One Identity Starling Governance

Administrationshandbuch für die Integration mit One Identity Active Roles

Legende

WARNUNG: Das Symbol WARNUNG weist auf ein potenzielles Risiko von Körperverletzungen oder Sachschäden hin, für das Sicherheitsvorkehrungen nach Industriestandard empfohlen werden. Dieses Symbol ist oft verbunden mit elektrischen Gefahren bezüglich Hardware.

VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

Starling Governance Administrationshandbuch für die Integration mit One Identity Active Roles
Aktualisiert - 12. Mai 2021, 15:11 Uhr

Inhalt

1

Über dieses Handbuch

One Identity Starling Governance integriert One Identity Active Roles und One Identity Manager in dem cloud-basierten Service Starling Governance. Die Synchronisation zwischen einer über One Identity Active Roles verwalteten Active Directory-Umgebung und Starling Governance richten Sie mit dem Starling Governance Agent ein.

Das *One Identity Starling Governance Administrationshandbuch für die Integration mit One Identity Active Roles* beschreibt, wie Sie den Starling Governance Service für Ihr Unternehmen bereitstellen. Dazu gehört die Installation und die Arbeit mit dem Starling Governance Agent. Sie erfahren, welche Voraussetzungen Sie zur Installation benötigen und wie Sie die Komponenten des Starling Governance Agent nutzen.

Das *One Identity Starling Governance Administrationshandbuch für die Integration mit One Identity Active Roles* richtet sich an Active Roles Administratoren, die Starling Governance zur Unterstützung bei der Verwaltung einer Active Directory-Umgebung über One Identity Active Roles einsetzen und damit Zugriffsanforderungen bearbeiten und Zugriffszertifizierungen durchführen.

Wie Sie Zugriffsanforderungen bearbeiten und Zugriffszertifizierungen durchführen, erfahren Sie im *One Identity Starling Governance Web Portal Benutzerhandbuch*.

Verfügbare Dokumentation

Die Online Version der Starling Governance Dokumentation finden Sie im Support-Portal unter Starling Governance Online-Dokumentation.

Grundlagen zu Starling Governance

Mit One Identity Starling Governance können Sie Zugriffsanforderungen und Zugriffszertifizierungen als Software-as-a-Service-Lösung für Ihr Unternehmen bereitstellen. Starling Governance ergänzt One Identity Active Roles um Genehmigungen, Benachrichtigungen, Eskalationen und andere Geschäftsprozesse für Ihre hybride Umgebung. Mit Starling Governance erfüllen Sie mühelos die Anforderungen von Attestierungs- und Rezertifizierungsrichtlinien und bieten Auditoren, was sie brauchen.

Mit dem Starling Governance Agent richten Sie die Synchronisation zwischen einer über One Identity Active Roles verwalteten Active Directory-Umgebung und Starling Governance ein. Die Synchronisation überträgt alle für die Zugriffssteuerung benötigten Daten, wie Benutzerkonten, Gruppen und Gruppenmitgliedschaften.

Über das Starling Governance Web Portal können Benutzer Mitgliedschaften in Active Directory Gruppen bestellen (Zugriffsanforderung). Manager und Compliance-Verantwortliche können sowohl die Richtigkeit der Zugriffsanforderungen bescheinigen als auch mit regelmäßigen Attestierungsvorgängen bereits vorhandene Mitgliedschaften rezertifizieren (Zugriffszertifizierung). Alle Mitgliedschaften sind konkreten Identitäten zugeordnet. Dadurch kann auch geprüft werden, ob Zugriffsberechtigungen in ihrer Kombination zulässig sind. Die Einhaltung regulatorischer Anforderungen kann damit sichergestellt werden. Wenn bei der Attestierung bestimmte Zugriffsberechtigungen als nicht zulässig erkannt werden und die Zertifizierung daher abgelehnt wird, werden die betroffenen Mitgliedschaften automatisch entfernt. Änderungen, wie genehmigte Zugriffsanforderungen oder entzogene Zugriffsberechtigungen, werden sofort in die angebundene Active Directory Domäne provisioniert und sind damit zeitnah wirksam.

Das Starling Governance Web Portal stellt verschiedene Berichte zur Verfügung, in denen Informationen über die synchronisierten Daten, vorhandene Zugriffsberechtigungen oder abgeschlossene Attestierungen zusammengestellt sind. Diese Berichte können Sie für die Analyse und Zusammenfassung wichtiger Informationen nutzen.

Starling Governance ist als Service in One Identity Starling integriert (https://cloud.oneidentity.com). Sie können eine Testversion des Service mit vorgeladenen Beispieldaten abonnieren, um die Funktionen besser zu verstehen, bevor Sie sich für ein kostenpflichtiges Abonnement entscheiden. Das Vertriebsteam von One Identity kann Sie auch unterstützen, wenn Sie einen Proof-of-Concept-Test mit Ihren eigenen Daten durchführen möchten.

Unterstützte Browser

Für den Zugriff auf Starling Governance können alle Browser genutzt werden, die durch One Identity Starling unterstützt werden. Ausführliche Informationen dazu finden Sie im *One Identity Starling User Guide*.

Zusätzliche Hardware- und Software-Voraussetzungen

Für Starling Governance gelten die Hardware- und Software-Voraussetzungen von One Identity Starling. Voraussetzung für die Registrierung und Anmeldung an One Identity Starling ist ein Azure Active Directory Mandant. Für die Registrierung nutzen Sie Ihre Azure Active Directory Anmeldeinformationen. Ausführliche Informationen dazu finden Sie im *One Identity Starling User Guide*.

Starling Governance als Service nutzen

Um Starling Governance als Starling Service nutzen zu können, benötigen Sie eine Starling Organisation. Sie können den Starling Governance Service zu einer bestehenden Organisation hinzufügen oder eine neue Organisation erstellen. Ausführliche Informationen zu Organisationen finden Sie im *One Identity Starling User Guide*.

Sobald Sie eine Starling Organisation erstellt haben, können Sie den Starling Governance Service zu dieser Organisation hinzufügen. Für Starling Governance können folgende Abonnementtypen ausgewählt werden:

- Kostenpflichtige Abonnements auf Seite 10
- Test-Abonnements auf Seite 7

Test-Abonnements

Starling Governance kann für einen begrenzten Zeitraum abonniert werden, um das Produkt zu testen, bevor Sie sich für eine längerfristige Nutzung entscheiden. Wenn Sie sich nicht für ein Upgrade Ihres Abonnements entscheiden, verlieren Sie den Zugriff auf Starling Governance.

Sie haben zwei Möglichkeiten Starling Governance zu testen.

1. Wenn Sie sehen möchten, wie die Hauptfunktionen von Starling Governance funktionieren, starten Sie einen Demo-Test. Damit können Sie alle Funktionen mit einem Standardsatz an Beispieldaten testen, ohne die Starling Governance-Umgebung mit Ihrer eigenen One Identity Active Roles-Umgebung zu verbinden. Ein Demo-Test ist zeitlich auf 5 Tage begrenzt. Falls Sie mehr Zeit benötigen, können Sie innerhalb der Laufzeit des Testabonnements einen neuen Demo-Test starten.
2. Wenn Sie die Starling Governance Funktionen mit Daten aus ihrer eigenen One Identity Active Roles-Umgebung testen möchten, starten Sie einen Proof-of-Concept-Test. Damit testen Sie die Funktionen des Starling Governance Web Portal und können außerdem nachvollziehen, wie die Daten zwischen Active Roles und Starling Governance synchronisiert werden. Das Produkt verhält sich genau so, wie bei einem kostenpflichtigen Abonnement. Es gibt keine Einschränkungen. Für einen Proof-of-Concept-Test installieren Sie alle lokal benötigten Komponenten auf einer Arbeitsstation in Ihrer Umgebung.

   Ein Proof-of-Concept-Test ist zeitlich auf 14 Tage begrenzt. Falls Sie mehr Zeit benötigen, können Sie innerhalb der Laufzeit des Testabonnements einen neuen Proof-of-Concept-Test starten.

   Um eine Proof-of-Concept-Testlizenz zu erwerben, kontaktieren Sie den One Identity Vertrieb.

Ein Test-Abonnement ist auf 30 Tage begrenzt. Innerhalb dieser Zeit können Sie Demo-Tests und Proof-of-Concept-Tests beliebig oft beenden und neu starten. Wenn der Zeitraum für das Test-Abonnement abgelaufen ist und Sie noch mehr Zeit zum Testen benötigen, können Sie den Testzeitraum einmalig um weitere 30 Tage verlängern lassen. Kontaktieren Sie dafür den One Identity Vertrieb.

Detaillierte Informationen zum Thema

- Test-Abonnement starten auf Seite 8
- Test-Abonnement beenden auf Seite 9

Verwandte Themen

- Kostenpflichtige Abonnements auf Seite 10
- Starling Governance als Service nutzen auf Seite 7

Test-Abonnement starten

Sobald Sie sich bei One Identity Starling angemeldet haben, können Sie den Starling Governance Service testen.

Um ein Test-Abonnement zu starten

1. Melden Sie sich an Starling an.
2. Auf der Startseite wählen Sie den Starling Governance Service und klicken **Trial**.

3. Im Dialog **Your Location** wählen Sie Ihr Land und Bundesland oder Provinz.

   Dieser Dialog erscheint nur beim ersten Start eines Test-Abonnements, nachdem Sie Starling Governance neu zu Ihrer Organisation hinzugefügt haben.
4. Klicken Sie **Confirm**.
5. Erfassen Sie einen Domänennamen für Ihre Starling Governance Testinstanz.

   Der Domänenname darf nicht länger als 40 Zeichen sein und muss innerhalb von Starling eindeutig sein.
6. Um einen Demo-Test zu starten, klicken Sie **Demo trial**.

   - ODER -

   Um einen Proof-of-Concept-Test zu starten, klicken Sie **Proof of concept trial**.
7. Die Testinstanz wird bereitgestellt.

   Das nimmt einige Zeit in Anspruch. Sie erhalten eine E-Mail mit einem Link zu Ihrer Testinstanz, sobald diese genutzt werden kann.
8. Wenn Sie einen Proof-of-Concept-Test gestartet haben, installieren Sie nun den Starling Governance Agent und richten Sie die Synchronisation mit Ihrer One Identity Active Roles-Umgebung ein.

   Weitere Informationen finden Sie unter Einrichten der Initialsynchronisation auf Seite 12.
9. Wenn Sie einen Demo-Test gestartet haben, klicken Sie auf der Starling Governance Webseite **GO**.

   Das Starling Governance Web Portal wird geöffnet.

Der Governance Service wird als neue Kachel auf der Starling Startseite im Bereich **My Services** angezeigt und kann bis zum Ende des Testzeitraums genutzt werden. Die Anzahl der verbleibenden Tage der Testphase wird durch einen Countdown auf der Kachel angezeigt. Sie können zu jedem Zeitpunkt der Testphase ein kostenpflichtiges Abonnement erwerben. Klicken Sie **More Information** auf der Governance Kachel, um sich zu informieren, wie Sie das Produkt erwerben können.

Verwandte Themen

- Test-Abonnement beenden auf Seite 9
- Kostenpflichtige Abonnements auf Seite 10

Test-Abonnement beenden

Ein Test-Abonnement ist auf 30 Tage begrenzt. Innerhalb dieser Zeit können Sie Demo-Tests und Proof-of-Concept-Tests jederzeit beenden und neu starten. Sobald der Testzeitraum überschritten ist, steht der Service nicht mehr zur Verfügung. Wenn Sie ein kostenpflichtiges Abonnement erworben haben oder einen neuen Test starten möchten, können Sie das aktuelle Test-Abonnement vorzeitig beenden.

Um ein Test-Abonnement vorzeitig zu beenden

1. Klicken Sie im Bereich **Trial Details** auf der Starling Governance Webseite **End Trial**.
2. Klicken Sie **OK**.

Verwandte Themen

- Test-Abonnement starten auf Seite 8
- Kostenpflichtige Abonnements auf Seite 10

Kostenpflichtige Abonnements

Ein Starling Governance Abonnement kann über eine Starling Organisation erworben werden. Ein kostenpflichtiges Abonnement bietet Ihnen vollen Zugriff auf das Produkt (einschließlich des Starling Governance Agent) für die Dauer Ihres Vertrags und eine bestimmte Anzahl von Benutzerlizenzen. Informationen zum Erwerb eines Abonnements für den Starling Governance Service erhalten Sie auf der Starling Startseite über die Schaltfläche **More Information**. Weitere Informationen finden Sie unter Kostenpflichtiges Abonnement starten auf Seite 10.

HINWEIS: Um ein kostenpflichtiges Abonnement zu beenden, kontaktieren Sie den One Identity Vertrieb oder Support.

Verwandte Themen

- Test-Abonnements auf Seite 7
- Starling Governance als Service nutzen auf Seite 7

Kostenpflichtiges Abonnement starten

Um ein kostenpflichtiges Abonnement zu starten, melden Sie sich bei One Identity Starling an und wenden Sie sich an den Vertrieb.

Um ein kostenpflichtiges Abonnement zu starten

1. Melden Sie sich an Starling an.
2. Auf der Startseite wählen Sie den Starling Governance Service und kontaktieren den Vertrieb.

   Sie erhalten eine E-Mail, sobald Ihre Starling Governance Instanz bereitgestellt und das Abonnement eingerichtet wurden.
3. Wenn Ihr Testzeitraum noch nicht abgelaufen ist, beenden Sie den Test.

   Weitere Informationen finden Sie unter Test-Abonnement beenden auf Seite 9.

4. Erfassen Sie einen Domänennamen für Ihre produktive Starling Governance Instanz.

   Der Domänenname darf nicht länger als 40 Zeichen sein und muss innerhalb von Starling eindeutig sein.
5. Klicken Sie **Production**.
6. Die Starling Governance Instanz wird bereitgestellt.

   Das nimmt einige Zeit in Anspruch. Sie erhalten eine E-Mail mit einem Link zu Ihrer Instanz, sobald diese genutzten werden kann.

   Die Instanz wird komplett neu eingerichtet. Daten, die während der Testphase synchronisiert wurden, stehen hier nicht mehr zur Verfügung.
7. Installieren Sie den Starling Governance Agent und richten Sie die Synchronisation mit Ihrer One Identity Active Roles-Umgebung ein.

   Weitere Informationen finden Sie unter Einrichten der Initialsynchronisation auf Seite 12.

Verwandte Themen

- Kostenpflichtige Abonnements auf Seite 10

Aktualisieren der Starling Governance Instanz

Von Zeit zu Zeit wird Ihre Starling Governance Instanz wegen Wartungsaufgaben nicht verfügbar sein. Ihr Starling Administrator wird über bevorstehende Wartungsarbeiten benachrichtigt. Administrative Benutzer sehen auf der Starling Governance Webseite einen Warnhinweis. Wenn die Instanz nicht erreichbar ist, sehen alle Benutzer einen entsprechenden Hinweis.

Einrichten der Initialsynchronisation

Nachdem Sie den Starling Governance Service für Ihre Organisation vorbereitet haben, richten Sie nun die initiale Synchronisation mit Ihrer Active Roles-Umgebung ein. Dazu installieren Sie den Starling Governance Agent auf einer administrativen Arbeitsstation. Stellen Sie sicher, dass alle Systemanforderungen erfüllt sind. Weitere Informationen finden Sie unter Systemanforderungen des Starling Governance Agent auf Seite 19.

Um die Synchronisation mit Active Roles einzurichten

1. Klicken Sie in der **Subscription is ready** E-Mail auf die Schaltfläche **Get Started**.

   Die Starling Governance Webseite wird geöffnet.
2. Laden Sie das Starling Governance Agent-Installationspaket auf eine Arbeitsstation herunter.
   a. Unter **Step 1** klicken Sie **Download Agent**.
   b. Kopieren Sie den Starling Governance Agent Schlüssel in die Zwischenablage. Unter **Step 2** klicken Sie **Copy**.

      WICHTIG: Speichern Sie Ihren Starling Governance Agent Schlüssel an einem sicheren Ort, da Sie ihn später erneut benötigen.
3. Installieren Sie den Starling Governance Agent auf der Arbeitsstation.
   a. Entpacken Sie das Starling Governance Agent-Installationspaket in ein temporäres Verzeichnis auf der administrativen Arbeitsstation.
   b. Starten Sie die Datei `autorun.exe` aus dem temporären Verzeichnis.

      Der Installationsassistent wird gestartet.
   c. Auf der Startseite wählen Sie die Sprache für den Installationsassistenten.
   d. Bestätigen Sie die Lizenzbedingungen.
   e. Auf der Seite **Einstellungen für die Installation** erfassen Sie die folgenden Informationen.
      - **Installationsquelle**: Wählen Sie das temporäre Verzeichnis mit den Installationsdateien.
      - **Installationsverzeichnis**: Wählen Sie das Verzeichnis, in das die Dateien des Starling Governance Agent installiert werden sollen.

> HINWEIS: Um weitere Konfigurationseinstellungen vorzunehmen, klicken Sie auf die Pfeil-Schaltfläche neben dem Eingabefeld. Hier können Sie festlegen, ob die Installation auf einem 64-Bit-Betriebssystem oder auf einem 32-Bit-Betriebssystem erfolgt.
>
> Für eine Standardinstallation nehmen Sie keine weiteren Konfigurationseinstellungen vor.

f. Auf der letzten Seite des Installationsassistenten klicken Sie **Starten**, um das Starling Governance Agent Launchpad auszuführen.

   Beim ersten Start des Launchpad geben Sie den Starling Governance Agent Schlüssel zu Ihrer Starling Governance Instanz an.

   i. Im Dialog **Starling Governance Konfigurationsdaten**, kopieren Sie Ihren Starling Governance Agent Schlüssel in das Textfeld.

   ii. Klicken Sie **OK**.

g. Um den Installationsassistenten zu beenden, klicken Sie **Ende**.

4. Beim ersten Start des Launchpad wird der Starling Governance Agent automatisch aktualisiert. Dabei wird die aktuellste Version des Starling Governance Agent geladen und installiert.

   - Klicken Sie **Ja**.

5. Melden Sie sich mit Ihren Starling Anmeldedaten an.

   - Klicken Sie **Next**.

     Das Launchpad wird gestartet.

6. Installieren Sie den Starling Governance Agent Service.

   Der Starling Governance Agent Service wird remote auf einem Jobserver installiert.

   Voraussetzungen:

   a. Der Server erfüllt die minimalen Systemanforderungen. Weitere Informationen finden Sie unter Minimale Systemanforderungen für den Jobserver auf Seite 20.

   b. In Ihrer Active Roles-Umgebung steht ein Benutzerkonto mit folgenden Berechtigungen bereit:

      - All Objects - Read All Properties
      - All Objects - Full Control
      - Mitglied in der Gruppe Active Roles Administratoren

      Dieses Benutzerkonto wird als Dienstkonto für den Starling Governance Agent Service eingetragen.

   a. Wählen Sie im Launchpad **Administrative Aufgaben > Systemkonfiguration > Dienst installieren**.

   b. Klicken Sie **Starten**.

   c. Auf der Startseite des Server Installer klicken Sie **Weiter**.

d. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.

e. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.

- **Computer**: Name oder IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
- **Dienstkonto**: Angaben zum Benutzerkonto des Starling Governance Agent Service.
  - Um den Dienst unter einem anderen Konto zu starten, deaktivieren Sie die Option **Lokales Systemkonto** und erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung. Nutzen Sie das Benutzerkonto, welches Sie in Ihrer Active Roles-Umgebung für diesen Zweck bereitgestellt haben.
- **Installationskonto**: Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.
  - Um das Benutzerkonto des angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Aktuellen Benutzer verwenden**.
  - Um ein anderes Benutzerkonto zu verwenden, deaktivieren Sie die Option **Aktuellen Benutzer verwenden** und geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.
- Um das Installationsverzeichnis, den Namen, den Anzeigenamen oder die Beschreibung für den Starling Governance Agent Service zu ändern, nutzen Sie die weiteren Optionen.

f. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.

g. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

> HINWEIS: In einer Standardinstallation wird der Dienst mit der Bezeichnung **Starling Governance Agent Service** in der Dienstverwaltung des Servers eingetragen.

7. Installieren Sie den Active Roles ADSI Provider.

a. Wählen Sie im Launchpad **Administrative Aufgaben > Datensynchronisation > Active Roles ADSI Provider installieren**.

b. Klicken Sie **Installieren**.

c. Wählen Sie über den Dateibrowser den Pfad zur Datei `ActiveRoles.exe`. Wählen Sie diese aus und klicken Sie **Öffnen**.

Die Installation wird ausgeführt.

Wenn die Installation beendet ist, ist im Launchpad die Schaltfläche **Installieren** deaktiviert.

8. Richten Sie die Synchronisation mit der Active Roles-Umgebung ein.

    a. Wählen Sie im Launchpad **Administrative Aufgaben > Datensynchronisation > Synchronisation einrichten**.

    b. Klicken Sie **Starten**.

    Der Systemverbindungsassistent wird gestartet.

    c. Auf der Startseite des Systemverbindungsassistenten klicken Sie **Weiter**.

    d. Auf der Seite **Zielserver** geben den Active Roles Server an, gegen den Sie sich verbinden möchten. Die möglichen Server werden, wenn möglich, automatisch ermittelt.

    - Wählen Sie unter **Hostname/IP Adresse** den Zielserver aus.
    - Kann der Server nicht automatisch ermittelt werden, tragen Sie unter **Hostname/IP Adresse** den DNS Namen oder die IP Adresse des Servers ein.

    e. Auf der Seite **Anmeldeinformationen** geben Sie das Benutzerkonto und dass Kennwort für den Zugriff auf das Active Roles an.

    Nutzen Sie das Benutzerkonto, welches Sie als Dienstkonto für den Starling Governance Agent Service eingetragen haben.

    f. Auf der Seite **Auswahl der Domäne/des Wurzeleintrages** wählen Sie die Domäne, die Sie synchronisieren möchten oder tragen Sie den definierten Namen des Wurzeleintrages ein.

    g. Auf der letzten Seite des Systemverbindungsassistenten klicken Sie **Fertig**.

    Die Synchronisation wird eingerichtet.

    Im Launchpad wird die Aufgabe **Synchronisationen verwalten** angezeigt.

9. Starten Sie die Synchronisation.

    a. Wählen Sie im Launchpad **Administrative Aufgaben > Datensynchronisation > Synchronisationen verwalten**.

    b. Klicken Sie **Starten**.

    c. Im Dialog **Synchronisationen verwalten** wählen Sie die Domäne.

    d. Klicken Sie **Synchronisation starten**.

    e. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

    f. Schließen Sie das Meldungsfenster mit **Ok**.

TIPP: Über ein Browserfrontend können Sie die Protokolldatei des Starling Governance Agent Service anzeigen. Die Protokolldatei zeigt Ihnen den Synchronisationsfortschritt. Hier können Sie prüfen, ob der Starling Governance Agent Service korrekt arbeitet.

Weitere Informationen finden Sie unter Protokolldatei des Starling Governance Agent Service anzeigen auf Seite 44.

Wenn die Synchronisation beendet ist, sehen Sie die synchronisierten Daten im Governance Portal.

10. Prüfen Sie, ob die Daten korrekt synchronisiert wurden.
    a. Wechseln Sie zur Starling Governance Webseite und klicken Sie **GO**.

       Das Governance Portal wird geöffnet.
    b. Wählen Sie im Menü **Daten > Daten-Explorer**.
    c. Klicken Sie in der Navigation des Daten-Explorers nacheinander **Identitäten**, **Benutzerkonten** und **Systemberechtigungen** und prüfen Sie die angezeigten Daten.

    Ausführliche Informationen zum Starling Governance Web Portal finden Sie im *One Identity Starling Governance Web Portal Benutzerhandbuch*.

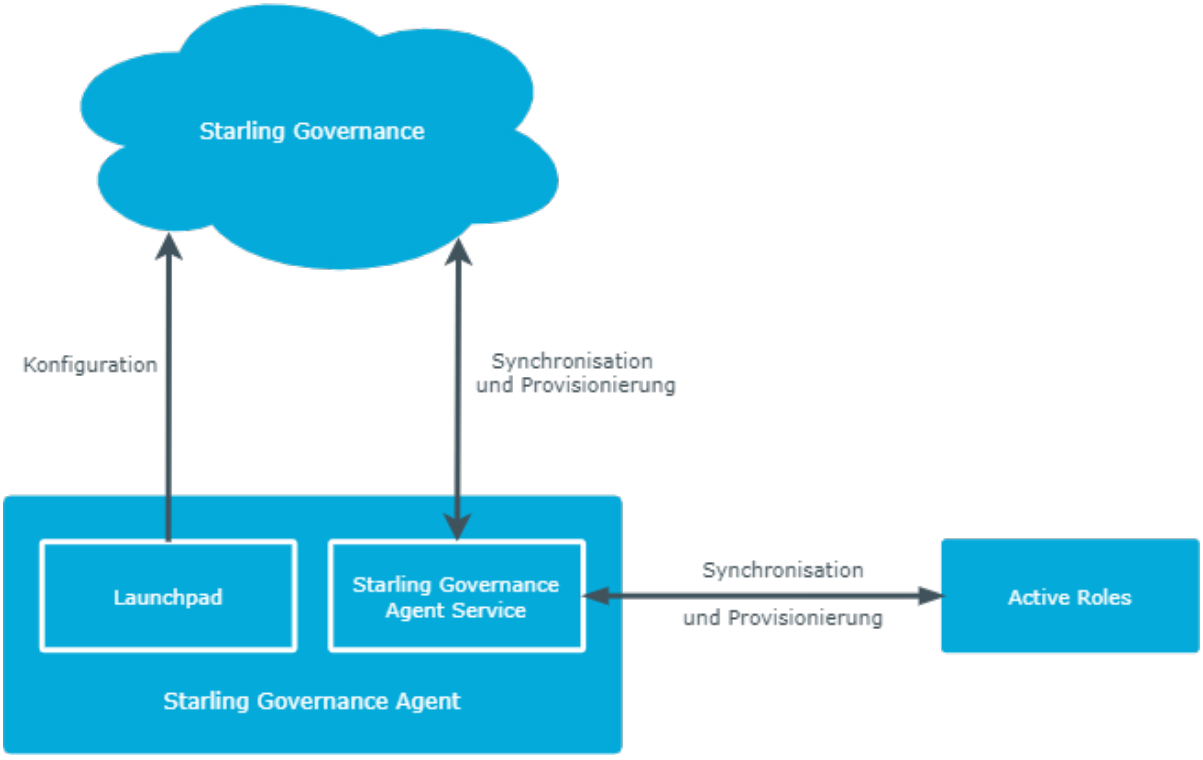
Detaillierte Informationen zum Thema

- Installieren des Starling Governance Agent auf einer Arbeitsstation auf Seite 26
- Starling Governance Agent Service installieren auf Seite 32
- Minimale Systemanforderungen für den Jobserver auf Seite 20
- Benötigte Berechtigungen des Starling Governance Agent Service für die Synchronisation mit One Identity Active Roles auf Seite 24
- Active Roles ADSI Provider installieren auf Seite 40
- Synchronisation mit einer Active Directory Domäne einrichten auf Seite 40

Architektur des Starling Governance Agent

Der Starling Governance Agent sorgt für den Austausch der Daten zwischen Starling Governance und einer über One Identity Active Roles verwalteten Active Directory-Umgebung. Er übernimmt die Synchronisation der Active Directory-Umgebung und provisioniert Änderungen, die in Starling Governance veranlasst werden, sofort in die angebundenen Active Directory Domänen. Die Synchronisation wird einmal täglich gestartet.

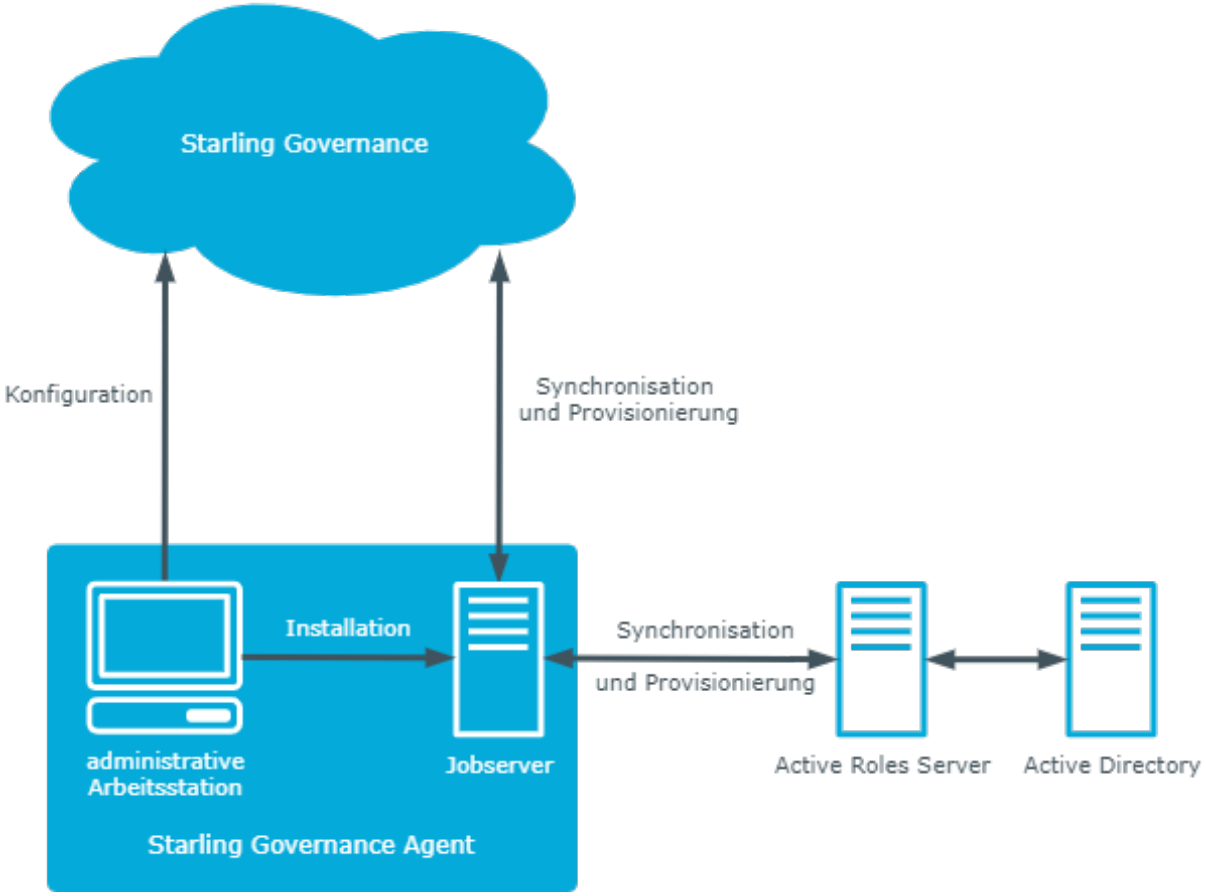
Abbildung 1: Architektur des Starling Governance Agent



Der Starling Governance Agent wird auf einer administrativen Arbeitsstation installiert. Hier starten Sie das Starling Governance Agent Launchpad, über das Sie den Starling

Governance Agent Service auf einem Jobserver installieren. Der Starling Governance Agent Service übernimmt die Synchronisation der über One Identity Active Roles angebundenen Active Directory-Umgebung.

Abbildung 2: Topologie des Starling Governance Agent



Systemanforderungen des Starling Governance Agent

Die nachfolgend beschriebenen Installationsvoraussetzungen stellen Mindestanforderungen zur Inbetriebnahme und uneingeschränkten Nutzung des Starling Governance Agent dar.

Jede Starling Governance Agent Installation kann virtualisiert werden. Stellen Sie sicher, dass der jeweiligen Starling Governance Agent-Komponente die laut Systemanforderung spezifizierte Leistung und Ressourcen zur Verfügung stehen. Die Virtualisierung einer Starling Governance Agent Installation sollte von Experten mit einem fundierten Wissen über Virtualisierungstechniken vorgenommen werden. Weitere Informationen zur Umgebungsvirtualisierung finden Sie in den Richtlinien für den Produkt-Support.

Detaillierte Informationen zum Thema

Minimale Systemanforderungen für die administrative Arbeitsstation

Zur Darstellung und Bearbeitung von Daten wird der Starling Governance Agent auf einer administrativen Arbeitsstation installiert. Dafür sind die folgenden Systemvoraussetzungen zu gewährleisten.

Tabelle 1: Minimale Systemanforderungen - Administrative Arbeitsstation

Prozessor	4 physische Kerne mit 2 GHz+ Taktung
Arbeitsspeicher	4 GB+ RAM
Freier Festplattenspeicher	1 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: • Windows 10 (32-Bit oder 64-Bit) mindestens Version 1511 • Windows 8.1 (32-Bit oder 64-Bit) mit dem aktuellen Service Pack
Zusätzliche Software	• Microsoft .NET Framework Version 4.7.2 oder höher • Active Roles ADSI Provider der anzubindenden Active Roles Version Für die Einrichtung der Synchronisation mit einer Active Directory Domäne muss die Verbindung über Port **15172** (TCP) zum Active Roles Server möglich sein. Gegebenenfalls muss eine entsprechende Firewall-Regel auf dem Active Roles Server eingerichtet werden.
Unterstützte Browserversionen	• Internet Explorer 11 oder höher • Firefox (Release Channel) • Chrome (Release Channel) • Microsoft Edge (Release Channel)

Minimale Systemanforderungen für den Jobserver

Der Starling Governance Agent Service sorgt für die Verbreitung der in Starling Governance verwalteten Informationen im Netzwerk. Der Starling Governance Agent Service übernimmt folgende Aufgaben:

- Synchronisation zwischen Starling Governance und Active Roles
- Versand von E-Mail-Benachrichtigungen
- Generierung von Berichten

Zur Installation des Starling Governance Agent Service sind auf einem Server folgende Systemvoraussetzungen zu gewährleisten.

Tabelle 2: Minimale Systemanforderungen - Jobserver

Prozessor	8 physische Kerne mit 2.5 GHz+ Taktung
Arbeitsspeicher	16 GB RAM
Freier Festplattenspeicher	40 GB
Betriebssystem	Windows Betriebssysteme Unterstützt werden die Versionen: • Windows Server 2019 • Windows Server 2016 • Windows Server 2012 R2 • Windows Server 2012
Zusätzliche Software	• Microsoft .NET Framework Version 4.7.2 oder höher HINWEIS: Für die Zielsystemanbindung beachten Sie die Empfehlungen des Zielsystemherstellers. • One Identity Active Roles Management Shell for Active Directory (x64) Auf 32-Bit Betriebssystemen ist das Active Roles Management Shell for Active Directory (x86) Paket zu verwenden. Die Anleitung zur Installation entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*. • Folgende Pakete müssen vom Active Roles Installationsmedium nachinstalliert werden: Auf 32-Bit Betriebssystemen: • `<source>\Redistributables\vc_redist.x86.exe` • `<source>\Components\ActiveRoles ADSI Provider\ADSI_x86.msi` Auf 64-Bit Betriebssystemen: • `<source>\Redistributables\vc_redist.x64.exe` • `<source>\Components\ActiveRoles ADSI Provider\ADSI_x64.msi` Weiterhin ist es notwendig, dass vom Jobserver aus Verbindungen über Port **15172** (TCP) zum Active Roles Server möglich sind. Gegebenenfalls muss eine entsprechende Firewall-Regel auf dem Active Roles Server eingerichtet werden.

Für die Remote-Installation des Starling Governance Agent Service benötigen Sie eine administrative Arbeitsstation, auf der die Starling Governance Agent-Komponenten installiert sind.

Verwandte Themen

- Starling Governance Agent Service installieren auf Seite 32
- Minimale Systemanforderungen für die administrative Arbeitsstation auf Seite 19

Einrichten der Berechtigung zum Erstellen eines HTTP Server

Die Anzeige der Protokolldateien des Starling Governance Agent Service kann über einen HTTP Server erfolgen (http://<Servername>:<Portnummer>).

Damit ein Benutzer einen HTTP Server öffnen kann, muss er dazu berechtigt werden. Dazu muss der Administrator dem Benutzer die URL Genehmigung erteilen. Dies kann über folgenden Kommandozeilenaufruf erfolgen:

```
netsh http add urlacl url=http://*:<Portnummer>/ user=<Domäne>\<Benutzername>
```

Muss der Starling Governance Agent Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so müssen explizit Berechtigungen für den internen Webservice vergeben werden. Dies kann über folgenden Kommandozeilenaufruf erfolgen:

```
netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"
```

Das Ergebnis können Sie gegebenenfalls über folgenden Kommandozeilenaufruf prüfen:

```
netsh http show urlacl
```

Kommunikationsports und Firewall Konfiguration

Der Starling Governance Agent besteht aus verschiedenen Komponenten, die in verschiedenen Netzwerksegmenten laufen können. Zusätzlich benötigt der Starling Governance Agent Zugriff auf verschiedene Netzwerkdienste, welche ebenfalls in verschiedenen Netzwerksegmenten installiert sein können. Abhängig davon, welche Komponenten und Dienste Sie hinter ihrer Firewall installieren möchten, müssen Sie verschiedene Ports öffnen.

Die folgenden Basisports werden benötigt.

Tabelle 3: Kommunikationsports

Standardport	Beschreibung
1433	Port zur Kommunikation mit Starling Governance.

Standardport	Beschreibung
1880	Port für das HTTP-basierte Protokoll des Starling Governance Agent Service.
88	Kerberos-Authentifizierungssystem (wenn Kerberos Authentifizierung eingesetzt wird).
135	Microsoft End Point Mapper (EPMAP) (auch DCE/RPC Locator Service).
137	NetBIOS Name Service.
139	NetBIOS Session Service.

Benutzer für den Starling Governance Agent

Für die Arbeit mit dem Starling Governance Agent und die Synchronisation mit Active Roles werden Benutzer mit den folgenden Berechtigungen eingesetzt:

Tabelle 4: Benutzer für den Starling Governance Agent

Benutzer	Berechtigungen
Benutzer zur Anmeldung am Starling Governance Agent	Der Benutzer, mit dem Sie sich initial für One Identity Starling registriert haben, hat standardmäßig administrative Berechtigungen für den Starling Governance Agent. Dieser Benutzer kann weitere administrative Benutzer für den Zugriff auf den Starling Governance Agent berechtigen. Benutzer, die sich am Starling Governance Agent Launchpad anmelden werden über OAuth 2.0 authentifiziert.
Benutzerkonto für den Starling Governance Agent Service	Das Benutzerkonto für den Starling Governance Agent Service benötigt die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten. Das Benutzerkonto muss der Gruppe **Domänen-Benutzer** angehören. Das Benutzerkonto benötigt das erweiterte Benutzerrecht **Anmelden als Dienst**. Das Benutzerkonto benötigt Berechtigungen für den internen Webservice. HINWEIS: Muss der Starling Governance Agent Service unter dem Benutzerkonto des Network Service (**NT Authority\NetworkService**) laufen, so können Sie die Berechtigungen für den internen Webservice über folgenden Kommandozeilenaufruf vergeben:

Benutzer	Berechtigungen
	`netsh http add urlacl url=http://<IP-Adresse>:<Portnummer>/ user="NT AUTHORITY\NETWORKSERVICE"` Für die automatische Aktualisierung des Starling Governance Agent Services benötigt das Benutzerkonto Vollzugriff auf das Starling Governance Agent-Installationsverzeichnis. In der Standardinstallation wird der Starling Governance Agent installiert unter: • `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen) • `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen)

Verwandte Themen

- Starling Governance Agent Administratoren verwalten auf Seite 31
- Benötigte Berechtigungen des Starling Governance Agent Service für die Synchronisation mit One Identity Active Roles auf Seite 24

Benötigte Berechtigungen des Starling Governance Agent Service für die Synchronisation mit One Identity Active Roles

Für die Verbindung zu einer Active Directory-Umgebung über Active Roles wird die Einrichtung eines eigenen Benutzerkontos für den Starling Governance Agent Service empfohlen. Zur Einrichtung verwenden Sie die Active Roles Zugriffsvorlagen. Über Zugriffsvorlagen delegieren Sie administrationsrelevante Berechtigungen an ein Active Directory Benutzerkonto ohne jedoch diese Berechtigungen direkt im Active Directory zu erteilen. Weitere Informationen zu Active Roles Zugriffsvorlagen entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.

Folgende Zugriffsvorlagen werden für das Delegieren der Berechtigungen vorgeschlagen:

- All Objects - Read All Properties
- All Objects - Full Control

Der Starling Governance Agent arbeitet ohne die Ansteuerung von Active Roles Arbeitsabläufen. Um eventuell vorhandene Active Roles Arbeitsabläufe zu umgehen, müssen Sie das Benutzerkonto in die Gruppe der Active Roles Administratoren aufnehmen. Diese Gruppe wird während der Installation des Active Roles erzeugt. Der Name der Gruppe ist in der Registrierungsdatenbank abgelegt unter:

- Registrierungsschüssel: HKEY_Local_Machine\Software\Aelita\Enterprise Directory Manager
- Wert: DSAdministrators

Installieren des Starling Governance Agent auf einer Arbeitsstation

Der Starling Governance Agent wird auf einer administrativen Arbeitsstation installiert. Bei der Installation des Starling Governance Agent werden Sie durch einen Installationsassistenten unterstützt.

WICHTIG: Stellen Sie vor Beginn der Installation sicher, dass die Arbeitsstation alle Systemanforderungen erfüllt. Weitere Informationen finden Sie unter Systemanforderungen des Starling Governance Agent auf Seite 19.

Um den Starling Governance Agent zu installieren

1. Entpacken Sie das Starling Governance Agent-Installationspaket in ein temporäres Verzeichnis auf der administrativen Arbeitsstation.
2. Starten Sie die Datei `autorun.exe` aus dem temporären Verzeichnis.

   Der Installationsassistent wird gestartet.
3. Auf der Startseite wählen Sie die Sprache für den Installationsassistenten.
4. Bestätigen Sie die Lizenzbedingungen.
5. Auf der Seite **Einstellungen für die Installation** erfassen Sie die folgenden Informationen.
   - **Installationsquelle**: Wählen Sie das temporäre Verzeichnis mit den Installationsdateien.
   - **Installationsverzeichnis**: Wählen Sie das Verzeichnis, in das die Dateien des Starling Governance Agent installiert werden sollen.

     HINWEIS: Um weitere Konfigurationseinstellungen vorzunehmen, klicken Sie auf die Pfeil-Schaltfläche neben dem Eingabefeld. Hier können Sie festlegen, ob die Installation auf einem 64-Bit-Betriebssystem oder auf einem 32-Bit-Betriebssystem erfolgt.

     Für eine Standardinstallation nehmen Sie keine weiteren Konfigurationseinstellungen vor.
6. Auf der letzten Seite des Installationsassistenten klicken Sie **Starten**, um das Starling Governance Agent Launchpad auszuführen.
7. Um den Installationsassistenten zu beenden, klicken Sie **Ende**.

Der Starling Governance Agent wird für alle Benutzerkonten auf der Arbeitsstation installiert. In der Standardinstallation wird der Starling Governance Agent installiert unter:

- `%ProgramFiles(x86)%\One Identity` (auf 32-Bit Betriebssystemen)
- `%ProgramFiles%\One Identity` (auf 64-Bit Betriebssystemen)

Verwandte Themen

- Arbeiten mit dem Starling Governance Agent auf Seite 28
- Starling Governance Agent Launchpad starten auf Seite 29

Arbeiten mit dem Starling Governance Agent

Mit dem Starling Governance Agent richten Sie die Synchronisation zwischen einer über Active Roles verwalteten Active Directory-Umgebung und Starling Governance ein. Dabei werden die Active Directory Domänen als primäres System betrachtet. Änderungen im primären System werden täglich nach Starling Governance übertragen. Änderungen an Active Directory Gruppenmitgliedschaften in Starling Governance werden sofort in die Active Directory-Umgebung publiziert.

Mit dem Starling Governance Agent führen Sie folgende Arbeiten aus:

- Administratoren für den Starling Governance Agent verwalten
- Starling Governance Agent Service installieren
- Versand von E-Mail-Benachrichtigungen konfigurieren
- Active Roles ADSI Provider installieren
- Synchronisation mit einer Active Directory-Umgebung über One Identity Active Roles einrichten und ausführen
- Status des Starling Governance Agent Service anzeigen
- Automatische Personenzuordnung konfigurieren

TIPP: Um die Hilfe für ein Thema zu öffnen, klicken Sie ? an der jeweiligen Aufgabe.

Detaillierte Informationen zum Thema

- Starling Governance Agent Launchpad starten auf Seite 29
- Starling Governance Agent Administratoren verwalten auf Seite 31
- Starling Governance Agent Service installieren auf Seite 32
- Automatische Zuordnung zu Identitäten konfigurieren auf Seite 39
- Active Roles ADSI Provider installieren auf Seite 40
- Synchronisation mit einer Active Directory Domäne einrichten auf Seite 40
- Synchronisationen verwalten auf Seite 42
- Protokolldatei des Starling Governance Agent Service anzeigen auf Seite 44

Starling Governance Agent Launchpad starten

Über das Starling Governance Agent Launchpad können Sie alle Funktionen des Starling Governance Agent ausführen.

Um das Launchpad zu starten

1. Wählen Sie im Windows Startmenü **Starling Governance Agent Launchpad**.
2. Wenn angefordert, geben Sie die Konfigurationsdaten zu Ihrer Starling Governance Instanz an.

    a. Im Dialog **Starling Governance Konfigurationsdaten**, kopieren Sie Ihren Starling Governance Agent Schlüssel in das Textfeld.

    b. Klicken Sie **OK**.
3. Melden Sie sich mit Ihren Starling Anmeldedaten an.
4. Klicken Sie **Next**.

    Das Launchpad wird gestartet.
5. Um die Anwendung in die Taskleiste zu minimieren, klicken Sie **Schließen**.

Verwandte Themen

- Arbeiten mit dem Starling Governance Agent auf Seite 28
- Konfigurationsdaten der Starling Governance Instanz laden auf Seite 29

Konfigurationsdaten der Starling Governance Instanz laden

Für die Kommunikation mit Starling Governance benötigt der Starling Governance Agent den Starling Governance Agent Schlüssel Ihrer Starling Governance Instanz. Dieser Schlüssel wird beispielsweise benötigt, wenn das Launchpad erstmalig gestartet oder die Synchronisation eingerichtet wird. Der Schlüssel wird aus Sicherheitsgründen nicht dauerhaft gespeichert und daher bei Bedarf erneut angefordert.

Um den Starling Governance Agent Schlüssel zu nutzen

1. Öffnen Sie die Starling Governance Webseite Ihrer Starling Governance Instanz.
2. Kopieren Sie den Starling Governance Agent Schlüssel in die Zwischenablage. Unter **Step 2** klicken Sie **Copy**.

WICHTIG: Speichern Sie Ihren Starling Governance Agent Schlüssel an einem sicheren Ort, da Sie ihn später erneut benötigen.

Um die Konfigurationsdaten zu laden

1. Im Dialog **Starling Governance Konfigurationsdaten**, kopieren Sie Ihren Starling Governance Agent Schlüssel in das Textfeld.
2. Klicken Sie **OK**.

Verwandte Themen

- Einrichten der Initialsynchronisation auf Seite 12
- Arbeiten mit dem Starling Governance Agent auf Seite 28
- Starling Governance Agent Launchpad starten auf Seite 29
- Starling Governance Agent Service installieren auf Seite 32
- Synchronisation mit einer Active Directory Domäne einrichten auf Seite 40

Allgemeine Einstellungen bearbeiten

Bei der ersten Anmeldung am Launchpad wird die Systemsprache zur Anzeige der Benutzeroberfläche verwendet. Über die allgemeinen Einstellungen des Launchpad können Sie die verwendete Sprache und Kultur ändern.

Um allgemeine Einstellungen zu ändern

1. Klicken Sie in der Kopfzeile des Launchpad ⌄.
2. Wählen Sie **Einstellungen**.
3. Bearbeiten Sie die folgenden Einstellungen.
    - **Allgemeine Kultur**: Sprache für die Formatierung von Daten, wie beispielsweise Datumsformate, Zeitformate oder Zahlenformate.
    - **Andere Sprache der Programmoberfläche**: Gibt an, ob die Anwendungstexte des Starling Governance Agent in einer anderen Sprache ausgegeben werden sollen. Die Änderung der Sprache wird mit dem Neustart des Launchpad wirksam.
4. Klicken Sie **OK**.
5. Starten Sie das Launchpad neu.

Verwandte Themen

- Starling Governance Agent Launchpad starten auf Seite 29

Starling Governance Agent Administratoren verwalten

Der Benutzer, mit dem Sie sich initial für One Identity Starling registriert haben, hat standardmäßig administrative Berechtigungen für den Starling Governance Agent. Dieser Benutzer kann weitere administrative Benutzer für den Zugriff auf den Starling Governance Agent berechtigen.

Starling Governance Agent Administratoren erhalten automatisch die administrativen Berechtigungen für Starling Governance. Sie sind Zielsystemverantwortliche für Active Roles, administrieren Personen, konfigurieren Attestierungen und den IT Shop für Bestellungen.

Um einen administrativen Benutzer hinzuzufügen

1. Wählen Sie im Launchpad **Administrative Aufgaben > Systemkonfiguration > Administratoren verwalten**.
2. Klicken Sie **Starten**.

   Der Dialog **Starling Governance Agent Administratoren verwalten** wird geöffnet.
3. Klicken Sie **Neu**.
4. Erfassen Sie die E-Mail-Adresse des zusätzlichen Benutzers.
5. Klicken Sie **OK**.

Um einen administrativen Benutzer zu bearbeiten

1. Wählen Sie im Launchpad **Administrative Aufgaben > Systemkonfiguration > Administratoren verwalten**.
2. Klicken Sie **Starten**.

   Der Dialog **Starling Governance Agent Administratoren verwalten** wird geöffnet.
3. Wählen Sie den Benutzer.
4. Klicken Sie **Bearbeiten**.
5. Bearbeiten Sie die E-Mail-Adresse des Benutzers.
6. Klicken Sie **OK**.

Um einen administrativen Benutzer zu löschen

1. Wählen Sie im Launchpad **Administrative Aufgaben > Systemkonfiguration > Administratoren verwalten**.
2. Klicken Sie **Starten**.

   Der Dialog **Starling Governance Agent Administratoren verwalten** wird geöffnet.

3. Wählen Sie den Benutzer.
4. Klicken Sie **Löschen**.
5. Klicken Sie **OK**.

Verwandte Themen

- Arbeiten mit dem Starling Governance Agent auf Seite 28

Starling Governance Agent Service installieren

WICHTIG: Stellen Sie vor Beginn der Installation sicher, dass der Server alle Systemanforderungen erfüllt. Weitere Informationen finden Sie unter Systemanforderungen des Starling Governance Agent auf Seite 19.

Der Starling Governance Agent Service übernimmt die Synchronisation zwischen Starling Governance und der angebundenen Active Roles-Umgebung. Um den Starling Governance Agent Service zu installieren, führen Sie das Programm Server Installer über das Launchpad aus. Das Programm installiert, konfiguriert und startet den Starling Governance Agent Service auf einem Server.

HINWEIS: Das Programm führt eine Remote-Installation des Starling Governance Agent Service aus. Eine lokale Installation des Dienstes ist mit diesem Programm nicht möglich.

HINWEIS: Zusätzlich zur Installation des Starling Governance Agent Service aus dem Launchpad stellt One Identity ein Docker-Image für eine einfache und standardisierte Installation und Ausführung des Starling Governance Agent Service in Docker-Containern zur Verfügung. Das Starling Governance Agent Docker-Image und seine Beschreibung finden Sie unter https://hub.docker.com/r/oneidentity/oneim-job.

Um den Starling Governance Agent Service zu installieren und zu konfigurieren

1. Wählen Sie im Launchpad **Administrative Aufgaben > Systemkonfiguration > Dienst installieren**.
2. Klicken Sie **Starten**.
3. Auf der Startseite des Server Installer klicken Sie **Weiter**.
4. Wenn angefordert, geben Sie die Konfigurationsdaten zu Ihrer Starling Governance Instanz an.

    a. Im Dialog **Starling Governance Konfigurationsdaten**, kopieren Sie Ihren Starling Governance Agent Schlüssel in das Textfeld.

    b. Klicken Sie **OK**.

5. Auf der Seite **Installationsquelle festlegen** prüfen Sie das Verzeichnis mit den Installationsdateien. Ändern Sie gegebenenfalls das Verzeichnis.
6. Auf der Seite **Serverzugang** erfassen Sie die Installationsinformationen für den Dienst.
    - **Computer**: Name oder IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
    - **Dienstkonto**: Angaben zum Benutzerkonto des Starling Governance Agent Service.
        - Um den Dienst unter einem anderen Konto zu starten, deaktivieren Sie die Option **Lokales Systemkonto** und erfassen Sie Benutzerkonto, Kennwort und Kennwortwiederholung. Nutzen Sie das Benutzerkonto, welches Sie in Ihrer Active Roles-Umgebung für diesen Zweck bereitgestellt haben.
    - **Installationskonto**: Angaben zum administrativen Benutzerkonto für die Installation des Dienstes.
        - Um das Benutzerkonto des angemeldeten Benutzers zu verwenden, aktivieren Sie die Option **Aktuellen Benutzer verwenden**.
        - Um ein anderes Benutzerkonto zu verwenden, deaktivieren Sie die Option **Aktuellen Benutzer verwenden** und geben Sie Benutzerkonto, Kennwort und Kennwortwiederholung ein.
    - Um das Installationsverzeichnis, den Namen, den Anzeigenamen oder die Beschreibung für den Starling Governance Agent Service zu ändern, nutzen Sie die weiteren Optionen.
7. Um die Installation des Dienstes zu starten, klicken Sie **Weiter**.

    Die Installation des Dienstes wird automatisch ausgeführt und kann einige Zeit dauern.
8. Auf der letzten Seite des Server Installer klicken Sie **Fertig**.

    HINWEIS: In einer Standardinstallation wird der Dienst mit der Bezeichnung **Starling Governance Agent Service** in der Dienstverwaltung des Servers eingetragen.

Verwandte Themen

- Minimale Systemanforderungen für den Jobserver auf Seite 20
- Arbeiten mit dem Starling Governance Agent auf Seite 28
- Konfigurationsdaten der Starling Governance Instanz laden auf Seite 29
- Starling Governance Agent Service als Docker-Container starten auf Seite 45

E-Mail-Versand konfigurieren

Starling Governance Agent stellt eine Konfiguration zum Versenden von E-Mail-Benachrichtigungen an die Benutzer von Starling Governance bereit. E-Mail-Benachrichtigungen werden beispielsweise bei der Entscheidung von Bestellungen oder bei Rezertifizierungen versendet. Die Konfiguration der E-Mail-Benachrichtigungen kann mit dem Launchpad angepasst werden, beispielsweise um ein Postfach in Ihrer Microsoft Exchange- oder Exchange Online-Umgebung zu nutzen. Folgende Einstellungen sind möglich:

- E-Mail-Versand über einen internen SMTP-Server konfigurieren
- Sicherer E-Mail-Versand durch Verschlüsselung und Signierung von E-Mails
- Entscheidung per E-Mail aktivieren

Um den Versand von E-Mail-Benachrichtigungen zu konfigurieren

1. Wählen Sie im Launchpad **Administrative Aufgaben > Systemkonfiguration > E-Mail-Versand konfigurieren**.
2. Klicken Sie **Starten**.
3. Auf der Startseite des E-Mail-Konfigurationsassistenten klicken Sie **Weiter**.
4. Auf der Seite **Verbindung zum SMTP-Server** konfigurieren Sie die Verbindung zum SMTP-Server, der für den E-Mail-Versand genutzt werden soll.
    - Um die Angaben zum Benutzerkonto zu testen, klicken Sie **Verbindung prüfen**.
    - **SMTP-Server**: SMTP-Server, der zum Versenden von E-Mail-Benachrichtigungen genutzt wird. Ist kein Server angegeben, wird **localhost** verwendet.
    - **Benutzername**: Name des Benutzerkontos zur Authentifizierung am SMTP Server.
    - **Domäne**: Domäne des Benutzerkontos zur Authentifizierung am SMTP Server.
    - **Kennwort** und **Kennwortwiederholung**: Kennwort des Benutzerkontos zur Authentifizierung am SMTP Server.
    - **Port**: Port des SMTP-Dienstes auf dem SMTP Server. Standard: **25**
    - **Transportsicherheit**: Verschlüsselungsverfahren beim Versenden vom E-Mail-Benachrichtigungen. Wenn keine der folgenden Optionen angegeben wird, richtet sich das Verhalten nach dem Port (Port 25: ohne Verschlüsselung; Port 465: mit SSL/TLS Verschlüsselung).

      Zulässige Werte sind:

        - **Auto**: Automatische Erkennung des Verschlüsselungsverfahrens.
        - **SSL**: Verschlüsseln der gesamten Sitzung mit SSL/TLS.

- **STARTTLS**: Verwenden der STARTTLS-Mailserver-Erweiterung. Schaltet die TLS-Verschlüsselung nach dem Greeting und dem Lesen der Capabilities des Servers an. Die Verbindung scheitert, wenn der Server die STARTTLS-Erweiterung nicht unterstützt.
- **STARTTLSWhenAvailable**: Verwenden der STARTTLS-Mailserver-Erweiterung, wenn verfügbar. Schaltet die TLS-Verschlüsselung nach dem Greeting und dem Lesen der Capabilities des Servers an, jedoch nur, wenn dieser die STARTTLS-Erweiterung unterstützt.
- **None**: Keine Sicherheit der Transportschicht. Alle Daten werden als Klartext gesendet.

- **Selbstsignierte Zertifikate akzeptieren**: Gibt an, ob selbstsignierte Zertifikate für TLS-Verbindungen akzeptiert werden.
- **Servernamenkonflikte in Zertifikaten zulassen**: Gibt an, ob nicht passende Servernamen bei den Zertifikaten für TLS-Verbindungen zulässig sind.

5. Auf der Seite **E-Mail-Einstellungen** können Sie die Standard-E-Mail-Adresse von Absender und Empfänger sowie das Layout der E-Mails definieren.

   - **Adresse des Empfängers**: Standard-E-Mail-Adresse des Empfängers von Benachrichtigungen.
   - **Adresse des Senders**: Standard-E-Mail-Adresse des Absenders beim Versenden von automatisch generierte Benachrichtigungen.

     Syntax:

     ```
     sender@example.com
     ```

     Beispiel:

     ```
     NoReply@company.com
     ```

     Zusätzlich zur E-Mail-Adresse kann der Anzeigename des Absenders angegeben werden. Beachten Sie, dass die E-Mail-Adresse in diesem Fall durch spitze Klammern (**<>**) umschlossen wird.

     Beispiel:

     ```
     One Identity <NoReply@company.com>
     ```

   - **Sprachkultur**: Standardsprachkultur, in der E-Mail-Benachrichtigungen versendet werden, wenn für einen Empfänger keine Sprachkultur ermittelt werden kann.
   - **Sprache**: Standardsprache, in der E-Mail-Benachrichtigungen versendet werden.
   - **Schriftart**: Standardschriftart für E-Mail-Benachrichtigungen.
   - **Schriftgröße**: Standardschriftgröße für E-Mail-Benachrichtigungen.
   - **Unterschrift**: Unterschrift unter die Grußformel.
   - **Unternehmen**: Name des Unternehmens.
   - **Link**: Link auf die Unternehmenswebseite.

- **Link-Darstellung**: Anzeigetext für den Link zur Unternehmenswebseite.

6. Auf der Seite **Datensicherheit** können Sie die Einstellungen für die Datensicherheit konfigurieren.

   - **Fingerabdruck des Zertifikats**: SHA1-Fingerabdruck des zur Signierung zu verwendenden Zertifikats. Dieses kann im Zertifikatsspeicher des Computers oder des Benutzers liegen. Wenn Sie eine digitale Signatur nutzen wollen, aktivieren Sie **Fingerabdruck des Zertifikats** und geben Sie den Fingerabdruck an.
   - **E-Mails verschlüsseln**: Gibt an, ob E-Mails verschlüsselte werden sollen. Wenn Sie die Funktion aktivieren, werden die dafür benötigten Einstellungen angezeigt.
   - **Domänen-Controller**: Domänen-Controller der abzufragenden Domäne, der verwendet werden soll.
   - **Domäne**: Definierter Name der abzufragenden Domäne.
   - **Benutzerkonto**: Benutzerkonto, mit dem das Active Directory abgefragt wird.
   - **Kennwort** und **Kennwortwiederholung**: Kennwort des Benutzerkontos.

7. Auf der Seite **E-Mail-Benachrichtigungen über Bestellungen** nehmen Sie allgemeine Einstellungen für E-Mail-Benachrichtigungen über Bestellungen vor und Sie definieren, ob die Funktion **Entscheidung per E-Mail** für Bestellungen genutzt werden kann. Wenn Sie die Funktion aktivieren, werden die dafür benötigten Einstellungen angezeigt.

   - **Adresse des Senders**: Standard-E-Mail-Adresse des Absenders beim Versenden von automatisch generierte Benachrichtigungen.

     Syntax:

     ```
     sender@example.com
     ```

     Beispiel:

     ```
     NoReply@company.com
     ```

     Zusätzlich zur E-Mail-Adresse kann der Anzeigename des Absenders angegeben werden. Beachten Sie, dass die E-Mail-Adresse in diesem Fall durch spitze Klammern (**<>**) umschlossen wird.

     Beispiel:

     ```
     One Identity <NoReply@company.com>
     ```

   - **IT Shop Entscheidungen per E-Mail**: Gibt an, ob für die Entscheidung von Bestellungen auch die Funktion **Entscheidung per E-Mail** genutzt werden kann. Wenn Sie die Funktion aktivieren, bearbeiten Sie die dafür benötigten Einstellungen.
   - **Benutzername**: Name des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
   - **Domäne**: Domäne des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.

- **Kennwort** und **Kennwortwiederholung**: Kennwort des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
- **Webservice URL**: Gibt an, ob die URL des Microsoft Exchange Webdienstes für den Zugriff auf das Postfach genutzt werden soll. Wenn Sie die Funktion aktivieren, erfassen Sie die URL.
- **Postfach**: Microsoft Exchange Postfach, an das Entscheidungen per E-Mail gesendet werden.
- **Löschverhalten**: Gibt die Art und Weise an, wie E-Mails im Posteingang gelöscht werden sollen.
- **Anwendungs-ID**: Exchange Online Anwendungs-ID für die Authentifizierung über OAuth 2.0. Wenn der Wert nicht gesetzt ist, werden die Authentifizierungsmethoden **Basic** oder **NTML** verwendet.

8. Auf der Seite **E-Mail-Benachrichtigungen über Attestierungen** nehmen Sie allgemeine Einstellungen für E-Mail-Benachrichtigungen über Attestierungen vor und Sie definieren, ob die Funktion **Entscheidung per E-Mail** für Attestierungen genutzt werden kann. Wenn Sie die Funktion aktivieren, werden die dafür benötigten Einstellungen angezeigt.

   - **Adresse des Senders**: Standard-E-Mail-Adresse des Absenders beim Versenden von automatisch generierte Benachrichtigungen.

     Syntax:

     `sender@example.com`

     Beispiel:

     `NoReply@company.com`

     Zusätzlich zur E-Mail-Adresse kann der Anzeigename des Absenders angegeben werden. Beachten Sie, dass die E-Mail-Adresse in diesem Fall durch spitze Klammern (**<>**) umschlossen wird.

     Beispiel:

     `One Identity <NoReply@company.com>`
   - **Attestierung per E-Mail**: Gibt an, ob für Attestierungen auch die Funktion **Entscheidung per E-Mail** genutzt werden kann. Wenn Sie die Funktion aktivieren, bearbeiten Sie die dafür benötigten Einstellungen.
   - **Benutzername**: Name des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
   - **Domäne**: Domäne des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
   - **Kennwort** und **Kennwortwiederholung**: Kennwort des Benutzerkontos zur Authentifizierung am Postfach, das für Entscheidungen per E-Mail genutzt wird.
   - **Webservice URL**: Gibt an, ob die URL des Microsoft Exchange Webdienstes für den Zugriff auf das Postfach genutzt werden soll. Wenn Sie die Funktion aktivieren, erfassen Sie die URL.

- **Postfach**: Microsoft Exchange Postfach, an das Entscheidungen per E-Mail gesendet werden.
- **Löschverhalten**: Gibt die Art und Weise an, wie E-Mails im Posteingang gelöscht werden sollen.
- **Anwendungs-ID**: Exchange Online Anwendungs-ID für die Authentifizierung über OAuth 2.0. Wenn der Wert nicht gesetzt ist, werden die Authentifizierungsmethoden **Basic** oder **NTML** verwendet.

9. Auf der Seite **Berichtsabonnements** können Sie die Standardeinstellungen für Berichtsabonnements ändern.

   - **Adresse des Senders**: Standard-E-Mail-Adresse des Absenders beim Versenden von automatisch generierte Benachrichtigungen über Berichtsabonnements. Ersetzen Sie den Standardwert durch eine gültige E-Mail-Adresse.

     Syntax:

     `sender@example.com`

     Beispiel:

     `NoReply@company.com`

     Zusätzlich zur E-Mail-Adresse kann der Anzeigename des Absenders angegeben werden. Beachten Sie, dass die E-Mail-Adresse in diesem Fall durch spitze Klammern (**<>**) umschlossen wird.

     Beispiel:

     `One Identity <NoReply@company.com>`
   - **Standard-Berichtsvorlage**: Standardbericht, der als Vorlage zur Erstellung von einfachen Listenberichten verwendet wird.
   - **Zentrale Berichtsablage**: Gibt an, ob abonnierte Berichte in einem Ablageverzeichnis gespeichert werden sollen. Wenn Sie die Funktion aktivieren, bearbeiten Sie die dafür benötigten Einstellungen.
   - **Ablageverzeichnis für Berichte**: Pfad für die Ablage der abonnierten Berichte. Syntax: `\\<Server>\<Share>`
   - **Aufbewahrungszeitraum (Tage)**: Maximale Verweildauer (in Tagen), während der ein abonnierter Bericht im Ablageverzeichnis verfügbar ist. Nach Ablauf dieser Frist werden Berichte gelöscht.

10. Auf der Seite **E-Mail-Benachrichtigungen über Aktionen im Zielsystem** können Sie eine E-Mail-Adresse für Benachrichtigungen über Aktionen im Zielsystem hinterlegen. Das können Fehler- oder Erfolgsmeldungen über Änderungen im Zielsystem sein.

    - Um E-Mail-Benachrichtigungen mit Fehler- oder Erfolgsmeldungen über Änderungen im Zielsystem zu erhalten, aktivieren Sie **Active Directory** und geben Sie die E-Mail-Adresse an, an welche die Benachrichtigungen gesendet werden sollen.

11. Auf der letzten Seite des E-Mail-Konfigurationsassistenten klicken Sie **Fertig**.

Verwandte Themen

- Arbeiten mit dem Starling Governance Agent auf Seite 28

Automatische Zuordnung zu Identitäten konfigurieren

Beim Einfügen eines Benutzerkontos kann automatisch eine vorhandene Identität zugeordnet werden. Im Bedarfsfall kann eine Identität neu erstellt werden. Dabei werden die Stammdaten der Identität anhand vorhandener Benutzerstammdaten erzeugt. Dieser Mechanismus kann auf die Erstellung eines neuen Benutzerkontos durch manuelle Anlage oder Synchronisation folgen.

An administrative Benutzerkonten sollten Identitäten nicht automatisch zugeordnet werden. Über eine Ausschlussliste können Sie die Benutzerkonten festlegen, denen keine Identitäten automatisch zugeordnet werden sollen. Jeder Eintrag in der Liste wird als Teil eines regulären Ausdrucks behandelt.

Um die Ausschlussliste zu bearbeiten

1. Wählen Sie im Launchpad **Administrative Aufgaben > Systemkonfiguration > Automatische Identitätenzuordnung konfigurieren**.
2. Klicken Sie **Starten**.

   Der Dialog **Ausschlussliste für die automatische Personenzuordnung** wird geöffnet.
3. Um einen neuen Eintrag einzufügen, klicken Sie **Neu**.

   Um einen Eintrag zu bearbeiten, wählen Sie den Eintrag und klicken Sie **Bearbeiten**.
4. Erfassen Sie die Bezeichnung des Benutzerkontos, dem Identitäten nicht automatisch zugeordnet werden sollen.

   Metazeichen für reguläre Ausdrücke können verwendet werden.
5. Um einen Eintrag zu löschen, wählen Sie den Eintrag und klicken Sie **Löschen**.
6. Klicken Sie **OK**.

Verwandte Themen

- Arbeiten mit dem Starling Governance Agent auf Seite 28

Active Roles ADSI Provider installieren

Der Active Roles Konnektor des Starling Governance Agent verwendet das Active Roles ADSI Interface für die Kommunikation mit einer Active Roles Instanz. Der Active Roles Konnektor wird für die Synchronisation und Provisionierung der Active Directory-Umgebung eingesetzt. Der Active Roles Konnektor verbindet sich zu einer Active Roles Instanz, die dann die Verbindung zum Active Directory Domänen-Controller herstellt.

Um die Verbindung herzustellen, muss auf der administrativen Arbeitsstation der Active Roles ADSI Provider installiert sein.

Um den Active Roles ADSI Provider zu installieren

1. Wählen Sie im Launchpad **Administrative Aufgaben > Datensynchronisation > Active Roles ADSI Provider installieren**.
2. Klicken Sie **Installieren**.
3. Wählen Sie über den Dateibrowser den Pfad zur Datei `ActiveRoles.exe`. Wählen Sie diese aus und klicken Sie **Öffnen**.

   Die Installation wird ausgeführt.

   Wenn die Installation beendet ist, ist im Launchpad die Schaltfläche **Installieren** deaktiviert.

Verwandte Themen

- Starling Governance Agent Launchpad starten auf Seite 29

Synchronisation mit einer Active Directory Domäne einrichten

Um Active Directory Benutzerkonten und Gruppen mit Starling Governance zu verwalten, richten Sie die Synchronisation zwischen Active Roles und Starling Governance ein. Dafür halten Sie die folgenden Informationen bereit:

Tabelle 5: Benötigte Informationen für die Einrichtung der Synchronisation

Angaben	Erläuterungen
Definierter Name der Domäne	Definierter LDAP Name der Active Directory Domäne.
Benutzerkonto und Kennwort zur Anmeldung	Benutzerkonto und Kennwort zur Anmeldung am Active Roles. Stellen Sie ein Benutzerkonto mit ausreichend Berechtigungen bereit. Weitere Informationen finden Sie unter Benötigte Berechtigungen des Starling

Angaben	Erläuterungen
am Active Roles	Governance Agent Service für die Synchronisation mit One Identity Active Roles auf Seite 24.
DNS Name oder IP Adresse des Active Roles Servers	Vollständiger Name oder IP Adresse des Active Roles Servers, gegen den sich der Synchronisationsserver verbindet. Beispiel: `<Name des Servers>.<Vollqualifizierter Domänenname>`

WICHTIG: Richten Sie die Synchronisation für alle Active Directory Domänen ein, die über Ihre Active Roles-Umgebung verwaltet werden. Führen Sie die hier beschriebenen Schritte für jede Domäne erneut aus.

Um die Synchronisation einer Active Directory Domäne über Active Roles einzurichten

1. Wählen Sie im Launchpad **Administrative Aufgaben > Datensynchronisation > Synchronisation einrichten**.
2. Klicken Sie **Starten**.

   Der Systemverbindungsassistent wird gestartet.
3. Wenn angefordert, geben Sie die Konfigurationsdaten zu Ihrer Starling Governance Instanz an.

   a. Im Dialog **Starling Governance Konfigurationsdaten**, kopieren Sie Ihren Starling Governance Agent Schlüssel in das Textfeld.

   b. Klicken Sie **OK**.
4. Auf der Startseite des Systemverbindungsassistenten klicken Sie **Weiter**.
5. Auf der Seite **Zielserver** geben den Active Roles Server an, gegen den Sie sich verbinden möchten. Die möglichen Server werden, wenn möglich, automatisch ermittelt.
   - Wählen Sie unter **Hostname/IP Adresse** den Zielserver aus.
   - Kann der Server nicht automatisch ermittelt werden, tragen Sie unter **Hostname/IP Adresse** den DNS Namen oder die IP Adresse des Servers ein.
6. Auf der Seite **Anmeldeinformationen** geben Sie das Benutzerkonto und dass Kennwort für den Zugriff auf das Active Roles an.

   Nutzen Sie das Benutzerkonto, welches Sie als Dienstkonto für den Starling Governance Agent Service eingetragen haben.
7. Auf der Seite **Auswahl der Domäne/des Wurzeleintrages** wählen Sie die Domäne, die Sie synchronisieren möchten oder tragen Sie den definierten Namen des Wurzeleintrages ein.
8. Auf der letzten Seite des Systemverbindungsassistenten klicken Sie **Fertig**.

   Die Synchronisation wird eingerichtet.

Im Launchpad wird die Aufgabe **Synchronisationen verwalten** angezeigt.

TIPP: Auf die gleiche Weise richten Sie die Synchronisation weiterer Active Directory Domänen ein.

Verwandte Themen

- Arbeiten mit dem Starling Governance Agent auf Seite 28
- Synchronisationen verwalten auf Seite 42
- Konfigurationsdaten der Starling Governance Instanz laden auf Seite 29
- Minimale Systemanforderungen für die administrative Arbeitsstation auf Seite 19

Synchronisationen verwalten

Wenn die Synchronisation für eine Active Directory Domäne eingerichtet ist, können Sie folgende Aufgaben ausführen:

- Synchronisation manuell starten
- Systemverbindung bearbeiten
- Synchronisationskonfiguration löschen

Verwandte Themen

- Arbeiten mit dem Starling Governance Agent auf Seite 28
- Synchronisation mit einer Active Directory Domäne einrichten auf Seite 40

Synchronisation manuell starten

Standardmäßig wird die Synchronisation der Active Directory Domäne einmal täglich automatisch gestartet. Bei Bedarf können Sie die Synchronisation auch manuell starten.

Um die Synchronisation für eine Active Directory Domäne manuell zu starten

1. Wählen Sie im Launchpad **Administrative Aufgaben > Datensynchronisation > Synchronisationen verwalten**.
2. Klicken Sie **Starten**.
3. Im Dialog **Synchronisationen verwalten** wählen Sie die Domäne.
4. Klicken Sie **Synchronisation starten**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.
6. Schließen Sie das Meldungsfenster mit **Ok**.

Verwandte Themen

- Synchronisationen verwalten auf Seite 42
- Protokolldatei des Starling Governance Agent Service anzeigen auf Seite 44

Systemverbindung bearbeiten

Die Einstellungen der Systemverbindung zur synchronisierten Active Directory Domäne können nachträglich angepasst werden. Dabei wird der Systemverbindungsassistent erneut ausgeführt.

Um die Systemverbindung zu einer Active Directory Domäne zu bearbeiten

1. Wählen Sie im Launchpad **Administrative Aufgaben > Datensynchronisation > Synchronisationen verwalten**.
2. Klicken Sie **Starten**.
3. Im Dialog **Synchronisationen verwalten** wählen Sie die Domäne.
4. Klicken Sie **Systemverbindung bearbeiten**.
5. Folgen Sie den Anweisungen des Systemverbindungsassistenten und ändern Sie die gewünschten Eigenschaften.

Verwandte Themen

- Synchronisationen verwalten auf Seite 42
- Synchronisation mit einer Active Directory Domäne einrichten auf Seite 40

Systemverbindung löschen

Wenn zu einem späteren Zeitpunkt keine Daten mehr zwischen einer Active Directory Domäne und Starling Governance ausgetauscht werden sollen, kann die entsprechende Systemverbindung entfernt werden. Ab diesem Zeitpunkt werden keine Daten zwischen dieser Domäne und Starling Governance synchronisiert. Bestehende Daten, die bis dahin über diese Systemverbindung synchronisiert wurden, bleiben in beiden Systemen erhalten.

Um die Verbindungsdaten einer Active Directory Domäne zu löschen

1. Wählen Sie im Launchpad **Administrative Aufgaben > Datensynchronisation > Synchronisationen verwalten**.
2. Klicken Sie **Starten**.
3. Im Dialog **Synchronisationen verwalten** wählen Sie die Domäne.
4. Klicken Sie **Systemverbindung löschen**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Verwandte Themen

- Synchronisationen verwalten auf Seite 42

Protokolldatei des Starling Governance Agent Service anzeigen

Den aktuellen Status der Prozessverarbeitung können Sie in der Protokolldatei des Starling Governance Agent Service prüfen. Die Protokolldatei können Sie über ein Browserfrontend anzeigen. Sie wird über den Standardport 1880 aufgerufen.

Um die Protokolldatei des Starling Governance Agent Service anzuzeigen

1. Wählen Sie im Launchpad **Administrative Aufgaben > Datensynchronisation > Protokolldatei des Dienstes anzeigen**.
2. Klicken Sie **Anzeigen**.

   Die verschiedenen Dienste des Starling Governance Agent Service werden im Browser angezeigt.
3. Um den Inhalt der Protokolldatei anzuzeigen, wählen Sie in der Navigationsansicht **Log File**.

Die auf der Webseite anzuzeigenden Meldungen können interaktiv gefiltert werden. Dazu gibt es auf der Webseite eine Auswahlliste.

Zur besseren Übersichtlichkeit werden die Protokollausgaben farbig gekennzeichnet.

Tabelle 6: Farbcode in der Protokolldatei

Farbe	Bedeutung
Grün	Die Verarbeitung war erfolgreich.
Gelb	Bei der Verarbeitung wurden Warnung ausgegeben.
Rot	Bei der Verarbeitung sind schwerwiegende Fehler aufgetreten.

Verwandte Themen

- Arbeiten mit dem Starling Governance Agent auf Seite 28
- Einrichten der Berechtigung zum Erstellen eines HTTP Server auf Seite 22

Starling Governance Agent Service als Docker-Container starten

Der Starling Governance Agent Service übernimmt die Synchronisation zwischen Starling Governance und der angebundenen Active Roles-Umgebung. Zusätzlich zur Installation des Starling Governance Agent Service aus dem Launchpad stellt One Identity ein Docker-Image für eine einfache und standardisierte Installation und Ausführung des Starling Governance Agent Service in Docker-Containern zur Verfügung. Da für die Verbindung des Starling Governance Agent Service zur Active Roles-Umgebung der Active Roles ADSI Provider in der zur Active Roles Version passenden Version installiert sein muss, muss dieses Docker-Image auf Ihrem Windows-Docker-Host selbst gebaut werden. Nutzen Sie als Basis das One Identity Manager Docker-Image, das im Docker-Hub bereitsteht.

Um ein Docker-Image für Ihren Starling Governance Agent Service zu erstellen

1. Legen Sie auf Ihrem Windows-Docker-Host ein neues Verzeichnis an.
2. Legen Sie in diesem Verzeichnis den Unterordner `files` an.
3. Kopieren Sie in diesen Unterordner die zur Version des Active Roles Server passende Installationsdatei `ActiveRoles.exe`.
4. Im Hauptverzeichnis erstellen Sie eine Datei mit dem Namen `Dockerfile` und folgendem Inhalt:

   ```
   # base image (see https://hub.docker.com/r/oneidentity/oneim-job)
   FROM oneidentity/oneim-job:windows-amd64-latest-windowsservercore-1903

   # copy and install Active Roles ADSI Provider
   COPY files/ActiveRoles.exe /Installer/
   RUN C:/installer/ActiveRoles.exe /quiet /install ADDLOCAL=Tools
   /IAcceptActiveRolesLicenseTerms
   ```

5. Um das Docker-Image zu bauen, öffnen Sie eine Kommandozeilenkonsole im Hauptverzeichnis und führen Sie folgenden Befehl aus:

   ```
   docker build -t local/oneim-job-ars:windows-amd64-latest-windowsservercore-
   1903 .
   ```

   Sobald der Build-Vorgang abgeschlossen ist, steht das Docker-Image mit dem Namen **local/oneim-job-ars:windows-amd64-latest-windowsservercore-1903** zur Verfügung.

Um den Docker-Container zu starten

1. Definieren Sie die folgenden Parameter als Secret oder als Umgebungsvariablen.

   HTTP_User

   Benutzername, welcher zum Zugriff auf die Status-Webseite des Dienstes benötigt wird.

   HTTP_PWD

   Kennwort, welches zum Zugriff auf die Status-Webseite des Dienstes benötigt wird.

   CLOUDCONFIG

   Verbindungs-Zeichenkette Ihrer Starling Governance Instanz, welche auf der Starling Governance Webseite für Ihre Instanz zur Verfügung gestellt wird.

2. Starten Sie den Container.

Beispiel für den Start des Containers über Windows PowerShell

In diesem Beispiel werden die Parameter als Secrets gesetzt.

```
$secrets='C:\Path\To\secrets'

# Create directory
New-Item -ItemType Directory -Force -Path "$secrets"

# Create secrets
Set-Content -NoNewline -Path "$secrets\HTTP_USER" -Value "<Benutzer für Status-
Website>"
Set-Content -NoNewline -Path "$secrets\HTTP_PWD" -Value "<Passwort für Status-
Website>"
Set-Content -NoNewline -Path "$secrets\CLOUDCONFIG" -Value "<Verbindungs-
Zeichenkette>"

# Create Container
docker run -d `
--name "StarlingGovernanceAgentService" `
--hostname "DockerService" `
--cpus="4.0" `
-m 4GB `
-p 1880:1880 `
-v $secrets/:C:/ProgramData/Docker/secrets:ro `
local/oneim-job-ars:windows-amd64-latest-windowsservercore-1903
```

Ausführliche Informationen zum One Identity Manager Docker-Image finden Sie unter https://hub.docker.com/r/oneidentity/oneim-job.

Verwandte Themen

- Starling Governance Agent Service installieren auf Seite 32

Über uns

One Identity Lösungen eliminieren die Komplexität und die zeitaufwendigen Prozesse, die häufig bei der Identity Governance, der Verwaltung privilegierter Konten und dem Zugriffsmanagement aufkommen. Unsere Lösungen fördern die Geschäftsagilität und bieten durch lokale, hybride und Cloud-Umgebungen eine Möglichkeit zur Bewältigung Ihrer Herausforderungen beim Identitäts- und Zugriffsmanagement.

Kontaktieren Sie uns

Bei Fragen zum Kauf oder anderen Anfragen, wie Lizenzierungen, Support oder Support-Erneuerungen, besuchen Sie https://www.oneidentity.com/company/contact-us.aspx.

Technische Supportressourcen

Technische Unterstützung steht für One Identity Kunden mit einem gültigen Wartungsvertrag und Kunden mit Testversionen zur Verfügung. Sie können auf das Support Portal unter https://support.oneidentity.com/ zugreifen.

Das Support Portal bietet Selbsthilfe-Tools, die Sie verwenden können, um Probleme schnell und unabhängig zu lösen, 24 Stunden am Tag, 365 Tage im Jahr. Das Support Portal ermöglicht Ihnen:

- Senden und Verwalten von Serviceanfragen
- Anzeigen von Knowledge Base Artikeln
- Anmeldung für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Videos unter www.YouTube.com/OneIdentity
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

Index

S

T

W