine tatsächliche Clientidentität (vom Browser) erfordert, können Sie die CGI-Variablen HTTP_IV_USER, HTTP_IV_GROUP und HTTP_IV_CREDS verwenden. Für Scripts und Servlets verwenden Sie die entsprechenden für Cloud Identity Service spezifischen HTTP-Header. – iv-user – iv-groups – iv-creds • **Ignore**. WebSEAL-Authentifizierung mithilfe eines Basisauthentifizierungsheaders ist mit dieser Option nicht zulässig. Bei dieser Option wird der Basisauthentifizierungsheader für den ursprünglichen Clientbenutzernamen und das entsprechende Kennwort verwendet. WebSEAL-Authentifizierung mithilfe eines Clientzertifikats ist mit dieser Option zulässig. • **Supply**. WebSEAL-Authentifizierung mithilfe eines Basisauthentifizierungsheaders ist mit dieser Option nicht zulässig. Bei dieser Option wird der Basisauthentifizierungsheader für den ursprünglichen Clientbenutzernamen und ein Pseudokennwort verwendet. WebSEAL-Authentifizierung mithilfe eines Clientzertifikats ist mit dieser Option zulässig.

Tabelle 31. Optionale Einstellungen (Forts.)

Einstellung	Beschreibung
Client Headers	Clientheader setzen über die gesamte Hostverbindung hinweg für Cloud Identity Service spezifische Clientbenutzeridentitätsinformationen in HTTP-Header ein. Die Headertypen können jede beliebige Kombination der folgenden HTTP-Headertypen enthalten. • Standardheader. – **Short user names**. Fügt den Anmeldenamen des Benutzers in einen HTTP-Header namens "iv-user" ein und fügt diesen allen Back-End-Anforderungen an die Verbindungshosts hinzu. – **Long user names**. Fügt den für Cloud Identity Service definierten Namen des Benutzers in einen HTTP-Header namens "iv-user-l" ein und fügt diesen allen Back-End-Anforderungen an die Verbindungshosts hinzu. – **Group names**. Fügt eine durch Kommas getrennte Liste der Gruppen, zu denen ein Benutzer gehört, in einen HTTP-Header namens "iv-groups" ein und fügt diesen allen Back-End-Anforderungen an die Verbindungshosts hinzu. – **User credentials**. Fügt den Cloud Identity Service-Benutzerberechtigungsnachweis in eine Base64-kodierte Zeichenfolge in einen HTTP-Header namens "iv-creds" ein und fügt diesen allen Back-End-Anforderungen an die Verbindungshosts hinzu. – **Insert client IP Address**. Fügt die IP-Adresse des Benutzers in einen HTTP-Header namens "iv-remote-address" ein und fügt diesen allen Back-End-Anforderungen an die Verbindungshosts hinzu. • Angepasste Header. – Angepasste Attribute müssen für Ihre Konfiguration von Cloud Identity Service konfiguriert und aktiviert werden, damit sie für angepasste Header verfügbar sind. Das ausgewählte Attribut wird in einen HTTP-Header eingefügt. Für den Header für ein Name eingegeben werden.

Tabelle 31. Optionale Einstellungen (Forts.)

Einstellung	Beschreibung
HTTP Header Encoding	Gibt an, welche Codierung zu verwenden ist, wenn HTTP-Header generiert werden, die an Verbindungshosts gesendet werden. Diese Codierung verhindert, dass bei einer Konvertierung in eine Nicht-UTF-8-Codepage Daten verloren gehen. Mögliche Werte für die Codierung. • **UTF-8 Binary**. Nichtcodierte UTF-8-Daten. Diese Einstellung ermöglicht eine Datenübertragung ohne Datenverlust. Der Kunde muss die Daten nicht aus einem URI decodieren. Diese Einstellung muss mit Vorsicht verwendet werden, da sie nicht Teil der HTTP-Spezifikation ist. • **UTF-8 URI Encoded**. In einem URI codierte UTF-8-Daten. Alle Leerzeichen und Nicht-ASCII-Bytes werden mit %XY codiert, wobei X und Y für Hexadezimalwerte stehen (0-F). • **Local Page Code Binary**. Nichtcodierte lokale Codepagedaten. Dieser Modus wurde in Versionen von WebSEAL vor Version 5.1 verwendet. Bei Verwendung dieses Modus ist eine Migration von früheren Versionen möglich. Er wird in Upgradeumgebungen verwendet. Verwenden Sie diesen Modus vorsichtig, da er zu Datenverlust führen kann. • **Local Code Page URI Encoded**. In einem URI codierte lokale Codepagedaten. Alle UTF-8-Zeichen, die nicht in eine lokale Codepage konvertiert werden können, werden in Fragezeichen konvertiert (?). Verwenden Sie diese Option vorsichtig und nur in Umgebungen, in denen die lokale Codepage die gewünschten Zeichenfolgen erzeugt.
Basic Authentication	Gibt an, dass der Verbindungshost ebenfalls ein WebSEAL-Server ist. Bei Aktivierung wird die Verbindung zwischen den Servern mithilfe einer proprietären Authentifizierungseinrichtung authentifiziert. • **WebSEAL username**. Die Benutzer-ID, die Cloud Identity Service-WebSEAL-Server verwenden, um sich gegenüber den Verbindungshosts zu authentifizieren. • **WebSEAL password**. Das Kennwort, das Cloud Identity Service-WebSEAL-Server verwenden, um sich gegenüber den Verbindungshosts zu authentifizieren.
Mutual Authentication	Ermöglicht die Clientauthentifizierung für die Verbindung mit einem Zertifikat. • **Certificate**. Das zu verwendende Zertifikat.
Junction Cookie	Einfügen der ID über ein Cookie-Script.

Tabelle 31. Optionale Einstellungen (Forts.)

Einstellung	Beschreibung
Cookie Location	Nur anwendbar, wenn **Junction Cookie** aktiviert ist. Gibt die Speicherposition auf den Seiten an, die von Verbindungshosts bereitgestellt werden, bei denen die ID über ein Cookie-Script eingefügt wird. • **None**. Wenn **None** angegeben wurde, wird das Script standardmäßig am Anfang des Antworthauptteils geschrieben. • **Header**. Fügt das Script zwecks Kompatibilität mit HTML 4.01 zwischen den Tags `<head> und </head>` ein. • **Trailer**. Hängt das Script an die vom Back-End-Server zurückgegebene HTML-Seite an (statt ihm ein Präfix hinzuzufügen). • **Trailer on Focus**. Verwendet den Onfocus-Ereignishandler im Script, um sicherzustellen, dass in einem Szenario mit mehreren Verbindungen bzw. mehreren Browserfenstern das richtige Verbindungscookie verwendet wird. • **XHTML 1.0**. Fügt einen mit XHTML 1.0 (und HTML 4.01) kompatiblen JavaScript-Block im Browser ein, der das Dokument interpretiert.
Cookie Handling	• **Script Cookie**. Liefert eine Kennzeichnung der Verbindung in einem Cookie zur Bearbeitung scriptgenerierter, relativer Server-URLs. • **Preserve Cookie Path**. Stellt sicher, dass Verbindungshosts eindeutige Set-Cookie-Headernamensattribute für Cookies festlegen, indem sie jeden Cookiepfad in den neu geschriebenen Cookienamen einfügen. • **Preserve Cookie Name**. Stellt sicher, dass der von einem Verbindungshost festgelegte Set-Cookie-Header nicht von Cloud Identity Service neu geschrieben wird, indem der Verbindungsname in den Cookienamen eingefügt wird.
Transparent Path Junction	Nichtvirtuelle Option. Gibt an, ob die Verbindung einen transparenten Pfad verwendet. Anstatt ein Präfix zu allen gefilterten URLs mit */Verbindungsname* hinzuzufügen, wird angenommen, dass der gesamte Inhalt auf den Verbindungshosts über ein Kontextstammelement bereitgestellt wird, das */Verbindungsname* entspricht. Durch einen transparenten Pfad wird vermieden, dass Cloud Identity Service relative Server-URLs filtern muss.

Grundlegende Verbindungseinstellungen:

Tabelle 32. Grundlegende Verbindungseinstellungen

Einstellung	Beschreibung
Connection Name	Der Name der Verbindung. Der Name der Verbindung bestimmt den URL-Pfad, der verwendet wird, um auf den Anwendungsserver zuzugreifen, der über diese Verbindung angeschlossen ist. Wenn z. B. die Verbindung den Namen `webapp_1` hat, lautet die URL für den Root des Anwendungsservers `https://`*`Cloud_Identity_Portal-Adresse_des_Clients`*`/webapp_1/`.
Description	Verbindungsbeschreibung.
Type	Verbindungsprotokoll, TCP oder SSL.

Tabelle 32. Grundlegende Verbindungseinstellungen (Forts.)

Einstellung	Beschreibung
Virtuelle Verbindung	Virtuelle Verbindungen kommunizieren mit virtuellen Hosts. HTTP-Host-Header werden in Clientanforderungen verwendet, um diese Anforderungen zur richtigen Speicherposition auf verbundenen Servern zu leiten. Ein Benutzer kann mithilfe des Hostnamens des verbundenen Servers direkt auf Ressourcen zugreifen (`http://`*`geschützter_Server`*`/resource`), anstatt indirekt mithilfe des Hostnamens des WebSEAL-Servers und eines möglicherweise geänderten Ressourcenpfads (`http://`*`WebSEAL/Verbindung/`*`resource`). Für den direkten Zugriff auf die Ressource mithilfe des Hostnamens des verbundenen Servers ist keine URL-Filterung nötig.
Connection Servers	Wird beim Einrichten einer neuer Verbindung nicht verwendet. Die für die Verbindung einzurichtenden Serveradressen, -pfade und -ports. Klicken Sie auf **Add Server**, um eine Serververbindung hinzuzufügen. Weitere Informationen zum Hinzufügen eines Servers finden Sie unter „Verbindungsserver hinzufügen" auf Seite 132.

Servereinstellungen für die Standardverbindung:

Tabelle 33. Verbindungsservereinstellungen

Einstellung	Beschreibung
Location	Der Hostname oder die IP-Adresse des Endpunkts, der die Verbindung bildet.
Port	Der Port, über den die Verbindung zum Hostsystem hergestellt werden soll. Die Standardeinstellung ist der Standard-HTTPS-Port 443. Diese Angabe ist nur erforderlich, wenn die Verbindung über einen anderen Port hergestellt werden soll.
Distinguished Name	Der Zertifikats-DN, der Cloud Identity Service angegeben wird, wenn Verbindungen zum Anwendungsserver hergestellt werden. Dieses Feld kann verwendet werden, um die Sicherheit zu erweitern, indem Cloud Identity Service erlaubt wird, die zertifizierte Identität des Servers zu prüfen, bevor eine Verbindung zu ihm hergestellt wird.
Virtual Host	Der HTTP-Host-Header, der mit den Webanforderungen an den Anwendungsserver übertragen wird. Für mit HTTP Version 1.1 konforme Web-Server kann dieser Header erforderlich sein, um die Anforderungen an die entsprechende Konfiguration des virtuellen Hosts weiterzuleiten. **Anmerkung:** Nur erforderlich, wenn der Name des virtuellen Hosts von dem im Feld **Location** angegebenen Wert abweicht.
Query Script Path	Die Position des Query Contents-Tools, das optional auf einem Clientanwendungsserver installiert werden kann. Mit dem Query Contents-Tool kann Cloud Identity Service seinen Web-Space überprüfen und über die im Fenster **Connection Object Space** angezeigte Pfadobjekthierarchie darstellen. Wenn dieser Wert nicht angegeben wird, wird der Standardwert `/cgi-bin/query_contents` verwendet.

Tabelle 33. Verbindungsservereinstellungen (Forts.)

Einstellung	Beschreibung
Case sensitive URLs	Steuert, ob Cloud Identity Service bei URLs die Groß-/Kleinschreibung beachtet, wenn eine Berechtigungsprüfung für eine Anforderung an einen Verbindungshost ausgeführt wird. Nach einer erfolgreichen Prüfung der Zugriffssteuerungsliste wird die ursprüngliche Groß-/Kleinschreibung der URL wiederhergestellt, wenn die Anforderung an den Server gesendet wird.
Win32 support	Steuert, ob Cloud Identity Service Berechtigungsprüfungen für traditionelle Windows-Dateipfade ausführt. Cloud Identity Service führt Sicherheitsprüfungen für Clientanforderungen an Verbindungshosts auf der Grundlage der in der URL angegebenen Dateipfade aus. Bei dieser Sicherheitsprüfung kann ein Kompromiss erfolgen, da Win32-Dateisysteme zwei verschiedene Methoden zum Zugriff auf lange Dateinamen erlaubt. Bei der ersten Methode wird der gesamte Dateiname berücksichtigt, z. B. `abcdefghijkl.txt`. Bei der zweiten Methode wird zwecks Kompatibilität mit früheren Versionen das alte 8.3-Dateinamensformat anerkannt, z. B. `abcdef~1.txt`. Wenn Sie einen Verbindungshost in einer Windows-Umgebung hinzufügen, ist es wichtig, die Zugriffskontrolle auf eine einzige Objektdarstellung zu beschränken. Diese Beschränkung dient dazu, einen möglichen Backdoor-Zugriff zu verhindern, bei dem der Sicherheitsmechanismus umgangen wird. Die Win32-Unterstützungsoption bietet deshalb eine Reihe von Schutzmaßnahmen. • Sie verhindert die Verwendung des 8.3-Dateinamensformats. Ein Benutzer kann eine explizite Zugriffssteuerungsliste für einen langen Dateinamen nicht umgehen, indem er die Kurzform (von Version 8.3) des Dateinamens verwendet. Cloud Identity Service meldet den Fehler "403 Forbidden", wenn ein Dateiname in Kurzform eingegeben wird. • Sie lässt abschließende Punkte in Verzeichnis- und Dateinamen nicht zu. Wenn ein Datei- oder Verzeichnisname abschließende Punkte enthält, wird der Fehler "403 Forbidden" gemeldet. • Sie setzt die Nichtbeachtung der Groß-/Kleinschreibung durch, indem die Option **Case sensitive URLs** aktiviert wird.

Optionale Verbindungseinstellungen:

Tabelle 34. Optionale Einstellungen

Einstellung	Beschreibung
Stateful Connection	Gibt an, dass die Verbindung statusabhängige Anwendungen unterstützt. Standardmäßig sind Verbindungen nicht statusabhängig.
Boolean Rule	Ermöglicht, dass verweigerte Anforderungen und Informationen zu Fehlerursachen von Berechtigungsregeln im Header für boolesche Regeln (AM_AZN_FAILURE) über die gesamte Verbindung hinweg gesendet werden.

Tabelle 34. Optionale Einstellungen (Forts.)

Einstellung	Beschreibung
Thread Limit	Definiert die variablen und festen Grenzwerte für die Nutzung von Worker-Threads.
HTTP Basic Authentication Header	Definiert, wie der WebSEAL-Reverse-Proxy-Server Informationen zur Clientidentität in HTTP-Basisauthentifizierungsheadern an die Webanwendungsserver übergibt. Optionen für die Handhabung von Clientidentitätsinformationen. • **Filter**. Standardoption. Diese Option wird verwendet, wenn WebSEAL-Authentifizierung für die Verwendung von Basisauthentifizierungsheader-Informationen eingestellt ist. Der WebSEAL-Basisauthentifizierungsheader wird für alle nachfolgenden HTTP-Transaktionen verwendet. Für den Back-End-Server erscheint WebSEAL als immer angemeldet. WebSEAL-Authentifizierung mithilfe eines Clientzertifikats ist mit dieser Option zulässig. Wenn der Back-End-Server eine tatsächliche Clientidentität (vom Browser) erfordert, können Sie die CGI-Variablen HTTP_IV_USER, HTTP_IV_GROUP und HTTP_IV_CREDS verwenden. Für Scripts und Servlets verwenden Sie die entsprechenden für Cloud Identity Service spezifischen HTTP-Header. – iv-user – iv-groups – iv-creds • **Ignore**. WebSEAL-Authentifizierung mithilfe eines Basisauthentifizierungsheaders ist mit dieser Option nicht zulässig. Bei dieser Option wird der Basisauthentifizierungsheader für den ursprünglichen Clientbenutzernamen und das entsprechende Kennwort verwendet. WebSEAL-Authentifizierung mithilfe eines Clientzertifikats ist mit dieser Option zulässig. • **Supply**. WebSEAL-Authentifizierung mithilfe eines Basisauthentifizierungsheaders ist mit dieser Option nicht zulässig. Bei dieser Option wird der Basisauthentifizierungsheader für den ursprünglichen Clientbenutzernamen und ein Pseudokennwort verwendet. WebSEAL-Authentifizierung mithilfe eines Clientzertifikats ist mit dieser Option zulässig.

Tabelle 34. Optionale Einstellungen (Forts.)

Einstellung	Beschreibung
Client Headers	Clientheader setzen über die gesamte Hostverbindung hinweg für Cloud Identity Service spezifische Clientbenutzeridentitätsinformationen in HTTP-Header ein. Die Headertypen können jede beliebige Kombination der folgenden HTTP-Headertypen enthalten. • Standardheader. – **Short user names**. Fügt den Anmeldenamen des Benutzers in einen HTTP-Header namens "iv-user" ein und fügt diesen allen Back-End-Anforderungen an die Verbindungshosts hinzu. – **Long user names**. Fügt den für Cloud Identity Service definierten Namen des Benutzers in einen HTTP-Header namens "iv-user-l" ein und fügt diesen allen Back-End-Anforderungen an die Verbindungshosts hinzu. – **Group names**. Fügt eine durch Kommas getrennte Liste der Gruppen, zu denen ein Benutzer gehört, in einen HTTP-Header namens "iv-groups" ein und fügt diesen allen Back-End-Anforderungen an die Verbindungshosts hinzu. – **User credentials**. Fügt den Cloud Identity Service-Benutzerberechtigungsnachweis in eine Base64-kodierte Zeichenfolge in einen HTTP-Header namens "iv-creds" ein und fügt diesen allen Back-End-Anforderungen an die Verbindungshosts hinzu. – **Insert client IP Address**. Fügt die IP-Adresse des Benutzers in einen HTTP-Header namens "iv-remote-address" ein und fügt diesen allen Back-End-Anforderungen an die Verbindungshosts hinzu. • Angepasste Header. – Angepasste Attribute müssen für Ihre Konfiguration von Cloud Identity Service konfiguriert und aktiviert werden, damit sie für angepasste Header verfügbar sind. Das ausgewählte Attribut wird in einen HTTP-Header eingefügt. Für den Header für ein Name eingegeben werden.

Tabelle 34. Optionale Einstellungen (Forts.)

Einstellung	Beschreibung
HTTP Header Encoding	Gibt an, welche Codierung zu verwenden ist, wenn HTTP-Header generiert werden, die an Verbindungshosts gesendet werden. Diese Codierung verhindert, dass bei einer Konvertierung in eine Nicht-UTF-8-Codepage Daten verloren gehen. Mögliche Werte für die Codierung. • **UTF-8 Binary**. Nichtcodierte UTF-8-Daten. Diese Einstellung ermöglicht eine Datenübertragung ohne Datenverlust. Der Kunde muss die Daten nicht aus einem URI decodieren. Diese Einstellung muss mit Vorsicht verwendet werden, da sie nicht Teil der HTTP-Spezifikation ist. • **UTF-8 URI Encoded**. In einem URI codierte UTF-8-Daten. Alle Leerzeichen und Nicht-ASCII-Bytes werden mit %XY codiert, wobei X und Y für Hexadezimalwerte stehen (0-F). • **Local Page Code Binary**. Nichtcodierte lokale Codepagedaten. Dieser Modus wurde in Versionen von WebSEAL vor Version 5.1 verwendet. Bei Verwendung dieses Modus ist eine Migration von früheren Versionen möglich. Er wird in Upgradeumgebungen verwendet. Verwenden Sie diesen Modus vorsichtig, da er zu Datenverlust führen kann. • **Local Code Page URI Encoded**. In einem URI codierte lokale Codepagedaten. Alle UTF-8-Zeichen, die nicht in eine lokale Codepage konvertiert werden können, werden in Fragezeichen konvertiert (?). Verwenden Sie diese Option vorsichtig und nur in Umgebungen, in denen die lokale Codepage die gewünschten Zeichenfolgen erzeugt.
Basic Authentication	Gibt an, dass der Verbindungshost ebenfalls ein WebSEAL-Server ist. Bei Aktivierung wird die Verbindung zwischen den Servern mithilfe einer proprietären Authentifizierungseinrichtung authentifiziert. • **WebSEAL username**. Die Benutzer-ID, die Cloud Identity Service-WebSEAL-Server verwenden, um sich gegenüber den Verbindungshosts zu authentifizieren. • **WebSEAL password**. Das Kennwort, das Cloud Identity Service-WebSEAL-Server verwenden, um sich gegenüber den Verbindungshosts zu authentifizieren.
Mutual Authentication	Ermöglicht die Clientauthentifizierung für die Verbindung mit einem Zertifikat. • **Certificate**. Das zu verwendende Zertifikat.
Junction Cookie	Einfügen der ID über ein Cookie-Script.

Tabelle 34. Optionale Einstellungen (Forts.)

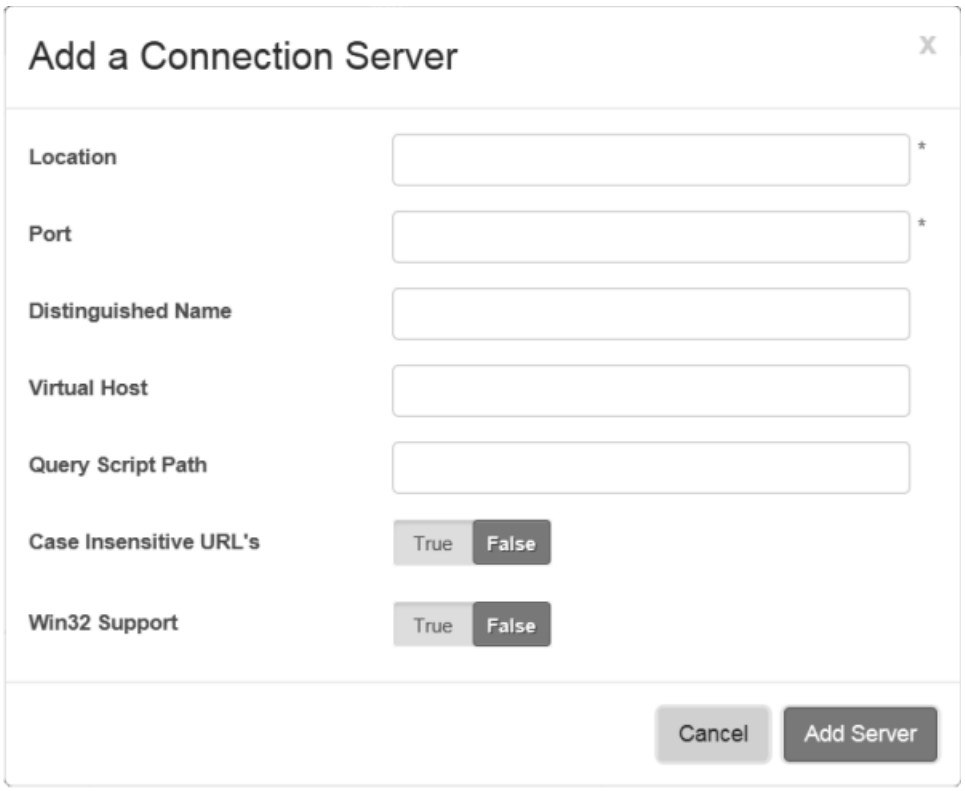
Einstellung	Beschreibung
Cookie Location	Nur anwendbar, wenn **Junction Cookie** aktiviert ist. Gibt die Speicherposition auf den Seiten an, die von Verbindungshosts bereitgestellt werden, bei denen die ID über ein Cookie-Script eingefügt wird. • **None**. Wenn **None** angegeben wurde, wird das Script standardmäßig am Anfang des Antworthauptteils geschrieben. • **Header**. Fügt das Script zwecks Kompatibilität mit HTML 4.01 zwischen den Tags `<head> und </head>` ein. • **Trailer**. Hängt das Script an die vom Back-End-Server zurückgegebene HTML-Seite an (statt ihm ein Präfix hinzuzufügen). • **Trailer on Focus**. Verwendet den Onfocus-Ereignishandler im Script, um sicherzustellen, dass in einem Szenario mit mehreren Verbindungen bzw. mehreren Browserfenstern das richtige Verbindungscookie verwendet wird. • **XHTML 1.0**. Fügt einen mit XHTML 1.0 (und HTML 4.01) kompatiblen JavaScript-Block im Browser ein, der das Dokument interpretiert.
Cookie Handling	• **Script Cookie**. Liefert eine Kennzeichnung der Verbindung in einem Cookie zur Bearbeitung scriptgenerierter, relativer Server-URLs. • **Preserve Cookie Path**. Stellt sicher, dass Verbindungshosts eindeutige Set-Cookie-Headernamensattribute für Cookies festlegen, indem sie jeden Cookiepfad in den neu geschriebenen Cookienamen einfügen. • **Preserve Cookie Name**. Stellt sicher, dass der von einem Verbindungshost festgelegte Set-Cookie-Header nicht von Cloud Identity Service neu geschrieben wird, indem der Verbindungsname in den Cookienamen eingefügt wird.
Transparent Path Junction	Nichtvirtuelle Option. Gibt an, ob die Verbindung einen transparenten Pfad verwendet. Anstatt ein Präfix zu allen gefilterten URLs mit */Verbindungsname* hinzuzufügen, wird angenommen, dass der gesamte Inhalt auf den Verbindungshosts über ein Kontextstammelement bereitgestellt wird, das */Verbindungsname* entspricht. Durch einen transparenten Pfad wird vermieden, dass Cloud Identity Service relative Server-URLs filtern muss.

Verbindungsserver hinzufügen

Die für die Verbindung einzurichtenden Verbindungsserveradressen, -pfade und -ports.

Vorgehensweise

1. Wenn die Verbindung, für die Sie den Verbindungsserver einrichten möchten, nicht geöffnet ist, suchen Sie die Verbindung und wählen Sie sie aus.
2. Klicken Sie unter **Connection Servers** auf **Add new server**.



3. Geben Sie die Verbindungsservereinstellungen ein.

Tabelle 35. Verbindungsservereinstellungen

Einstellung	Beschreibung
Location	Der Hostname oder die IP-Adresse des Endpunkts, der die Verbindung bildet.
Port	Der Port, über den die Verbindung zum Hostsystem hergestellt werden soll. Die Standardeinstellung ist der Standard-HTTPS-Port 443. Diese Angabe ist nur erforderlich, wenn die Verbindung über einen anderen Port hergestellt werden soll.
Distinguished Name	Der Zertifikats-DN, der Cloud Identity Service angegeben wird, wenn Verbindungen zum Anwendungsserver hergestellt werden. Dieses Feld kann verwendet werden, um die Sicherheit zu erweitern, indem Cloud Identity Service erlaubt wird, die zertifizierte Identität des Servers zu prüfen, bevor eine Verbindung zu ihm hergestellt wird.
Virtual Host	Der HTTP-Host-Header, der mit den Webanforderungen an den Anwendungsserver übertragen wird. Für mit HTTP Version 1.1 konforme Web-Server kann dieser Header erforderlich sein, um die Anforderungen an die entsprechende Konfiguration des virtuellen Hosts weiterzuleiten. **Anmerkung:** Nur erforderlich, wenn der Name des virtuellen Hosts von dem im Feld **Location** angegebenen Wert abweicht.
Query Script Path	Die Position des Query Contents-Tools, das optional auf einem Clientanwendungsserver installiert werden kann. Mit dem Query Contents-Tool kann Cloud Identity Service seinen Web-Space überprüfen und über die im Fenster **Connection Object Space** angezeigte Pfadobjekthierarchie darstellen. Wenn dieser Wert nicht angegeben wird, wird der Standardwert `/cgi-bin/query_contents` verwendet.

Tabelle 35. Verbindungsservereinstellungen (Forts.)

Einstellung	Beschreibung
Case sensitive URLs	Steuert, ob Cloud Identity Service bei URLs die Groß-/Kleinschreibung beachtet, wenn eine Berechtigungsprüfung für eine Anforderung an einen Verbindungshost ausgeführt wird. Nach einer erfolgreichen Prüfung der Zugriffssteuerungsliste wird die ursprüngliche Groß-/Kleinschreibung der URL wiederhergestellt, wenn die Anforderung an den Server gesendet wird.
Win32 support	Steuert, ob Cloud Identity Service Berechtigungsprüfungen für traditionelle Windows-Dateipfade ausführt. Cloud Identity Service führt Sicherheitsprüfungen für Clientanforderungen an Verbindungshosts auf der Grundlage der in der URL angegebenen Dateipfade aus. Bei dieser Sicherheitsprüfung kann ein Kompromiss erfolgen, da Win32-Dateisysteme zwei verschiedene Methoden zum Zugriff auf lange Dateinamen erlaubt. Bei der ersten Methode wird der gesamte Dateiname berücksichtigt, z. B. `abcdefghijkl.txt`. Bei der zweiten Methode wird zwecks Kompatibilität mit früheren Versionen das alte 8.3-Dateinamensformat anerkannt, z. B. `abcdef~1.txt`. Wenn Sie einen Verbindungshost in einer Windows-Umgebung hinzufügen, ist es wichtig, die Zugriffskontrolle auf eine einzige Objektdarstellung zu beschränken. Diese Beschränkung dient dazu, einen möglichen Backdoor-Zugriff zu verhindern, bei dem der Sicherheitsmechanismus umgangen wird. Die Win32-Unterstützungsoption bietet deshalb eine Reihe von Schutzmaßnahmen. • Sie verhindert die Verwendung des 8.3-Dateinamensformats. Ein Benutzer kann eine explizite Zugriffssteuerungsliste für einen langen Dateinamen nicht umgehen, indem er die Kurzform (von Version 8.3) des Dateinamens verwendet. Cloud Identity Service meldet den Fehler "403 Forbidden", wenn ein Dateiname in Kurzform eingegeben wird. • Sie lässt abschließende Punkte in Verzeichnis- und Dateinamen nicht zu. Wenn ein Datei- oder Verzeichnisname abschließende Punkte enthält, wird der Fehler "403 Forbidden" gemeldet. • Sie setzt die Nichtbeachtung der Groß-/Kleinschreibung durch, indem die Option **Case sensitive URLs** aktiviert wird.

4. Klicken Sie auf **Add Server**.

Richtlinien für geschützte Objekte erstellen

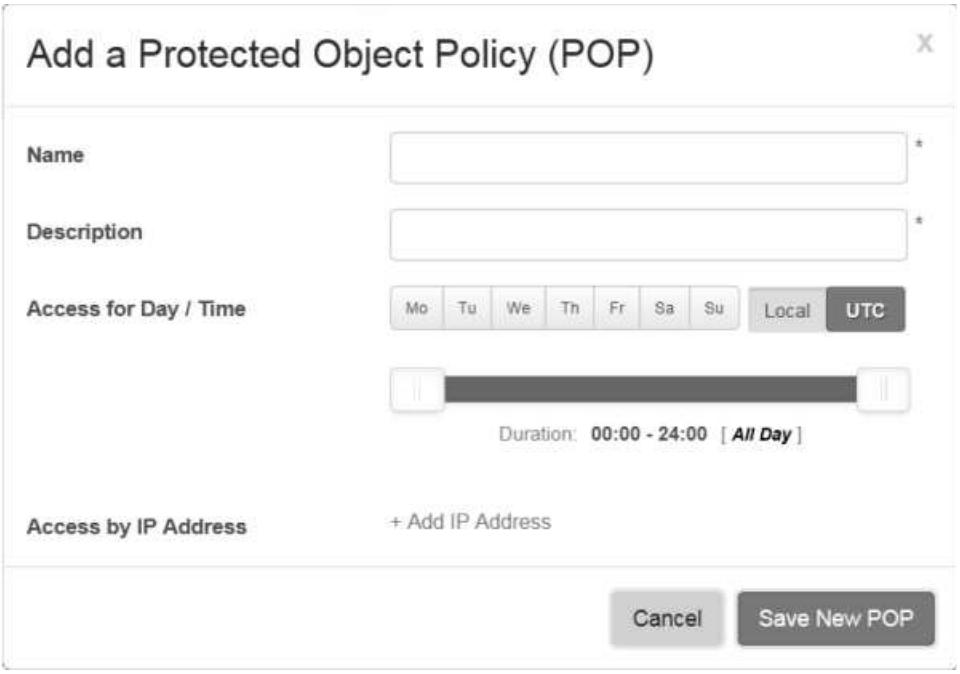
Mithilfe von Richtlinien für geschützte Objekte (POPs) können Sie Richtlinienanforderungen qualifizieren. Sie können Zugriffsanforderungen anhand der Uhrzeit und der Netzadresse qualifizieren.

Informationen zu diesem Vorgang

Die Richtlinie tritt erst in Kraft, wenn sie an eine Verbindung angehängt wird.

Vorgehensweise

1. Wenn die Verbindung, für die Sie die Richtlinie für geschützte Objekte erstellen möchten, nicht geöffnet ist, suchen Sie die Verbindung und wählen Sie sie aus.
2. Wählen Sie **Add a new policy** in der Dropdown-Liste **Protected Object Policy (POP)** aus.



3. Geben Sie einen Namen und eine Beschreibung ein.
4. Geben Sie die übrigen POP-Einstellungen ein.

Einstellung	Beschreibung
Access for Day/ Time	Gibt die Tage und die Uhrzeit an, an/zu denen der Zugriff gestattet wird. Die Uhrzeit kann als lokale Uhrzeit für die Servicehostumgebung oder als koordinierte Weltzeit ausgedrückt werden. Wählen Sie die Tage aus, an denen der Zugriff gestattet wird. Anhand der Schiebeleiste können Sie den Zugriff auf eine ausgewählte Zeitspanne einschränken.

Einstellung	Beschreibung	
Access by IP Address	IP-Authentifizierungseinstellungen für Richtlinien für geschützte Objekte (POPs). Der Zugriff wird durch die IP-Adresse und die Authentifizierungsebene qualifiziert. Benutzern kann der Zugriff auf die Ressource über die angegebenen IP-Adressen erlaubt oder verweigert werden. Klicken Sie auf **Add IP Address**, um Einschränkungen für IP-Adressen hinzuzufügen.	
	Any Other Network	Wird verwendet als Netzbereich, der allen Netzen entspricht, die nicht anderweitig in der Richtlinie für geschützte Objekte angegeben sind. Anhand dieser Methode können Sie einen Standardeintrag erstellen, der entweder alle IP-Adressen ohne Entsprechung ablehnt oder allen Personen Zugriff gewährt, die die Anforderung auf Authentifizierungsebene erfüllen.
	IP Address	Die Werte für das Netz sind TCP/IP-Adressen. Die Optionen für Netz und Netzmaske müssen in der gleichen IP-Version angegeben werden.
	Netmask	Die Werte für die Netzmaske sind TCP/IP-Adressen. Die Optionen für Netz und Netzmaske müssen in der gleichen IP-Version angegeben werden. Die Zahl 0 dient in der Netzmaske als Platzhalter für alle IP-Adressen für das betreffende Teilnetz. Die IP-Adresse 9.1.2.3 mit der Netzmaske 255.255.255.0 gilt z. B. für alle IP-Adressen im Bereich 9.1.2.[0-255].
	Forbidden	Der Zugriff wird untersagt.
	Authentication Level	Anwendungsspezifische ganzzahlige Werte, die die Ebenen für erweiterte Authentifizierung definieren. Alle ganzzahligen Werte bis ausschließlich 1000 werden unterstützt. 0 ist die niedrigste Ebene. Authentifizierungsebenen werden während der Erstkonfiguration von Cloud Identity Service für Ihre Organisation definiert.
Multi-Factor Authentication		Gibt an, ob die Mehrfaktorauthentifizierung aktiviert werden soll.

5. Klicken Sie auf **Save New POP**.

Beispiel

Die Standardeinstellung für eine Richtlinie für geschützte Objekte ist, dass jedes Netz Zugriff auf jeder Authentifizierungsebene erhält:

- **Authentication Level** ist 0.

Im folgenden Beispiel gilt der Clientzugriff ausgehend von einer Gruppe von IP-Adressen als sicher. Ein anderer Netzbereich gilt als weniger sicher und erfordert eine höhere Berechtigungsstufe. Der Zugriff von jedem anderen Netzbereich muss abgelehnt werden. Zwei IP-Authentizierungseinträge müssen für die Richtlinie für geschützte Objekte erstellt werden, einer für den Bereich sicherer IP-Adressen und einer für die weniger sicheren IP-Adressen.

Der erste Bereich gilt für alle Clients, die auf die Webressource mit einer IP-Adresse von 9.180.168.* zugreifen.

- **IP Address** ist 9.180.168.0.
- **Netmask** ist 255.255.255.0.

- **Authentication Level** ist 0.

Der zweite Bereich verwendet die Optionen **Any Other Network** und **Forbidden** zum Ausschließen von IP-Adressen. Webclients, deren Ursprungs-IP-Adresse nicht dem Bereich 9.180.168.* entspricht, werden standardmäßig diesem Bereich zugewiesen und abgelehnt. Nur Web-Clients mit IP-Adressen aus dem Bereich 9.180.168.* können auf eine Webressource zugreifen, die durch diese Richtlinie für geschützte Objekte geschützt wird. Dieses Beispiel gilt möglicherweise auch für den von einer Unternehmensfirewall verwendeten NAT-Bereich (Network Address Translation, Netzadressumsetzung).

- **Any Other Network** ist aktiviert.
- **Forbidden** ist wahr.

Auf der Seite **Protected Object Policy** für die Richtlinie werden die beiden IP-Bereiche angezeigt.

Zugriffssteuerungslisten erstellen

Eine Zugriffssteuerungsliste enthält eine Zuordnung zwischen einem Benutzer, Gruppen und Services und einem Berechtigungssatz. Sie können neue Zugriffssteuerungslisten erstellen, um Benutzern, Gruppenmitgliedern und Servicemitgliedern Zugriff auf eine geschützte Ressource zu erteilen.

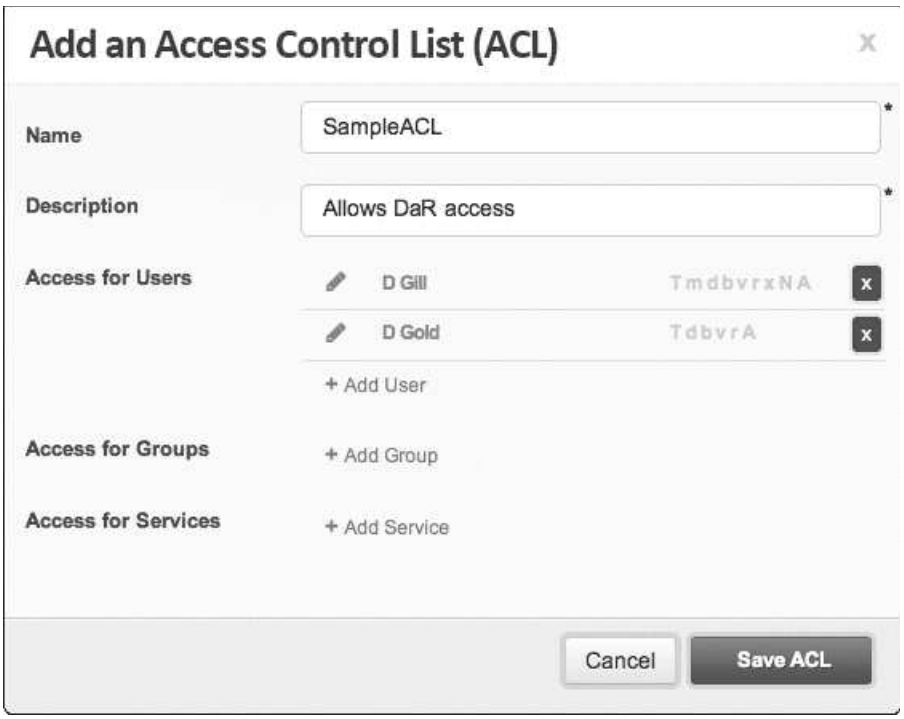
Informationen zu diesem Vorgang

Eine Zugriffssteuerungsliste besteht aus einer Reihe von Zugriffssteuerungslisteneinträgen. In jedem Zugriffssteuerungslisteneintrag werden Benutzer, Gruppen und Services mit einer Liste der Berechtigungen angegeben, die diesen Benutzern, Gruppen und Services erteilt werden. Eine Zugriffssteuerungsliste tritt erst in Kraft, wenn sie einer Verbindung hinzugefügt wird.

Wichtig: Standardzugriffssteuerungslisten dürfen nicht geändert oder gelöscht werden.

Vorgehensweise

1. Wenn die Verbindung, für die Sie die Zugriffssteuerungsliste erstellen möchten, nicht geöffnet ist, suchen Sie die Verbindung und wählen Sie sie aus.
2. Wählen Sie **Add a new list** in der Dropdown-Liste **Access Control List (ACL)** aus.



3. Geben Sie einen Namen und eine Beschreibung ein.
4. Geben Sie die übrigen ACL-Einstellungen ein.

Einstellung	Beschreibung
Access for Users	Zugriff für einzelne Benutzer. Jedem hinzugefügten Benutzer wird Zugriff auf die Ressource erteilt. Klicken Sie auf **Add User**, um einen Benutzer hinzuzufügen. Um einen Benutzer zu suchen und auszuwählen, geben Sie die ersten drei Zeichen seines Vornamens, Nachnamens, Benutzernamens oder seiner E-Mail-Adresse ein. Wählen Sie die Berechtigungen für jeden Eintrag aus. Sie können die folgenden Berechtigungen für Cloud Identity Service-Benutzer, -Gruppen und -Services verwenden: • **r**. Read (lesen). Ermöglicht Benutzern, das Objekt anzuzeigen. • **x**. Execute (ausführen). Ermöglicht Benutzern, eine Datei oder ein Script aus dem Objekt auszuführen. • **T**. Traverse (durchqueren). Ermöglicht Benutzern, auf Objekte zuzugreifen, die sich weiter unten in der Hierarchie befinden. **Anmerkung:** Alle anderen Berechtigungen gelten für Verwaltungsfunktionen und sind nicht auf Cloud Identity Service-Benutzer, Gruppen und Services anwendbar.
Access for Groups	Zugriff für Gruppenmitglieder. Jedem Mitglied einer hinzugefügten Gruppe wird Zugriff auf die Ressource erteilt. Klicken Sie auf **Add Group**, um eine Gruppe hinzuzufügen. Um eine Gruppe zu suchen und auszuwählen, geben Sie mindestens die ersten drei Zeichen des Gruppennamens ein. Wählen Sie die Berechtigungen für jeden Eintrag aus.

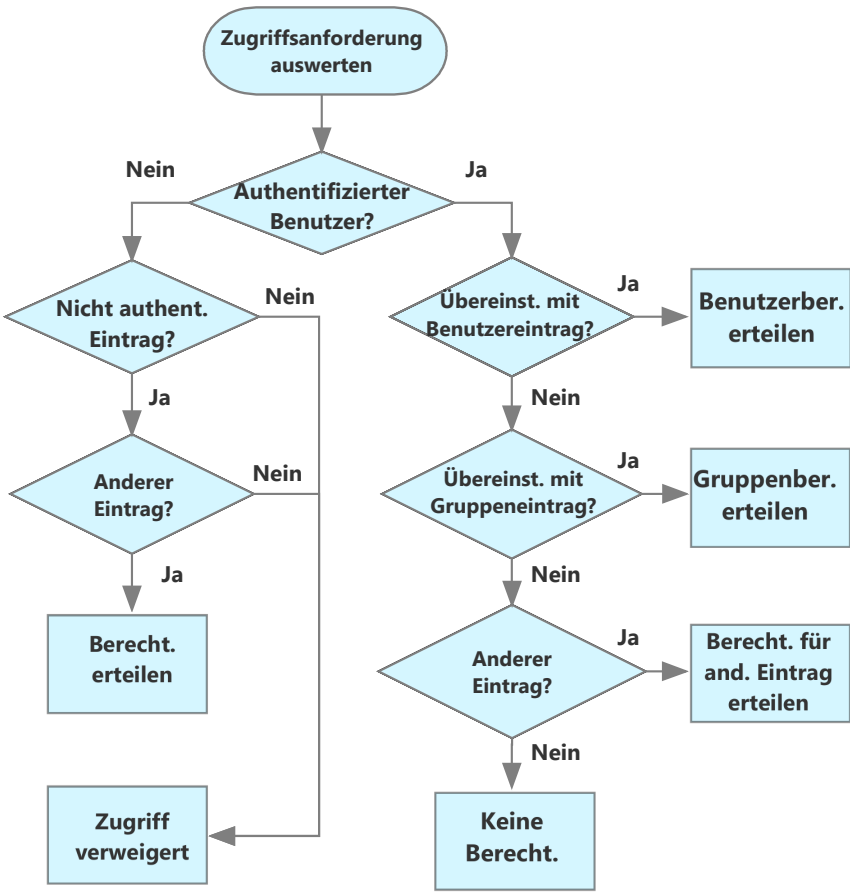
Einstellung	Beschreibung
Access for Services	Zugriff für Servicemitglieder. Jedem Mitglied eines hinzugefügten Service wird Zugriff auf die Ressource erteilt. Klicken Sie auf **Add Service**, um einen Service hinzuzufügen. Um einen Service zu suchen und auszuwählen, geben Sie mindestens die ersten drei Zeichen des Servicenamens ein. Wählen Sie die Berechtigungen für jeden Eintrag aus.
Unauthenticated Access	Gibt Zugriffsberechtigungen für nicht authentifizierte Benutzer an. Möglicherweise benötigen nicht authentifizierte Benutzer Berechtigungen. Vielleicht möchten Sie z. B. nicht authentifizierten Benutzern Zugriff auf Ressourcen, die sich weiter unten in der Hierarchie befinden, erteilen, indem Sie die Transitberechtigung festlegen. Um Berechtigungen zu erteilen, klicken Sie auf **Allow** und wählen Sie Berechtigungen für nicht authentifizierte Benutzer aus.
Any Other Access	Legt Zugriffsberechtigungen für alle anderen authentifizierten Benutzer fest, die nicht im Zugriff für Benutzer, Gruppen oder Services angegeben sind. Möglicherweise benötigen alle authentifizierten Benutzer Berechtigungen. Vielleicht möchten Sie z. B. allen authentifizierten Benutzern Zugriff auf Ressourcen, die sich weiter unten in der Hierarchie befinden, erteilen, indem Sie die Transitberechtigung festlegen. Um Berechtigungen zu erteilen, klicken Sie auf **Allow** und wählen Sie Berechtigungen für alle anderen authentifizierten Benutzer aus.

5. Klicken Sie auf **Save New ACL**.

Auswertung der Zugriffssteuerungsliste

Wenn Benutzer versuchen, auf eine geschützte Ressource zuzugreifen, wird die entsprechende Zugriffssteuerungsliste für die geschützte Ressource ausgewertet, um zu ermitteln, ob der Zugriff erteilt wird.

Der erste Schritt der Auswertung besteht darin, zu ermitteln, ob der Benutzer, der den Zugriff anfordert, über eine aktive Anmeldesitzung verfügt (d. h. authentifiziert ist) oder nicht (nicht authentifiziert).



Wenn ein authentifizierter Benutzer versucht, auf eine geschützte Ressource zuzugreifen, erfolgt die Auswertung in der folgenden Reihenfolge.

- Die Benutzer-ID wird mit den Zugriffssteuerungslisteneinträgen für die Benutzer abgeglichen. Die Auswertung stoppt, wenn ein entsprechender Benutzereintrag gefunden wird. Die erteilten Berechtigungen sind die Berechtigungen in dem entsprechenden Benutzereintrag.
- Wenn es keinen entsprechenden Benutzereintrag gibt, werden die Gruppen ermittelt, zu denen der Benutzer gehört. Diese Gruppen werden anschließend mit den Gruppeneinträgen in der Zugriffssteuerungsliste abgeglichen. Die Auswertung stoppt, wenn ein entsprechender Gruppeneintrag gefunden wird. Wenn mehrere entsprechende Gruppeneinträge gefunden werden, werden die Einträge mit den umfassendsten Berechtigungen angewandt.
- Wenn kein entsprechender Benutzer- oder Gruppeneintrag gefunden wird, werden die Berechtigungen für Sonstige (Any-other) erteilt, falls vorhanden.
- Wenn weder ein entsprechender Benutzer- oder Gruppeneintrag noch ein Eintrag für Sonstige (Any-other) gefunden wird, werden dem Benutzer keine Berechtigungen erteilt.

Wenn ein nicht authentifizierter Benutzer versucht, auf eine geschützte Ressource zuzugreifen, erfolgt die Auswertung auf folgende Weise.

- Wenn die Zugriffssteuerungsliste keinen Eintrag für nicht authentifizierte Benutzer enthält, wird der Zugriff verweigert.
- Wenn die Zugriffssteuerungsliste keinen Eintrag für Sonstige (Any-other) enthält, wird der Zugriff verweigert.

- Wenn die Zugriffssteuerungsliste einen Eintrag für nicht authentifizierte Benutzer und einen Eintrag für Sonstige (Any-other) enthält, werden die Berechtigungen für beide Einträge, nicht authentifizierte Benutzer und Sonstige, erteilt. Die nicht authentifizierten Benutzern erteilten Berechtigungen sind nicht umfassender als die Berechtigungen für den Eintrag für Sonstige.

Geschützte Objekte erstellen

Geschützte Objekte stellen die Elemente für den logischen Pfad dar, die über eine Verbindung zugänglich gemacht werden.

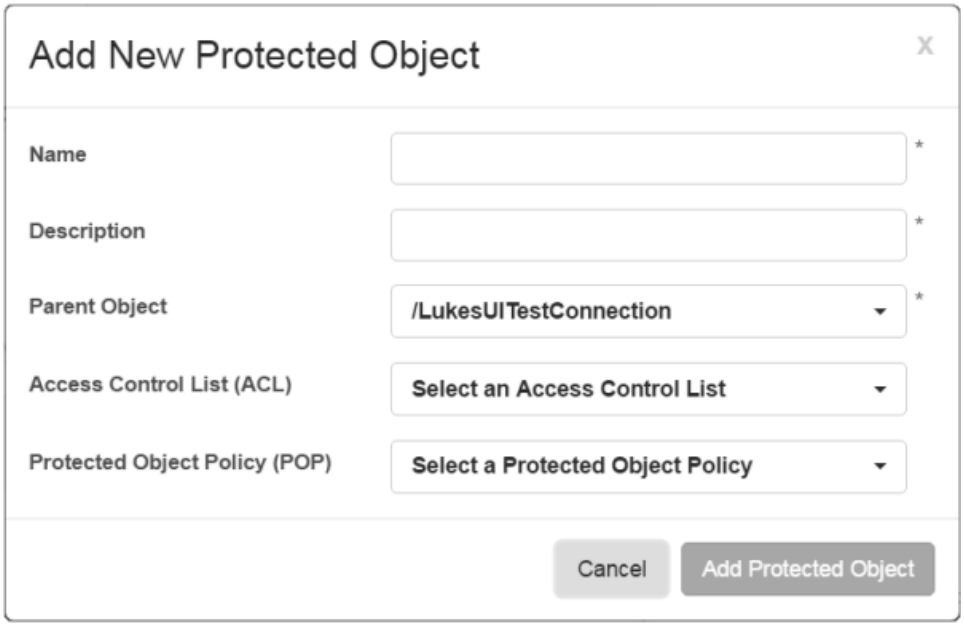
Informationen zu diesem Vorgang

Der Verbindungsobjektbereich stellt die logischen Pfade zu den geschützten Objekten aus der Verbindung dar. Zum Beispiel Pfade zu Verzeichnissen, Dateien, Programmen oder Speicherpositionen. Sie können so viele geschützte Objekte zu einer Verbindung hinzufügen, wie nötig. Sie können jedes vorhandene Objekt aus der inaktiven Verbindung auswählen, um eine Hierarchie zu erstellen, die so tief und komplex ist, wie nötig.

Sie können Zugriffssteuerungslisten (Access Control Lists, ACLs) und Richtlinien für geschützte Objekte (Protected Object Policies, POPs) an ein geschütztes Objekt anhängen. Wenn eine Richtlinie an ein Objekt angehängt wird, wird die Richtlinie auf das Objekt und alle untergeordneten Objekte angewandt. Eine geerbte Richtlinie wird außer Kraft gesetzt, wenn andere Richtlinien auf einer niedrigeren Ebene angehängt werden.

Vorgehensweise

1. Wenn die Verbindung, für die Sie ein geschütztes Objekt hinzufügen möchten, nicht geöffnet ist, suchen Sie die Verbindung und wählen Sie sie aus.
2. Klicken Sie auf **Add a New Protected Object** unter **Connection Object Space**.



3. Geben Sie einen Namen und eine Beschreibung ein.

Das geschützte Objekt muss nach dem Objekt benannt werden, das es darstellt. Wenn das Objekt z. B. eine Seite mit dem Namen `page1.jsp` darstellt, die sich am Stamm der Junction befindet, muss das Pfadobjekt mit dem Namen `page1.jsp` erstellt werden.

4. Geben Sie die übrigen Objekteinstellungen ein.

Einstellung	Beschreibung
Parent object	Das übergeordnete Objekt des geschützten Objekts. Das übergeordnete Objekt kann das Verbindungsobjekt oder ein beliebiges bereits vorhandenes geschütztes Objekt unterhalb der Verbindung sein.
Access Control List (ACL)	Die Zugriffssteuerungsliste, die an das Objekt angehängt wird.
Protected Object Policy (POP)	Die Richtlinie für geschützte Objekte, die an das Objekt angehängt wird.

5. Klicken Sie auf **Add Protected Object**.

Launchpad-Services verwalten

Im Self-Service-Portal können Webverbindungen und Webverbindungen für föderierte Partner über das Launchpad für Benutzer zur Verfügung gestellt werden. Benutzer müssen zu den entsprechenden Services hinzugefügt werden, damit sie über das Launchpad auf Webverbindungen zugreifen können.

Benutzer zu Launchpad-Services hinzufügen

Benutzer können über das Launchpad, einer einzelnen Position in ihrem Self-Service-Portal, auf Webanwendungen zugreifen.

Informationen zu diesem Vorgang

Für jede Webverbindung und Verbindung für einen föderierten Partner, die erstellt wird, wird ein entsprechender Service erstellt. Der Service erhält denselben Namen wie die Verbindung oder im Fall von föderierten Webanwendungen denselben Namen wie das Verbindungsalias. Damit die Webanwendung für einen Benutzer über das Launchpad zur Verfügung gestellt wird, muss der Benutzer zu dem entsprechenden Service hinzugefügt werden.

Anmerkung: Namen von nicht virtuellen Verbindungen beginnen mit einem normalen Schrägstrich, wie z. B. `/my_connection_1`. Die Servicenamen für nicht virtuelle Verbindungen beginnen ebenfalls mit einem normalen Schrägstrich.

Anmerkung: Wenn das Verbindungsalias für einen föderierten Partner geändert wird, wird ein neuer Service mit dem neuen Aliasnamen erstellt. Mitglieder des Service, der zuvor von der Verbindung verwendet wurde, werden zu dem neuen Service migriert und der alte Service wird entfernt.

Sie können Benutzer zu einem Service hinzufügen, indem Sie den Service manuell oder dynamisch mithilfe einer Richtlinie verwalten.

Vorgehensweise

Fügen Sie Benutzer zu einem Launchpad-Service hinzu.

- Fügen Sie Benutzer durch manuelle Verwaltung des Service hinzu.
- Fügen Sie Benutzer durch dynamische Verwaltung des Service hinzu.

Föderierten SSO-Webzugriff verwalten

Das Management des föderierten SSO-(Single Sign-on-)Webzugriffs umfasst das Management von Netzverbindungen zu Anwendungen anderer Anbieter. Föderiertes Single Sign-on (SSO) ermöglicht Benutzern mit einem Cloud Identity Service-Account, mithilfe ihrer vorhandenen Identität auf Anwendungsservices anderer Anbieter zuzugreifen.

Überblick über föderiertes SSO

Über föderiertes Single Sign-on (SSO) können Benutzer mit einem Cloud Identity Service-Account nahtlos auf Services zugreifen, die von einer oder mehreren Partnerorganisationen bereitgestellt werden, ohne eine separate Anmeldung bei der Partnersite.

Wenn ein Benutzer auf eine URL für föderierte Anmeldung klickt, erstellt Cloud Identity Service ein digital signiertes Token, das von der Partnerorganisation überprüft (und damit anerkannt) werden kann. Dieses Token wird vom Browser des Benutzers an die SSO-URL des Partners übergeben, unter der eine Sitzung eingerichtet wird.

Eine Beziehung zwischen föderierten Partnern beinhaltet zwei getrennte Rollen für die beiden beteiligten Parteien, den Identitätsprovider (IdP) und den Service-Provider (SP). Der Identitätsprovider liefert eine vertrauenswürdige Identität in Form eines digitalen Tokens. Der Service-Provider validiert das digitale Token, erstellt eine Sitzung für den Benutzer und erlaubt diesem den Zugriff auf seine Anwendungsumgebung. Cloud Identity Service ist der Identitätsprovider und der Partner ist der Service-Provider.

Eine einzelne Cloud Identity Service-Umgebung kann mehrere Föderationspartner unterstützen. Für jede URL für föderierte Anmeldung müssen Verbindungsdetails zu den Eigenschaften der Partnerföderation definiert werden. Jede Verbindung muss über ein Paar aus einem öffentlichen und einem privaten Schlüssel verfügen, die durch ein persönliches Zertifikat und ein Unterzeichnerzertifikat bereitgestellt werden.

Cloud Identity Portal bietet vorkonfigurierte Vorlagen für die gängigsten Partneranwendungsservices, die föderiertes Single Sign-on mit SAML 2.0 unterstützen. Wenn für den Partner, für den Sie eine Verbindung einrichten möchten, keine Vorlage vorhanden ist, kann eine kundenspezifische Konfiguration verwendet werden.

Schlüsselmanagement

Jede Verbindung muss über ein Paar aus einem öffentlichen und einem privaten Schlüssel verfügen. Diese Schlüssel werden durch ein persönliches Zertifikat und ein Unterzeichnerzertifikat bereitgestellt.

Ein Unterzeichnerzertifikat stellt ein Zertifikat und einen öffentlichen Schlüssel bereit, der einem persönlichen Zertifikat zugeordnet ist. Das Unterzeichnerzertifikat dient zur Überprüfung persönlicher Zertifikate Der Eigentümer des privates Schlüssels kann Verbindungen zu Partneranwendungsservices herstellen. Das Unterzeichnerzertifikat vertraut explizit Verbindungen zum Eigentümer des zugehörigen persönlichen Zertifikats oder von diesem hergestellte Verbindungen.

In Cloud Identity Portal ist ein einziges persönliches Zertifikat aktiviert. Sie müssen das zu verwendende persönliche Zertifikat nicht explizit auswählen, wenn Sie

eine Verbindung definieren. Das aktivierte persönliche Zertifikat wird standardmäßig für jede Verbindung verwendet, die Sie einrichten. Sie müssen für jede eingerichtete Verbindung das passende Unterzeichnerzertifikat auswählen. Unterzeichnerzertifikate werden normalerweise von Service-Providern bereitgestellt. Sie können Unterzeichnerzertifikate importieren. Sie können auch selbst signierte Zertifikate und Schlüssel für niedrige Empfindlichkeit, für andere Einsätze als in der Produktion oder für andere Anforderungen zum schnellen Gebrauch erstellen.

Verbindungsmanagement

Sie können eine beliebige Anzahl von Verbindungen zur Unterstützung einer beliebigen Anzahl föderierter Partner einrichten. Für die gängigsten Partneranwendungsservices werden eine Reihe vorkonfigurierter Vorlagen bereitgestellt. Mit diesen Vorlagen können Sie Verbindungen zu Ihren föderierten Partnern einrichten. Durch die Vorlagen werden so viele Partnerverbindungsdetails wie möglich vorkonfiguriert. Wenn für einen Partner keine Vorlage vorhanden ist oder wenn Sie eine Verbindung zu einer internen Anwendung oder einem internen Service einrichten möchten, können Sie eine Verbindung mit einer generischen Vorlage einrichten. Bei jeder erfolgreich eingerichteten Verbindung wird eine Anmelde-URL generiert. Über diese URL wird Single Sign-on bei Ihrem Partner eingeleitet.

Einige Provider ermöglichen das Erstellen von Benutzerdatensätzen durch den Service-Provider beim ersten erfolgreichen Anmeldeversuch eines Benutzers. Das Erstellen von Benutzerdatensätzen wird als automatische Einrichtung (Autoprovisioning) bezeichnet.

Föderierte Partnerverbindungen verwalten

Partnerverbindungen verwalten

Verbindungen zu föderierten Webanwendungen suchen

Sie können nach Netzverbindungen zu föderierten Webanwendungen suchen, um eine Verbindung anzuzeigen, zu ändern oder zu löschen.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Applications** > **Connection Management** und dann auf **Federated Applications**.
2. Geben Sie im Feld **Search** mindestens die ersten drei Zeichen der Verbindung ein. Die Feldbeschriftung ändert sich in **Searching For**.

   Die Ihren Suchkriterien entsprechenden Verbindungen werden aufgelistet. Wählen Sie eine Verbindung aus, die Sie ändern oder anzeigen möchten.

Verbindung zu einem föderierten Partner hinzufügen

Sie können eine beliebige Anzahl von Verbindungen zur Unterstützung einer beliebigen Anzahl föderierter Partner einrichten. Für die gängigsten Partneranwendungsservices werden eine Reihe von vorkonfigurierten Vorlagen bereitgestellt.

Informationen zu diesem Vorgang

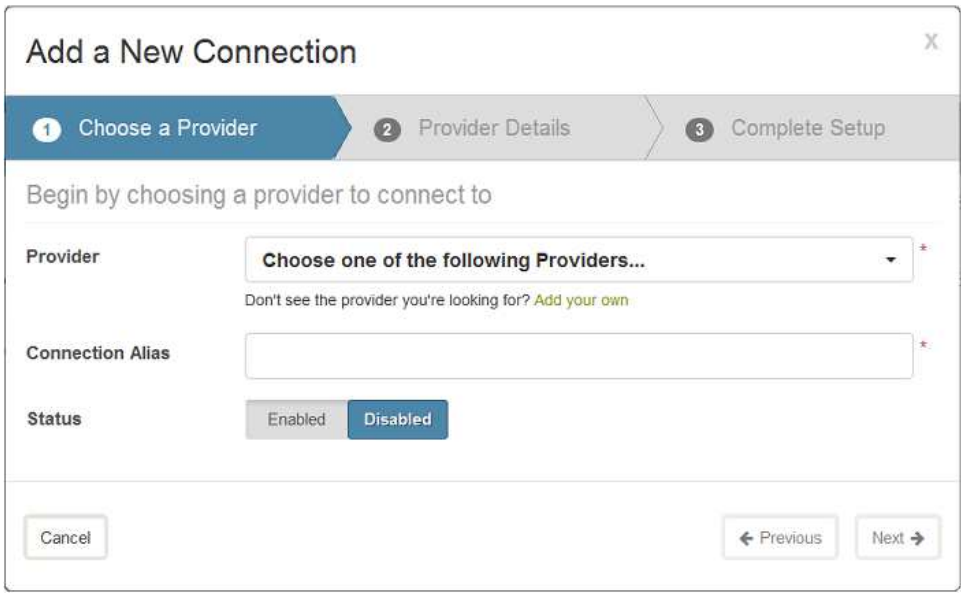
Cloud Identity Portal bietet eine Reihe von Vorlagen zum Hinzufügen von Verbindungen für föderierte Partner. Sie können eine Verbindung zu anderen Providern hinzufügen, indem Sie eine generische Vorlage verwenden. Mit der generischen Vorlage können Sie auch Verbindungen für interne Anwendungen erstellen.

Einige Provider ermöglichen das Erstellen von Benutzerdatensätzen durch den Service-Provider beim ersten erfolgreichen Anmeldeversuch eines Benutzers. Für Part-

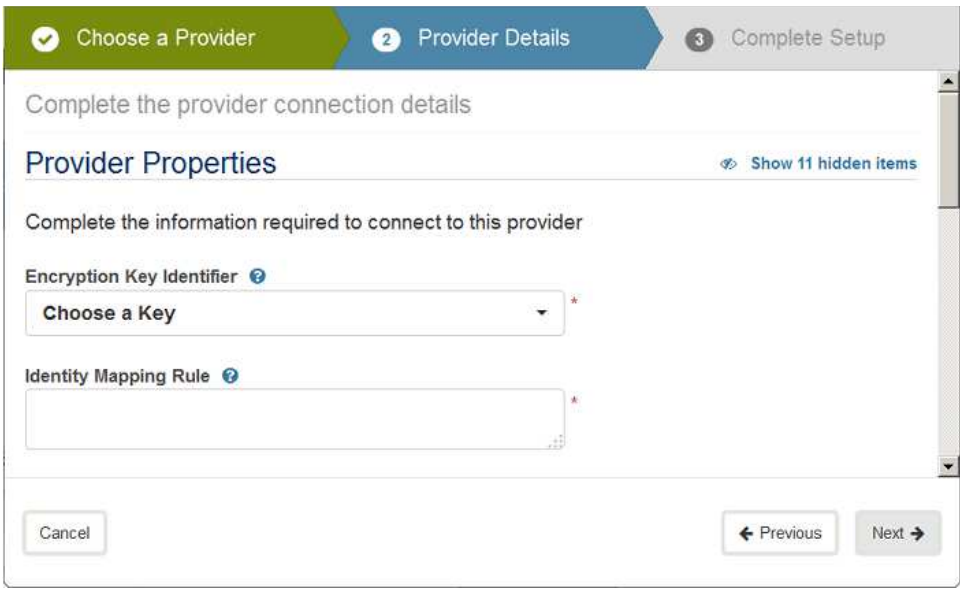
ner sind Vorlagen zur automatischen Einrichtung verfügbar, die das Erstellen von Benutzerdatensätzen ermöglichen. Für die automatische Einrichtung von Benutzerdatensätzen benötigen Service-Provider normalerweise zusätzliche Informationen. Diese zusätzlichen Informationen werden bereitgestellt, indem LDAP-Attribute aus Cloud Identity Service entsprechenden Partnerattributen zugeordnet werden.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Applications** > **Connection Management** und klicken Sie dann auf **Federated Applications** > **Add a New Connection**.



2. Wählen Sie den Providernamen im Menü **Provider** aus.
   - Um eine auf einer Partnervorlage basierende Verbindung einzurichten, wählen Sie den Provider im Menü **Provider** aus. Provider werden, wenn möglich, durch ein Symbol gekennzeichnet. Wenn kein Providersymbol verfügbar ist, wird ein allgemeines Symbol verwendet.
   - Um eine Verbindung für einen Partner, der über keine Vorlage verfügt, oder für eine interne Anwendung einzurichten, klicken Sie auf **Add your own** oder wählen Sie **Generic SAML2.0 Service Provider** im Menü **Provider** aus.
3. Geben Sie den Verbindungsalias im Feld **Connection Alias** ein.
4. Klicken Sie auf **Next**.



5. Geben Sie die Details zu den Providereigenschaften ein.

   Anmerkung: Die Angabe aller verbindlichen Felder ist nicht möglich, da die Validierung einer Verbindung auf der Serverseite erfolgt.

   Anmerkung: Für auf einer Vorlage basierende Verbindungen werden eine Reihe von Details für Sie eingegeben. Die vorausgefüllten Standardfelder werden während der Einrichtung der Verbindung ausgeblendet. Wenn Sie die Standardfelder anzeigen oder bearbeiten möchten, klicken Sie auf **Show hidden items**. Sie können die Werte oder die Einstellungen für Standardfelder bearbeiten. Das Ändern der Einstellungen oder Werte für Standardfelder kann die Verbindung ungültig machen.

   Um die Standardfelder zu bearbeiten, klicken Sie auf **Enable editing of default fields**. Eine Warnung wird angezeigt. Klicken Sie auf **Enable Fields**, um Standardfelder zu bearbeiten.

   Wichtig: Für Clarizen-Verbindungen kann die URL des Assertion Consumer Service abhängig von der Clarizen-Umgebung, die Sie verwenden, einen der folgenden Werte aufweisen:

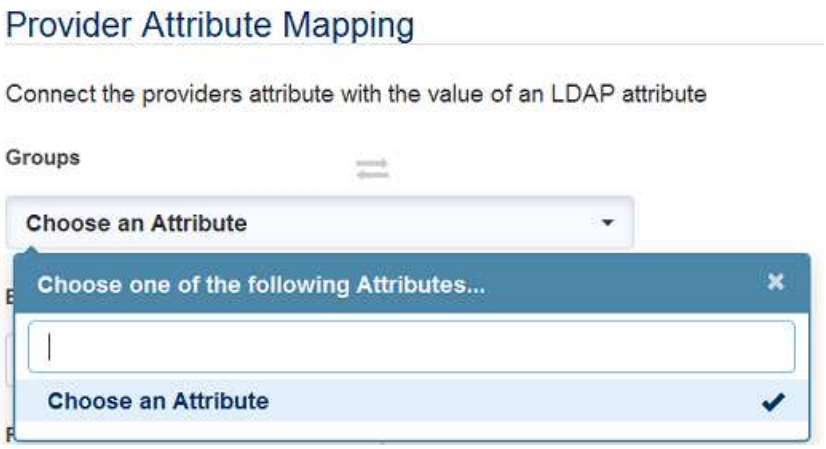
   - EU-Umgebung. `https://eu1.clarizen.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx`
   - SV-Umgebung. `https://app2.clarizen.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx`
   - TB-Umgebung. `https://app.clarizentb.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx`

   Der Standardwert in der Vorlage ist `https://app2.clarizen.com/Clarizen/Pages/Integrations/SAML/SamlResponse.aspx`. Wenn Sie diesen Wert ändern müssen, verwenden Sie die Option **Enable editing of default fields**.

6. Für Provider, die Attributzuordnungen erfordern, geben Sie die Providerattributzuordnungen ein.

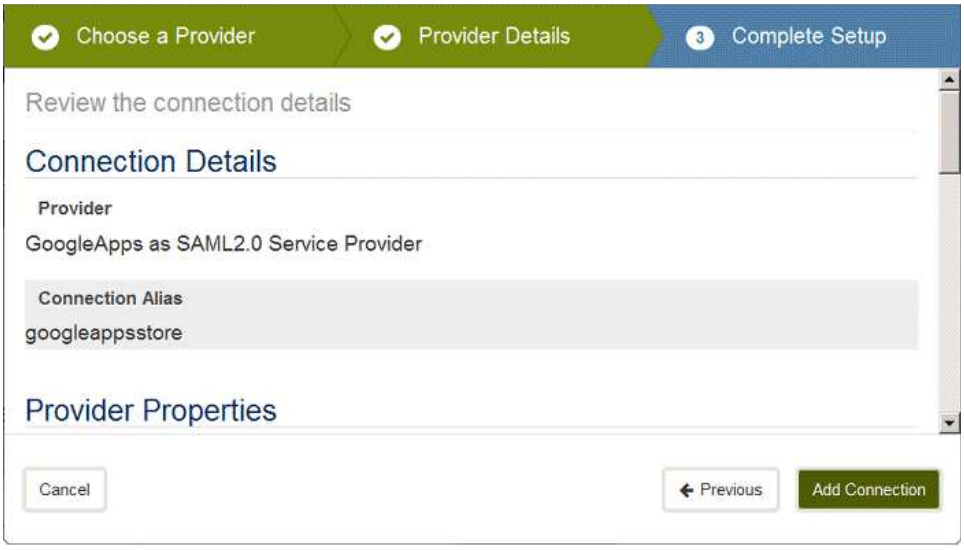
   Einige Provider erfordern, dass eine Reihe von Attributen den LDAP-Attributen von Cloud Identity Service zugeordnet werden. Zugeordnete Attribute werden in die SAML-Zusicherung geladen und vom Service-Provider zur Identifizierung des Benutzers verwendet. Der im LDAP-Attribut gespeicherte Wert wird

einer Variablen für den Provider zugeordnet.



7. Optional: Geben Sie ein Attribut ein und ordnen Sie es anderen Attributen zu. Wenn der Provider Attributzuordnungen akzeptiert, können Sie andere Attribute hinzufügen.
   a. Geben Sie den Namen des Partnerattributs im Feld **Add an Attribute Mapping** ein und klicken Sie auf **Add Attribute**.

   b. Wählen Sie das zuzuordnende LDAP-Attribut im Feld **Choose an Attribute** aus.
8. Klicken Sie auf **Next**.



9. Klicken Sie auf **Add Connection**.

Verbindungseinstellungen für föderierte Partner:

Verbindungseinstellungen für föderierte Partner umfassen Verbindungsaliasse, Status, Anmelde-URL, Attributzuordnungseigenschaften und Service-Provider-Eigenschaften.

Tabelle 36. Providerinformationen

Einstellung	Beschreibung
Provider	Der Service-Provider.
Connection Alias	Der Verbindungsalias.
Status	Der Verbindungsstatus. Wenn die Verbindung inaktiviert ist, schlägt sie fehl.
Sign-On URL	Die URL, über die Single Sign-on zu Ihrem Partner eingeleitet wird.

Tabelle 37. Attributzuordnungen

Einstellung	Beschreibung
Provider Attribute Mapping	Erforderliche Providerattributzuordnungen. Einige Provider erfordern, dass eine Reihe von Attributen den Cloud Identity Service-LDAP-Attributen zugeordnet werden. Die erforderlichen Attribute werden in die SAML-Zusicherung geladen und vom Service-Provider zur Identifizierung des Benutzers verwendet.
Add an Attribute Mapping	Optionale Attributzuordnungen.

Tabelle 38. Providereigenschaften

Einstellung	Beschreibung
Assertion Consumer Service URL	Der Endpunkt des Service-Providers, der Zusicherungen empfängt.
Company Name	Der Firmenname des Service-Providers.
Enabled	Gibt an, ob dem Partner aktiviert ist. Wenn der Partner nicht aktiviert ist, schlägt die Verbindung fehl.
Encrypt Assertion	Gibt an, ob Zusicherungen verschlüsselt werden.
Encrypt Assertion Attributes	Gibt an, ob Zusicherungsattribute verschlüsselt werden.
Encryption Key Identifier	Der Name des Chiffrierschlüssels.
Encrypt Name Id	Gibt an, ob die Namens-IDs verschlüsselt werden müssen.
Identity Mapping Rule	Eine optionale interne JavaScript-Zuordnungsregel zum Ändern der Informationen, die erforderlich sind, um ein SAML-2.0-Token zu erstellen. Der Inhalt der JavaScript-Zuordnungsregel muss angegeben werden.
Identity Mapping Rule Reference	Eine optionale interne JavaScript-Zuordnungsregel zum Ändern der Informationen, die erforderlich sind, um ein SAML-2.0-Token zu erstellen. Ein relativer URI zu einer JavaScript-Zuordnungsregel, die von der REST-API für Zuordnungsregeln verwaltet wird, muss angegeben werden, z. B. `/iam/access/v8/mapping-rules/mapping_rule_id`. Wenn **`identityMappingRuleReference`** angegeben wird, hat dies Vorrang vor **`identityMappingRule`**.
Provider Id	Eine eindeutige ID des Service-Providers.
Session Not On Or After	Die Anzahl von Sekunden, nach der der für den Principal eingerichtete Sicherheitskontext vom Service-Provider verworfen werden muss.
Sign Assertion	Gibt an, ob die Zusicherungen unterzeichnet werden müssen.

Tabelle 38. Providereigenschaften (Forts.)

Einstellung	Beschreibung
Signature Validation Key Identifier	Der Name des Signaturprüfschlüssels.
Sign Authn Response	Gibt an, ob die Authentifizierungsantworten unterzeichnet werden müssen.
Validate Authn Request	Gibt an, ob die digitale Signatur einer Authentifizierungsanforderung geprüft werden muss.

Partnerseitige Konfiguration mit schneller Verbindungserstellung

Partnerseitige Konfiguration mit schneller Verbindungserstellung über Single Sign-on (SSO).

Für einen in Cloud Identity Service konfigurierten Partner muss die über die Vorlage für schnelle Verbindungserstellung generierte Anmelde-URL Benutzern bereitgestellt werden. Die Anmelde-URL ermöglicht Benutzern, sich bei einer Partnersite über SAML-SSO anzumelden, indem sie einen Link verwenden, den normalerweise Cloud Identity Service Benutzern zur Verfügung stellt. Bei einer partnerseitigen Konfiguration muss ein Administrator die Anmelde-URL von Cloud Identity Service und ein SAML-Zusicherungsprüfungszertifikat zum Konfigurieren der SAML-2.0-SSO-Einstellungen für den Service-Provider-Partner verwenden. Bei der partnerseitigen Konfiguration wird auch ein Prozess oder eine Methode zum Erstellen von Benutzern auf Partnerseite verwendet. Einige Partner unterstützen Just-in-time-(JIT-)Einrichtung. Wenn bei der JIT-Einrichtung ein Cloud Identity Service-Benutzer auf Partnerseite nicht vorhanden ist, wird der Benutzer automatisch anhand der Attribute erstellt, die bei der SAML-Zusicherung weitergeleitet werden.

Damit SSO für alle Partner funktioniert, muss der Cloud Identity Service-Benutzername normalerweise mit dem Benutzernamen übereinstimmen, der vom Service-Provider verwendet wird. Ausgenommen von dieser Anforderung sind Partner, bei denen JIT-Einrichtung aktiviert ist. In diesem Fall ist das SAML-Subjekt einer Föderations-ID auf Service-Partner-Seite zugeordnet.

Einstellungen für schnelle Verbindungserstellung auf Partnerseite

Damit Single Sign-on mit den vorkonfigurierten Föderationsvorlagen für schnelle Verbindungserstellung funktioniert, dürfen einige partnerseitige Einstellungen nur bestimmte Werte oder Einstellungen verwenden. In der folgenden Tabelle sind nicht alle partnerseitigen SAML-2.0-Einstellungen aufgelistet. In der Tabelle werden bestimmte Einstellungen aufgelistet, bei denen die Föderationsvorlagen nur bestimmte Werte oder Optionen unterstützen.

Administratoren können Eigenschaften der Föderationsvorlagen für schnelle Verbindungserstellung auf Connectorebene außer Kraft setzen. Cloud Identity Service unterstützt sowohl vom Identitätsprovider (IdP) als auch vom Service-Provider (SP) initiiertes SSO.

Anmerkung: SAML-Zusicherungen (Antworten) an alle SPs werden mit dem gleichen Schlüssel signiert.

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
ADFS	1. Auf der Registerkarte **Advanced** der "ADFS Claim Provider Trusts Properties", muss **Secure Hash Algorithm** auf **RSA-SHA1** eingestellt sein. 2. SAML-2.0-Authentifizierungsanforderungen müssen nicht durch ADFS signiert werden.	nein	SP
Adobe Creative Cloud	nicht zutreffend	nein	SP
Adobe Echo Sign Provisioning	nicht zutreffend	nein	IdP und SP
Agiloft	nicht zutreffend	ja	SP
Aha	nicht zutreffend	ja	IdP und SP
Amazon Web Services (AWS)	• Erstellen Sie eine IAM-Rolle für SSO in AWS. Die IAM-Rolle führt Vertrauen zum Identitätsprovider ein und definiert Berechtigungen für den föderierten Benutzer. • Wählen Sie **Role for Identity Access** mit der Option **Grant Web SSO access to SAML providers** aus. • Die Felder **Role** und **RoleSessionName** sind für die SAML-Zusicherung erforderlich.	nein	IdP
ANCILE uAlign			IdP und SP
AnswerHub			IdP und SP
ArcGIS		ja	IdP und SP
Asana	nicht zutreffend	nein	IdP und SP
Assembla			IdP
BambooHR	nicht zutreffend	nein	IdP und SP
BIME	nicht zutreffend	nein	SP
Bitium	nicht zutreffend	nein	IdP und SP
BlueJeans	Für durch den IdP initiiertes SSO muss der RelayState in der Ziel-ID eingegeben werden.	ja	IdP und SP
Bonusly	nicht zutreffend	nein	IdP und SP
Boomi AtomSphere		nein	IdP und SP

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung (Forts.)

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
Box	Sowohl für aktivierte als auch für inaktivierte automatische Einrichtung sind die folgenden Einstellungen erforderlich. 1. Die SAML-Anforderung muss für vom SP initiiertes SSO signiert werden. 2. Der Signaturalgorithmus zum Signieren der SAML-Anforderung muss RSA-SHA1 sein. 3. Wenn BOX-Gruppen und E-Mail-Aliasse über eine SAML-Zusicherung gesendet werden sollen, müssen die folgenden Attributnamen verwendet werden: • Für BOX-Gruppen verwenden Sie `groups` als Attributnamen. • Für BOX-E-Mail-Aliasse verwenden Sie `email_aliases` als Attributnamen. Wenn automatische Einrichtung für BOX aktiviert ist, müssen die folgenden Attributnamen verwendet werden. 1. Für "First Name"/"GivenName" verwenden Sie `firstname` (Vorname) als Attributnamen. 2. Für "Last Name"/"Surname" verwenden Sie `lastname` (Nachname) als Attributnamen.	ja	IdP und SP
Brightcove	nicht zutreffend	nein	IdP und SP
Chatter	Chatter ist in einem Salesforce-Entwickleraccount verfügbar. Informationen zur SAML-SSO-Konfiguration finden Sie unter SAML-Einstellungen für Salesforce.	ja	IdP und SP
Citrix-Anwendungen	Eine eigene Ziel-ID für die einzelnen Anwendungen ist für vom SP initiiertes SSO erforderlich. Citrix-Anwendungen. • Citrix OpenVoice • Citrix Online • GoTo Assist • GoToAssist Concierge • GoToAssist Remote Support • GoToAssist Seeit • GoToAssist ServiceDesk • GoTo Webinar		
Citrix Sharefile		nein	IdP und SP
Clarizen	nicht zutreffend	nein	IdP und SP
ClearSlide	nicht zutreffend	ja	IdP und SP

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung (Forts.)

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
Cloud Drop	• Ein Salesforce-Entwickleraccount muss verfügbar sein. Informationen zur SAML-SSO-Konfiguration finden Sie unter SAML-Einstellungen für Salesforce. • Suchen Sie in Salesforce AppExchange nach der App "Cloud Drop" und installieren Sie sie im Salesforce-Entwickleraccount.	ja	IdP und SP
Cloud Passage	Für aktivierte automatische Einrichtung sind die folgenden Einstellungen erforderlich. • **admin**. Um anzugeben, ob der Benutzer ein Halo-Siteadministrator ist. • **ghostport_access**. Um anzugeben, ob der Benutzer ein GhostPorts-Benutzer ist. • **portal_access**. Um anzugeben, ob der Benutzer über Zugriff auf Portal verfügt. • **firstname**. • **lastname**. • **email**. • **sms**. Die Mobiltelefonnummer des Benutzers zum Empfangen von SMS-Authentifizierungscodes. • **Yubikey (optional)**. Der YubiKey-Schlüsselwert des Benutzers. • **Account ID**. Die ID des Halo-Accounts Ihrer Organisation für den Identitätsprovider. Diese wird in der Zusicherung als Consumer-URL weitergeleitet.	ja	IdP
Concur	nicht zutreffend	nein	IdP
CrashPlan	nicht zutreffend	nein	IdP
Data.com	Data.com ist in einem Salesforce-Entwickleraccount verfügbar. Informationen zur SAML-SSO-Konfiguration finden Sie unter SAML-Einstellungen für Salesforce.	ja	IdP und SP
Datadog	Eine eigene ACS-URL ist für von IdP und von SP initiiertes SSO erforderlich. • IdP. `https://app.datadoghq.com/account/saml/assertion/id/`*`AccountID`* • SP. `https://app.datadoghq.com/account/saml/assertion`	ja	IdP und SP
Desk.com	nicht zutreffend	ja	IdP und SP
DeskPRO	nicht zutreffend	ja	IdP und SP
DocuSign	nicht zutreffend	nein	IdP und SP
Dropbox	nicht zutreffend	nein	IdP und SP

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung (Forts.)

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
DupeBlocker	• Ein Salesforce-Entwickleraccount muss verfügbar sein. Informationen zur SAML-SSO-Konfiguration finden Sie unter SAML-Einstellungen für Salesforce. • Suchen Sie in Salesforce AppExchange nach der App "DupeBlocker" und installieren Sie sie im Salesforce-Entwickleraccount.	ja	IdP und SP
Egnyte	• Stellen Sie **Default user mapping** auf **Email address** ein. • Stellen Sie **Use Domain specific issuer value** auf **Enabled** ein. Die URL lautet `https://`*`Egnyte-Domäne`*`.egnyte.com`.	nein	IdP und SP
eSignLive		ja	IdP und SP
Fairsail		ja	IdP und SP
GitHub	nicht zutreffend	ja	IdP und SP
Google Analytics	Wie SAML-Einstellungen für Google Apps.	nein	IdP und SP

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung (Forts.)

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
Google Apps	• Die Google Apps-Vorlage unterstützt in der Standardeinstellung keinen domänenspezifischen Aussteller. Als Aussteller-/Provider-ID wird nur ein statischer Wert von `google.com` unterstützt. • Wenn SAML-2.0-SSO für Google Apps konfiguriert ist, darf die Option **Use a Domain specific issuer** nicht ausgewählt werden. • Der Domänenname muss geprüft werden. • Für vom SP initiiertes SSO muss für jede Anwendung die jeweilige Ziel-ID in der URL angegeben werden. Google Apps-Anwendungen. • Google Admin • Google Books • Google Code • Google Drive • Google Forms • Google Groups • Google Hangouts • Google Keep • Google Maps • Google Photos • Google Play • Google Sheets • Google Slides • Google Translate • Google Trends • Google Videos • Google + • Blogger • Gmail	nein	IdP und SP
Google Calendar	Wie SAML-Einstellungen für Google Apps.	nein	IdP und SP
Google Docs	Wie SAML-Einstellungen für Google Apps.	nein	IdP und SP
Google Finance	Wie SAML-Einstellungen für Google Apps.	nein	IdP und SP
Google Site	Wie SAML-Einstellungen für Google Apps.	nein	IdP und SP
GoToMeeting	Eine gültige Domäne für Ihre Organisation muss für SAML-2.0-SSO registriert und geprüft werden.	nein	IdP und SP
Greenhouse	nicht zutreffend	ja	IdP und SP

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung (Forts.)

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
HappyFox	nicht zutreffend	ja	IdP und SP
Huddle	nicht zutreffend	ja	IdP und SP
IBM® Bluemix	nicht zutreffend	ja	IdP und SP
IBM Blueworks Live	nicht zutreffend	ja	IdP und SP
IBM Cloud Security Enforcer	• Geben Sie eine Authentifizierungs-URL und eine Ziel-URL für den Zugriff über Dashboard und Launchpad ein, z. B.: – `https://`*`mein_Domänenname`*`/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=https://`*`Partnerprovider_Domänenname`*`/idaas/mtfim/sps/idaas/saml20&NameIdFormat=Email&Target=https://`*`Partnerprovider_Domänenname`*`/ui/launchpad` – `https://`*`mein_Domänenname`*`/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=https://`*`Partnerprovider_Domänenname`*`/idaas/mtfim/sps/idaas/saml20&NameIdFormat=Email&Target=https://`*`Partnerprovider_Domänenname`*`/ui/dashboard` • Um den Zugriff auf das Dashboard sicherzustellen, muss die SAML-Zusicherung das Attribut **`groups`** mit dem Wert **`admin`** enthalten.	nein	IdP und SP
IBM Connections Cloud	Für durch den IdP initiiertes SSO muss für jede Anwendung die Ziel-ID angegeben werden. IBM Connections Cloud-Anwendungen. • IBM Connections Activities • IBM Connections Chat • IBM Connections Files • IBM Connections Meetings • IBM Connections Notebook • IBM Connections ToDo • IBM SmartCloud Notes Web • IBM Verse	nein	IdP und SP
IBM Kenexa Talent Suite		nein	IdP und SP
IBM MaaS360		nein	SP
IBM Softlayer	nicht zutreffend	nein	IdP

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung (Forts.)

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
Igloo Software	Die Provider-ID und die Ziel-ID müssen in der ACS-URL (Assertion Consumer Service) angegeben werden.	ja	IdP und SP
Informatica Cloud		ja	IdP und SP
Intacct	Die **SSO Issuer URL** für Intacct muss `https://saml.intacct.com` lauten.	nein	IdP und SP
Invision	nicht zutreffend	nein	IdP
JIRA (Altassian)	nicht zutreffend	nein	IdP und SP
Kanban Tool			IdP und SP
kiteworks	nicht zutreffend	ja	IdP und SP
Knowledge	Ein Salesforce-Entwickleraccount muss verfügbar sein. Informationen zur SAML-SSO-Konfiguration finden Sie unter SAML-Einstellungen für Salesforce.	ja	IdP und SP
Lesson.ly		nein	IdP und SP
LiquidPlanner	nicht zutreffend	nein	IdP und SP
Litmos			IdP
LivePerson	nicht zutreffend	nein	IdP
LogMeIn	Geben Sie eine Authentifizierungs-URL und eine Ziel-URL ein, z. B.: • `https://mein_Domänenname/isam/mtfim/sps/saml20ip/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://accounts.logme.in&NameIdFormat=Email&Target=https://secure.logmein.com/central/Central.aspx`	ja	IdP und SP
Lucidchart	Aktivieren Sie in SAML die Option **Send Nameid format in SAML Request**.	ja	IdP und SP
Mozy	Geben Sie eine Authentifizierungs-URL ein, die über **`RequestBinding`**, **`PartnerID`** und **`NameIDFormat`** verfügt, z. B.: • `https://eigene_Domäne/isam/mtfim/sps/saml20ip/saml20/logininitial?RequestBinding=HTTPPost&PartnerId=https://auth2.mozy.com/Mozy-Domäne/saml&NameIdFormat=Email`	nein	IdP und SP
Namely	nicht zutreffend	nein	IdP und SP
NetSuite	nicht zutreffend	nein	IdP
New Relic	nicht zutreffend	nein	IdP und SP

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung (Forts.)

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
Office 365	• Melden Sie sich bei Microsoft Office 365 an und fügen Sie eine Domäne hinzu. • Prüfen Sie die Domäne. • Föderieren Sie die Domäne mithilfe von PowerShell-Befehlen. Verwenden Sie das Azure Active Directory Module für das PowerShell-Tool von Windows.	nein	SP
Okta	nicht zutreffend	ja	IdP und SP
OneDrive/ SkyDrive	OneDrive ist in einem Office 365-Account verfügbar. Weitere Informationen finden Sie unter SAML-Einstellungen für Office 365.	nein	SP
OpenDataSoft	Die Ziel-ID muss in der SSO-URL angegeben werden.	nein	IdP und SP
OpenDNS		nein	IdP und SP
PagerDuty	nicht zutreffend	ja	IdP und SP
ProofHQ	nicht zutreffend	ja	IdP und SP
Redbooth	nicht zutreffend	nein	IdP und SP
Remedyforce	Besorgen Sie sich einen Remedyforce-Account. Informationen zur SAML-SSO-Konfiguration finden Sie unter SAML-Einstellungen für Salesforce.	ja	IdP und SP
Roambi Business	Die Ziel-ID muss in der SSO-URL angegeben werden.	nein	IdP und SP
Sales Cloud	Registrieren Sie sich für einen Salesforce Service Cloud-Account. Informationen zur SAML-SSO-Konfiguration finden Sie unter SAML-Einstellungen für Salesforce.	ja	IdP und SP
Salesforce	Wenn JIT-Einrichtung aktiviert ist, sind die folgenden Einstellungen erforderlich: • **Request Signature Method** muss auf **RSA-SHA1** eingestellt sein. • **Assertion Decryption Certificate** muss auf **Assertion not encrypted** eingestellt sein. • **SAML Identity Location** muss auf **Identity is in the NameIdentifier element of the Subject statement** eingestellt sein. • **Service Provider Initiated Request Binding** muss auf **HTTP Redirect** eingestellt sein. • **SAML Identity Type** muss auf **Federation ID from the User object** eingestellt sein. • **User Provisioning Type** muss auf **Standard** eingestellt sein.	ja	IdP und SP
Samanage	nicht zutreffend	ja	IdP und SP

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung (Forts.)

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
SAP Netweaver		nein	IdP und SP
Service Cloud	Registrieren Sie sich für einen Salesforce Service Cloud-Account. Informationen zur SAML-SSO-Konfiguration finden Sie unter SAML-Einstellungen für Salesforce.	ja	IdP und SP
ServiceNow	nicht zutreffend	nein	IdP und SP
SharePoint Online	SharePoint Online ist in einem Office 365-Account verfügbar. Weitere Informationen finden Sie unter SAML-Einstellungen für Office 365.	nein	SP
Skilljar		ja	IdP und SP
Slack	Für **Service Provider ID** muss `https://`*`Domänenname`*`.slack.com/` festgelegt sein.	ja	IdP und SP
Small Improvements		nein	IdP und SP
Soonr Workplace	nicht zutreffend	nein	IdP und SP
SpringCM	Geben Sie eine Authentifizierungs-URL und eine Ziel-URL ein, z. B.: • `https://`*`ISAM_Domänenname`*`/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=https://`*`Partner_Domänenname`*`/atlas/sso&NameIdFormat=Email&Target=https://`*`Partnerprovider_Domänenname`*`/atlas/Documents/BrowseDocuments.aspx?aid=`*`ID`*	nein	IdP und SP
StatusPage	nicht zutreffend	nein	IdP und SP
SuccessFactors	Die folgenden Einstellungen sind erforderlich. • **Require Mandatory Signature** muss auf **Assertion** eingestellt sein. • **Enable SAML Flag** muss auf **Enabled** eingestellt sein. • **SAML Profile** muss auf **Browser/Post Profile** eingestellt sein. • **NameID Format** muss auf **unspecified** eingestellt sein. • **Enable sp initiated login (AuthnRequest)** muss auf **Yes** eingestellt sein. • **Default issuer** muss ausgewählt sein.	nein	IdP und SP
SugarCRM	nicht zutreffend	nein	IdP und SP
Symantec Endpoint Manager			IdP und SP
Syncplicity	nicht zutreffend	nein	SP

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung (Forts.)

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
Tableau			IdP und SP
TOPdesk		nein	IdP und SP
Unifyle	nicht zutreffend	ja	IdP und SP
UserVoice			IdP und SP
Ustream		nein	IdP und SP
VersionOne	Die Ziel-ID muss in der SSO-URL angegeben werden.	nein	IdP und SP
WalkMe	• Ein Salesforce-Entwickleraccount muss verfügbar sein. Informationen zur SAML-SSO-Konfiguration finden Sie unter SAML-Einstellungen für Salesforce. • Installieren Sie die App "WalkMe" im Salesforce-Entwickleraccount.	ja	IdP und SP
WebEx	• In der SAML-Zusicherung muss für **NameID Format** "email" festgelegt sein. • Wenn in Cloud Identity Portal ein Benutzer erstellt wird, müssen **`UID`** und **`gtwayPrincipalName`** unterschiedlich sein. **`gtwayPrincipalName`** muss im E-Mail-Format angegeben werden und bei **`UID`** muss es sich um den Benutzernamen vom Provider handeln.	ja	IdP und SP
WordPress	nicht zutreffend	ja	IdP und SP
Workday	• Für durch den IdP und den SP initiiertes SSO muss die Option **Service Provider ID** auf `http://www.workday.com/` eingestellt sein. • Für durch den SP initiiertes SSO muss die Option **Do Not Deflate SP-initiated Authentication Request** aktiviert sein. • Die Option **Sign SP-Initiated Authentication Request** muss inaktiviert sein.	nein	IdP und SP
Yammer	Yammer ist in einem Office 365-Account verfügbar. Weitere Informationen finden Sie unter SAML-Einstellungen für Office 365.	nein	SP
Zendesk	nicht zutreffend	nein	IdP und SP

Tabelle 39. SAML-2.0-Einstellungen für Föderationsvorlagen für schnelle Verbindungserstellung (Forts.)

Partner	Anwendungen und SAML 2.0-Einstellungen	Unterstützung für automatische Einrichtung	Von IdP oder SP initiiertes SSO
Zoho-Anwendungen	nicht zutreffend Zoho-Anwendungen. • Site 24x7 (Service Desk Plus) • ZoHo Books • Zoho Bugtracker • Zoho Campaigns • Zoho Chat • Zoho Connect • Zoho CRM • Zoho Docs • Zoho Forms • Zoho Invoice • Zoho Mail • Zoho Meeting • Zoho Projects • Zoho Reports • Zoho SalesIQ • Zoho Sites • Zoho Social • Zoho Support • Zoho Survey • Zoho Vault	nein	IdP und SP
Zscaler	Sowohl bei aktiver als auch bei inaktiver automatischer Einrichtung muss für durch den IdP initiiertes SSO die Ziel-ID an die Anmelde-URL angehängt werden, z. B.: • `https://eigene_Domäne/isam/mtfim/sps/saml20ip/saml20/logininitial?PartnerId=zscalerbeta.net&Target=http://gateway.zscalerbeta.net/test`	ja	IdP und SP
Zuora	Für die IdP-SSO-Anmeldung muss die föderierte ID angegeben werden.	nein	IdP

Launchpad-Services verwalten

Im Self-Service-Portal können Webverbindungen und Webverbindungen für föderierte Partner über das Launchpad für Benutzer zur Verfügung gestellt werden. Benutzer müssen zu den entsprechenden Services hinzugefügt werden, damit sie über das Launchpad auf Webverbindungen zugreifen können.

Benutzer zu Launchpad-Services hinzufügen

Benutzer können über das Launchpad, einer einzelnen Position in ihrem Self-Service-Portal, auf Webanwendungen zugreifen.

Informationen zu diesem Vorgang

Für jede Webverbindung und Verbindung für einen föderierten Partner, die erstellt wird, wird ein entsprechender Service erstellt. Der Service erhält denselben Namen wie die Verbindung oder im Fall von föderierten Webanwendungen denselben Namen wie das Verbindungsalias. Damit die Webanwendung für einen Benutzer über das Launchpad zur Verfügung gestellt wird, muss der Benutzer zu dem entsprechenden Service hinzugefügt werden.

Anmerkung: Namen von nicht virtuellen Verbindungen beginnen mit einem normalen Schrägstrich, wie z. B. `/my_connection_1`. Die Servicenamen für nicht virtuelle Verbindungen beginnen ebenfalls mit einem normalen Schrägstrich.

Anmerkung: Wenn das Verbindungsalias für einen föderierten Partner geändert wird, wird ein neuer Service mit dem neuen Aliasnamen erstellt. Mitglieder des Service, der zuvor von der Verbindung verwendet wurde, werden zu dem neuen Service migriert und der alte Service wird entfernt.

Sie können Benutzer zu einem Service hinzufügen, indem Sie den Service manuell oder dynamisch mithilfe einer Richtlinie verwalten.

Vorgehensweise

Fügen Sie Benutzer zu einem Launchpad-Service hinzu.

- Fügen Sie Benutzer durch manuelle Verwaltung des Service hinzu.
- Fügen Sie Benutzer durch dynamische Verwaltung des Service hinzu.

Schlüssel verwalten

Sie können die Client- und Serverzertifikate verwalten, die Sie zum Sichern Ihrer Verbindungen verwenden.

Clientzertifikat erstellen

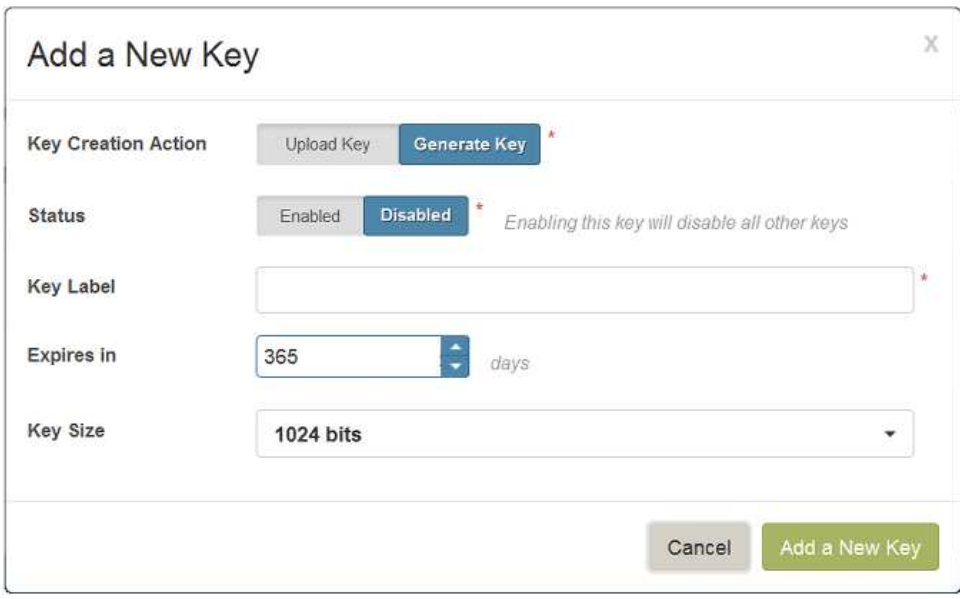
Clientzertifikate enthalten einen privaten und einen öffentlichen Schlüssel. Ein Clientzertifikat wird von einem Clientsystem verwendet, um authentifizierte Anforderungen an einen fernen Server auszugeben. Sie können Clientzertifikate erstellen oder, wenn Sie über eine Zertifikatsdatei verfügen, die Sie verwenden möchten, diese Datei nach Cloud Identity Portal hochladen.

Informationen zu diesem Vorgang

Das aktivierte Zertifikat wird standardmäßig für jede Verbindung verwendet, die Sie erstellen. Nur ein Schlüssel kann auf einmal aktiviert sein.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Applications** > **Key Management** und klicken Sie dann auf **Client Certificates** und **Add a New Key**.



2. Geben Sie die Einstellungen für Clientzertifikatsschlüssel ein.
3. Klicken Sie auf **Add a New Key**.

Einstellungen für Clientzertifikatsschlüssel

Zu den Einstellungen für Clientzertifikatsschlüssel gehören der Schlüsselkennsatz, die Zeit bis zum Ablauf und die Schlüsselgröße.

Tabelle 40. Einstellungen für Clientzertifikatsschlüssel

Einstellung	Beschreibung
Key Creation Action	• **Upload Key**. Wenn Sie über eine Zertifikatsdatei verfügen, die Sie verwenden möchten, können Sie die Datei hochladen. • **Generate Key**. Wenn Sie nicht über eine Zertifikatsdatei verfügen, kann Cloud Identity Portal einen Schlüssel generieren.
Status	• **Enabled**. Wenn Sie den Schlüssel aktivieren, werden der vorher aktivierte Schlüssel und alle anderen Zertifikatsschlüssel inaktiviert. Nur ein Schlüssel kann auf einmal aktiviert sein. **Wichtig:** Wenn Sie den Schlüssel aktivieren, wird der vorher aktivierte Schlüssel inaktiviert. Alle Verbindungen, die den vorher aktivierten Schlüssel verwenden, werden ungültig. • **Disabled**. Der Schlüssel ist inaktiviert.
Key Label	• Für einen hochgeladenen Schlüssel muss ein Kennsatz eingegeben werden, wenn der Status auf "Enabled" gesetzt ist. Der Schlüsselkennsatz ist der Name der Zertifikatsdatei, die Sie hochladen. • Für einen generierten Schlüssel ist dies eine eindeutige ID, die ein Zertifikat darstellt. Der Kennsatz gibt einen Namen an, über den auf ein Zertifikat Bezug genommen werden kann, wenn Schlüsselmanagementfunktionen ausgeführt werden.

Tabelle 40. Einstellungen für Clientzertifikatsschlüssel (Forts.)

Einstellung	Beschreibung
Key File	Nur für hochgeladene Schlüssel: Klicken Sie auf **Browse**, um zur Datei zu blättern, die hochgeladen werden soll, und diese auszuwählen. Die Formate JKS, PEM und P12 werden unterstützt.
Key Password	Nur für hochgeladene Schlüssel: das Schlüsselkennwort. Das Kennwort muss mit dem Kennwort in der Zertifikatsdatei übereinstimmen, die Sie hochladen.
Expires in	Die Anzahl der Tage, für die der Schlüssel gültig ist.
Key Size	Die Schlüsselgröße.

Nach einem Clientzertifikat suchen

Wenn Sie ein Zertifikat aktivieren, inaktivieren oder löschen möchten, suchen Sie nach dem Zertifikat.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Applications** > **Key Management** und dann auf **Client Certificates**.
2. Geben Sie im Feld **Narrow Your Search** Ihre Suchkriterien ein.

   Sie können nach einer beliebigen Zeichenfolge aus drei Zeichen suchen, die der Schlüsselkennsatz des Zertifikats enthält. Um z. B. nach einem Zertifikat mit dem Schlüsselkennsatz "certificate1" zu suchen, können Sie `cer` oder `te1` eingeben. Zertifikate, die Ihren Suchkriterien entsprechen, werden aufgeführt. Sie können ein Zertifikat auswählen, um es zu aktivieren, zu inaktivieren, zu löschen oder zu ersetzen.

Schlüssel aktivieren und inaktivieren

Nur ein Schlüssel kann auf einmal aktiviert sein.

Informationen zu diesem Vorgang

Wenn Sie einen Schlüssel für ein Zertifikat aktivieren, wird der vorher aktivierte Schlüssel automatisch inaktiviert. Sie können den derzeit aktivierten Schlüssel inaktivieren, indem Sie nur einen anderen Schlüssel aktivieren.

Wichtig: Wenn Sie einen Schlüssel aktivieren, wird der vorher aktivierte Schlüssel inaktiviert. Alle Verbindungen, die den vorher aktivierten Schlüssel verwenden, werden ungültig.

Vorgehensweise

1. Suchen Sie den Schlüssel, den Sie aktivieren möchten, und wählen Sie ihn aus.

2. Klicken Sie auf **Enabled**. Der Schlüssel ist aktiviert. Alle neuen Verbindungen verwenden nun den neu aktivierten Zertifikatsschlüssel.

Zertifikat herunterladen

Sie können ein Zertifikat herunterladen.

Informationen zu diesem Vorgang

Für eine Partnerverbindung, bei der der Partner Authentifizierungsanforderungen verschlüsselt und Authentifizierungssignaturen prüft, können Sie das öffentliche Zertifikat für den privaten Zertifikatsschlüssel herunterladen, der bei der Verbindung verwendet wird.

Das öffentliche Zertifikat wird bei der partnerseitigen Connectorkonfiguration verwendet.

Vorgehensweise

1. Suchen Sie den Schlüssel, für den Sie ein öffentliches Zertifikat herunterladen möchten, und wählen Sie ihn aus.
2. Klicken Sie auf **Download Public Certificate**.
3. Speichern Sie die Datei.

Schlüssel löschen

Sie können ein Zertifikat löschen, wenn es nicht mehr benötigt wird. Ein Schlüssel muss inaktiviert werden, bevor er gelöscht werden kann.

Vorgehensweise

1. Suchen Sie den Schlüssel, den Sie löschen möchten, und wählen Sie ihn aus.
2. Klicken Sie auf **Remove Key**.

   Sie werden aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf **Remove Key**. Der Schlüssel wird gelöscht.

Schlüssel ersetzen

In einer Umgebung, in der Zertifikate verwendet werden, müssen Zertifikate und deren Schlüssel aktualisiert werden. Außerdem müssen möglicherweise abgelaufene Zertifikate ersetzt werden.

Vorgehensweise

1. Suchen Sie den Schlüssel, den Sie ersetzen möchten, und wählen Sie ihn aus.
2. Klicken Sie auf **Replace Key**.

Serverzertifikat erstellen

Serverzertifikate werden zum Identifizieren eines Servers verwendet. Wenn Sie über eine Serverzertifikatsdatei verfügen, die Sie hinzufügen möchten, können Sie die Datei in Cloud Identity Portal hochladen.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Applications** > **Key Management** und klicken Sie dann auf **Server Certificates** und **Add a New Key**.

2. Geben Sie den Schlüsselkennsatz im Feld **Key Label** ein. Der Schlüsselkennsatz muss dem Namen der Zertifikatsdatei, die Sie hochladen, entsprechen.
3. Klicken Sie auf **Browse**, um zur hochzuladenden Zertifikatsdatei zu blättern und sie auszuwählen.
4. Klicken Sie auf **Add a New Key**.

Nach einem Serverzertifikat suchen

Wenn Sie ein Zertifikat löschen oder ersetzen möchten, suchen Sie nach dem Zertifikat.

Vorgehensweise

1. Klicken Sie im Navigationsmenü auf **Applications** > **Key Management** und dann auf **Server Certificates**.
2. Geben Sie im Feld **Narrow Your Search** Ihre Suchkriterien ein.

   Sie können nach einer beliebigen Zeichenfolge aus drei Zeichen suchen, die der Schlüsselkennsatz des persönlichen Zertifikats enthält. Um z. B. nach einem Zertifikat mit dem Schlüsselkennsatz "certificate1" zu suchen, können Sie `cer` oder `te1` eingeben. Zertifikate, die Ihren Suchkriterien entsprechen, werden aufgeführt. Sie können ein Zertifikat auswählen, um es zu löschen oder zu ersetzen.

Schlüssel löschen

Sie können ein Zertifikat löschen, wenn es nicht mehr benötigt wird.

Informationen zu diesem Vorgang

Wichtig: Wenn Sie ein Zertifikat löschen, schlagen Verbindungen, die dieses Zertifikat verwenden, fehl. Damit die Verbindungen gültig bleiben, müssen Sie ein gültiges Zertifikat für die Verbindung auswählen.

Vorgehensweise

1. Suchen Sie den Schlüssel, den Sie löschen möchten, und wählen Sie ihn aus.
2. Klicken Sie auf **Remove Key**.

   Sie werden aufgefordert, den Löschvorgang zu bestätigen. Klicken Sie auf **Remove Key**. Das Zertifikat wird gelöscht.

Schlüssel ersetzen

In einer Umgebung, in der Zertifikate verwendet werden, müssen Zertifikate und deren Schlüssel aktualisiert werden. Möglicherweise müssen abgelaufene Zertifikate ersetzt werden.

Vorgehensweise

1. Suchen Sie den Schlüssel, den Sie ersetzen möchten, und wählen Sie ihn aus.
2. Klicken Sie auf **Replace Key**.

Identitäten einrichten

Durch Identitätsmanagementfeeds können Identitätsdaten zwischen externen Identitätsrepositorys und der Identitätsmanagementumgebung von Cloud Identity Service fließen. Die Einrichtung von Identitäten kann eingehend oder ausgehend sein.

Überblick über die Identitätseinrichtung

Mit Identitätsmanagementfeeds können Benutzerdatensätze von externen Identitätsrepositorys oder für diese eingerichtet werden.

Cloud Identity Service kann mit verschiedenen Arten von Identitätsrepositorys verbunden werden, wie Active Directory, LDAP v3, relationalen Datenbanken, SOAP-Services, Nachrichtenwarteschlangen und SAP. Durch die Integration in diese anderen Identitätsrepositorys durch das Definieren einer eingehenden Verbindung können Benutzer in Cloud Identity Service automatisch hinzugefügt, geändert und gelöscht werden. Über eine abgehende Verbindung können Benutzer in externen Repositorys hinzugefügt, geändert und gelöscht werden.

Identitätsrepositorys

Identitätsdaten werden möglicherweise in vielen verschiedenen Systemen in Ihrer Organisation aufbewahrt. Diese Systeme werden als Identitätsrepositorys bezeichnet. Jedes Repository kann verschiedene Arten von Identitätsdaten enthalten. Einige enthalten z. B. einfache accountbezogene Daten für eine bestimmte Anwendung, wie etwa eine SQL-Datenbank. Andere Identitätsrepositorys enthalten möglicherweise umfassendere Identitätsdaten für verschiedene Systeme, wie etwa Oracle PeopleSoft. Die Daten in diesen Repositorys bestehen aus Identitätsattributen. Identitätsattribute identifizieren Benutzer und enthalten Benutzerdatensätze. Ein Benutzerdatensatz kann z. B. aus einem Benutzernamen, einem Vornamen, einem Nachnamen, einer E-Mail-Adresse und einem Aufgabenbereich bestehen. Cloud Identity Service fungiert als Identitätsmanagementsystem (IDM-System), indem es seine Identitätseinrichtungsfunktionalität nutzt, um Identitätsdaten zwischen den verschiedenen Repositorys in Ihrer Organisation korrekt, konsistent und aktuell aufzubewahren.

Feedmanagement

Wenn Repositorys in Cloud Identity Service integriert werden, ist es für die Synchronisierung von Daten zwischen Repositorys entscheidend, zu definieren, wie eine Verbindung zu diesen Systemen hergestellt wird und wie Identitätsdaten zwischen diesen Systemen eingerichtet werden. Durch das Feedmanagement können Identitätsdaten, wie Attribute, Gruppen, Rollen und Accountinformationen, zwischen Ihren anderen Identitätsrepositorys und Cloud Identity Service fließen.

Ein IDM-System kann als Radnabe mit Speichen betrachtet werden. Cloud Identity Service befindet sich wie eine Radnabe in der Mitte aller Ihrer Identitätsreposito-

rys. Die Identitätsdaten fließen zu und aus Cloud Identity Service sowie zu und aus Ihren anderen Identitätsrepositorys. Daten, die aus einem Identitätsrepository zu Cloud Identity Service fließen, sind eingehende Daten, und Daten, die aus Cloud Identity Service fließen, sind ausgehende Daten.

Ein Identitätsmanagementfeed enthält mehrere Arten von Geschäftsregeln, die definieren, wie Cloud Identity Service mit anderen Identitätsrepositorys kommuniziert:

- Verbindungsinformationen. Verbindungsinformationen bestimmen, wie und wann Cloud Identity Service eine Verbindung zu einem Repository herstellt und wie Informationen aus diesem Repository analysiert und interpretiert werden.
- Einrichtungsrichtlinie. Eine übergeordnete Einrichtungsrichtlinie bestimmt, unter welchen Bedingungen Cloud Identity Service Identitätsdaten an ein Repository überträgt oder von diesem empfängt. Einrichtungsrichtlinien bestimmen außerdem, welche Daten ignoriert werden.
- Attribute und Gruppenzuordnungsinformationen. Attribute und Gruppen in verschiedenen Identitätsrepositorys verwenden nicht die gleichen Namenskonventionen. Identitätsattribute können zwischen verschiedenen Repositorys den in Cloud Identity Service enthaltenen Informationen zugeordnet werden. Die Zuordnungsfunktionen der Identitätsmanagementfeeds von Cloud Identity Service ermöglichen einfache und komplexe Zuordnungslogik, einschließlich der Zuordnung zwischen Gruppen.

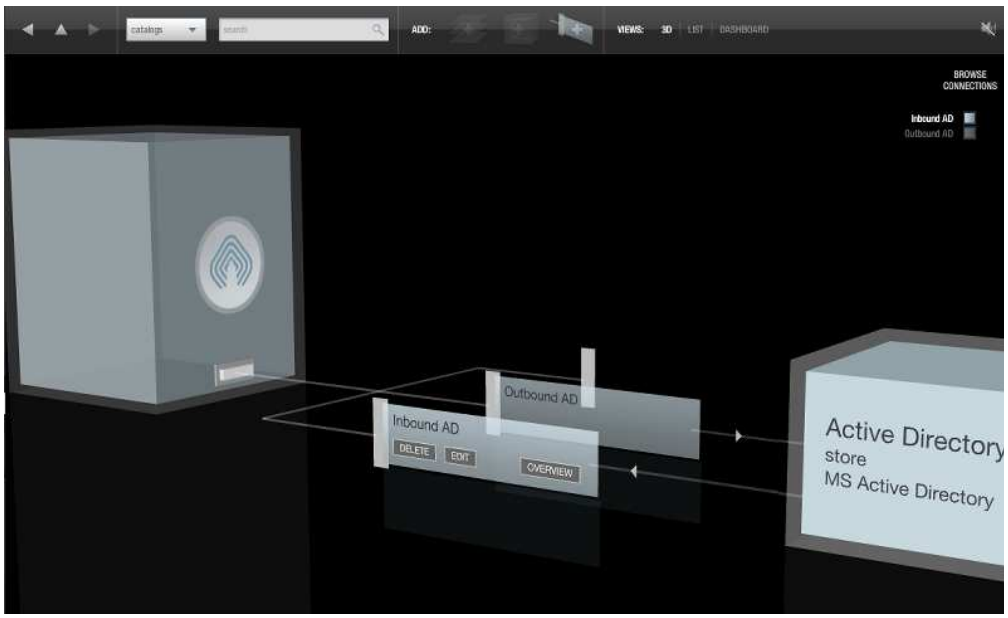
Assembly-Lines

In Cloud Identity Service werden Identitätsmanagementfeeds als Assembly-Lines bezeichnet. Assembly-Lines werden bei der Erstkonfiguration von Cloud Identity Service für Ihre Organisation konfiguriert. Assembly-Lines werden mithilfe von Assembly-Line-Vorlagen definiert. Jede Assembly-Line-Vorlage enthält mehrere konfigurierbare Optionen für Verbindungen.

Benutzerschnittstelle für das Feedmanagement

Die Benutzerschnittstelle für das Feedmanagement bietet eine grafische Darstellung konfigurierter Managementfeeds.

Cloud Identity Service kann mit verschiedenen Arten von Identitätsrepositorys verbunden werden, wie Active Directory, LDAP v3, relationalen Datenbanken, SOAP-Services, Nachrichtenwarteschlangen, SAP und PeopleSoft. Benutzer können durch Integration in diese anderen Identitätsrepositorys automatisch zu Cloud Identity Service hinzugefügt werden und können von Cloud Identity Service externen Repositorys hinzugefügt werden.



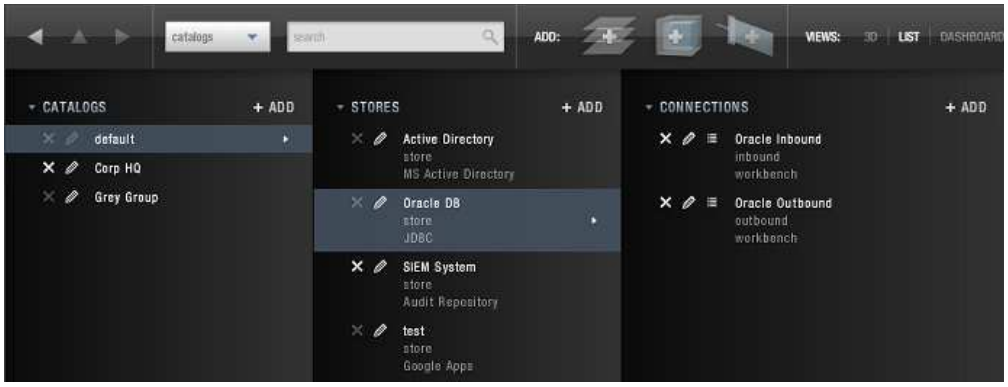
Kataloge, Speicher und Verbindungen

Kataloge bieten eine Möglichkeit zum Gruppieren externer Identitätsrepositorys, die mit Cloud Identity Service-Services verbunden sind. Ein Katalog kann z. B. für eine Unternehmensabteilung wie die Finanz- oder die IT-Abteilung definiert werden. Speicher sind externe Identitätsrepositorys, die in Katalogen gruppiert sind. Cloud Identity Service unterstützt die gängigsten Identitätsrepositorys, wie Active Directory, LDAP v3, relationale Datenbanken, SOAP-Services, Nachrichtenwarteschlangen und SAP.

Verbindungen definieren, wie Cloud Identity Service mit externen Identitätsrepositorys eine Verbindung herstellt und interagiert. Verbindungen sind eingehend oder abgehend.

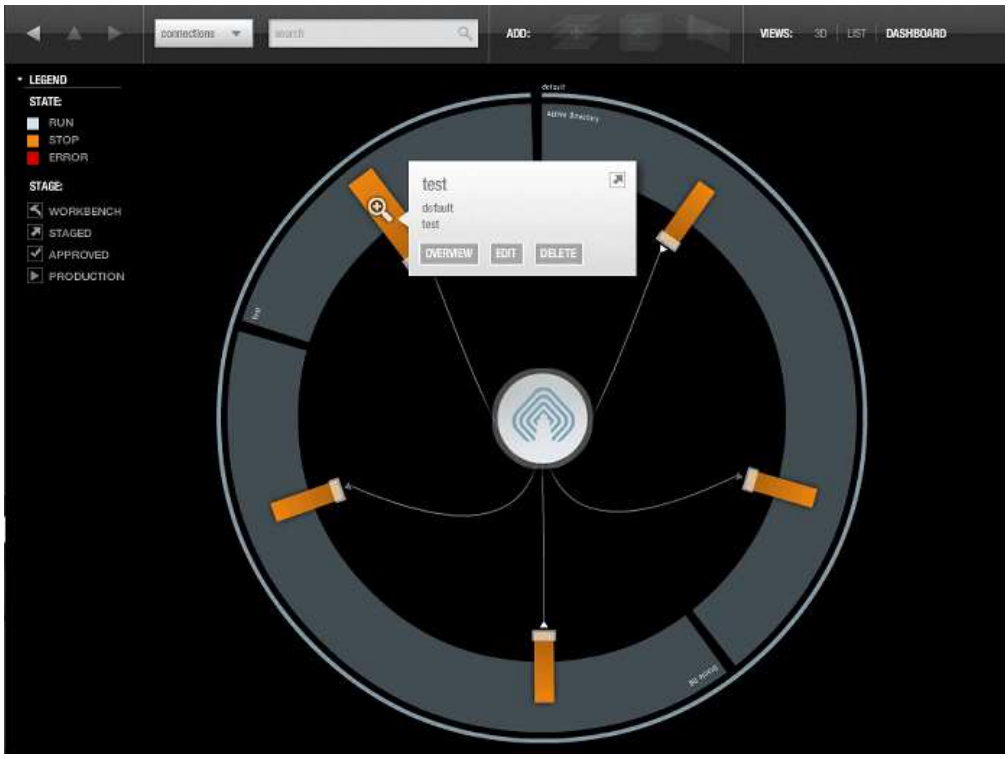
Listenansicht

Sie können Ihr Feedmanagementsystem in der Listenansicht anzeigen. Darin ist es einfacher, Kataloge, Speicher und Verbindungen zu durchsuchen, anzuzeigen, hinzuzufügen und zu bearbeiten.

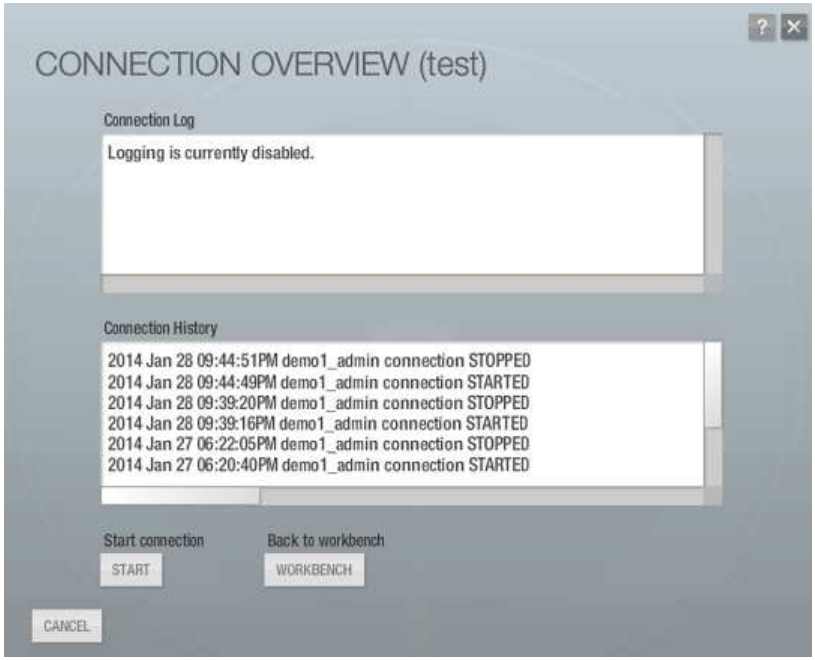


Dashboardansicht

Nachdem Verbindungen zu Speichern hergestellt sind, können Administratoren das gesamte Feedmanagementsystem im Dashboard anzeigen. Ein Farbcode zeigt den Status von Verbindungen an.



Administratoren können das Ereignisprotokoll für jede Verbindung anzeigen und eine Verbindung starten oder stoppen.



Reverse-Proxy-Einstellungen verwalten

Sie können Reverse-Proxy-Einstellungen verwalten, um die Zeitlimits für Benutzersitzungen für geschützte Ressourcen zu ändern.

Vorgehensweise

Klicken Sie auf **Applications** > **Reverse Proxy Settings**.

Reverse-Proxy-Einstellungen

Die Zeitlimits für Benutzersitzungen gelten im Rahmen aller Sitzungen für alle Webressourcen, die über Cloud Identity Service gesichert werden.

Zeitlimit

Das Zeitlimit bestimmt die maximale Laufzeit für alle authentifizierten und nicht authentifizierten Benutzersitzungen. Über das Zeitlimit wird die Zeitdauer festgelegt, für die Berechtigungsnachweise gelten. Benutzer müssen sich erneut authentifizieren, wenn das angegebene Zeitlimit erreicht wird. Das Standardzeitlimit für die Laufzeit eines Sitzungseintrags beträgt 3600 Sekunden. Durch den Wert 0 wird die Zeitlimitfunktion inaktiviert (das Zeitlimit ist uneingeschränkt).

Inaktives Zeitlimit

Über das inaktive Zeitlimit wird das Zeitlimit für Inaktivität während der Benutzersitzung festgelegt. Wenn ein Benutzer z. B. für einen Zeitraum inaktiv ist, der länger als das inaktive Zeitlimit ist, wird die Sitzung beendet oder die Sitzung erhält eine Markierung, dass eine erneute Authentifizierung erforderlich ist. Der Standardwert für das inaktive Zeitlimit für eine Anmeldesitzung beträgt 600 Sekunden. Durch den Wert 0 wird die Funktion für das Inaktivitätszeitlimit inaktiviert (das inaktive Zeitlimit ist uneingeschränkt).

Kapitel 8. Mobile-Anwendung

Benutzer können die IBM Mobile-App für den Zugriff auf Self-Service-Anwendungen über ihre mobilen Geräte verwenden.

Die IBM Mobile-App ist auch eine Voraussetzung für den Empfang von einmaligen Kennwörtern (OTP) und Push-Benachrichtigungen für die Authentifizierung bei Self-Service-Anwendungen.

Übersicht

Die IBM Mobile-App bietet Benutzern Zugriff auf Self-Service-Anwendungen über ihre mobilen Geräte.

Was macht IBM Mobile?

Benutzer können Serviceanforderungen über ihre mobilen Geräte mit der IBM Mobile-App stellen, während Manager Serviceanforderungen genehmigen und ablehnen können. Sie können auf Anwendungen zugreifen, die mit Ihren Services verknüpft sind. Die IBM Mobile-App verfügt außerdem über einen Einmalkennwortgenerator für die zweistufige Authentifizierung bei Self-Service-Anwendungen.

Warum benötigen Sie IBM Mobile?

Sie benötigen die App für den Zugriff auf Self-Service-Anwendungen über Ihre mobilen Geräte und zum Starten von Serviceanwendungen über Ihre mobilen Geräte.

Sie benötigen die App auch, wenn Ihr Unternehmen Mehrfaktorauthentifizierung für den Zugriff auf Self-Service-Anwendungen mit Push-Benachrichtigung oder Einmalkennwort (OTP) verwendet.

Welche mobilen Geräte werden von IBM Mobile unterstützt?

IBM Mobile unterstützt Apple-Geräte mit iOS ab Version 10.0.0 und Android-Geräte mit mindestens Lollipop.

Was ist Mehrfaktorauthentifizierung (MFA)?

MFA erfordert mehr als eine Methode aus verschiedenen Quellen für die Verifizierung einer Benutzeridentität. Cloud Identity Service verwendet eine zweistufige MFA. Ihre Identität wird über die Eingabe eines Benutzernamens und -kennworts sowie über die Eingabe eines Codes oder die Bestätigung einer Benachrichtigung, die an Ihr mobiles Gerät gesendet wurde, verifiziert.

Zweistufige Verifizierung funktioniert wie folgt.

1. Melden Sie sich bei Ihrer Self-Service-Anwendung wie gewohnt mit Ihrem Benutzernamen und Ihrem Kennwort an.
2. Über eine SMS-Nachricht, ein generiertes Einmalkennwort (OTP) oder eine Push-Benachrichtigung wird eine Verifizierungsbenachrichtigung an Ihr mobiles Gerät gesendet.
3. Bestätigen Sie Ihre Identität auf Ihrem mobilen Gerät, indem Sie den Code eingeben oder die Benachrichtigung akzeptieren.

Einführung

Starten Sie mit der IBM Mobile-App, indem Sie die App herunterladen und installieren und das Gerät mit Ihrem Cloud Identity Service-Account verbinden.

App herunterladen

Installieren Sie die App auf Ihrem Gerät.

Vorgehensweise

1. Starten Sie den App Store (iOS) oder den Google Play Store (Android).
2. Suchen Sie nach der IBM Mobile-App.
3. Tippen Sie zum Herunterladen der App auf **Get** und **Install**.
4. Tippen Sie zum Öffnen der App auf das App-Symbol.

Anmelden

Melden Sie sich bei Ihrem Cloud Identity Service-Account auf Ihrem mobilen Gerät an.

Informationen zu diesem Vorgang

Sie können für die Anmeldung bei Ihrem Account einen QR-Code scannen oder einen OTP-Code (Einmalkennwortcode) verwenden. Wenn Ihre Sitzung abläuft, können Sie sich erneut anmelden, indem Sie Ihren Benutzernamen und Ihr Kennwort eingeben.

Mit einem QR-Code anmelden

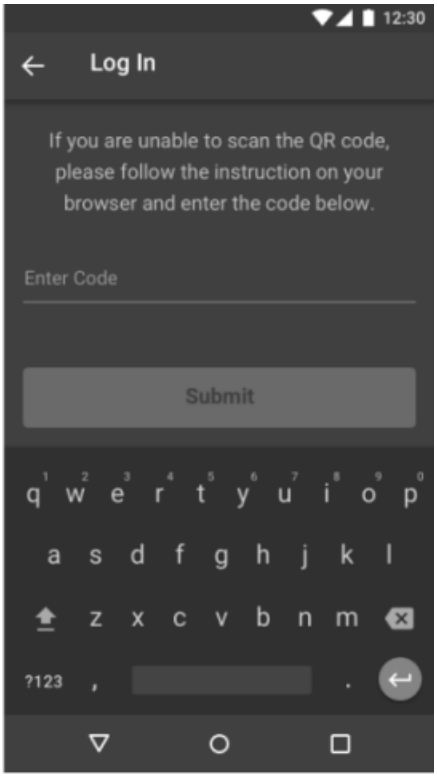
Scannen Sie einen QR-Code, um sich bei Ihrem Account anzumelden. Wenn Sie den QR-Code nicht scannen können, können Sie einen Code manuell eingeben.

Vorgehensweise

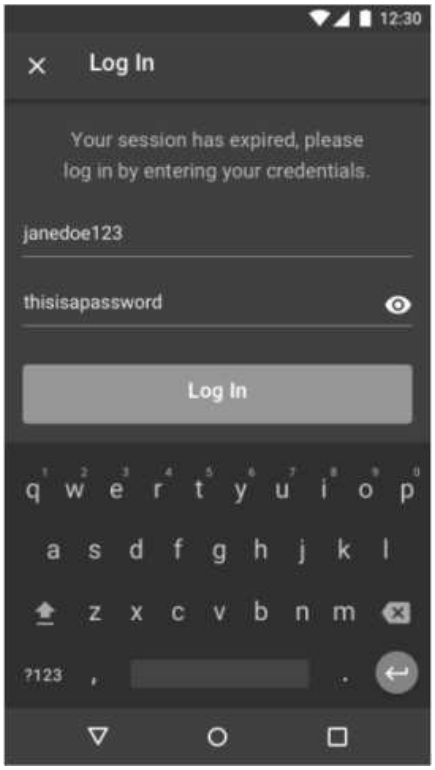
1. Suchen und öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Log In**.

Ein QR-Code wird an Ihren Account gesendet.

2. Rufen Sie auf einem anderen Gerät ***Unternehmen*.ibm.com** auf und scannen Sie den QR-Code. Wenn Sie den QR-Code nicht scannen können, tippen Sie auf **Unable to scan QR code** und befolgen Sie die Anweisungen, um einen Code manuell einzugeben.



3. Wenn Ihre Sitzung abläuft, geben Sie Ihren Benutzernamen und Ihr Kennwort ein und tippen Sie auf **Log In**.

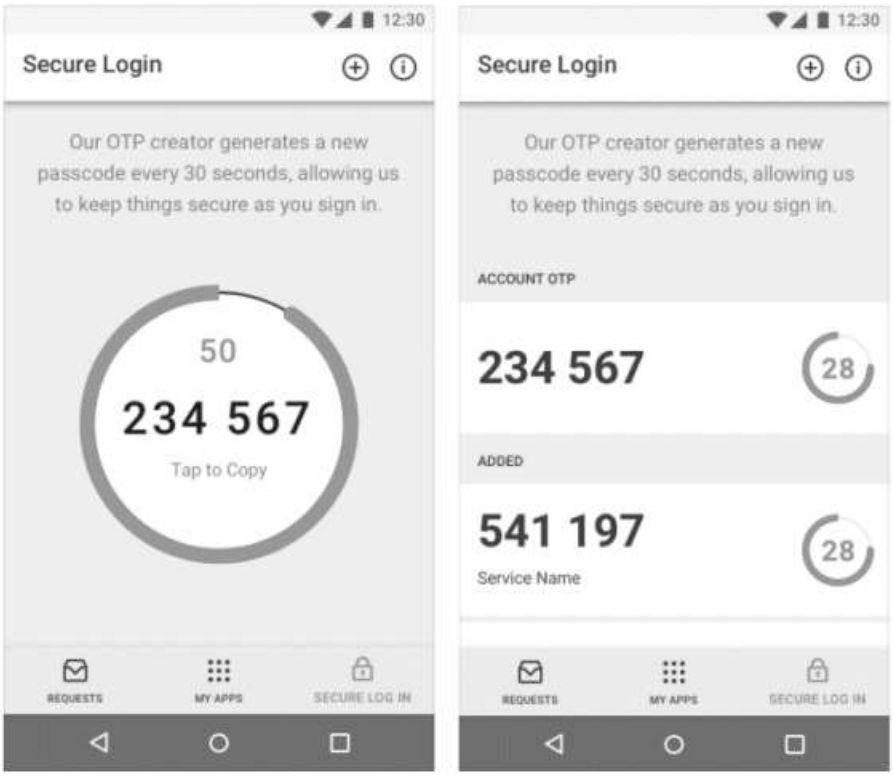


Mit einem Einmalkennwort (OTP) anmelden

Melden Sie sich mit einem OTP-Code an.

Vorgehensweise

Suchen und öffnen Sie die IBM Mobile-App auf Ihrem Gerät, tippen Sie auf **Secure Log In** und wählen Sie den OTP-Generatorservice aus, den Sie verwenden möchten.



Sie können einen OTP-Generatorservice hinzufügen, indem Sie einen QR-Code scannen oder manuell einen Code eingeben.

Ihre Geräte verwalten

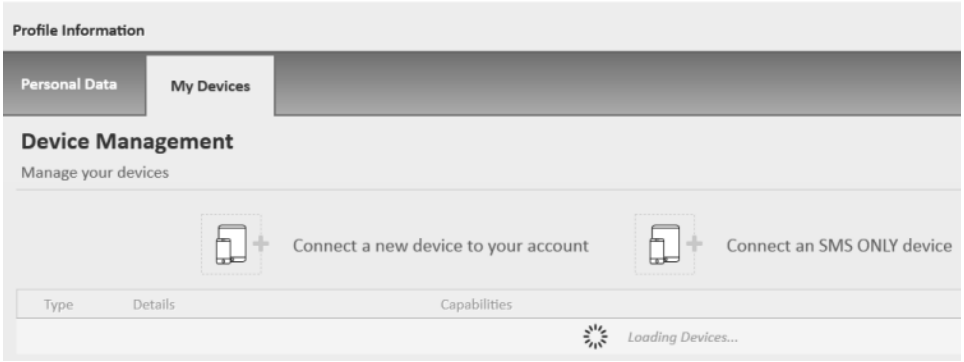
Registrieren und verwalten Sie Ihre Geräte über das Cloud Identity Service-Portal von Cloud Identity Service.

Informationen zu diesem Vorgang

Fügen Sie neue Geräte hinzu und entfernen Sie Geräte, die Sie nicht mehr verwenden. Sie können Nur-SMS-Geräte und vollständig aktivierte Geräte hinzufügen, indem Sie einen QR-Code scannen oder manuell einen Code eingeben. Sie registrieren ein Gerät, wenn Sie sich das erste Mal am Self-Service-Portal anmelden.

Vorgehensweise

1. Melden Sie sich von Ihrem Computer aus am Self-Service-Portal an.
2. Wählen Sie **Profile** > **My Devices** aus.



3. Fügen Sie Geräte hinzu oder entfernen Sie Geräte.

App löschen

Löschen Sie die App, wenn Sie das Gerät nicht mehr verwenden oder den Zugriff auf Cloud Identity Service nicht mehr benötigen.

Informationen zu diesem Vorgang

Anmerkung: Wenn Sie die IBM Mobile-App löschen, wird keine zweistufige Verifizierung entfernt, die für Ihren Cloud Identity Service-Account in Kraft ist.

Vorgehensweise

1. Suchen Sie die IBM Mobile-App auf Ihrem Gerät und wählen Sie sie aus.
2. Tippen Sie auf **Delete**.

Einführung

Starten Sie mit der IBM Mobile-App, indem Sie die App herunterladen und installieren und das Gerät mit Ihrem Cloud Identity Service-Account verbinden.

App herunterladen

Installieren Sie die App auf Ihrem Gerät.

Vorgehensweise

1. Starten Sie den App Store (iOS) oder den Google Play Store (Android).
2. Suchen Sie nach der IBM Mobile-App.
3. Tippen Sie zum Herunterladen der App auf **Get** und **Install**.
4. Tippen Sie zum Öffnen der App auf das App-Symbol.

Anmelden

Melden Sie sich bei Ihrem Cloud Identity Service-Account auf Ihrem mobilen Gerät an.

Informationen zu diesem Vorgang

Sie können für die Anmeldung bei Ihrem Account einen QR-Code scannen oder einen OTP-Code (Einmalkennwortcode) verwenden. Wenn Ihre Sitzung abläuft, können Sie sich erneut anmelden, indem Sie Ihren Benutzernamen und Ihr Kennwort eingeben.

Mit einem QR-Code anmelden:

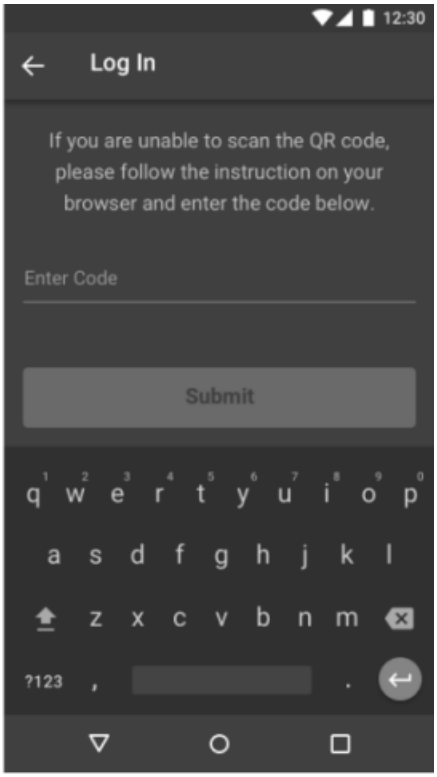
Scannen Sie einen QR-Code, um sich bei Ihrem Account anzumelden. Wenn Sie den QR-Code nicht scannen können, können Sie einen Code manuell eingeben.

Vorgehensweise

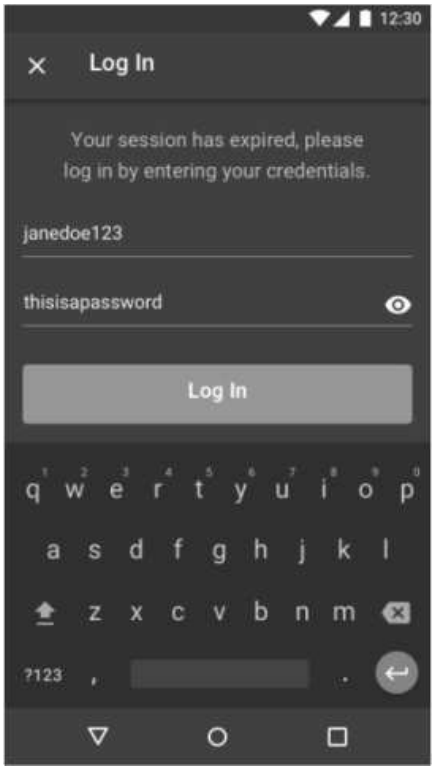
1. Suchen und öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Log In**.

Ein QR-Code wird an Ihren Account gesendet.

2. Rufen Sie auf einem anderen Gerät ***Unternehmen*.ibm.com** auf und scannen Sie den QR-Code. Wenn Sie den QR-Code nicht scannen können, tippen Sie auf **Unable to scan QR code** und befolgen Sie die Anweisungen, um einen Code manuell einzugeben.



3. Wenn Ihre Sitzung abläuft, geben Sie Ihren Benutzernamen und Ihr Kennwort ein und tippen Sie auf **Log In**.

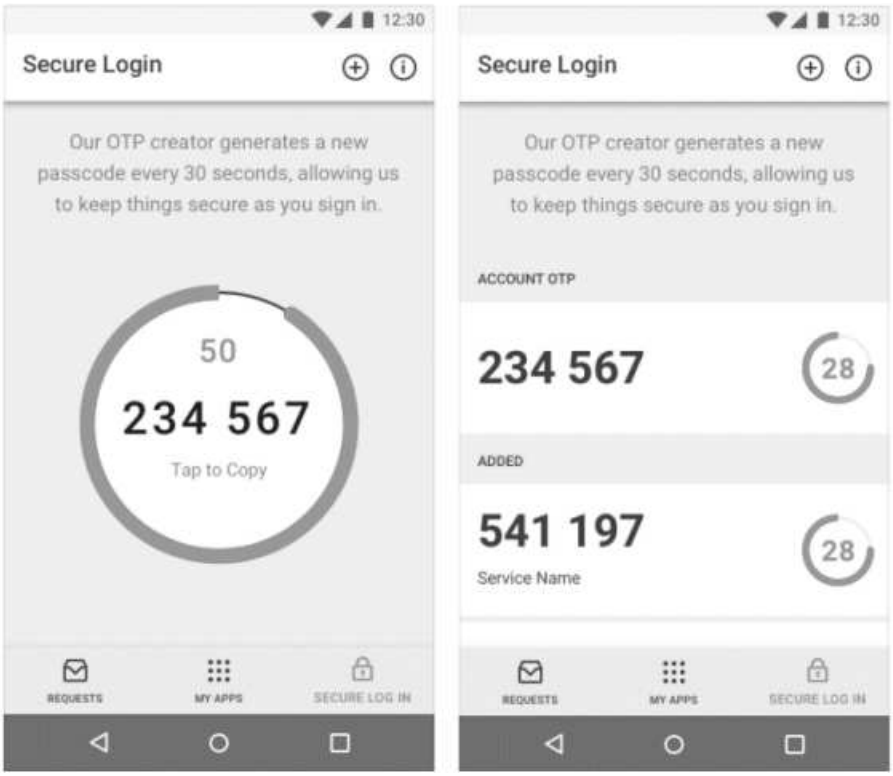


Mit einem Einmalkennwort (OTP) anmelden:

Melden Sie sich mit einem OTP-Code an.

Vorgehensweise

Suchen und öffnen Sie die IBM Mobile-App auf Ihrem Gerät, tippen Sie auf **Secure Log In** und wählen Sie den OTP-Generatorservice aus, den Sie verwenden möchten.



Sie können einen OTP-Generatorservice hinzufügen, indem Sie einen QR-Code scannen oder manuell einen Code eingeben.

Ihre Geräte verwalten

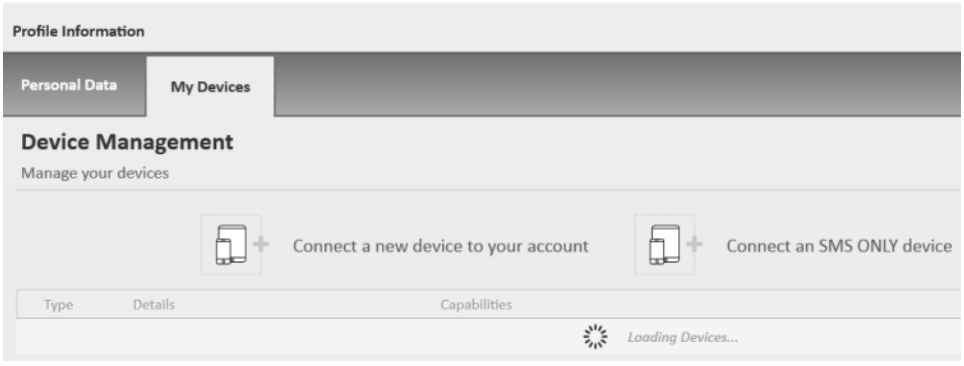
Registrieren und verwalten Sie Ihre Geräte über das Cloud Identity Service-Portal von Cloud Identity Service.

Informationen zu diesem Vorgang

Fügen Sie neue Geräte hinzu und entfernen Sie Geräte, die Sie nicht mehr verwenden. Sie können Nur-SMS-Geräte und vollständig aktivierte Geräte hinzufügen, indem Sie einen QR-Code scannen oder manuell einen Code eingeben. Sie registrieren ein Gerät, wenn Sie sich das erste Mal am Self-Service-Portal anmelden.

Vorgehensweise

1. Melden Sie sich von Ihrem Computer aus am Self-Service-Portal an.
2. Wählen Sie **Profile** > **My Devices** aus.



3. Fügen Sie Geräte hinzu oder entfernen Sie Geräte.

App löschen

Löschen Sie die App, wenn Sie das Gerät nicht mehr verwenden oder den Zugriff auf Cloud Identity Service nicht mehr benötigen.

Informationen zu diesem Vorgang

Anmerkung: Wenn Sie die IBM Mobile-App löschen, wird keine zweistufige Verifizierung entfernt, die für Ihren Cloud Identity Service-Account in Kraft ist.

Vorgehensweise

1. Suchen Sie die IBM Mobile-App auf Ihrem Gerät und wählen Sie sie aus.
2. Tippen Sie auf **Delete**.

Einführung

Starten Sie mit der IBM Mobile-App, indem Sie die App herunterladen und installieren und das Gerät mit Ihrem Cloud Identity Service-Account verbinden.

App herunterladen

Installieren Sie die App auf Ihrem Gerät.

Vorgehensweise

1. Starten Sie den App Store (iOS) oder den Google Play Store (Android).
2. Suchen Sie nach der IBM Mobile-App.
3. Tippen Sie zum Herunterladen der App auf **Get** und **Install**.
4. Tippen Sie zum Öffnen der App auf das App-Symbol.

Anmelden

Melden Sie sich bei Ihrem Cloud Identity Service-Account auf Ihrem mobilen Gerät an.

Informationen zu diesem Vorgang

Sie können für die Anmeldung bei Ihrem Account einen QR-Code scannen oder einen OTP-Code (Einmalkennwortcode) verwenden. Wenn Ihre Sitzung abläuft, können Sie sich erneut anmelden, indem Sie Ihren Benutzernamen und Ihr Kennwort eingeben.

Mit einem QR-Code anmelden:

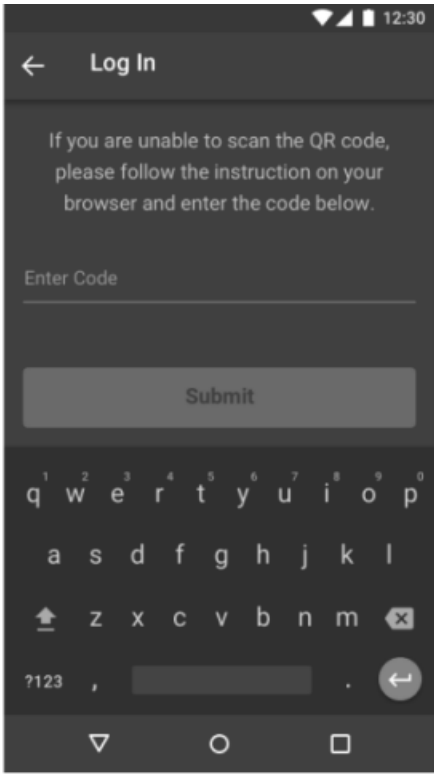
Scannen Sie einen QR-Code, um sich bei Ihrem Account anzumelden. Wenn Sie den QR-Code nicht scannen können, können Sie einen Code manuell eingeben.

Vorgehensweise

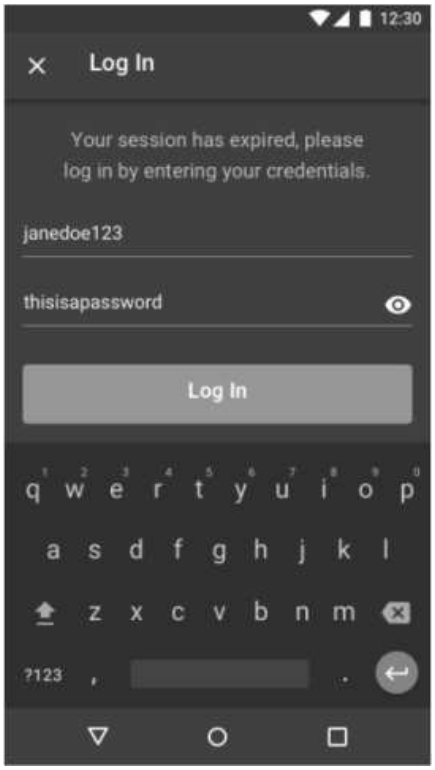
1. Suchen und öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Log In**.

Ein QR-Code wird an Ihren Account gesendet.

2. Rufen Sie auf einem anderen Gerät ***Unternehmen*.ibm.com** auf und scannen Sie den QR-Code. Wenn Sie den QR-Code nicht scannen können, tippen Sie auf **Unable to scan QR code** und befolgen Sie die Anweisungen, um einen Code manuell einzugeben.



3. Wenn Ihre Sitzung abläuft, geben Sie Ihren Benutzernamen und Ihr Kennwort ein und tippen Sie auf **Log In**.

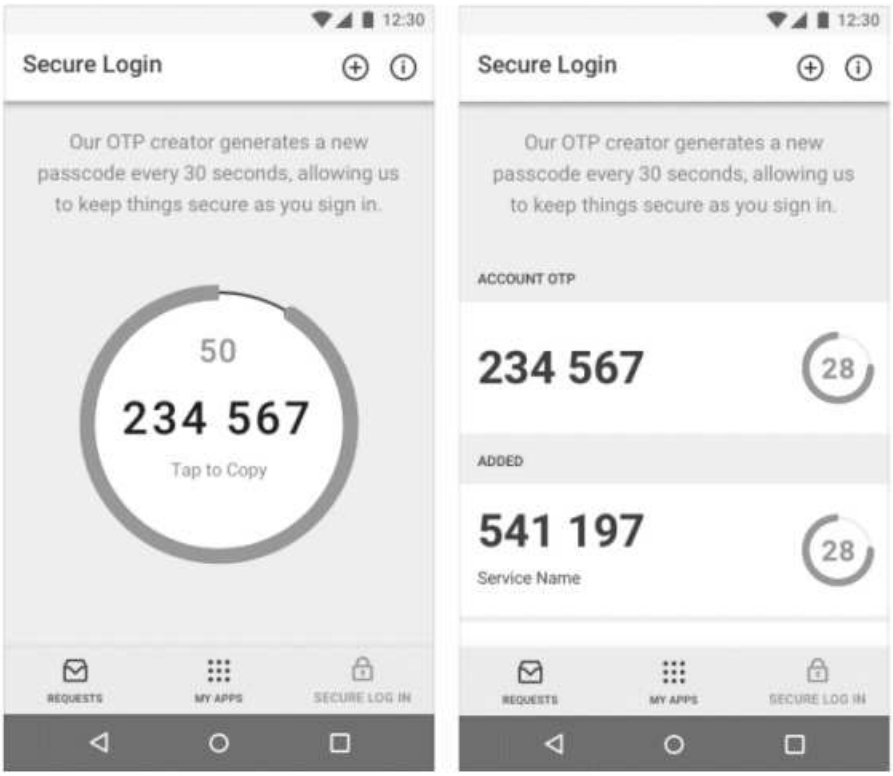


Mit einem Einmalkennwort (OTP) anmelden:

Melden Sie sich mit einem OTP-Code an.

Vorgehensweise

Suchen und öffnen Sie die IBM Mobile-App auf Ihrem Gerät, tippen Sie auf **Secure Log In** und wählen Sie den OTP-Generatorservice aus, den Sie verwenden möchten.



Sie können einen OTP-Generatorservice hinzufügen, indem Sie einen QR-Code scannen oder manuell einen Code eingeben.

Ihre Geräte verwalten

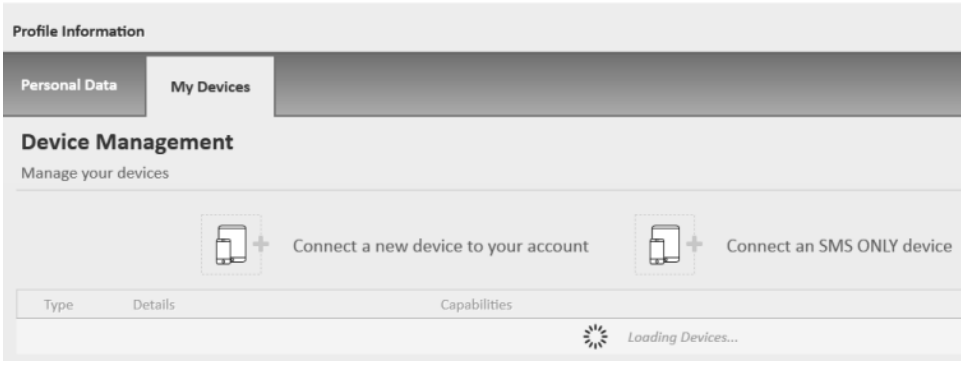
Registrieren und verwalten Sie Ihre Geräte über das Cloud Identity Service-Portal von Cloud Identity Service.

Informationen zu diesem Vorgang

Fügen Sie neue Geräte hinzu und entfernen Sie Geräte, die Sie nicht mehr verwenden. Sie können Nur-SMS-Geräte und vollständig aktivierte Geräte hinzufügen, indem Sie einen QR-Code scannen oder manuell einen Code eingeben. Sie registrieren ein Gerät, wenn Sie sich das erste Mal am Self-Service-Portal anmelden.

Vorgehensweise

1. Melden Sie sich von Ihrem Computer aus am Self-Service-Portal an.
2. Wählen Sie **Profile** > **My Devices** aus.



3. Fügen Sie Geräte hinzu oder entfernen Sie Geräte.

App löschen

Löschen Sie die App, wenn Sie das Gerät nicht mehr verwenden oder den Zugriff auf Cloud Identity Service nicht mehr benötigen.

Informationen zu diesem Vorgang

Anmerkung: Wenn Sie die IBM Mobile-App löschen, wird keine zweistufige Verifizierung entfernt, die für Ihren Cloud Identity Service-Account in Kraft ist.

Vorgehensweise

1. Suchen Sie die IBM Mobile-App auf Ihrem Gerät und wählen Sie sie aus.
2. Tippen Sie auf **Delete**.

Einführung

Starten Sie mit der IBM Mobile-App, indem Sie die App herunterladen und installieren und das Gerät mit Ihrem Cloud Identity Service-Account verbinden.

App herunterladen

Installieren Sie die App auf Ihrem Gerät.

Vorgehensweise

1. Starten Sie den App Store (iOS) oder den Google Play Store (Android).
2. Suchen Sie nach der IBM Mobile-App.
3. Tippen Sie zum Herunterladen der App auf **Get** und **Install**.
4. Tippen Sie zum Öffnen der App auf das App-Symbol.

Anmelden

Melden Sie sich bei Ihrem Cloud Identity Service-Account auf Ihrem mobilen Gerät an.

Informationen zu diesem Vorgang

Sie können für die Anmeldung bei Ihrem Account einen QR-Code scannen oder einen OTP-Code (Einmalkennwortcode) verwenden. Wenn Ihre Sitzung abläuft, können Sie sich erneut anmelden, indem Sie Ihren Benutzernamen und Ihr Kennwort eingeben.

Mit einem QR-Code anmelden:

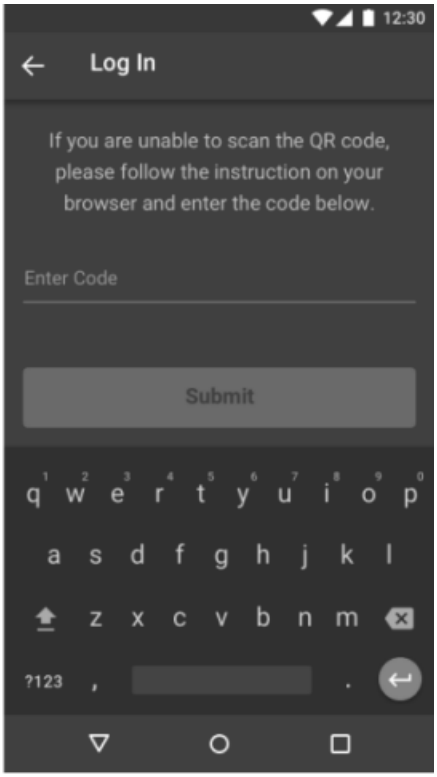
Scannen Sie einen QR-Code, um sich bei Ihrem Account anzumelden. Wenn Sie den QR-Code nicht scannen können, können Sie einen Code manuell eingeben.

Vorgehensweise

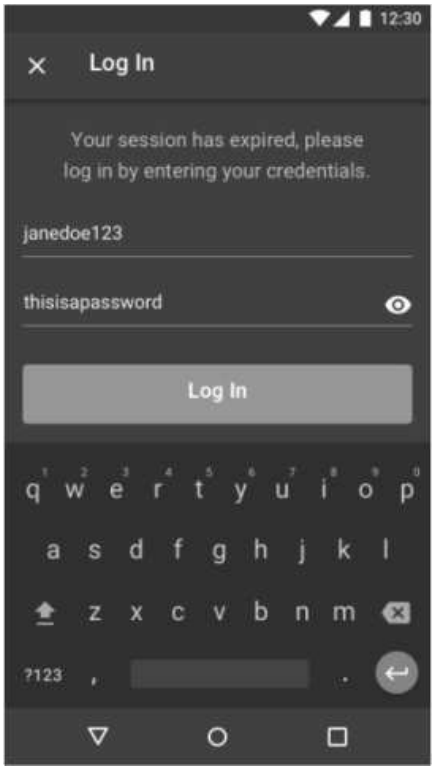
1. Suchen und öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Log In**.

Ein QR-Code wird an Ihren Account gesendet.

2. Rufen Sie auf einem anderen Gerät ***Unternehmen*.ibm.com** auf und scannen Sie den QR-Code. Wenn Sie den QR-Code nicht scannen können, tippen Sie auf **Unable to scan QR code** und befolgen Sie die Anweisungen, um einen Code manuell einzugeben.



3. Wenn Ihre Sitzung abläuft, geben Sie Ihren Benutzernamen und Ihr Kennwort ein und tippen Sie auf **Log In**.

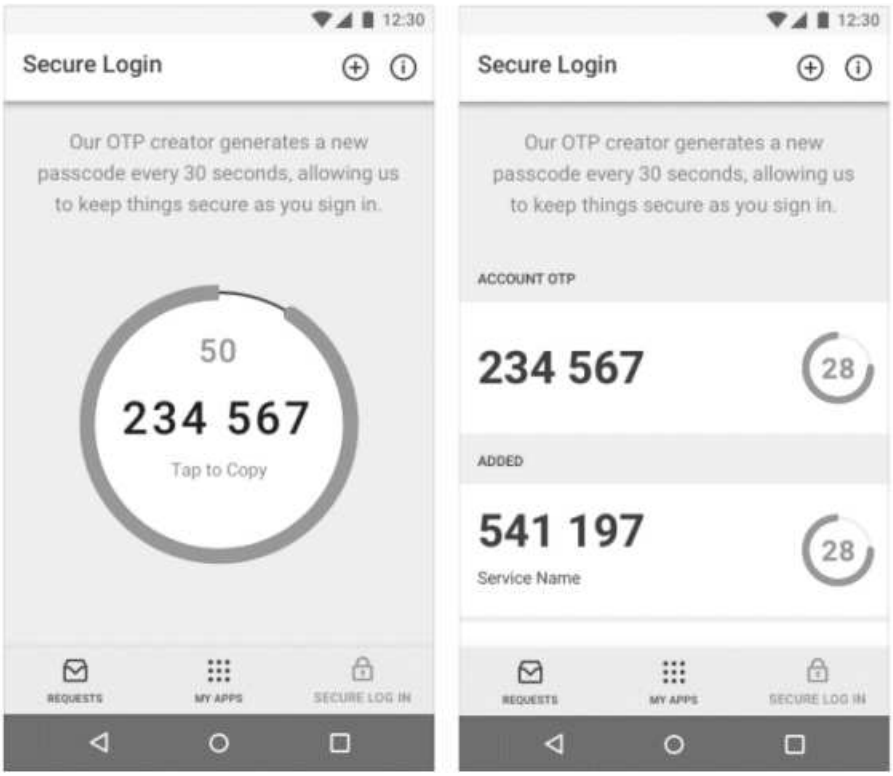


Mit einem Einmalkennwort (OTP) anmelden:

Melden Sie sich mit einem OTP-Code an.

Vorgehensweise

Suchen und öffnen Sie die IBM Mobile-App auf Ihrem Gerät, tippen Sie auf **Secure Log In** und wählen Sie den OTP-Generatorservice aus, den Sie verwenden möchten.



Sie können einen OTP-Generatorservice hinzufügen, indem Sie einen QR-Code scannen oder manuell einen Code eingeben.

Ihre Geräte verwalten

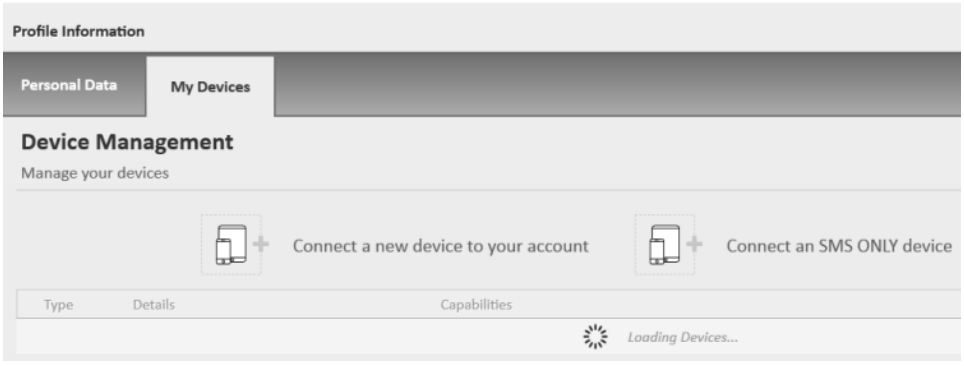
Registrieren und verwalten Sie Ihre Geräte über das Cloud Identity Service-Portal von Cloud Identity Service.

Informationen zu diesem Vorgang

Fügen Sie neue Geräte hinzu und entfernen Sie Geräte, die Sie nicht mehr verwenden. Sie können Nur-SMS-Geräte und vollständig aktivierte Geräte hinzufügen, indem Sie einen QR-Code scannen oder manuell einen Code eingeben. Sie registrieren ein Gerät, wenn Sie sich das erste Mal am Self-Service-Portal anmelden.

Vorgehensweise

1. Melden Sie sich von Ihrem Computer aus am Self-Service-Portal an.
2. Wählen Sie **Profile** > **My Devices** aus.



3. Fügen Sie Geräte hinzu oder entfernen Sie Geräte.

App löschen

Löschen Sie die App, wenn Sie das Gerät nicht mehr verwenden oder den Zugriff auf Cloud Identity Service nicht mehr benötigen.

Informationen zu diesem Vorgang

Anmerkung: Wenn Sie die IBM Mobile-App löschen, wird keine zweistufige Verifizierung entfernt, die für Ihren Cloud Identity Service-Account in Kraft ist.

Vorgehensweise

1. Suchen Sie die IBM Mobile-App auf Ihrem Gerät und wählen Sie sie aus.
2. Tippen Sie auf **Delete**.

Einführung

Starten Sie mit der IBM Mobile-App, indem Sie die App herunterladen und installieren und das Gerät mit Ihrem Cloud Identity Service-Account verbinden.

App herunterladen

Installieren Sie die App auf Ihrem Gerät.

Vorgehensweise

1. Starten Sie den App Store (iOS) oder den Google Play Store (Android).
2. Suchen Sie nach der IBM Mobile-App.
3. Tippen Sie zum Herunterladen der App auf **Get** und **Install**.
4. Tippen Sie zum Öffnen der App auf das App-Symbol.

Anmelden

Melden Sie sich bei Ihrem Cloud Identity Service-Account auf Ihrem mobilen Gerät an.

Informationen zu diesem Vorgang

Sie können für die Anmeldung bei Ihrem Account einen QR-Code scannen oder einen OTP-Code (Einmalkennwortcode) verwenden. Wenn Ihre Sitzung abläuft, können Sie sich erneut anmelden, indem Sie Ihren Benutzernamen und Ihr Kennwort eingeben.

Mit einem QR-Code anmelden:

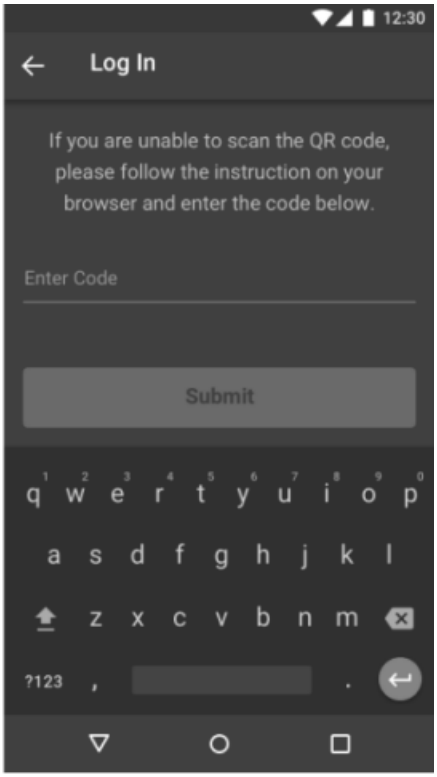
Scannen Sie einen QR-Code, um sich bei Ihrem Account anzumelden. Wenn Sie den QR-Code nicht scannen können, können Sie einen Code manuell eingeben.

Vorgehensweise

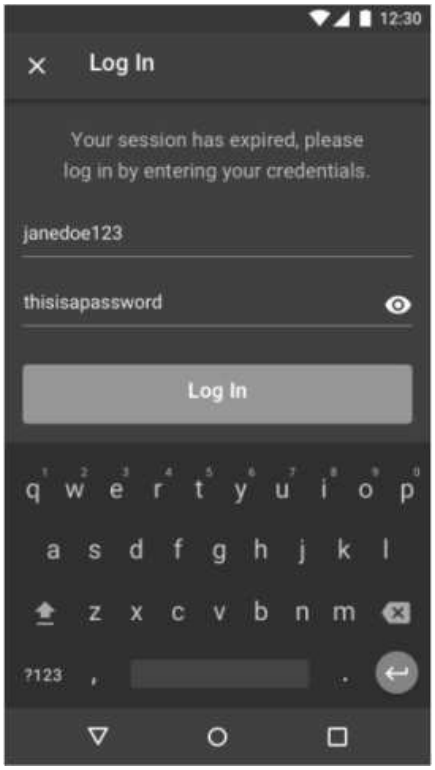
1. Suchen und öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Log In**.

Ein QR-Code wird an Ihren Account gesendet.

2. Rufen Sie auf einem anderen Gerät ***Unternehmen*.ibm.com** auf und scannen Sie den QR-Code. Wenn Sie den QR-Code nicht scannen können, tippen Sie auf **Unable to scan QR code** und befolgen Sie die Anweisungen, um einen Code manuell einzugeben.



3. Wenn Ihre Sitzung abläuft, geben Sie Ihren Benutzernamen und Ihr Kennwort ein und tippen Sie auf **Log In**.

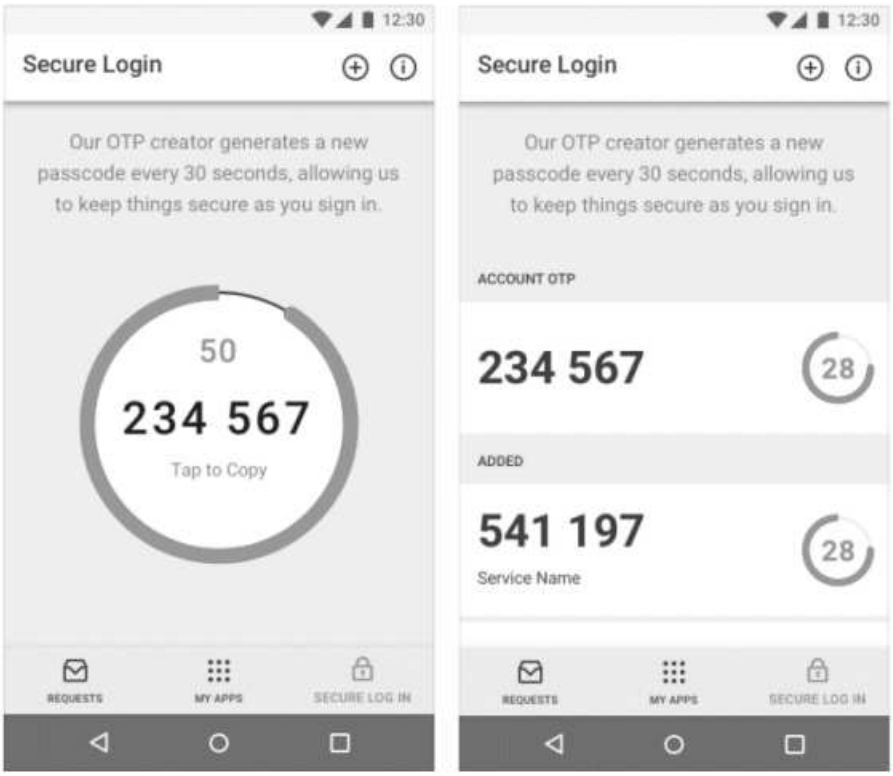


Mit einem Einmalkennwort (OTP) anmelden:

Melden Sie sich mit einem OTP-Code an.

Vorgehensweise

Suchen und öffnen Sie die IBM Mobile-App auf Ihrem Gerät, tippen Sie auf **Secure Log In** und wählen Sie den OTP-Generatorservice aus, den Sie verwenden möchten.



Sie können einen OTP-Generatorservice hinzufügen, indem Sie einen QR-Code scannen oder manuell einen Code eingeben.

Ihre Geräte verwalten

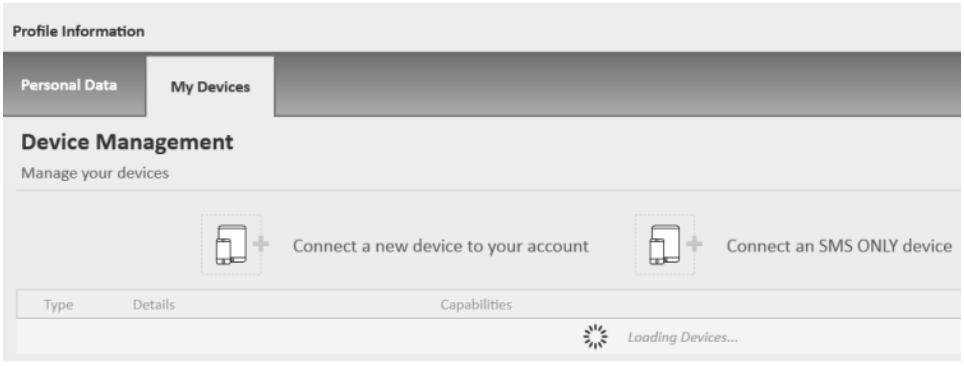
Registrieren und verwalten Sie Ihre Geräte über das Cloud Identity Service-Portal von Cloud Identity Service.

Informationen zu diesem Vorgang

Fügen Sie neue Geräte hinzu und entfernen Sie Geräte, die Sie nicht mehr verwenden. Sie können Nur-SMS-Geräte und vollständig aktivierte Geräte hinzufügen, indem Sie einen QR-Code scannen oder manuell einen Code eingeben. Sie registrieren ein Gerät, wenn Sie sich das erste Mal am Self-Service-Portal anmelden.

Vorgehensweise

1. Melden Sie sich von Ihrem Computer aus am Self-Service-Portal an.
2. Wählen Sie **Profile** > **My Devices** aus.



3. Fügen Sie Geräte hinzu oder entfernen Sie Geräte.

App löschen

Löschen Sie die App, wenn Sie das Gerät nicht mehr verwenden oder den Zugriff auf Cloud Identity Service nicht mehr benötigen.

Informationen zu diesem Vorgang

Anmerkung: Wenn Sie die IBM Mobile-App löschen, wird keine zweistufige Verifizierung entfernt, die für Ihren Cloud Identity Service-Account in Kraft ist.

Vorgehensweise

1. Suchen Sie die IBM Mobile-App auf Ihrem Gerät und wählen Sie sie aus.
2. Tippen Sie auf **Delete**.

Services verwalten und Apps starten

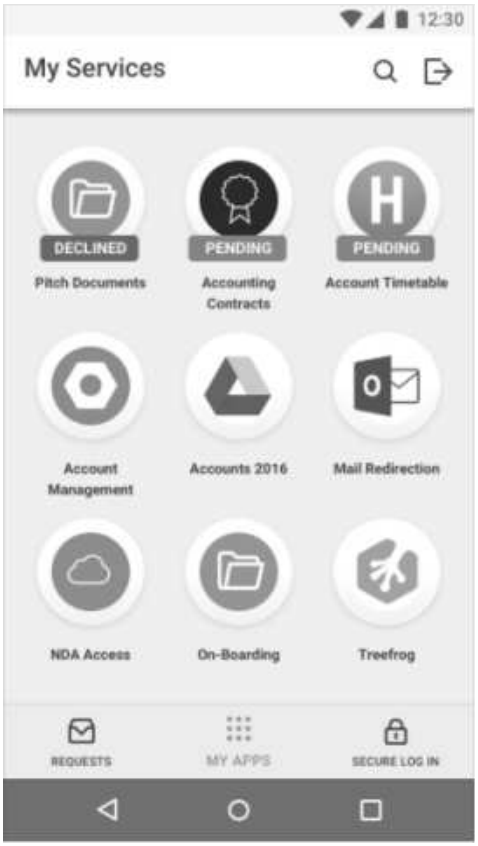
Verwenden Sie die IBM Mobile-App, um Ihre Services anzuzeigen und Zugriff auf Services anzufordern.

Services anzeigen und Anwendungen starten

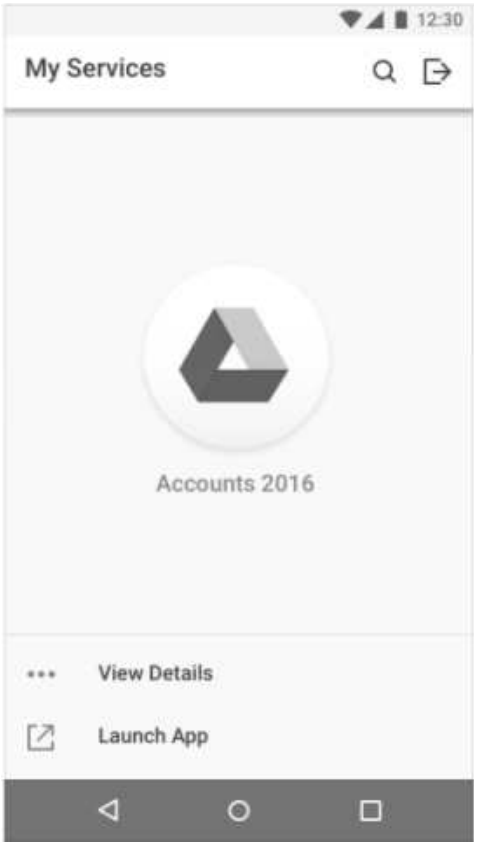
Sie können Services anzeigen, auf die Sie zugreifen können, und Sie können verlinkte Anwendungen starten.

Vorgehensweise

1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **My Apps**.



2. Tippen Sie zum Öffnen des Service auf das Symbol.



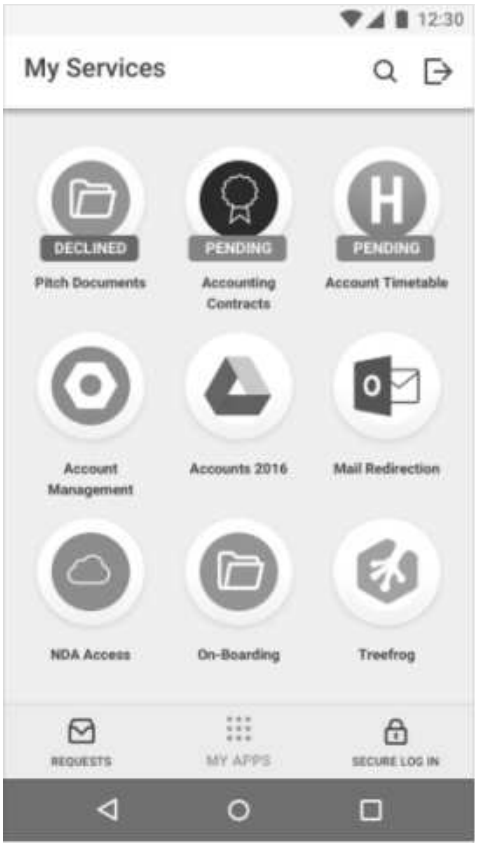
3. Tippen Sie auf **View Details**, um Details zum Service anzuzeigen, oder tippen Sie auf **Launch App**, um die mit dem Service verlinkte Anwendung zu starten.

Zugriff auf einen Service anfordern

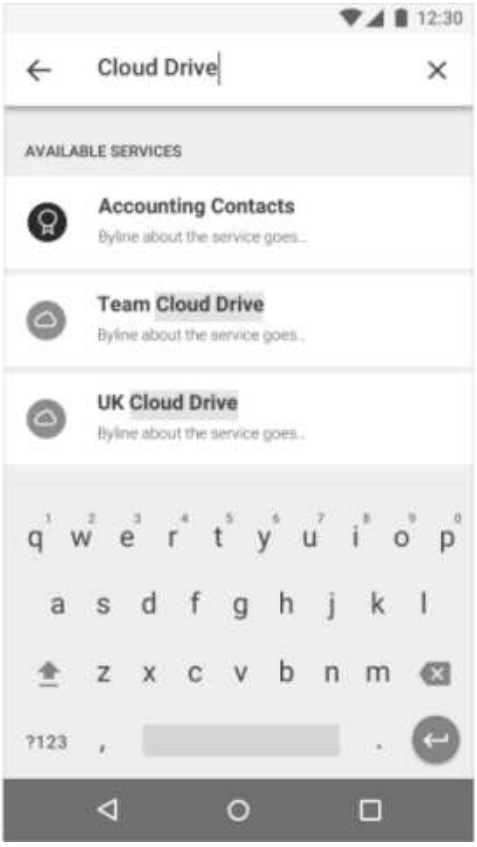
Um Zugriff auf Services und verlinkte Anwendungen zu erhalten, suchen Sie nach dem Service und übergeben Sie eine Anforderung.

Vorgehensweise

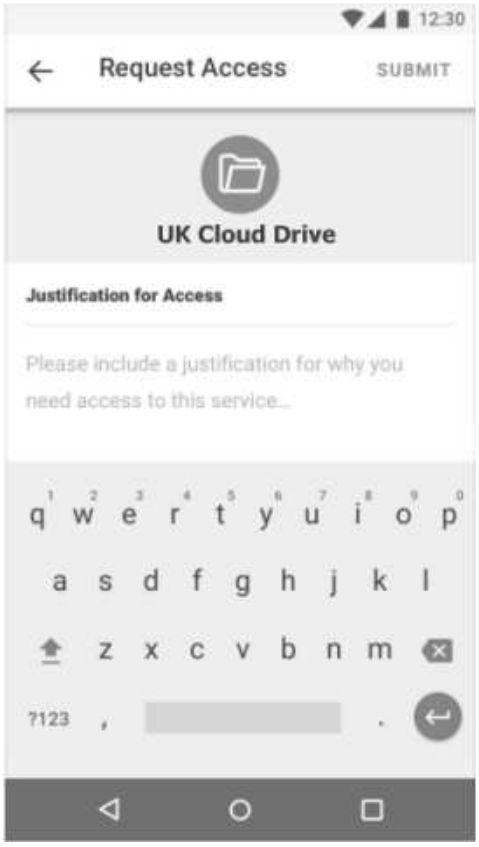
1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **My Apps**.



2. Suchen Sie unter den verfügbaren Services nach dem Service.



3. Tippen Sie zum Auswählen auf den Service, geben Sie eine Begründung für die Anforderung des Service ein und tippen Sie auf **Submit**.



Der Status des Service ändert sich in "pending" (anstehend). Ihr Manager kann Ihre Anforderung akzeptieren oder ablehnen.

Services verwalten und Apps starten

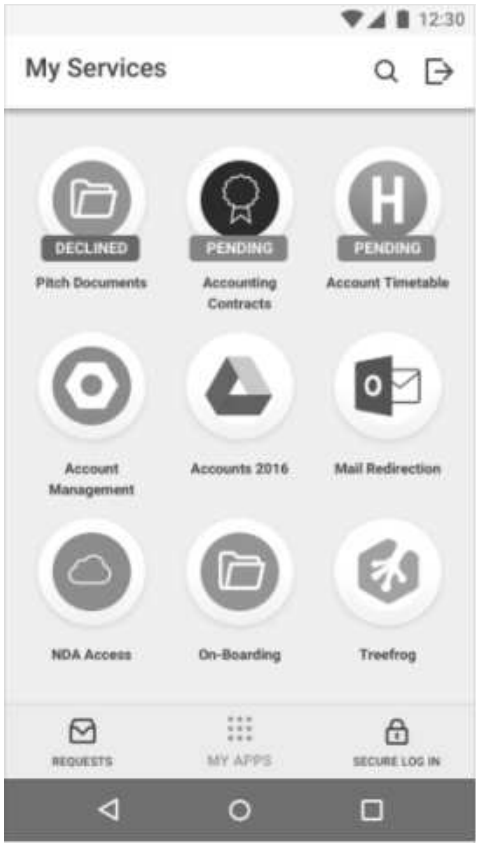
Verwenden Sie die IBM Mobile-App, um Ihre Services anzuzeigen und Zugriff auf Services anzufordern.

Services anzeigen und Anwendungen starten

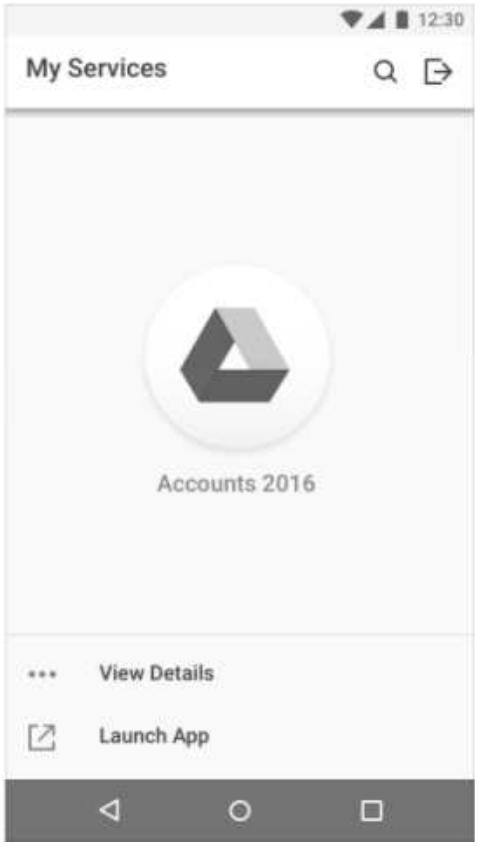
Sie können Services anzeigen, auf die Sie zugreifen können, und Sie können verlinkte Anwendungen starten.

Vorgehensweise

1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **My Apps**.



2. Tippen Sie zum Öffnen des Service auf das Symbol.



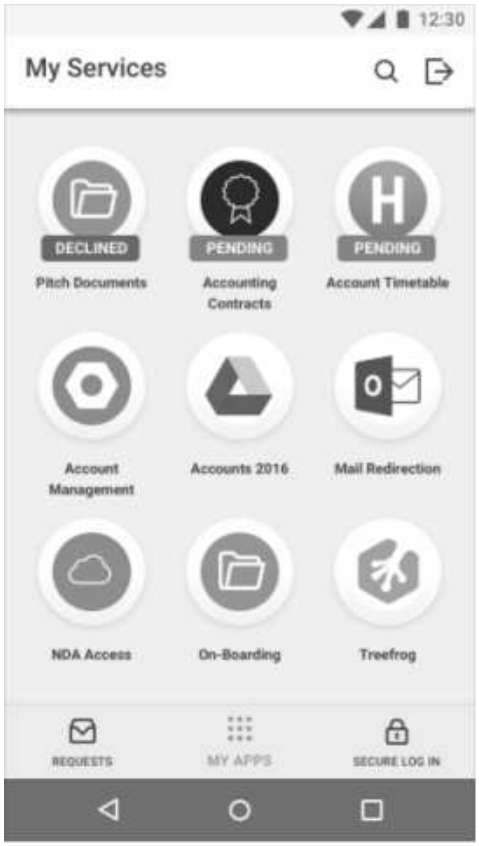
3. Tippen Sie auf **View Details**, um Details zum Service anzuzeigen, oder tippen Sie auf **Launch App**, um die mit dem Service verlinkte Anwendung zu starten.

Zugriff auf einen Service anfordern

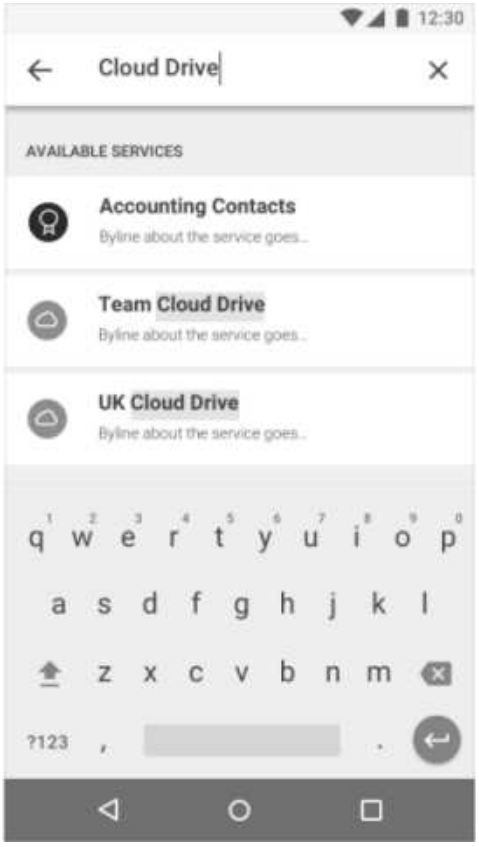
Um Zugriff auf Services und verlinkte Anwendungen zu erhalten, suchen Sie nach dem Service und übergeben Sie eine Anforderung.

Vorgehensweise

1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **My Apps**.



2. Suchen Sie unter den verfügbaren Services nach dem Service.



3. Tippen Sie zum Auswählen auf den Service, geben Sie eine Begründung für die Anforderung des Service ein und tippen Sie auf **Submit**.

Der Status des Service ändert sich in "pending" (anstehend). Ihr Manager kann Ihre Anforderung akzeptieren oder ablehnen.

Services verwalten und Apps starten

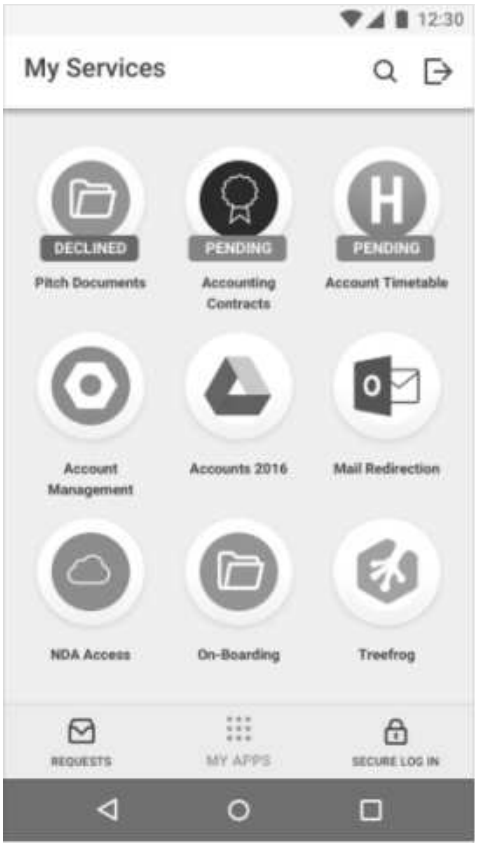
Verwenden Sie die IBM Mobile-App, um Ihre Services anzuzeigen und Zugriff auf Services anzufordern.

Services anzeigen und Anwendungen starten

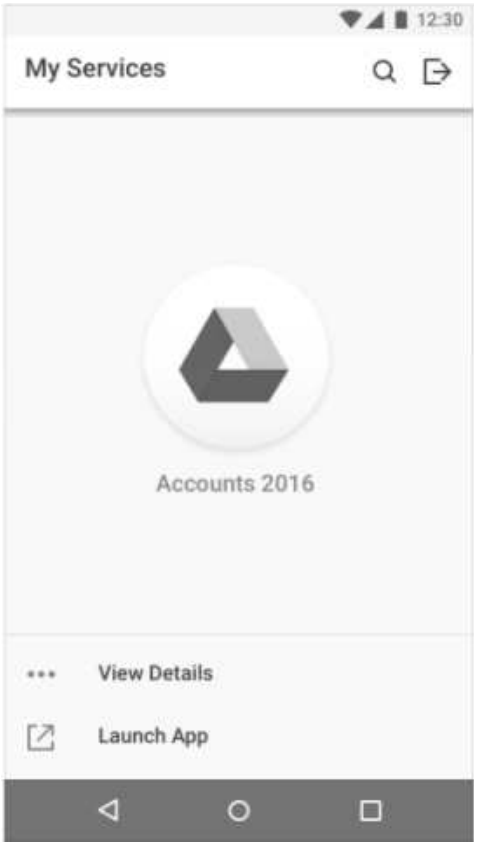
Sie können Services anzeigen, auf die Sie zugreifen können, und Sie können verlinkte Anwendungen starten.

Vorgehensweise

1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **My Apps**.



2. Tippen Sie zum Öffnen des Service auf das Symbol.



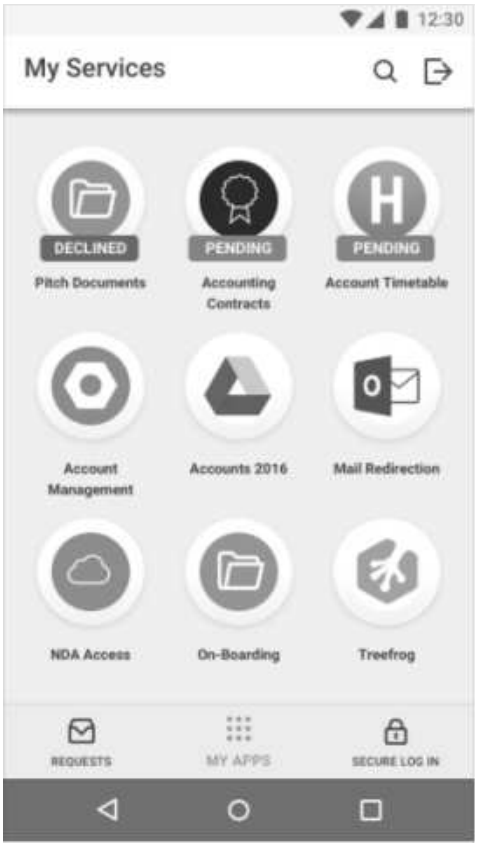
3. Tippen Sie auf **View Details**, um Details zum Service anzuzeigen, oder tippen Sie auf **Launch App**, um die mit dem Service verlinkte Anwendung zu starten.

Zugriff auf einen Service anfordern

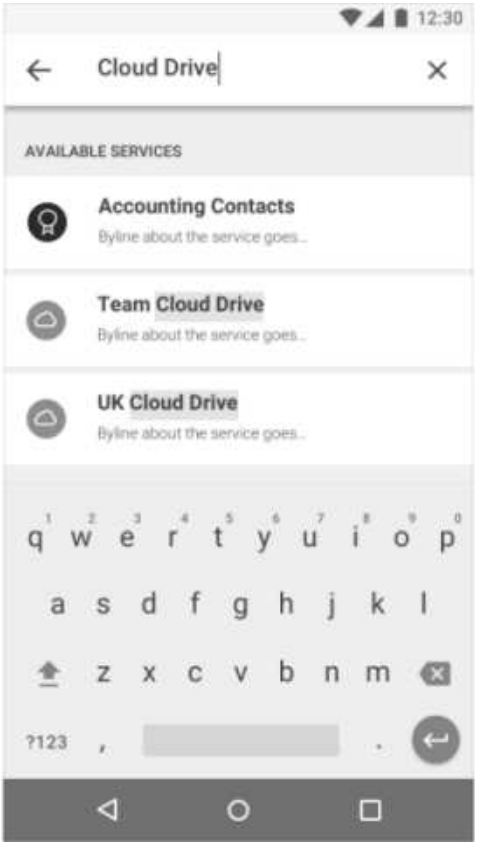
Um Zugriff auf Services und verlinkte Anwendungen zu erhalten, suchen Sie nach dem Service und übergeben Sie eine Anforderung.

Vorgehensweise

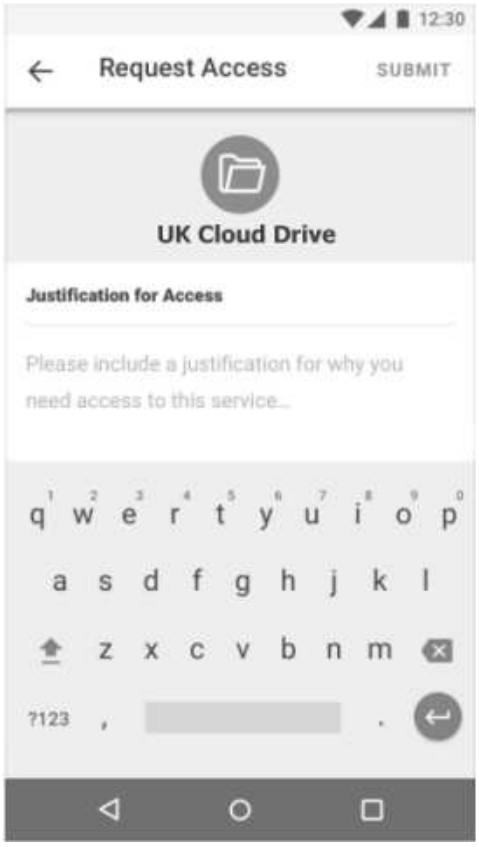
1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **My Apps**.



2. Suchen Sie unter den verfügbaren Services nach dem Service.



3. Tippen Sie zum Auswählen auf den Service, geben Sie eine Begründung für die Anforderung des Service ein und tippen Sie auf **Submit**.



Der Status des Service ändert sich in "pending" (anstehend). Ihr Manager kann Ihre Anforderung akzeptieren oder ablehnen.

Anforderungen verwalten

Verwenden Sie die IBM Mobile-App, um Anforderungen für Services zu genehmigen und abzulehnen.

Informationen zu diesem Vorgang

Diese Task dient Benutzermanagern zum Genehmigen oder Ablehnen von Mitarbeiteranforderungen bzgl. des Zugriffs auf Services. Sie können Anforderungen auswählen, indem Sie nach Mitarbeitern oder Services suchen.

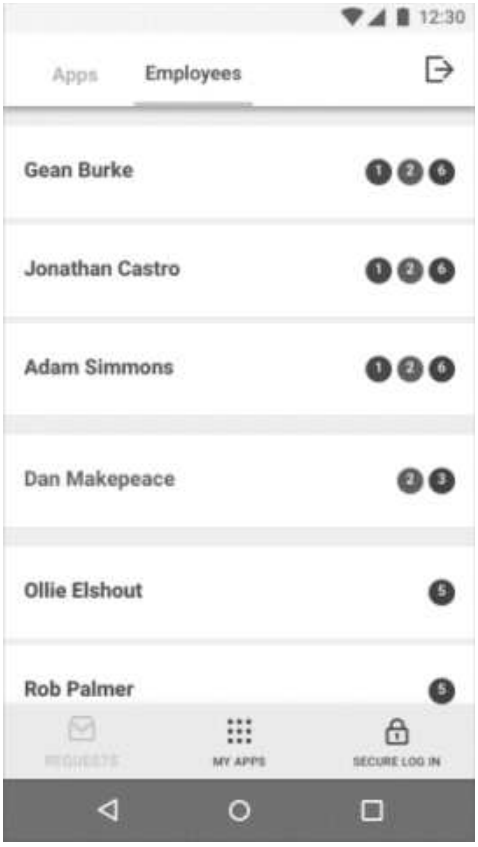
Die Anzahl der ausstehenden Genehmigungen und deren Status werden für jeden der verwalteten Benutzer angezeigt. Überfällige Genehmigungen werden rot dargestellt. Nahezu fällige Genehmigungen sind gelb gefärbt. Genehmigungen, die nicht überfällig oder nahezu überfällig sind, werden dunkelgrau gefärbt.

Nach Mitarbeitern suchen

Suchen Sie Genehmigungen nach Mitarbeitern.

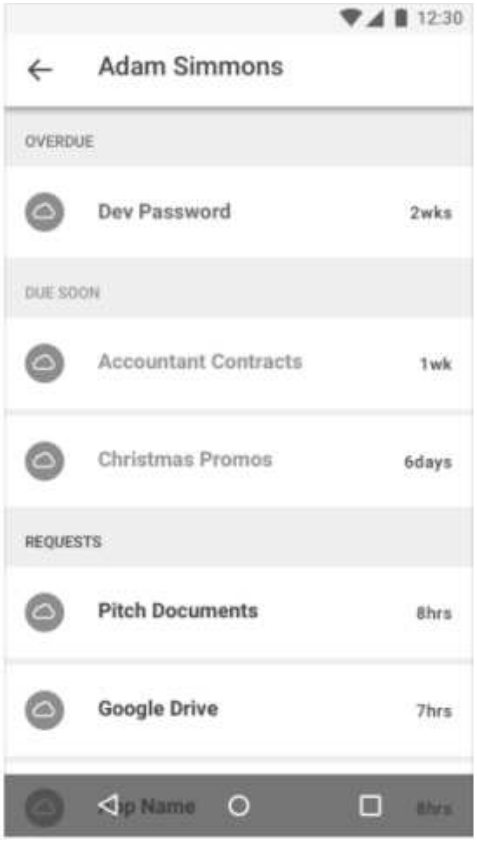
Vorgehensweise

1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Requests** und dann auf **Employees**.



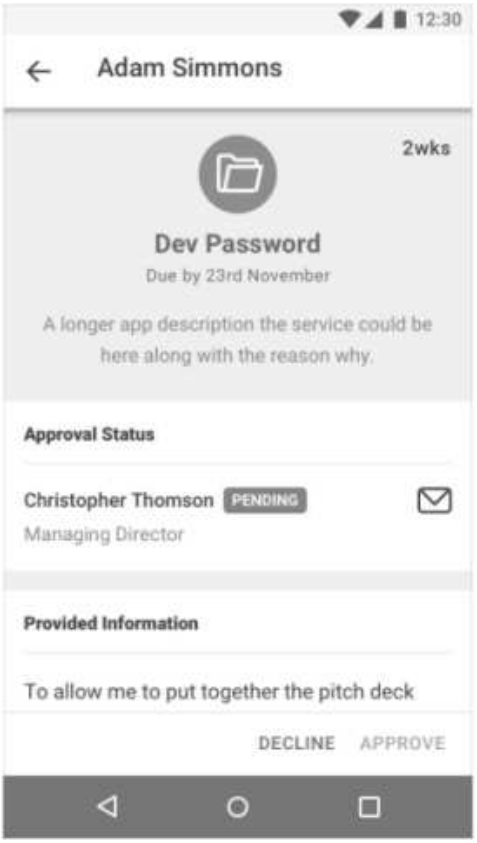
Mitarbeiteranforderungen werden nach Datum und Uhrzeit der Genehmigung geordnet. Mitarbeiter mit Anforderungen mit der höchsten Überfälligkeit werden zuerst angezeigt. Die Anzahl der Anforderungen und der Status der Anforderungen werden ebenfalls angezeigt.

2. Tippen Sie auf den Mitarbeiter, für den Sie Anforderungen verwalten möchten.

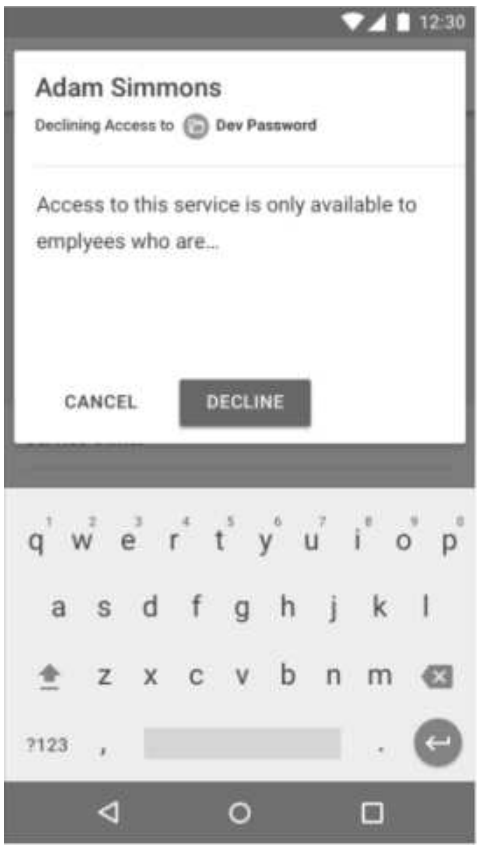


Anforderungen werden jetzt nach Service und nach Datum und Uhrzeit der Fälligkeit sortiert.

3. Tippen Sie auf einen Service, um die Anforderung für diesen Service anzuzeigen.



4. Genehmigen Sie die Anforderung oder lehnen Sie sie ab:
   - Tippen Sie zum Genehmigen der Anforderung auf **Approve**.
   - Tippen Sie zum Ablehnen der Anforderung auf **Decline** und geben Sie bei Bedarf eine Begründung ein.

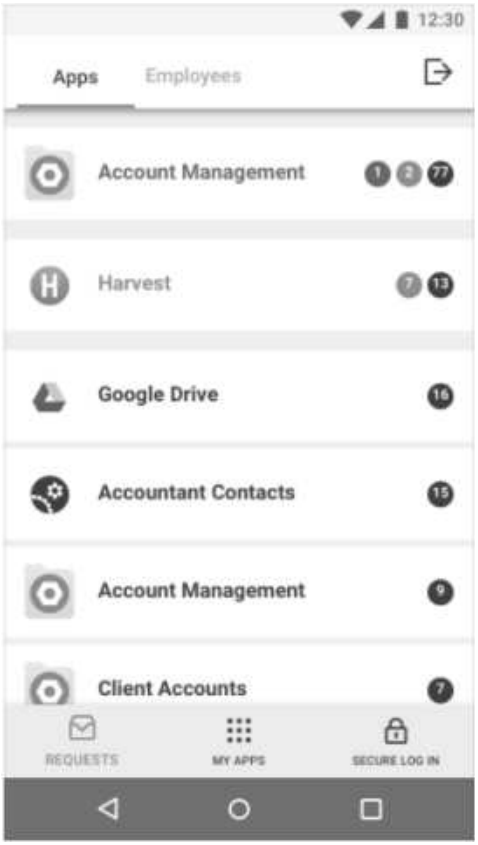


Nach Service suchen

Suchen Sie Genehmigungen nach Service.

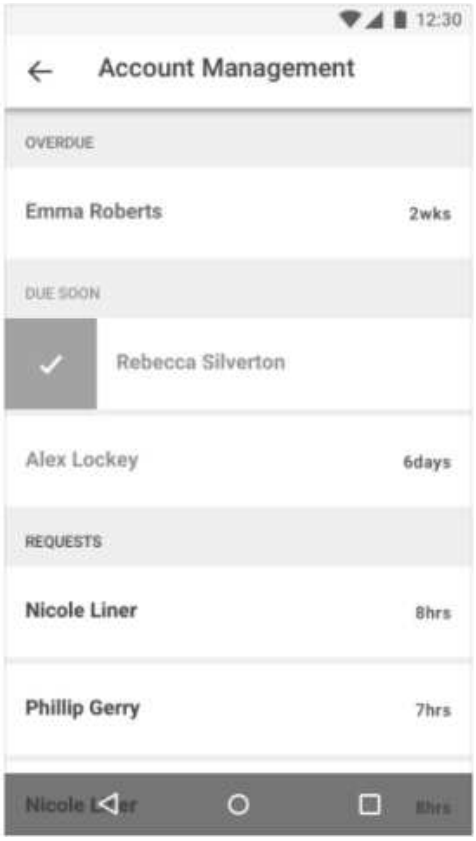
Vorgehensweise

1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Requests** und dann auf **Apps**.



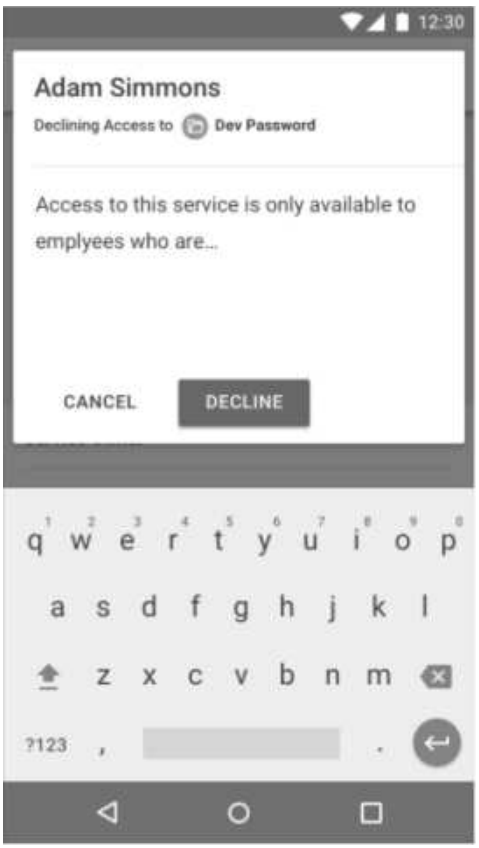
Anforderungen werden nach Datum und Uhrzeit der Genehmigung geordnet. Services mit Anforderungen mit der höchsten Überfälligkeit werden zuerst angezeigt. Die Anzahl der Anforderungen und der Status der Anforderungen werden ebenfalls angezeigt.

2. Tippen Sie auf den Service, für den Sie Anforderungen verwalten möchten.



Anforderungen werden jetzt nach Mitarbeiter und nach Datum und Uhrzeit der Fälligkeit sortiert.

3. Wählen Sie den Mitarbeiter aus, für den Sie die Anforderung verwalten möchten, und genehmigen Sie die Anforderung oder lehnen Sie sie ab:
   - Tippen Sie zum Genehmigen der Anforderung auf .
   - Tippen Sie zum Ablehnen der Anforderung auf und geben Sie bei Bedarf eine Begründung ein.



Anforderungen verwalten

Verwenden Sie die IBM Mobile-App, um Anforderungen für Services zu genehmigen und abzulehnen.

Informationen zu diesem Vorgang

Diese Task dient Benutzermanagern zum Genehmigen oder Ablehnen von Mitarbeiteranforderungen bzgl. des Zugriffs auf Services. Sie können Anforderungen auswählen, indem Sie nach Mitarbeitern oder Services suchen.

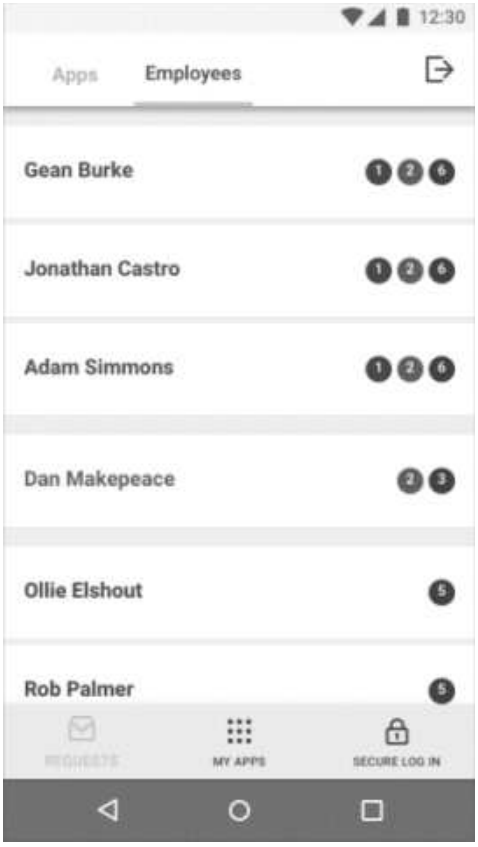
Die Anzahl der ausstehenden Genehmigungen und deren Status werden für jeden der verwalteten Benutzer angezeigt. Überfällige Genehmigungen werden rot dargestellt. Nahezu fällige Genehmigungen sind gelb gefärbt. Genehmigungen, die nicht überfällig oder nahezu überfällig sind, werden dunkelgrau gefärbt.

Nach Mitarbeitern suchen

Suchen Sie Genehmigungen nach Mitarbeitern.

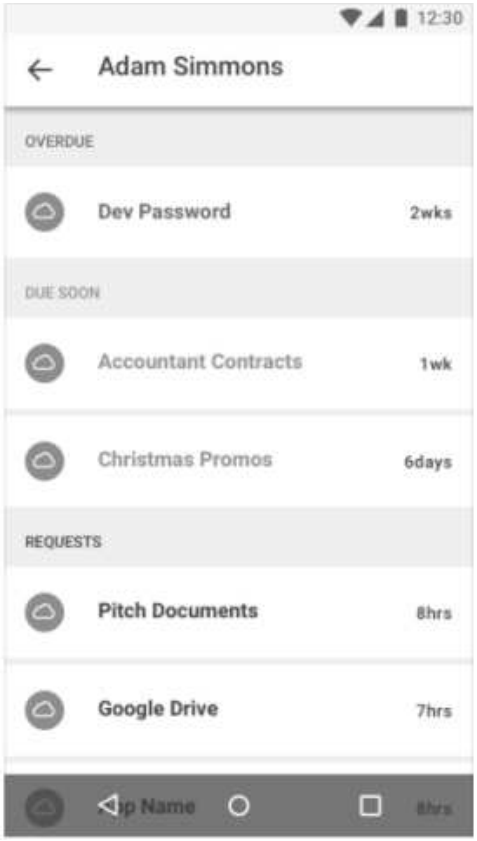
Vorgehensweise

1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Requests** und dann auf **Employees**.



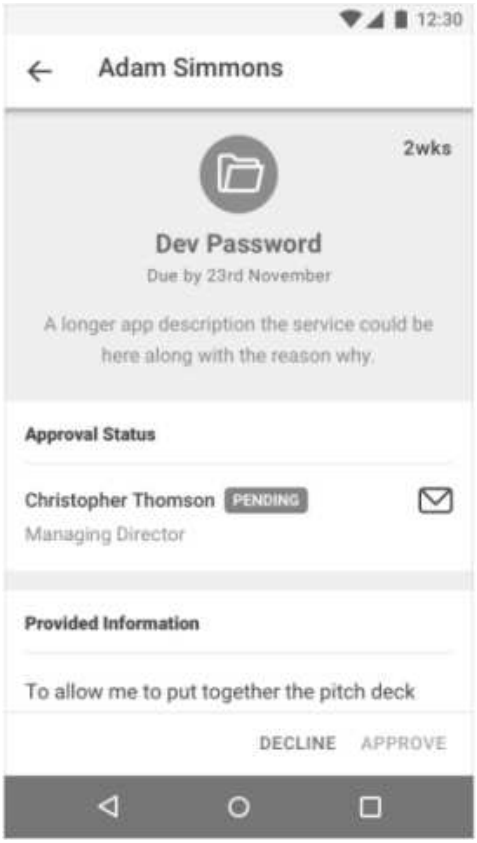
Mitarbeiteranforderungen werden nach Datum und Uhrzeit der Genehmigung geordnet. Mitarbeiter mit Anforderungen mit der höchsten Überfälligkeit werden zuerst angezeigt. Die Anzahl der Anforderungen und der Status der Anforderungen werden ebenfalls angezeigt.

2. Tippen Sie auf den Mitarbeiter, für den Sie Anforderungen verwalten möchten.

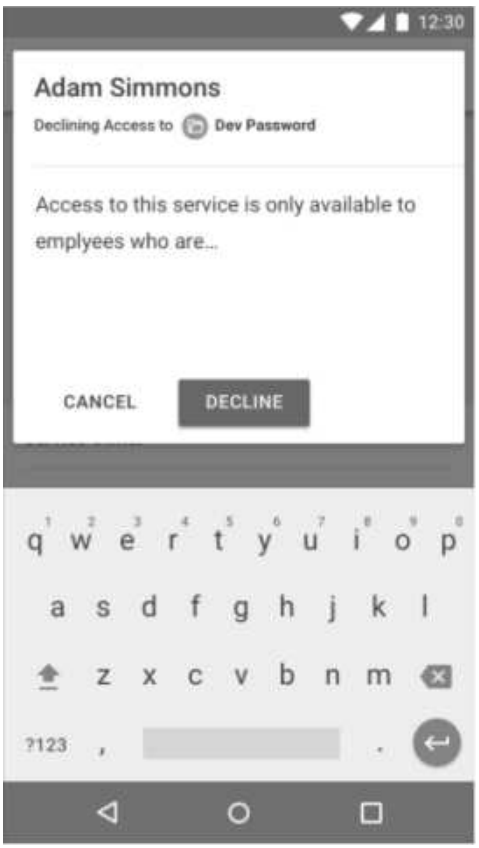


Anforderungen werden jetzt nach Service und nach Datum und Uhrzeit der Fälligkeit sortiert.

3. Tippen Sie auf einen Service, um die Anforderung für diesen Service anzuzeigen.



4. Genehmigen Sie die Anforderung oder lehnen Sie sie ab:
   - Tippen Sie zum Genehmigen der Anforderung auf **Approve**.
   - Tippen Sie zum Ablehnen der Anforderung auf **Decline** und geben Sie bei Bedarf eine Begründung ein.

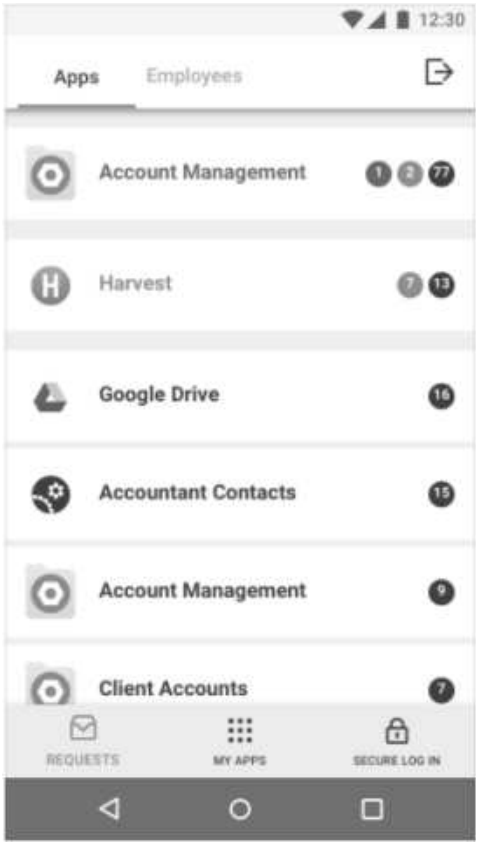


Nach Service suchen

Suchen Sie Genehmigungen nach Service.

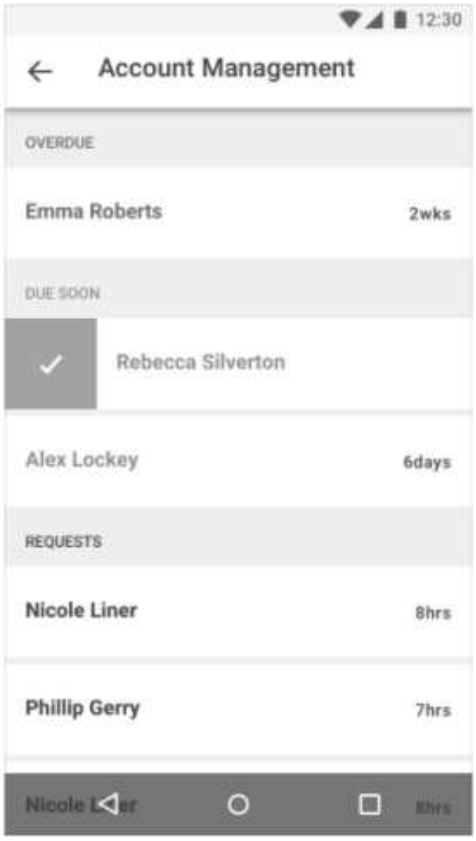
Vorgehensweise

1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Requests** und dann auf **Apps**.



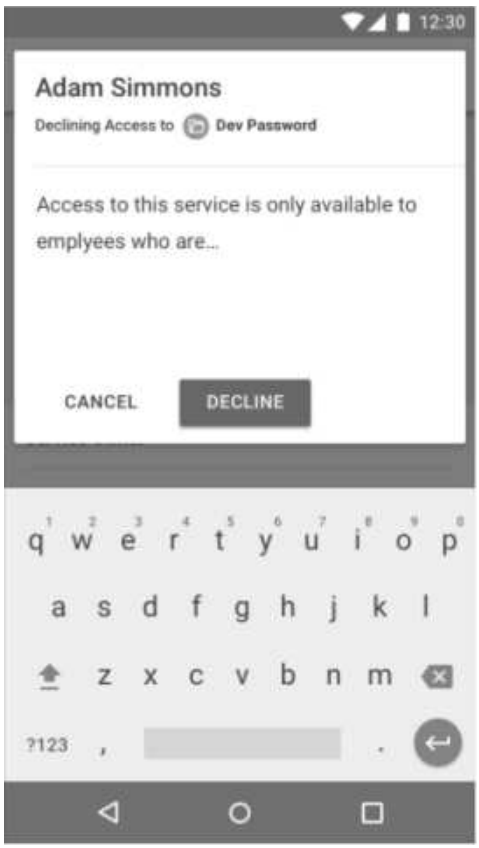
Anforderungen werden nach Datum und Uhrzeit der Genehmigung geordnet. Services mit Anforderungen mit der höchsten Überfälligkeit werden zuerst angezeigt. Die Anzahl der Anforderungen und der Status der Anforderungen werden ebenfalls angezeigt.

2. Tippen Sie auf den Service, für den Sie Anforderungen verwalten möchten.



Anforderungen werden jetzt nach Mitarbeiter und nach Datum und Uhrzeit der Fälligkeit sortiert.

3. Wählen Sie den Mitarbeiter aus, für den Sie die Anforderung verwalten möchten, und genehmigen Sie die Anforderung oder lehnen Sie sie ab:
   - Tippen Sie zum Genehmigen der Anforderung auf .
   - Tippen Sie zum Ablehnen der Anforderung auf und geben Sie bei Bedarf eine Begründung ein.



Anforderungen verwalten

Verwenden Sie die IBM Mobile-App, um Anforderungen für Services zu genehmigen und abzulehnen.

Informationen zu diesem Vorgang

Diese Task dient Benutzermanagern zum Genehmigen oder Ablehnen von Mitarbeiteranforderungen bzgl. des Zugriffs auf Services. Sie können Anforderungen auswählen, indem Sie nach Mitarbeitern oder Services suchen.

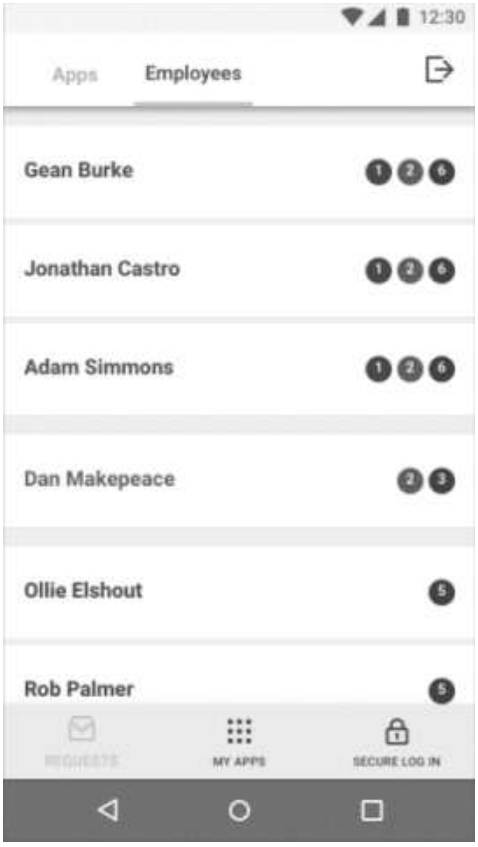
Die Anzahl der ausstehenden Genehmigungen und deren Status werden für jeden der verwalteten Benutzer angezeigt. Überfällige Genehmigungen werden rot dargestellt. Nahezu fällige Genehmigungen sind gelb gefärbt. Genehmigungen, die nicht überfällig oder nahezu überfällig sind, werden dunkelgrau gefärbt.

Nach Mitarbeitern suchen

Suchen Sie Genehmigungen nach Mitarbeitern.

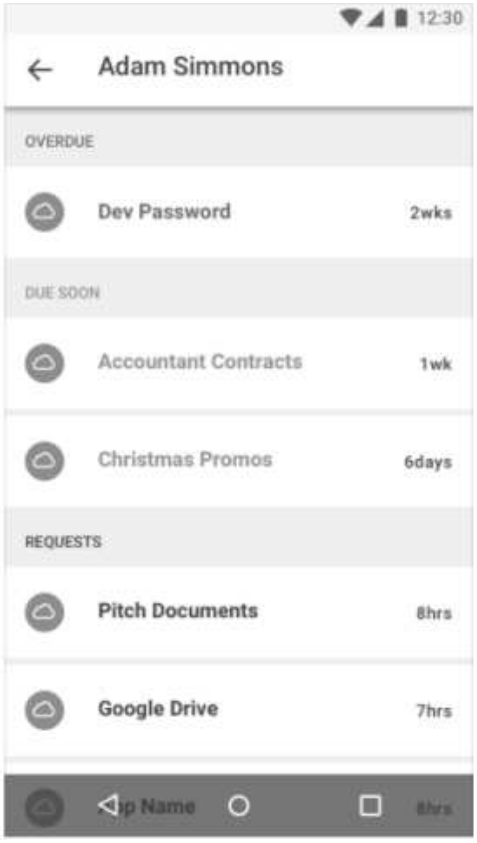
Vorgehensweise

1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Requests** und dann auf **Employees**.



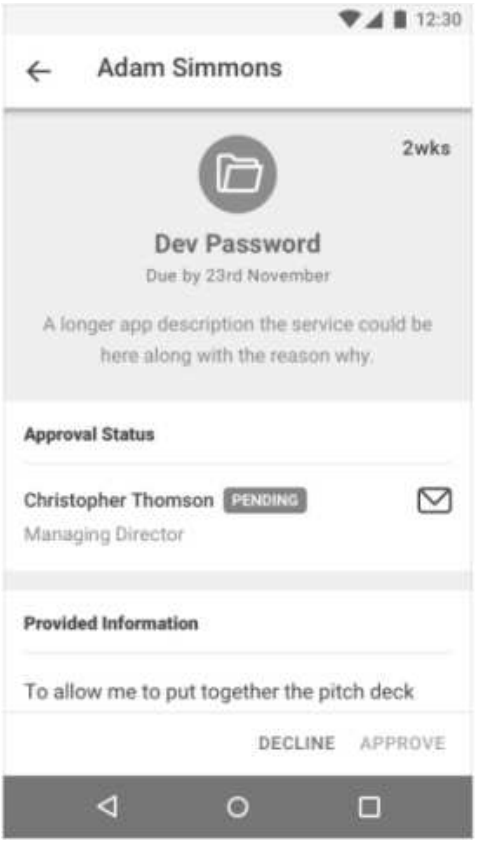
Mitarbeiteranforderungen werden nach Datum und Uhrzeit der Genehmigung geordnet. Mitarbeiter mit Anforderungen mit der höchsten Überfälligkeit werden zuerst angezeigt. Die Anzahl der Anforderungen und der Status der Anforderungen werden ebenfalls angezeigt.

2. Tippen Sie auf den Mitarbeiter, für den Sie Anforderungen verwalten möchten.

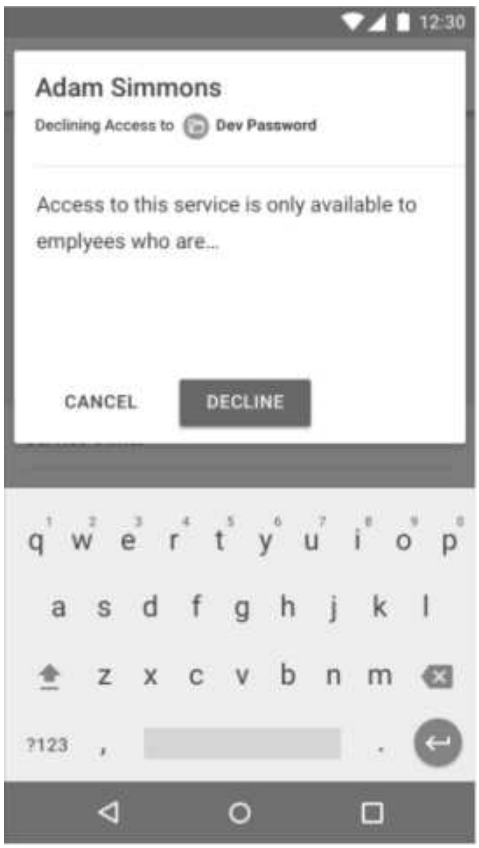


Anforderungen werden jetzt nach Service und nach Datum und Uhrzeit der Fälligkeit sortiert.

3. Tippen Sie auf einen Service, um die Anforderung für diesen Service anzuzeigen.



4. Genehmigen Sie die Anforderung oder lehnen Sie sie ab:
   - Tippen Sie zum Genehmigen der Anforderung auf **Approve**.
   - Tippen Sie zum Ablehnen der Anforderung auf **Decline** und geben Sie bei Bedarf eine Begründung ein.

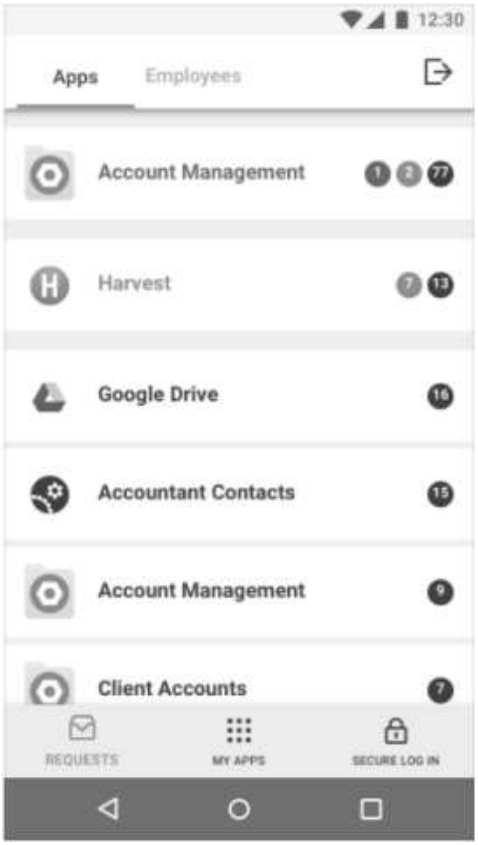


Nach Service suchen

Suchen Sie Genehmigungen nach Service.

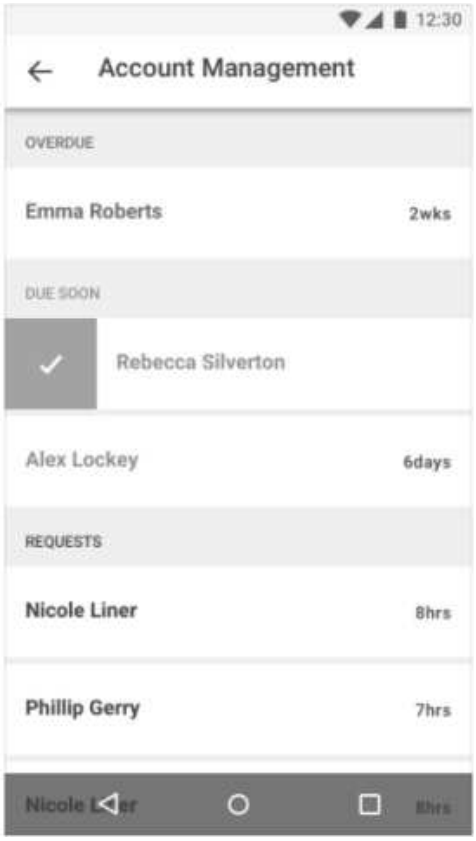
Vorgehensweise

1. Öffnen Sie die IBM Mobile-App auf Ihrem Gerät und tippen Sie auf **Requests** und dann auf **Apps**.



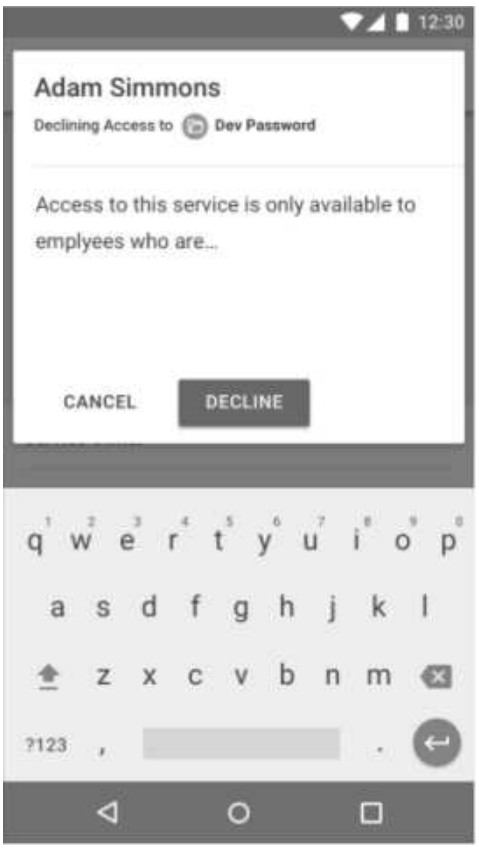
Anforderungen werden nach Datum und Uhrzeit der Genehmigung geordnet. Services mit Anforderungen mit der höchsten Überfälligkeit werden zuerst angezeigt. Die Anzahl der Anforderungen und der Status der Anforderungen werden ebenfalls angezeigt.

2. Tippen Sie auf den Service, für den Sie Anforderungen verwalten möchten.



Anforderungen werden jetzt nach Mitarbeiter und nach Datum und Uhrzeit der Fälligkeit sortiert.

3. Wählen Sie den Mitarbeiter aus, für den Sie die Anforderung verwalten möchten, und genehmigen Sie die Anforderung oder lehnen Sie sie ab:
   - Tippen Sie zum Genehmigen der Anforderung auf .
   - Tippen Sie zum Ablehnen der Anforderung auf und geben Sie bei Bedarf eine Begründung ein.


12:30
Adam Simmons
Declining Access to Dev Password
Access to this service is only available to emplyees who are...
CANCEL
DECLINE
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
?123

Kapitel 9. Richtlinien

Richtlinien werden verwendet, um den Benutzerzugriff auf verschiedene Ressourcen zu bestimmen oder zu optimieren.

Globale Benutzerrichtlinie erstellen

Benutzerrichtlinien definieren die maximale Anzahl an fehlgeschlagenen Anmeldeversuchen, die maximal zulässige Gültigkeitsdauer des Kennworts und das Accountablaufdatum für Benutzer. Globale Benutzerrichtlinien werden auf alle Benutzer angewandt.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Policies** > **Global User Policies**.
2. Legen Sie die gewünschten Benutzerrichtlinieneinstellungen fest.
3. Klicken Sie auf **Save**.

Benutzerrichtlinieneinstellungen

Tabelle 41. Benutzerrichtlinieneinstellungen

Einstellung	Beschreibung
Maximum Login Failures	Die maximale Anzahl an fehlgeschlagenen Anmeldeversuchen, die ein Benutzer durchführen kann, bevor der Account gesperrt wird. Ist diese Option auf "0" oder "Unset" gesetzt, ist die Anzahl der fehlgeschlagenen Anmeldeversuche unbegrenzt. • **Set**. Die maximale Anzahl der fehlgeschlagenen Anmeldeversuche. Ist diese Option auf "0" gesetzt, ist die Anzahl der fehlgeschlagenen Anmeldeversuche unbegrenzt. • **Unset**. Unbegrenzte Anzahl der fehlgeschlagenen Anmeldeversuche.

Tabelle 41. Benutzerrichtlinieneinstellungen (Forts.)

Einstellung	Beschreibung
Disable Time Interval	Gibt an, ob Benutzeraccounts gesperrt werden, nachdem die Anzahl für "Max Login Failures" überschritten wurde. • **Set**. Benutzeraccounts werden gesperrt, nachdem die Anzahl für "Max Login Failures" überschritten wurde. Accounts werden dauerhaft oder vorübergehend inaktiviert. • **Unset**. Benutzeraccounts werden nie aufgrund von fehlgeschlagenen Anmeldeversuchen gesperrt. "Unset" entspricht dem Festlegen des Werts für "Max Login Failures" auf "0" oder auf "Unset". Benutzer können eine unbegrenzte Anzahl an Anmeldeversuchen durchführen. • **Disable Permanently**. Der Benutzer wird dauerhaft gesperrt, bis ein Cloud Identity Portal-Administrator den Benutzerstatus des Benutzers auf "valid" setzt. • **Disable Temporarily**. Die Zeit in Sekunden, für die ein Benutzeraccount gesperrt bleibt, nachdem die zulässige Anzahl für "Max Login Failures" überschritten wurde. Der Account wird nach Ablauf der Intervallzeit entsperrt.
Minimum Length	Die minimale Anzahl der Zeichen, die für ein gültiges Accountkennwort erforderlich sind. • **Set**. Die minimale Anzahl der Zeichen für ein Kennwort. • **Unset**. Keine Mindestlänge für das Kennwort.
Minimum Alphas	Die minimale Anzahl der alphabetischen Zeichen, die für Accountkennwörter erforderlich sind. • **Set**. Die minimale Anzahl der alphabetischen Zeichen, die das Accountkennwort enthalten muss. • **Unset**. Es gibt keinen Mindestwert.
Minimum Non-Alphas	Die minimale Anzahl der nicht alphabetischen Zeichen (Zahlen oder Sonderzeichen), die für Accountkennwörter erforderlich sind. • **Set**. Die minimale Anzahl der nicht alphabetischen Zeichen, die das Accountkennwort enthalten muss. Ist der Wert auf "0" gesetzt, gibt es keinen Mindestwert. • **Unset**. Es gibt keinen Mindestwert.
Maximum Repeated Characters	Die maximale Anzahl der aufeinanderfolgenden wiederholten Zeichen, die in einem Accountkennwort gültig sind. • **Set**. Die maximale Anzahl an wiederholten Zeichen, die gültig sind. • **Unset**. Unbegrenzte Anzahl an wiederholten Zeichen.
Spaces Allowed?	Gibt an, ob Accountkennwörter Leerzeichen enthalten können. • **Set**. Gibt an, ob Leerzeichen zulässig sind. – **Yes**. Leerzeichen sind zulässig. – **No**. Leerzeichen sind nicht zulässig. • **Unset**. Leerzeichen sind zulässig.
Password Expires?	Die Höchstdauer, für die Kennwörter nach der Erstellung gültig bleiben, bevor sie ablaufen und geändert werden müssen. • **Yes**. Die Anzahl der Tage, Stunden, Minuten und Sekunden, für die ein Kennwort gültig bleibt. Wenn alle Werte auf 0 gesetzt sind, laufen Kennwörter nie ab. • **No**. Kennwörter laufen nie ab.

Tabelle 41. Benutzerrichtlinieneinstellungen (Forts.)

Einstellung	Beschreibung
Track Password Reuse?	Gibt an, ob bei einer Kennwortzurücksetzung dasselbe Kennwort verwendet werden kann. • **Yes**. Benutzer können nicht dasselbe Kennwort verwenden, wenn sie ihr Kennwort zurücksetzen oder ändern. Geben Sie die Anzahl neuer eindeutiger Kennwörter an, die angegeben werden muss, bevor ein altes Kennwort wiederverwendet werden kann. • **No**. Benutzer können dasselbe Kennwort verwenden, wenn sie ihr Kennwort zurücksetzen.
Account Expires?	Gibt ein Ablaufdatum an, nach dem alle Accounts ungültig werden. Diese Einstellung wird normalerweise nur zum Außerkraftsetzen einzelner Benutzerrichtlinien verwendet. Wenn z. B. ein Auftragnehmer über einen begrenzten Zugriffszeitraum für eine bestimmte Ressource verfügt, kann diese Option verwendet werden, um diesen Zugriff an einem bestimmten Datum zu inaktivieren. • **Set**. Das Ablaufdatum für Accounts. Geben Sie das Datum im Format MM/TT/JJJJ ein. • **Unset**. Unbegrenzter Gültigkeitszeitraum. Die Gültigkeit von Accounts läuft nie ab.
Limit Access?	Gibt eine Einschränkung bezüglich der Tageszeit an, zu der Benutzer auf das System zugreifen dürfen. • **Yes**. Die Tage und die Tageszeit, zu der Benutzer auf das Cloud Identity Service zugreifen dürfen. Die Zeit kann als Ortszeit für den Service oder als koordinierte Weltzeit (Coordinated Universal Time, UTC) angegeben werden. • **No**. Benutzer können jederzeit auf das Cloud Identity Service zugreifen.

Kapitel 10. Identitätsgovernance

Normalerweise werden Anforderungen von bestimmten Managern in Self-Service-Anwendungen verwaltet. Administratoren können bei Bedarf Benutzeranforderungen in Cloud Identity Portal verwalten.

Wenn der normale Genehmiger nicht verfügbar ist und es keinen delegierten Genehmiger gibt, muss möglicherweise ein Cloud Identity Portal-Administrator Benutzeranforderungen für Services verwalten.

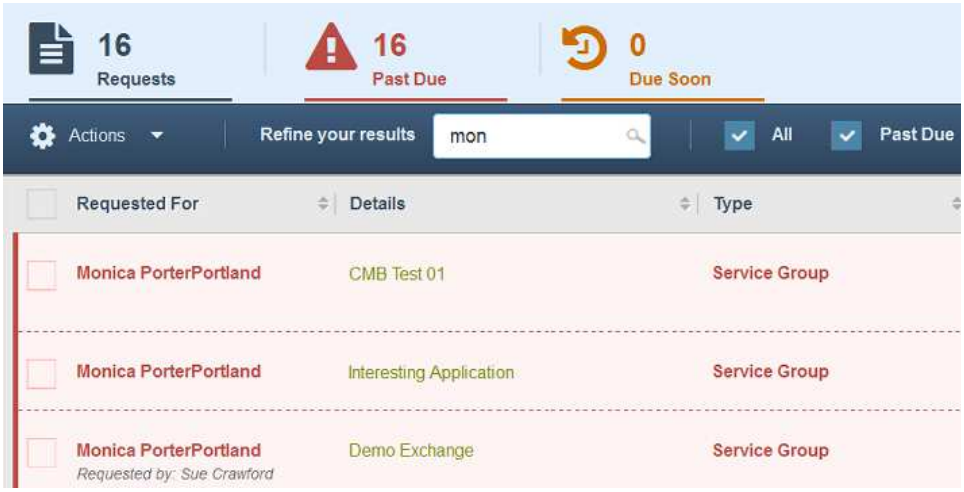
Nach einer Anforderung suchen

Sie suchen nach einer Anforderung, wenn Sie eine Anforderung genehmigen, neu zuordnen oder ablehnen möchten. Sie können auch eine Erinnerung an den Anforderungsgenehmiger senden.

Vorgehensweise

1. Klicken Sie im Navigationsfenster auf **Identity Governance** > **Request Management**.
2. Geben Sie im Feld **Refine your results** Ihre Suchkriterien ein.

   Sie können nach den ersten 3 oder mehr Zeichen im Vor- oder Nachnamen der Person suchen, in deren Auftrag die Anforderung erstellt wurde. Sie können auch nach den ersten 3 oder mehr Zeichen im Vor- oder Nachnamen des Genehmigers suchen. Um z. B. nach Anforderungen für einen Genehmiger mit dem Namen John Smith zu suchen, können Sie `smi` oder `joh` eingeben.



   Anforderungen, die Ihren Suchkriterien entsprechen, werden aufgeführt.

   Sie können die Liste mithilfe der Kontrollkästchen **All**, **Past Due** und **Due Soon** filtern. Sie können die Liste sortieren, indem Sie auf eine Spaltenüberschrift klicken, um die Liste nach dieser Spalte zu sortieren.

Anforderungen genehmigen, verweigern und neu zuordnen

Wird für eine Anforderung keine Aktion von einem Genehmiger ausgeführt, können Sie eine Anforderung genehmigen, neu zuordnen oder verweigern. Sie können auch eine Erinnerung an den Anforderungsgenehmiger senden.

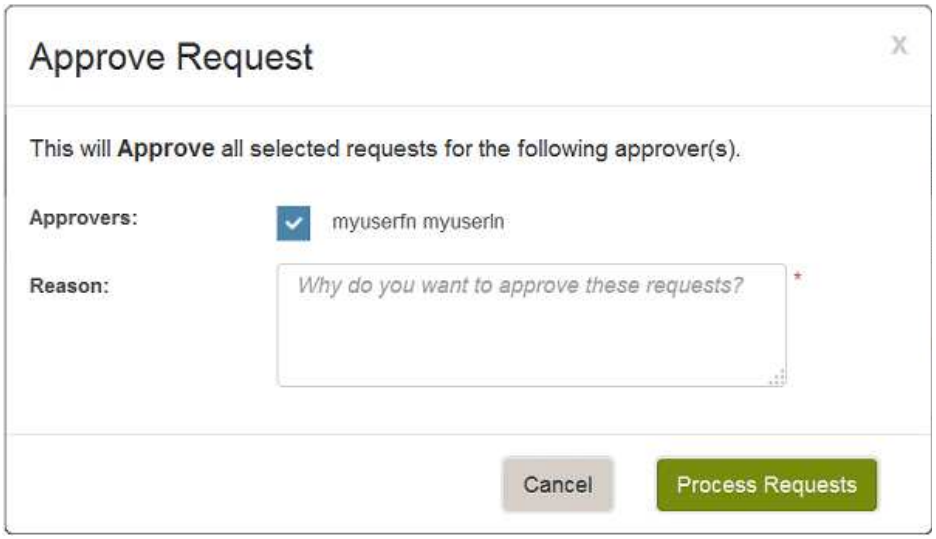
Informationen zu diesem Vorgang

Abgelaufene Genehmigungen werden in rot unterlegten Zeilen angezeigt. Nahezu abgelaufene Genehmigungen werden in gelb unterlegten Zeilen angezeigt.

Vorgehensweise

1. Suchen Sie nach der Anforderung.
2. Wählen Sie die Anforderung aus, klicken Sie auf das Menü **Action** und wählen Sie die Aktion aus, die Sie für die Anforderung ausführen möchten.

- Gehen Sie wie folgt vor, um eine Anforderung zu genehmigen:



  a. Wählen Sie die Genehmiger aus, in deren Auftrag die Anforderung genehmigt wird.
  b. Geben Sie einen Grund für die Genehmigung der Anforderung ein.
  c. Klicken Sie auf **Process Requests**.
- Gehen Sie zum Neuzuordnen einer Anforderung wie folgt vor:
  a. Wählen Sie die Genehmiger aus, in deren Auftrag die Anforderung neu zugeordnet wird.
  b. Suchen Sie nach dem Benutzer, dem die Anforderung neu zugeordnet wird, und wählen Sie ihn aus.

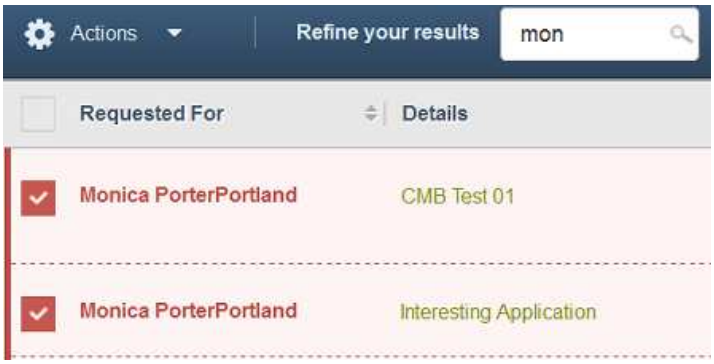
Sie können nach den ersten drei oder mehr Zeichen des Vornamens oder des Nachnamens des Managers suchen.

c. Geben Sie einen Grund für die Neuzuordnung der Anforderung ein.

d. Klicken Sie auf **Process Requests**.

- Gehen Sie wie folgt vor, um eine Erinnerung an den Genehmiger zu senden:
  a. Wählen Sie die Genehmiger aus, an die die Erinnerung gesendet werden soll.
  b. Geben Sie einen Grund für das Senden der Erinnerung ein.
  c. Klicken Sie auf **Process Requests**.

Sie können auch eine Aktion für mehrere Anforderungen ausführen, indem Sie die erforderlichen Anforderungskontrollkästchen auswählen.



Sie können alle Anforderungen auswählen, indem Sie das Kontrollkästchen in der Spaltenüberschrift verwenden. Verwenden Sie das Menü **Action** in der Spaltenüberschrift, um eine Aktion für mehrere Anforderungen auszuführen.

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Defense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
2Z4A/101

11400 Burnet Road
Austin, TX 79758
U.S.A

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesen Informationen beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind Marken oder eingetragene Marken der Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Gedruckt in Deutschland