One Identity Starling CertAccess

Demo-Test Leitfaden

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 CertAccess Demo-Test Leitfaden
Aktualisiert - 09 Juli 2021, 09:15

Inhalt

Starling CertAccess Demo-Tests

Starling CertAccess kann für einen begrenzten Zeitraum abonniert werden, um das Produkt zu testen, bevor Sie sich für eine längerfristige Nutzung entscheiden. Mit einem Demo-Test erfahren Sie, wie die Hauptfunktionen von Starling CertAccess funktionieren. Damit können Sie alle Funktionen mit einem Standardsatz an Beispieldaten testen, ohne die Starling CertAccess-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.

Mit einem Demo-Test können Sie verschiedene Anwendungsfälle testen. Folgende Anwendungsfälle sind hier Schritt-für-Schritt beschrieben:

- Szenario 1: Ein Standardbenutzer möchte die Active Directory Gruppe **Purchase Analysis** bestellen.
- Szenario 2: Ein Verantwortlicher für Attestierungen möchte eine Mitgliedschaft in der Active Directory Gruppe **Purchase Analysis** attestieren lassen. Die Attestierung soll genehmigt werden.
- Szenario 3: Ein Verantwortlicher für Attestierungen möchte eine Mitgliedschaft in der Active Directory Gruppe **Sales Analyst** attestieren lassen. Die Attestierung soll abgelehnt werden.
- Szenario 4: Ein Starling CertAccess-Administrator möchte Manager an Identitäten zuweisen.
- Szenario 5: Ein Starling CertAccess-Administrator möchte Produkteigner an Systemberechtigungen zuweisen.
- Szenario 6: Ein Standardbenutzer möchte die Verantwortung für die Active Directory Gruppe **Cert Publishers** übernehmen.

TIPP: Wenn Sie die Starling CertAccess-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 CertAccess Web Portals und können außerdem nachvollziehen, wie die Daten zwischen Active Roles und Starling CertAccess synchronisiert werden. Das Produkt verhält sich genau so, wie bei einem kostenpflichtigen Abonnement. Es gibt keine Einschränkungen. Ausführliche Informationen zum Proof-of-Concept-Test finden Sie im *One Identity Starling CertAccess Administrationshandbuch für die Integration mit One Identity Active Roles*.

Verfügbare Dokumentation

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

Demo-Test starten

Wenn Sie ein Test-Abonnement gestartet haben und die Testinstanz für den Demo-Test bereitgestellt wurde, können Sie den Demo-Test starten. Ausführliche Informationen zum Starten eines Test-Abonnements finden Sie im *One Identity Starling CertAccess Administrationshandbuch für die Integration mit One Identity Active Roles*.

Mit den Beispieldaten können Sie verschiedene Anwendungsfälle testen. Dafür werden fünf Identitäten bereitgestellt, mit denen Sie sich am Starling CertAccess Web Portal anmelden können. Weitere Informationen finden Sie unter Identitäten auf Seite 7.

Um einen Demo-Test zu starten

1. Klicken Sie in der E-Mail **Your Starling CertAccess subscription is ready** auf die Schaltfläche **Get Started**.

   Die Starling CertAccess-Webseite wird geöffnet.

   Hier sehen Sie die Benutzernamen aller Identitäten, die Sie für den Test nutzen können.
2. Neben der Identität, mit der Sie sich am Starling CertAccess Web Portal anmelden möchten, klicken Sie **Copy**.

   Der Anmeldename der Identität wird in die Zwischenablage kopiert.
3. Auf der Kachel **CertAccess Portal** klicken Sie **GO**.

   Die Anmeldeseite des Starling CertAccess Web Portals wird geöffnet.
4. Fügen Sie den Benutzernamen in das Eingabefeld **Benutzer** ein.
5. Wechseln Sie auf die Starling CertAccess-Webseite.
6. Auf der Kachel **Demo Trial** klicken Sie **Copy**.

   Das Kennwort für die Anmeldung am Starling CertAccess Web Portal wird in die Zwischenablage kopiert.
7. Wechseln Sie auf die Anmeldeseite des Starling CertAccess Web Portal.
8. Fügen Sie das Kennwort in das Eingabefeld **Kennwort** ein.
9. Klicken Sie **Anmelden**.

   Die Startseite des Starling CertAccess Web Portals wird geöffnet.

Verwandte Themen

- Demo-Test beenden auf Seite 6

Demo-Test beenden

Ein Demo-Test ist auf 5 Tage begrenzt. Innerhalb der Laufzeit Ihres Test-Abonnements (30 Tage) können Sie Demo-Tests jederzeit beenden und neu starten.

Um einen Demo-Test vorzeitig zu beenden

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

Verwandte Themen

- Demo-Test starten auf Seite 5

Anwendungsfälle und Identitäten

Mit den Beispieldaten werden verschiedene Identitäten bereitgestellt, mit denen Sie sich am Starling CertAccess Web Portal anmelden und verschiedene Anwendungsfälle testen können (siehe Identitäten auf Seite 7). Die folgenden Anwendungsfälle sind hier beschrieben.

> HINWEIS: Einige der Vorgänge, die in den Anwendungsfällen ausgelöst werden, können einige Zeit in Anspruch nehmen (beispielsweise das Anlegen von Attestierungsvorgängen nach dem Start einer Attestierung). Aktionen, die von diesen Vorgängen abhängig sind, stehen dann nicht sofort zur Verfügung. Ist eine Aktion noch nicht verfügbar, warten Sie einige Zeit ab und laden Sie die Seite erneut.

Anwendungsfälle

- Szenario 1: Ein Standardbenutzer möchte die Active Directory Gruppe **Purchase Analysis** bestellen.
- Szenario 2: Ein Verantwortlicher für Attestierungen möchte eine Mitgliedschaft in der Active Directory Gruppe **Purchase Analysis** attestieren lassen. Die Attestierung soll genehmigt werden.
- Szenario 3: Ein Verantwortlicher für Attestierungen möchte eine Mitgliedschaft in der Active Directory Gruppe **Sales Analyst** attestieren lassen. Die Attestierung soll abgelehnt werden.
- Szenario 4: Ein Starling CertAccess-Administrator möchte Manager an Identitäten zuweisen.
- Szenario 5: Ein Starling CertAccess-Administrator möchte Produkteigner an Systemberechtigungen zuweisen.

- Szenario 6: Ein Standardbenutzer möchte die Verantwortung für die Active Directory Gruppe **Cert Publishers** übernehmen.

Detaillierte Informationen zum Thema

Identitäten

Folgende Identitäten nutzen Sie in den beschriebenen Anwendungsfällen.

Celestine Eaton

- Benutzername: CELESTINEAT
- Rolle: Starling CertAccess Administrator
- Aufgaben:
  - Bestellungen und Attestierungsvorgänge betrachten
  - Daten im Daten-Explorer betrachten
  - Mitgliedschaften in Anwendungsrollen bearbeiten

Tony Denison

- Benutzername: TONYDEN
- Rolle: Manager
- Aufgaben: Zugriffsanforderungen (Bestellungen von Gruppenmitgliedschaften) für Tomas Grenier genehmigen

Tomas Grenier

- Benutzername: TOMASGRE
- Rolle: Standardbenutzer
- Aufgaben: Mitgliedschaften in folgenden Active Directory Gruppen bestellen

- Accounts payable
- Enterprise Contract Administrators
- Expense Manager
- Marketing Operations
- Purchase Analysis
- Sales Analyst
- Supplier Qualification

Dorreen Palacek

- Benutzername: DORREENPAL
- Rolle: Produkteigner von Systemberechtigungen
- Aufgaben: Zugriffsanforderungen für folgende Active Directory Gruppen genehmigen
  - Accounts payable
  - Enterprise Contract Administrators
  - Expense Manager
  - Marketing Operations
  - Purchase Analysis
  - Sales Analyst
  - Supplier Qualification

Quentin Payton

- Benutzername: QUENTINPAY
- Rolle: Verantwortlicher für Attestierungen
- Aufgaben: Attestierungen durchführen

Verwandte Themen

- Anwendungsfälle und Identitäten auf Seite 6

Szenario 1: Mitgliedschaft in einer Active Directory Gruppe bestellen

Ein Standardbenutzer möchte für sich selbst eine Mitgliedschaft in der Active Directory Gruppe **Purchase Analysis** bestellen. Die Bestellung durchläuft ein Genehmigungsverfahren. Die Bestellung wird durch den Manager des Standardbenutzers und durch den Eigentümer der Gruppe (Produkteigner) genehmigt. Sobald die Bestellung genehmigt wurde, wird das Active Directory Benutzerkonto des Standardbenutzers Mitglied

der bestellten Gruppe. Der Starling CertAccess-Administrator kann anschließend prüfen, ob das Benutzerkonto des Standardbenutzers an die Gruppe zugewiesen wurde.

Über Bestellungen können für die in Starling CertAccess verwalteten Identitäten Zugriffsberechtigungen in der angebundenen Active Directory-Umgebung beantragt werden. Alle Bestellungen durchlaufen ein Genehmigungsverfahren, in welchem Verantwortliche die Bestellungen genehmigen oder ablehnen können. Über die Bestellhistorie ist jederzeit nachvollziehbar, wer welche Zugriffsanforderungen gestellt oder genehmigt hat.

TIPP: Wenn eine Aktion noch nicht verfügbar ist, dann läuft ein Hintergrundprozess, beispielsweise zur Ermittlung des nächsten Entscheiders. Warten Sie einige Zeit ab und laden Sie die Seite erneut.

Um die Active Directory Gruppe Purchase Analysis zu bestellen

1. Melden Sie sich als **TOMASGRE** am Starling CertAccess Web Portal an.
2. Bestellen Sie die Active Directory Gruppe **Purchase Analysis**.
    a. In der Menüleiste klicken Sie **Bestellungen** > **Neue Bestellung**.
    b. Auf der Seite **Neue Bestellung** in der Kachel **Purchase Analysis** klicken Sie **In den Einkaufswagen**.
    c. Auf der Seite **Einkaufswagen** klicken Sie **Absenden**.

    Es wird eine Peer-Gruppen-Analyse durchgeführt.

    Tony Denison, der Manager von Tomas Grenier, wird als Entscheider ermittelt.
3. Melden Sie **TOMASGRE** ab.
4. Melden Sie sich als **TONYDEN** an.

    Eine offene Bestellung kann genehmigt werden.
5. Genehmigen Sie die Bestellung.
    a. In der Menüleiste klicken Sie **Bestellungen** > **Offene Bestellungen**.
    b. Auf der Seite **Offene Bestellungen** neben der Bestellung von **Purchase Analysis** klicken Sie **Genehmigen**.
    c. Im Bereich **Bestellung genehmigen** klicken Sie **Speichern**.

    Dorreen Palacek, Eigentümerin der Gruppe, wird als Entscheider ermittelt.
6. Melden Sie **TONYDEN** ab.
7. Melden Sie sich als **DORREENPAL** an.

    Eine offene Bestellung kann genehmigt werden.
8. Genehmigen Sie die Bestellung.
    a. In der Menüleiste klicken Sie **Bestellungen** > **Offene Bestellungen**.
    b. Auf der Seite **Offene Bestellungen** neben der Bestellung von **Purchase Analysis** klicken Sie **Genehmigen**.
    c. Im Bereich **Bestellung genehmigen** klicken Sie **Speichern**.

Damit ist die Bestellung final genehmigt und die Gruppenmitgliedschaft wird erzeugt.

9. Melden Sie **DORREENPAL** ab.
10. Melden Sie sich als **CELESTINEAT** an.
11. Prüfen Sie im Daten-Explorer, ob das Benutzerkonto der Gruppe zugewiesen wurde.
    a. In der Menüleiste klicken Sie **Daten** > **Daten-Explorer**.
    b. Im Daten-Explorer in der Navigation klicken Sie **Systemberechtigungen**.
    c. Im Eingabefeld **Suchen** geben Sie **Purchase Analysis** ein.
    d. In der Liste klicken Sie **Purchase Analysis**.
    e. Im Detailbereich klicken Sie den Tabreiter **Mitgliedschaften**.
    f. Im Tabreiter **Mitgliedschaften** prüfen Sie, ob das Benutzerkonto der Identität **Grenier, Tomas (TOMASGRE)** als Mitglied aufgelistet wird.

Verwandte Themen

- Identitäten auf Seite 7
- Szenario 2: Attestierung einer Gruppenmitgliedschaft mit Genehmigung auf Seite 10
- Szenario 3: Attestierung einer Gruppenmitgliedschaft mit Ablehnung auf Seite 12
- Szenario 4: Manager an Identitäten zuweisen auf Seite 14
- Szenario 5: Produkteigner an Systemberechtigungen zuweisen auf Seite 15
- Szenario 6: Verantwortung für eine Systemberechtigung übernehmen auf Seite 16

Szenario 2: Attestierung einer Gruppenmitgliedschaft mit Genehmigung

Ein Verantwortlicher für Attestierungen möchte eine Mitgliedschaft in der Active Directory Gruppe **Purchase Analysis** attestieren lassen. Die Mitgliedschaft soll bestätigt werden. Der Attestierungsvorgang wird dem Manager des Mitglieds und dem Eigentümer der Gruppe zugewiesen und bestätigt. Der Starling CertAccess-Administrator kann anschließend prüfen, ob das Benutzerkonto weiterhin Mitglied der Gruppe ist.

Mit der Attestierungsfunktion kann die Richtigkeit verschiedener Daten bescheinigt werden. Attestierungen werden entweder regelmäßig durchgeführt oder können durch Verantwortliche für Attestierungen explizit veranlasst werden. Sobald eine Attestierung veranlasst wird, werden Attestierungsvorgänge erstellt, die alle notwendigen Informationen über die Attestierungsobjekte und die verantwortlichen Attestierer enthalten. Die verantwortlichen Attestierer prüfen dann die Attestierungsobjekte. Sie bestätigen korrekte Daten und veranlassen Änderungen, wenn Daten internen Regelungen widersprechen. Attestierungsvorgänge zeichnen den gesamten Ablauf einer Attestierung auf. Im Attestierungsvorgang kann jeder einzelne Entscheidungsschritt der Attestierung revisionssicher nachvollzogen werden.

TIPP: Wenn eine Aktion noch nicht verfügbar ist, dann läuft ein Hintergrundprozess, beispielsweise zur Ermittlung des nächsten Attestierers. Warten Sie einige Zeit ab und laden Sie die Seite erneut.

Voraussetzung

- Szenario 1 wurde erfolgreich durchgeführt (siehe Szenario 1: Mitgliedschaft in einer Active Directory Gruppe bestellen auf Seite 8). Tomas Grenier ist Mitglied der Gruppe **Purchase Analysis**.

Um eine Mitgliedschaft in einer Active Directory Gruppe zu attestieren

1. Melden Sie sich als **QUENTINPAY** am Starling CertAccess Web Portal an.
2. Starten Sie die Attestierung.
    a. In der Menüleiste klicken Sie **Attestierung** > **Attestierungsrichtlinien**.
    b. Auf der Seite **Attestierungsrichtlinien** neben der Attestierungsrichtlinie **Attestierung von Mitgliedschaften in Systemberechtigungen (mit Peer-Gruppen-Analyse)** klicken Sie ⋮ (**Aktionen**) > **Attestierung starten**.
    c. Im Detailbereich klicken Sie neben **TomasGre - Purchase Analysis** auf **Attestierung starten**.

    Tony Denison, der Manager von Tomas Grenier, wird als Attestierer ermittelt.
3. Melden Sie **QUENTINPAY** ab.
4. Melden Sie sich als **TONYDEN** an.

    Eine offene Attestierung kann genehmigt werden.
5. Genehmigen Sie die Attestierung.
    a. In der Menüleiste klicken Sie **Attestierung** > **Offene Attestierungen**.
    b. Auf der Seite **Offene Attestierungen** neben dem Attestierungsvorgang **Soll die Identität "Grenier, Tomas (TOMASGRE)" über das Benutzerkonto "TomasGre" Zugriff auf die Systemberechtigung "Purchase Analysis" haben?** klicken Sie **Genehmigen**.
    c. Im Bereich **Genehmigen** klicken Sie **Speichern**.

    Dorreen Palacek, Eigentümerin der Gruppe, wird als Attestierer ermittelt.
6. Melden Sie **TONYDEN** ab.
7. Melden Sie sich als **DORREENPAL** an.

    Eine offene Attestierung kann genehmigt werden.
8. Genehmigen Sie die Attestierung.
    a. In der Menüleiste klicken Sie **Attestierung** > **Offene Attestierungen**.
    b. Auf der Seite **Offene Attestierungen** neben dem Attestierungsvorgang **Soll die Identität "Grenier, Tomas (TOMASGRE)" über das Benutzerkonto**

"TomasGre" Zugriff auf die Systemberechtigung "Purchase Analysis" haben? klicken Sie **Genehmigen**.

c. Im Bereich **Genehmigen** klicken Sie **Speichern**.

Damit ist der Attestierungsvorgang final genehmigt und die Gruppenmitgliedschaft bestätigt.

9. Melden Sie **DORREENPAL** ab.
10. Melden Sie sich als **CELESTINEAT** an.
11. Prüfen Sie im Daten-Explorer, ob das Benutzerkonto weiterhin der Gruppe zugewiesen ist.

    a. In der Menüleiste klicken Sie **Daten** > **Daten-Explorer**.

    b. Im Daten-Explorer in der Navigation klicken Sie **Systemberechtigungen**.

    c. Im Eingabefeld **Suchen** geben Sie **Purchase Analysis** ein.

    d. In der Liste klicken Sie **Purchase Analysis**.

    e. Im Detailbereich klicken Sie den Tabreiter **Mitgliedschaften**.

    f. Im Tabreiter **Mitgliedschaften** prüfen Sie, ob das Benutzerkonto der Identität **Grenier, Tomas (TOMASGRE)** als Mitglied aufgelistet wird.

Verwandte Themen

- Identitäten auf Seite 7
- Szenario 1: Mitgliedschaft in einer Active Directory Gruppe bestellen auf Seite 8
- Szenario 3: Attestierung einer Gruppenmitgliedschaft mit Ablehnung auf Seite 12
- Szenario 4: Manager an Identitäten zuweisen auf Seite 14
- Szenario 5: Produkteigner an Systemberechtigungen zuweisen auf Seite 15
- Szenario 6: Verantwortung für eine Systemberechtigung übernehmen auf Seite 16

Szenario 3: Attestierung einer Gruppenmitgliedschaft mit Ablehnung

Ein Verantwortlicher für Attestierungen möchte eine Mitgliedschaft in der Active Directory Gruppe **Sales Analyst** attestieren lassen. Die Mitgliedschaft soll abgelehnt werden. Der Attestierungsvorgang wird dem Manager des Mitglieds und dem Eigentümer der Gruppe zugewiesen. Ein Attestierer lehnt die bestehende Gruppenmitgliedschaft ab und die Zuweisung des Benutzerkontos an die Gruppe wird automatisch entfernt. Der Starling CertAccess-Administrator kann anschließend prüfen, ob die Gruppenmitgliedschaft tatsächlich entfernt wurde.

Mit der Attestierungsfunktion kann die Richtigkeit verschiedener Daten bescheinigt werden. Attestierungen werden entweder regelmäßig durchgeführt oder können durch Verantwortliche für Attestierungen explizit veranlasst werden. Sobald eine Attestierung

veranlasst wird, werden Attestierungsvorgänge erstellt, die alle notwendigen Informationen über die Attestierungsobjekte und die verantwortlichen Attestierer enthalten. Die verantwortlichen Attestierer prüfen dann die Attestierungsobjekte. Sie bestätigen korrekte Daten und veranlassen Änderungen, wenn Daten internen Regelungen widersprechen. Attestierungsvorgänge zeichnen den gesamten Ablauf einer Attestierung auf. Im Attestierungsvorgang kann jeder einzelne Entscheidungsschritt der Attestierung revisionssicher nachvollzogen werden.

TIPP: Wenn eine Aktion noch nicht verfügbar ist, dann läuft ein Hintergrundprozess, beispielsweise zur Ermittlung des nächsten Attestierers. Warten Sie einige Zeit ab und laden Sie die Seite erneut.

Voraussetzung

- Führen Sie Szenario 1 für die Gruppe **Sales Analyst** aus (siehe Szenario 1: Mitgliedschaft in einer Active Directory Gruppe bestellen auf Seite 8).
- Tomas Grenier ist anschließend Mitglied der Gruppe **Sales Analyst**.

Um eine Mitgliedschaft in einer Active Directory Gruppe zu attestieren und die Attestierung abzulehnen

1. Melden Sie sich als **QUENTINPAY** am Starling CertAccess Web Portal an.
2. Starten Sie die Attestierung.
   a. In der Menüleiste klicken Sie **Attestierung** > **Attestierungsrichtlinien**.
   b. Auf der Seite **Attestierungsrichtlinien** neben der Attestierungsrichtlinie **Attestierung von Mitgliedschaften in Systemberechtigungen (mit Peer-Gruppen-Analyse)** klicken Sie ⋮ (**Aktionen**) > **Attestierung starten**.
   c. Im Detailbereich klicken Sie neben **TomasGre - Sales Analyst** auf **Attestierung starten**.

   Tony Denison, der Manager von Tomas Grenier, wird als Attestierer ermittelt.
3. Melden Sie **QUENTINPAY** ab.
4. Melden Sie sich als **TONYDEN** an.

   Eine offene Attestierung kann genehmigt werden.
5. Genehmigen Sie die Attestierung.
   a. In der Menüleiste klicken Sie **Attestierung** > **Offene Attestierungen**.
   b. Auf der Seite **Offene Attestierungen** neben dem Attestierungsvorgang **Soll die Identität "Grenier, Tomas (TOMASGRE)" über das Benutzerkonto "TomasGre" Zugriff auf die Systemberechtigung "Sales Analyst" haben?** klicken Sie **Genehmigen**.
   c. Im Bereich **Genehmigen** klicken Sie **Speichern**.

   Dorreen Palacek, Eigentümerin der Gruppe, wird als Attestierer ermittelt.
6. Melden Sie **TONYDEN** ab.

7. Melden Sie sich als **DORREENPAL** an.

   Eine offene Attestierung kann genehmigt werden.

8. Lehnen Sie die Attestierung ab.

   a. In der Menüleiste klicken Sie **Attestierung** > **Offene Attestierungen**.

   b. Auf der Seite **Offene Attestierungen** neben dem Attestierungsvorgang **Soll die Identität "Grenier, Tomas (TOMASGRE)" über das Benutzerkonto "TomasGre" Zugriff auf die Systemberechtigung "Sales Analyst" haben?** klicken Sie **Ablehnen**.

   c. Im Bereich **Ablehnen** klicken Sie **Speichern**.

   Damit ist der Attestierungsvorgang final abgelehnt. Die Gruppenmitgliedschaft wird automatisch entfernt.

9. Melden Sie **DORREENPAL** ab.
10. Melden Sie sich als **CELESTINEAT** an.
11. Prüfen Sie im Daten-Explorer, ob die Gruppenmitgliedschaft entfernt wurde.

    a. In der Menüleiste klicken Sie **Daten** > **Daten-Explorer**.

    b. Im Daten-Explorer in der Navigation klicken Sie **Systemberechtigungen**.

    c. Im Eingabefeld **Suchen** geben Sie **Sales Analyst** ein.

    d. In der Liste klicken Sie **Sales Analyst**.

    e. Im Detailbereich klicken Sie den Tabreiter **Mitgliedschaften**.

    f. Im Tabreiter **Mitgliedschaften** prüfen Sie, ob das Benutzerkonto der Identität **Grenier, Tomas (TOMASGRE)** als Mitglied aufgelistet wird.

Verwandte Themen

- Identitäten auf Seite 7
- Szenario 1: Mitgliedschaft in einer Active Directory Gruppe bestellen auf Seite 8
- Szenario 2: Attestierung einer Gruppenmitgliedschaft mit Genehmigung auf Seite 10
- Szenario 4: Manager an Identitäten zuweisen auf Seite 14
- Szenario 5: Produkteigner an Systemberechtigungen zuweisen auf Seite 15
- Szenario 6: Verantwortung für eine Systemberechtigung übernehmen auf Seite 16

Szenario 4: Manager an Identitäten zuweisen

Ein Starling CertAccess-Administrator möchte alle Identitäten anzeigen, denen kein Manager zugewiesen ist. Der Starling CertAccess-Administrator möchte einer dieser Identitäten einen Manager zuweisen.

Um einer Identität einen Manager zuzuweisen

1. Melden Sie sich als **CELESTINEAT** am Starling CertAccess Web Portal an.
2. Zeigen Sie im Daten-Explorer alle Identitäten an, die keinen Manager haben und weisen Sie einer der Identitäten einen Manager zu.
    a. In der Menüleiste klicken Sie **Daten** > **Daten-Explorer**.
    b. Im Daten-Explorer klicken Sie ⚠ **Probleme gefunden**.
    c. Auf der Seite **Datenverfügbarkeit** neben **Identitäten** klicken Sie **Anzeigen**.
    d. In der Liste klicken Sie die Identität, der Sie einen Manager zuweisen möchten.
    e. Im Detailbereich in der Auswahlliste **Manager** wählen Sie den Manager, den Sie der Identität zuweisen möchten.
    f. Klicken Sie **Speichern**.

Verwandte Themen

- Identitäten auf Seite 7
- Szenario 1: Mitgliedschaft in einer Active Directory Gruppe bestellen auf Seite 8
- Szenario 2: Attestierung einer Gruppenmitgliedschaft mit Genehmigung auf Seite 10
- Szenario 3: Attestierung einer Gruppenmitgliedschaft mit Ablehnung auf Seite 12
- Szenario 5: Produkteigner an Systemberechtigungen zuweisen auf Seite 15
- Szenario 6: Verantwortung für eine Systemberechtigung übernehmen auf Seite 16

Szenario 5: Produkteigner an Systemberechtigungen zuweisen

Ein Starling CertAccess-Administrator möchte alle Systemberechtigungen anzeigen, denen kein Produkteigner zugewiesen ist. Der Starling CertAccess-Administrator möchte einer dieser Systemberechtigungen einen Produkteigner zuweisen. Der Starling CertAccess-Administrator kann eine Identität oder alle Mitglieder einer Anwendungsrolle als Produkteigner auswählen.

> TIPP: Produkteigner können beispielsweise als Entscheider für Bestellungen herangezogen werden.

Um einen Produkteigner an eine Systemberechtigung zuzuweisen

1. Melden Sie sich als **CELESTINEAT** am Starling CertAccess Web Portal an.
2. Zeigen Sie im Daten-Explorer alle Systemberechtigungen an, die keinen Produkteigner haben und weisen Sie einer der Systemberechtigungen einen Produkteigner zu.

a. In der Menüleiste klicken Sie **Daten** > **Daten-Explorer**.

b. Im Daten-Explorer klicken Sie ⚠ **Probleme gefunden**.

c. Auf der Seite **Datenverfügbarkeit** neben **Systemberechtigungen** klicken Sie **Anzeigen**.

d. In der Liste klicken Sie die Systemberechtigung, der Sie einen Produkteigner zuweisen möchten.

e. Im Detailbereich klicken Sie den Tabreiter **Leistungsposition**.

f. Im Tabreiter **Leistungsposition** nehmen Sie eine der folgenden Aktionen vor:

- Um Mitglieder einer Anwendungsrolle als Produkteigner festzulegen, aktivieren Sie die Option **Aus Rollen wählen**, klicken Sie im Feld **Produkteigner** auf **Zuweisen/Ändern** und wählen Sie anschließend die entsprechende Anwendungsrolle aus.
- Um eine Identität als Produkteigner festzulegen, aktivieren Sie die Option **Aus Identitäten wählen** und wählen Sie anschließend in der Auswahlliste **Identität** die entsprechende Identität aus.

g. Klicken Sie **Leistungsposition speichern**.

Verwandte Themen

- Identitäten auf Seite 7
- Szenario 1: Mitgliedschaft in einer Active Directory Gruppe bestellen auf Seite 8
- Szenario 2: Attestierung einer Gruppenmitgliedschaft mit Genehmigung auf Seite 10
- Szenario 3: Attestierung einer Gruppenmitgliedschaft mit Ablehnung auf Seite 12
- Szenario 4: Manager an Identitäten zuweisen auf Seite 14
- Szenario 6: Verantwortung für eine Systemberechtigung übernehmen auf Seite 16

Szenario 6: Verantwortung für eine Systemberechtigung übernehmen

Ein Standardbenutzer möchte die Verantwortung für die Active Directory Gruppe **Cert Publishers** übernehmen. Damit wird er als Produkteigner für diese Gruppe eingetragen und kann beispielsweise über Bestellungen dieser Gruppe entscheiden oder Mitgliedschaften in dieser Gruppe attestieren. Der Standardbenutzer selbst bestätigt im Rahmen einer Attestierung, dass diese Zuweisung korrekt ist.

> TIPP: Wenn eine Aktion noch nicht verfügbar ist, dann läuft ein Hintergrundprozess, beispielsweise zum Anlegen des Attestierungsvorganges. Warten Sie einige Zeit ab und laden Sie die Seite erneut.

Um die Verantwortung für die Active Directory Gruppe Cert Publishers zu übernehmen

1. Melden Sie sich als **TOMASGRE** am Starling CertAccess Web Portal an.
2. Weisen Sie einen Produkteigner zu.

    a. In der Menüleiste klicken Sie **Verantwortlichkeiten** > **Eigentümer zuweisen**.

    b. Auf der Seite **Eigentümer für eine Systemberechtigung zuweisen** in der Auswahlliste **Systemberechtigung** klicken Sie **Cert Publishers**.

    c. Klicken Sie **Weiter**.

    d. Im zweiten Schritt klicken Sie **Ich möchte die Verantwortung für diese Systemberechtigung übernehmen**.

    e. Klicken Sie **Weiter**.

    Es wird ein Attestierungsvorgang erstellt, in dem Tomas Grenier bestätigt, dass die Zuweisung korrekt ist.
3. Bestätigen Sie, dass Tomas Grenier die Verantwortung tatsächlich übernehmen möchte.

    a. In der Menüleiste klicken Sie **Attestierung** > **Offene Attestierungen**.

    b. Auf der Seite **Offene Attestierungen** neben dem Attestierungsvorgang **Wer ist der korrekte Eigentümer der Systemberechtigung "Cert Publishers"?** klicken Sie **Genehmigen**.

    c. Im Bereich **Genehmigen** klicken Sie **Speichern**.

    Tomas Grenier wird als Produkteigner zugewiesen.

Verwandte Themen

- Identitäten auf Seite 7
- Szenario 1: Mitgliedschaft in einer Active Directory Gruppe bestellen auf Seite 8
- Szenario 2: Attestierung einer Gruppenmitgliedschaft mit Genehmigung auf Seite 10
- Szenario 3: Attestierung einer Gruppenmitgliedschaft mit Ablehnung auf Seite 12
- Szenario 4: Manager an Identitäten zuweisen auf Seite 14
- Szenario 5: Produkteigner an Systemberechtigungen zuweisen auf Seite 15

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