



## One Identity Starling CertAccess

Administrationshandbuch für die  
Integration mit One Identity Active  
Roles

**Copyright 2022 One Identity LLC.**

**ALLE RECHTE VORBEHALTEN.**

Diese Anleitung enthält urheberrechtlich geschützte Informationen. Die in dieser Anleitung beschriebene Software wird unter einer Softwarelizenz oder einer Geheimhaltungsvereinbarung bereitgestellt. Diese Software darf nur in Übereinstimmung mit den Bestimmungen der geltenden Vereinbarung verwendet oder kopiert werden. Kein Teil dieser Anleitung darf ohne die schriftliche Erlaubnis von One Identity LLC in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch reproduziert oder übertragen werden, einschließlich Fotokopien und Aufzeichnungen für irgendeinen anderen Zweck als den persönlichen Gebrauch des Erwerbers.

Die Informationen in diesem Dokument werden in Verbindung mit One Identity Produkten bereitgestellt. Durch dieses Dokument oder im Zusammenhang mit dem Verkauf von One Identity LLC Produkten wird keine Lizenz, weder ausdrücklich oder stillschweigend, noch durch Duldung oder anderweitig, an jeglichem geistigen Eigentumsrecht eingeräumt. MIT AUSNAHME DER IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT GENANNTEN BEDINGUNGEN ÜBERNIMMT ONE IDENTITY KEINERLEI HAFTUNG UND SCHLIESST JEGLICHE AUSDRÜCKLICHE, IMPLIZIERTE ODER GESETZLICHE GEWÄHRLEISTUNG ODER GARANTIE IN BEZUG AUF IHRE PRODUKTE AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GEWÄHRLEISTUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ONE IDENTITY FÜR JEGLICHE DIREKTE, INDIREKTE, FOLGE-, STÖRUNGS-, SPEZIELLE ODER ZUFÄLLIGE SCHÄDEN (EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, SCHÄDEN FÜR VERLUST VON GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER VERLUST VON INFORMATIONEN), DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS RESULTIEREN, SELBST WENN ONE IDENTITY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN HAT. One Identity übernimmt keinerlei Zusicherungen oder Garantien hinsichtlich der Richtigkeit und Vollständigkeit des Inhalts dieses Dokuments und behält sich das Recht vor, Änderungen an Spezifikationen und Produktbeschreibungen jederzeit ohne vorherige Ankündigung vorzunehmen. One Identity verpflichtet sich nicht, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Wenn Sie Fragen zu Ihrer potenziellen Nutzung dieses Materials haben, wenden Sie sich bitte an:

One Identity LLC.  
Attn: LEGAL Dept  
4 Polaris Way  
Aliso Viejo, CA 92656

Besuchen Sie unsere Website (<http://www.OneIdentity.com>) für regionale und internationale Büro-Adressen.

**Patente**

One Identity ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente und anhängige Patente gelten. Für die aktuellsten Informationen über die geltenden Patente für dieses Produkt besuchen Sie bitte unsere Website unter <http://www.OneIdentity.com/legal/patents.aspx>.

**Marken**

One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC. in den USA und anderen Ländern. Für eine vollständige Liste der One Identity Marken besuchen Sie bitte unsere Website unter [www.OneIdentity.com/legal](http://www.OneIdentity.com/legal). Alle anderen Marken sind Eigentum der jeweiligen Besitzer.

**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.

# Inhalt

<b>Über dieses Handbuch</b> .....	<b>5</b>
<b>Grundlagen zu Starling CertAccess</b> .....	<b>6</b>
Unterstützte Browser .....	7
Zusätzliche Hardware- und Software-Voraussetzungen .....	7
Starling CertAccess als Starling Service nutzen .....	7
Test-Abonnements .....	8
Test-Abonnement starten .....	9
Test-Abonnement beenden .....	10
Kostspflichtige Abonnements .....	10
Kostpflichtiges Abonnement starten .....	10
Aktualisieren der Starling CertAccess Instanz .....	11
Prozessverarbeitung in Starling CertAccess .....	12
<b>Architektur des Starling CertAccess Agent</b> .....	<b>13</b>
<b>Einrichten der Initialsynchronisation mit Active Roles</b> .....	<b>16</b>
<b>Systemanforderungen des Starling CertAccess Agent</b> .....	<b>21</b>
Minimale Systemanforderungen für die administrative Arbeitsstation .....	21
Minimale Systemanforderungen für den Jobserver .....	22
Einrichten der Berechtigung zum Erstellen eines HTTP Server .....	24
Kommunikationsports und Firewall Konfiguration .....	24
Benutzer für den Starling CertAccess Agent .....	25
Benötigte Berechtigungen für die Synchronisation mit One Identity Active Roles .....	26
<b>Installieren, Aktualisieren und Deinstallieren der Starling CertAccess Agent Komponenten</b> .....	<b>27</b>
Starling CertAccess Agent auf einer Arbeitsstation installieren .....	27
Starling CertAccess Agent aktualisieren .....	29
Starling CertAccess Agent deinstallieren .....	29
<b>Arbeiten mit dem Starling CertAccess Agent</b> .....	<b>31</b>
Starling CertAccess Launchpad starten .....	32
Konfigurationsdaten der Starling CertAccess Instanz laden .....	32

Allgemeine Einstellungen bearbeiten .....	33
Starling CertAccess Administratoren verwalten .....	34
Starling CertAccess Service installieren .....	35
E-Mail-Versand konfigurieren .....	36
Automatische Zuordnung zu Identitäten konfigurieren .....	41
Automatische Zuordnung zum IT Shop konfigurieren .....	42
Active Roles ADSI Provider installieren .....	43
Synchronisation mit einer Active Directory Domäne einrichten .....	43
Synchronisationen verwalten .....	45
Synchronisation manuell starten .....	45
Systemverbindung bearbeiten .....	46
Irregulären Abbruch einer Synchronisation behandeln .....	46
Systemverbindung löschen .....	47
Protokolldatei des Starling CertAccess Service anzeigen .....	48
Anzeige der Starling CertAccess Service Protokolldatei über HTTPS konfigurieren ....	48
Starling CertAccess Service als Docker-Container starten .....	49
<b>Anhang: Abbildung der Active Roles Schematypen in Starling CertAccess</b> ....	<b>52</b>
<b>Über uns</b> .....	<b>53</b>
Kontaktieren Sie uns .....	53
Technische Supportressourcen .....	53
<b>Index</b> .....	<b>54</b>

# Über dieses Handbuch

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

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

Das *One Identity Starling CertAccess Administrationshandbuch für die Integration mit One Identity Active Roles* richtet sich an Active Roles Administratoren, die Starling CertAccess 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 CertAccess Web Portal Anwenderhandbuch*.

Das *One Identity Starling CertAccess Web Portal für Betriebsunterstützung Anwenderhandbuch* erläutert, wie Sie die Verarbeitung von Prozessen überwachen, den Synchronisationsstatus der angebotenen Zielsysteme überprüfen und fehlgeschlagene Prozesse identifizieren.

## Verfügbare Dokumentation

Die Online Version der Starling CertAccess Dokumentation finden Sie im Support-Portal unter [Starling CertAccess Online-Dokumentation](#).

## Grundlagen zu Starling CertAccess

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

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

Über das **Starling CertAccess 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 CertAccess 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.

Das **Starling CertAccess Web Portal für Betriebsunterstützung** unterstützt Sie beim Betrieb Ihrer Starling CertAccess Instanz. Hier können Sie unter anderem die Verarbeitung von Prozessen überwachen, fehlgeschlagene Prozesse identifizieren, Maßnahmen ableiten und die Prozesse erneut ausführen, den Synchronisationsstatus und Synchronisationsprotokolle anzeigen.

Starling CertAccess ist als Starling Service in One Identity Starling integriert (<https://cloud.oneidentity.com>). Sie können eine Testversion des Starling 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 CertAccess können alle Browser genutzt werden, die durch One Identity Starling unterstützt werden. Ausführliche Informationen dazu finden Sie im *One Identity Starling User Guide*.

Aktivieren Sie JavaScript in Ihrem Browser, um das Starling CertAccess Web Portal nutzen zu können. Für eine optimale Darstellung der grafischen Benutzeroberfläche empfehlen wir eine minimale Bildschirmauflösung von 1280 x 1024 Bildpunkten mit mindestens 16 Bit Farbtiefe. Für die mobile Ansicht, zum Beispiel bei der Verwendung von einem Tablet, empfehlen wir eine Display-Größe von mindestens 9,7 Zoll.

## Zusätzliche Hardware- und Software-Voraussetzungen

Für Starling CertAccess 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 CertAccess als Starling Service nutzen

Um Starling CertAccess als Starling Service nutzen zu können, benötigen Sie eine Starling Organisation. Sie können den Starling 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 Starling CertAccess als Starling Service zu dieser Organisation hinzufügen. Für Starling CertAccess können folgende Abonnementtypen ausgewählt werden:

- [Kostenpflichtige Abonnements](#) auf Seite 10
- [Test-Abonnements](#) auf Seite 8

# Test-Abonnements

Starling CertAccess 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 CertAccess.

Sie haben zwei Möglichkeiten Starling CertAccess zu testen.

1. Wenn Sie sehen möchten, wie die Hauptfunktionen von Starling CertAccess funktionieren, starten Sie einen Demo-Test. 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 Test-Abonnements einen neuen Demo-Test starten.
2. 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 Portal 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. 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 Test-Abonnements 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 9
- [Test-Abonnement beenden](#) auf Seite 10

## Verwandte Themen

- [Kostenpflichtige Abonnements](#) auf Seite 10
- [Starling CertAccess als Starling Service nutzen](#) auf Seite 7

# Test-Abonnement starten

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

## Um ein Test-Abonnement zu starten

1. Melden Sie sich an Starling an.
2. Auf der Startseite wählen Sie den Starling Service **Starling CertAccess** 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 CertAccess neu zu Ihrer Organisation hinzugefügt haben.
4. Klicken Sie **Confirm**.
5. Erfassen Sie einen Domänennamen für Ihre Starling CertAccess 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 CertAccess Agent und richten Sie die Synchronisation mit Ihrer One Identity Active Roles-Umgebung ein.  
Weitere Informationen finden Sie unter [Einrichten der Initialsynchronisation mit Active Roles](#) auf Seite 16.
9. Wenn Sie einen Demo-Test gestartet haben, klicken Sie auf der Starling CertAccess Webseite **GO**.  
Das Starling CertAccess Web Portal wird geöffnet.

Starling CertAccess 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 Starling CertAccess Kachel, um sich zu informieren, wie Sie das Produkt erwerben können.

## Verwandte Themen

- [Test-Abonnement beenden](#) auf Seite 10
- [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 CertAccess Webseite **End Trial**.
2. Klicken Sie **OK**.

## **Verwandte Themen**

- [Test-Abonnement starten](#) auf Seite 9
- [Kostenpflichtige Abonnements](#) auf Seite 10

# Kostenpflichtige Abonnements

Ein Starling CertAccess Abonnement kann über eine Starling Organisation erworben werden. Ein kostenpflichtiges Abonnement bietet Ihnen vollen Zugriff auf das Produkt (einschließlich des Starling CertAccess Agent) für die Dauer Ihres Vertrags und eine bestimmte Anzahl von Benutzerlizenzen. Informationen zum Erwerb eines Abonnements für Starling CertAccess als Starling 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 8
- [Starling CertAccess als Starling 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 Service **Starling CertAccess** und kontaktieren den Vertrieb.  
Sie erhalten eine E-Mail, sobald Ihre Starling CertAccess 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 10.
4. Erfassen Sie einen Domännennamen für Ihre produktive Starling CertAccess Instanz.  
Der Domänenname darf nicht länger als 40 Zeichen sein und muss innerhalb von Starling eindeutig sein.
5. Klicken Sie **Production**.
6. Die Starling CertAccess Instanz wird bereitgestellt.  
Das nimmt einige Zeit in Anspruch. Sie erhalten eine E-Mail mit einem Link zu Ihrer Instanz, sobald diese genutzt 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 CertAccess Agent und richten Sie die Synchronisation mit Ihrer One Identity Active Roles-Umgebung ein.  
Weitere Informationen finden Sie unter [Einrichten der Initialsynchronisation mit Active Roles](#) auf Seite 16.

### Verwandte Themen

- [Kostenpflichtige Abonnements](#) auf Seite 10

# Aktualisieren der Starling CertAccess Instanz

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

### Verwandte Themen

- [Starling CertAccess Agent aktualisieren](#) auf Seite 29

# Prozessverarbeitung in Starling CertAccess

Der Starling CertAccess Agent verwendet zur Abbildung von Geschäftsprozessen sogenannte Prozesse. Ein Prozess besteht aus Prozessschritten, die Verarbeitungsaufgaben darstellen und über Vorgänger-Nachfolger-Beziehungen miteinander verbunden sind. Beispielsweise steuert ein Prozess das Anlegen von Benutzerkonten, welche durch die Synchronisation in Ihre Starling CertAccess Instanz übertragen werden. Durch die einzelnen Prozessschritte werden die Benutzerkonten angelegt und Identitäten zugeordnet.

## Prozesse im Status Frozen

Im Starling CertAccess Web Portal für Betriebsunterstützung können Sie den Status der Prozessverarbeitung überwachen. An Prozessen, die gerade ausgeführt werden, wird für jeden Prozessschritt der Ausführungsstatus angezeigt. Besondere Aufmerksamkeit verdienen Prozessschritte mit dem Ausführungsstatus **Frozen**. Hier sind bei der Verarbeitung Fehler aufgetreten, die Sie im Einzelfall prüfen und beheben müssen. Anschließend können diese Prozessschritte reaktiviert und somit erneut verarbeitet werden.

## Nicht aufgelöste Referenzen

Bei der Synchronisation einer Zielsystemumgebung kann es vorkommen, dass Objektreferenzen nicht aufgelöst werden können. Das tritt dann auf, wenn referenzierte Objekte in Ihrer Starling CertAccess Instanz nicht existieren. Diese nicht-auflösbaren Referenzen werden in einen Synchronisationspuffer geschrieben. Damit ist sicher gestellt, dass diese Referenzen erhalten bleiben und bei der Provisionierung im Zielsystem nicht gelöscht werden. Im Web Portal für Betriebsunterstützung erhalten Sie eine Übersicht der nicht aufgelösten Referenzen. Sie können diese einzeln prüfen und dadurch im angebundenen Zielsystem korrigieren.

## Web Portal für Betriebsunterstützung für regelmäßige Prüfungen nutzen

Sowohl bei der Synchronisation als auch bei der Prozessverarbeitung können Fehler auftreten, die gegebenenfalls zu inkonsistenten oder fehlerhaften Daten in Ihrer Starling CertAccess Instanz oder im angebundenen Zielsystem führen können. Nutzen Sie daher das Web Portal für Betriebsunterstützung regelmäßig, um

- die Übersicht über Prozesse im Status **Frozen** zu überwachen,
- die Synchronisationsprotokolle einzusehen,
- die nicht aufgelösten Referenzen zu prüfen

und nehmen Sie die erforderlichen Korrekturen vor.

Ausführliche Informationen dazu finden Sie im *One Identity Starling CertAccess Web Portal für Betriebsunterstützung Anwenderhandbuch*.

# Architektur des Starling CertAccess Agent

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

Der Starling CertAccess Agent enthält die On-Premises Komponenten, die für die Starling CertAccess Konfiguration und für die Synchronisation mit One Identity Active Roles benötigt werden.

Der Starling CertAccess Agent enthält folgende Komponenten:

- **Starling CertAccess Launchpad**

Mit dem Starling CertAccess Launchpad führen Sie die verschiedenen administrativen Aufgaben aus:

- Starling CertAccess Administratoren verwalten
- Starling CertAccess 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 CertAccess Service anzeigen
- Automatische Identitätenzuordnung konfigurieren
- Automatische Zuordnung von Systemberechtigungen zum IT Shop konfigurieren

Das Starling CertAccess Launchpad wird auf einer administrativen Arbeitsstation installiert.

- **Starling CertAccess Service**

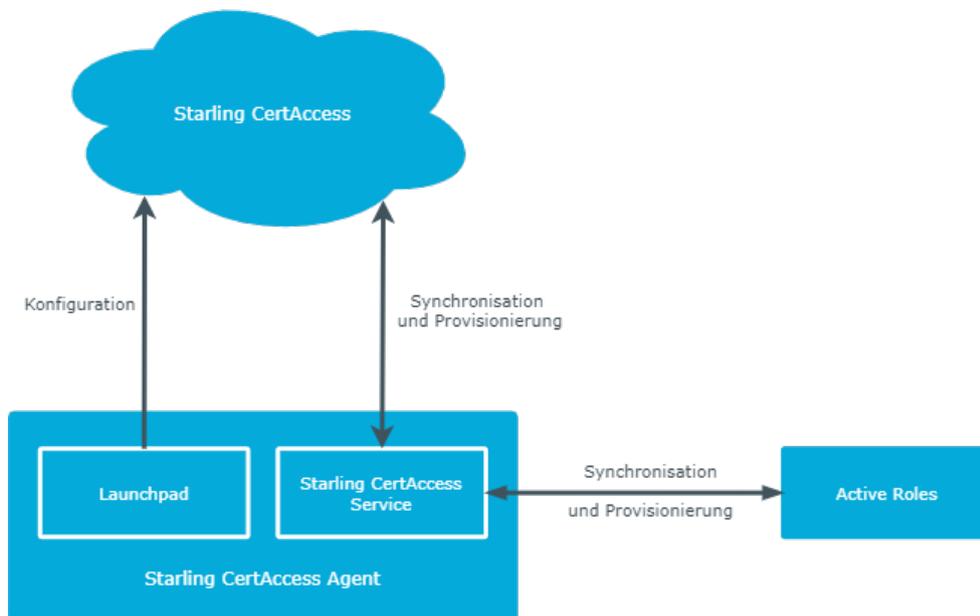
Der Starling CertAccess Service übernimmt folgende Aufgaben:

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

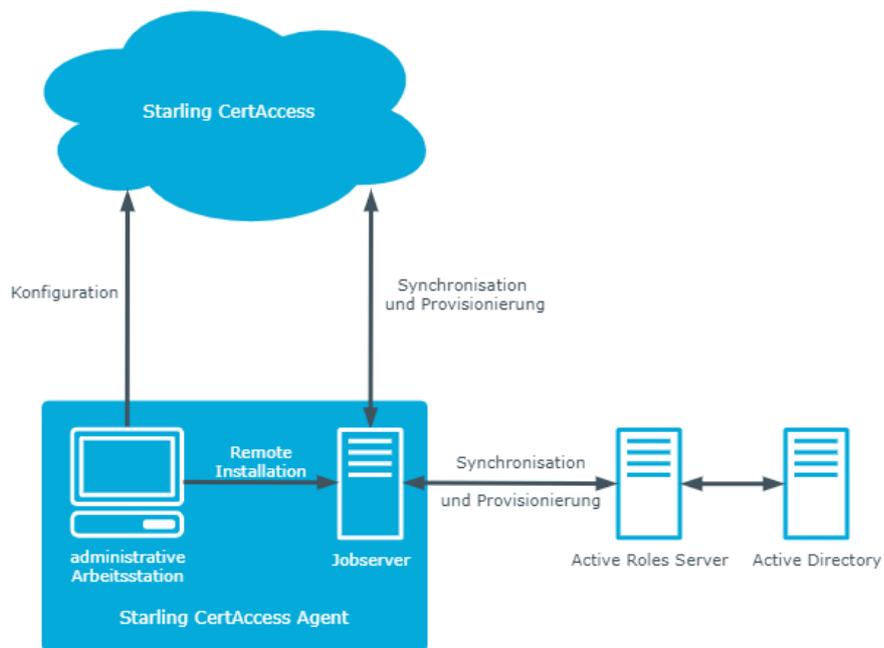
Der Starling CertAccess Service wird auf einem Server installiert. Auf dem Server muss für die Kommunikation mit Active Roles der Active Roles ADSI Client passend zur Version von Active Roles installiert sein. Ein Server, auf dem der Starling CertAccess Service installiert ist, wird nachfolgend als Jobserver bezeichnet.

Der Starling CertAccess Agent unterstützt die Synchronisation mit Active Roles in den Versionen 7.4.1, 7.4.3 und 7.4.4.

**Abbildung 1: Architektur des Starling CertAccess Agent**



**Abbildung 2: Topologie des Starling CertAccess Agent**



## Verwandte Themen

- [Prozessverarbeitung in Starling CertAccess](#) auf Seite 12

## Einrichten der Initialsynchronisation mit Active Roles

Wenn Sie Starling CertAccess für Ihre Organisation vorbereitet haben, richten Sie die initiale Synchronisation mit Ihrer One Identity Active Roles-Umgebung ein. Dafür installieren Sie den Starling CertAccess Agent auf einer administrativen Arbeitsstation. Mit dem Starling CertAccess Launchpad installieren Sie den Starling CertAccess Service auf einem Jobserver.

Stellen Sie sicher, dass alle Systemanforderungen an die Arbeitsstation und den Jobserver erfüllt sind. Weitere Informationen finden Sie unter [Systemanforderungen des Starling CertAccess Agent](#) auf Seite 21.

### Um die Synchronisation mit Active Roles einzurichten

1. Klicken Sie in der **Subscription is ready** E-Mail auf die Schaltfläche **Get Started**. Die Starling CertAccess Webseite wird geöffnet.
2. Laden Sie das Starling CertAccess Agent-Installationspaket auf eine Arbeitsstation herunter.
  - a. Unter **Step 1** klicken Sie **Download Agent**.
  - b. Kopieren Sie den Starling CertAccess Agent Schlüssel in die Zwischenablage. Unter **Step 2** klicken Sie **Copy**.  
**WICHTIG:** Speichern Sie Ihren Starling CertAccess Agent Schlüssel an einem sicheren Ort, da Sie ihn später erneut benötigen.
3. Installieren Sie den Starling CertAccess Agent auf der Arbeitsstation.
  - a. Entpacken Sie das Starling CertAccess 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 CertAccess 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 Seite **WebView2 installieren** werden Sie aufgefordert, Microsoft Edge WebView2 zu installieren. Die Benutzeroberfläche einiger Starling CertAccess Agent-Komponenten benötigt Microsoft Edge WebView2, um bestimmte Inhalte darstellen zu können.
 

**HINWEIS:** Diese Seite wird nur angezeigt, wenn Sie Starling CertAccess Agent-Komponenten installieren möchten, die WebView2 erwarten und WebView2 noch nicht installiert ist.
  - g. Auf der letzten Seite des Installationsassistenten klicken Sie **Starten**, um das Starling CertAccess Launchpad auszuführen.
 

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

    - i. Im Dialog **Starling CertAccess Konfigurationsdaten**, kopieren Sie Ihren Starling CertAccess Agent Schlüssel in das Textfeld.
    - ii. Klicken Sie **OK**.
  - h. Um den Installationsassistenten zu beenden, klicken Sie **Ende**.
4. Beim ersten Start des Launchpad wird der Starling CertAccess Agent automatisch aktualisiert. Dabei wird die aktuellste Version des Starling CertAccess 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 CertAccess Service.
 

Der Starling CertAccess Service wird remote auf einem Jobserver installiert.

Voraussetzungen:

    - Der Server erfüllt die minimalen Systemanforderungen. Weitere Informationen finden Sie unter [Minimale Systemanforderungen für den Jobserver](#) auf Seite 22.

- 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:** Erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
  - **Dienstkonto:** Erfassen Sie die Angaben zum Benutzerkonto unter dem der Starling CertAccess Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen. Angaben zum Starling CertAccess Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den Starling CertAccess Service.

- 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 CertAccess 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 über Active Roles**

### **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 das Kennwort für den Zugriff auf Active Roles an.
- 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**.

Im Dialog **Synchronisationen verwalten** wird der aktuelle Status der Synchronisation angezeigt.

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

Weitere Informationen finden Sie unter [Protokolldatei des Starling CertAccess Service anzeigen](#) auf Seite 48.

Wenn die Synchronisation beendet ist, sehen Sie die synchronisierten Daten im Starling CertAccess Web Portal.

### 10. Prüfen Sie, ob die Daten korrekt synchronisiert wurden.

- a. Wechseln Sie zur Starling CertAccess Webseite und klicken Sie **GO**.  
Das Starling CertAccess Web 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 CertAccess Web Portal finden Sie im *One Identity Starling CertAccess Web Portal Anwenderhandbuch*.

## Detaillierte Informationen zum Thema

- [Architektur des Starling CertAccess Agent](#) auf Seite 13
- [Starling CertAccess Agent auf einer Arbeitsstation installieren](#) auf Seite 27
- [Starling CertAccess Service installieren](#) auf Seite 35
- [Minimale Systemanforderungen für den Jobserver](#) auf Seite 22
- [Benötigte Berechtigungen für die Synchronisation mit One Identity Active Roles](#) auf Seite 26
- [Active Roles ADSI Provider installieren](#) auf Seite 43
- [Synchronisation mit einer Active Directory Domäne einrichten](#) auf Seite 43
- [Abbildung der Active Roles Schematypen in Starling CertAccess](#) auf Seite 52

# Systemanforderungen des Starling CertAccess Agent

Der Starling CertAccess Agent unterstützt die Synchronisation mit Active Roles in den Versionen 7.4.1, 7.4.3 und 7.4.4. Die beschriebenen Systemanforderungen stellen Mindestanforderungen zur Inbetriebnahme und uneingeschränkten Nutzung des Starling CertAccess Agent dar.

Jede Starling CertAccess Agent Installation kann virtualisiert werden. Stellen Sie sicher, dass der jeweiligen Starling CertAccess Agent-Komponente die laut Systemanforderung spezifizierte Leistung und Ressourcen zur Verfügung stehen. Die Virtualisierung einer Starling CertAccess 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](#) auf Seite 21
- [Minimale Systemanforderungen für den Jobserver](#) auf Seite 22
- [Einrichten der Berechtigung zum Erstellen eines HTTP Server](#) auf Seite 24
- [Kommunikationsports und Firewall Konfiguration](#) auf Seite 24
- [Benutzer für den Starling CertAccess Agent](#) auf Seite 25
- [Benötigte Berechtigungen für die Synchronisation mit One Identity Active Roles](#) auf Seite 26

## Minimale Systemanforderungen für die administrative Arbeitsstation

Zur Darstellung und Bearbeitung von Daten wird der Starling CertAccess 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: <ul style="list-style-type: none"><li>• Windows 10 (32-Bit oder 64-Bit) mindestens Version 1511</li><li>• Windows 8.1 (32-Bit oder 64-Bit) mit dem aktuellen Service Pack</li></ul>
Zusätzliche Software	<ul style="list-style-type: none"><li>• Microsoft .NET Framework Version 4.7.2 oder höher</li><li>• Microsoft Edge WebView2</li><li>• Active Roles ADSI Provider der anzubindenden Active Roles Version</li></ul> <p>Für die Einrichtung der Synchronisation mit einer Active Directory Domäne muss die Verbindung über Port <b>15172</b> (TCP) zum Active Roles Server möglich sein. Gegebenenfalls muss eine entsprechende Firewall-Regel auf dem Active Roles Server eingerichtet werden.</p>
Unterstützte Browserversionen	<ul style="list-style-type: none"><li>• Firefox (Release Channel)</li><li>• Chrome (Release Channel)</li><li>• Microsoft Edge (Release Channel)</li></ul>

## Minimale Systemanforderungen für den Jobserver

Zur Installation des Starling CertAccess 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 CertAccess Service benötigen Sie eine administrative Arbeitsstation, auf der die Starling CertAccess Agent-Komponenten installiert sind.

## Verwandte Themen

- [Starling CertAccess Service installieren](#) auf Seite 35
- [Minimale Systemanforderungen für die administrative Arbeitsstation](#) auf Seite 21

# Einrichten der Berechtigung zum Erstellen eines HTTP Server

Die Anzeige der Protokolldateien des Starling CertAccess 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 CertAccess 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 CertAccess Agent besteht aus verschiedenen Komponenten, die in verschiedenen Netzwerksegmenten laufen können. Zusätzlich benötigt der Starling CertAccess 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 CertAccess.
1880	Port für das HTTP-basierte Protokoll des Starling CertAccess Service.
88	Kerberos-Authentifizierungssystem (wenn Kerberos Authentifizierung eingesetzt wird).
135	Microsoft End Point Mapper (EPMAP) (auch DCE/RPC Locator Service).

Standardport	Beschreibung
137	NetBIOS Name Service.
139	NetBIOS Session Service.

## Benutzer für den Starling CertAccess Agent

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

**Tabelle 4: Benutzer für den Starling CertAccess Agent**

Benutzer	Berechtigungen
Benutzer zur Anmeldung am Starling CertAccess Agent	<p>Der Benutzer, mit dem Sie sich initial für One Identity Starling registriert haben, hat standardmäßig administrative Berechtigungen für Starling CertAccess und den Starling CertAccess Agent. Dieser Benutzer kann weitere administrative Benutzer für den Zugriff auf Starling CertAccess berechtigen.</p> <p>Benutzer, die sich am Starling CertAccess Launchpad anmelden, werden über OAuth 2.0 authentifiziert.</p>
Benutzerkonto für den Starling CertAccess Service	<p>Das Benutzerkonto für den Starling CertAccess Service benötigt die Benutzerrechte, um die Operationen auf Dateiebene durchzuführen, beispielsweise Verzeichnisse und Dateien anlegen und bearbeiten.</p> <p>Das Benutzerkonto muss der Gruppe <b>Domänen-Benutzer</b> angehören.</p> <p>Das Benutzerkonto benötigt das erweiterte Benutzerrecht <b>Anmelden als Dienst</b>.</p> <p>Das Benutzerkonto benötigt Berechtigungen für den internen Webservice.</p> <p><b>HINWEIS:</b> Muss der Starling CertAccess Service unter dem Benutzerkonto des Network Service (<b>NT Authority\NetworkService</b>) laufen, so können Sie die Berechtigungen für den internen Webservice über folgenden Kommandozeilenaufruf vergeben:</p> <pre>netsh http add urlacl url=http://&lt;IP-Adresse&gt;:&lt;Portnummer&gt;/ user="NT AUTHORITY\NETWORKSERVICE"</pre> <p>Für die automatische Aktualisierung des Starling CertAccess Services benötigt das Benutzerkonto Vollzugriff auf das Starling CertAccess Agent-Installationsverzeichnis.</p> <p>In der Standardinstallation wird der Starling CertAccess Agent</p>

Benutzer	Berechtigungen
----------	----------------

installiert unter:

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

### Verwandte Themen

- [Starling CertAccess Administratoren verwalten](#) auf Seite 34

## Benötigte Berechtigungen 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 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 CertAccess 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.

Bearbeiten Sie die Active Roles Admins im Active Roles Configuration Center. Sollte es der Fall sein, dass im Active Roles Configuration Center ein Benutzerkonto als Active Roles Admin eingetragen ist, muss dieses Benutzerkonto verwendet werden. Ausführliche Informationen zum Bearbeiten der Gruppe oder des Benutzerkontos für den administrativen Zugriff entnehmen Sie Ihrer *One Identity Active Roles Dokumentation*.

# Installieren, Aktualisieren und Deinstallieren der Starling CertAccess Agent Komponenten

Für die Arbeit mit Starling CertAccess installieren Sie die Komponenten des Starling CertAccess Agent auf einer administrativen Arbeitsstation und auf einem Server. Folgende Komponenten werden installiert:

- Arbeitsstation: Starling CertAccess Launchpad
- Server: Starling CertAccess Service

Alle Komponenten werden automatisch aktualisiert, wenn Ihre Starling CertAccess Instanz aktualisiert wurde. Um die Komponenten zu deinstallieren, nutzen Sie die Windows Standardfunktionalität zur Deinstallation von Programmen direkt auf der Arbeitsstation und dem Server.

## Detaillierte Informationen zum Thema

- [Starling CertAccess Agent auf einer Arbeitsstation installieren](#) auf Seite 27
- [Starling CertAccess Service installieren](#) auf Seite 35
- [Starling CertAccess Agent aktualisieren](#) auf Seite 29
- [Starling CertAccess Agent deinstallieren](#) auf Seite 29

## Starling CertAccess Agent auf einer Arbeitsstation installieren

Der Starling CertAccess Agent wird auf einer administrativen Arbeitsstation installiert. Bei der Installation des Starling CertAccess 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 CertAccess Agent](#) auf Seite 21.

### **Um den Starling CertAccess Agent zu installieren**

1. Entpacken Sie das Starling CertAccess 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 CertAccess 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 Seite **WebView2 installieren** werden Sie aufgefordert, Microsoft Edge WebView2 zu installieren. Die Benutzeroberfläche einiger Starling CertAccess Agent-Komponenten benötigt Microsoft Edge WebView2, um bestimmte Inhalte darstellen zu können.

**HINWEIS:** Diese Seite wird nur angezeigt, wenn Sie Starling CertAccess Agent-Komponenten installieren möchten, die WebView2 erwarten und WebView2 noch nicht installiert ist.

7. Auf der letzten Seite des Installationsassistenten klicken Sie **Starten**, um das Starling CertAccess Launchpad auszuführen.
8. Um den Installationsassistenten zu beenden, klicken Sie **Ende**.

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

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

### **Verwandte Themen**

- [Arbeiten mit dem Starling CertAccess Agent](#) auf Seite 31
- [Starling CertAccess Launchpad starten](#) auf Seite 32
- [Starling CertAccess Agent aktualisieren](#) auf Seite 29

# Starling CertAccess Agent aktualisieren

Wenn Ihre Starling CertAccess Instanz aktualisiert wurde, wird der Starling CertAccess Agent beim nächsten Start des Launchpad automatisch aktualisiert. Dabei wird die aktuellste Version des Starling CertAccess Agent geladen und installiert. Ebenso werden die Komponenten des Starling CertAccess Agent auf dem Jobserver automatisch aktualisiert.

## Verwandte Themen

- [Starling CertAccess Launchpad starten](#) auf Seite 32
- [Aktualisieren der Starling CertAccess Instanz](#) auf Seite 11

# Starling CertAccess Agent deinstallieren

Um den Starling CertAccess Agent zu deinstallieren, entfernen Sie die Komponenten des Starling CertAccess Agent von der administrativen Arbeitsstation und von dem Server, der den Dienst Starling CertAccess Service ausführt (Jobserver). Nutzen Sie dafür die Windows Standardfunktionalität zur Deinstallation von Programmen.

## **Um den Starling CertAccess Agent von der Arbeitsstation zu entfernen**

1. Starten Sie die Deinstallation des Starling CertAccess Agent über die Windows Standardfunktionalität zur Deinstallation von Programmen.  
Der Starling CertAccess Assistent zur Deinstallation wird gestartet.
2. Auf der Startseite wählen Sie die Sprache für den Assistenten und klicken Sie **Weiter**.
3. Auf der Seite **Deinstallation** wird das Verzeichnis angezeigt, aus dem die Starling CertAccess Agent-Komponenten entfernt werden.
  - a. (Optional) Um auch Protokolldateien und Konfigurationsdaten (beispielsweise Registry-Einträge) zu entfernen, aktivieren Sie **Alle Konfigurationsdaten und Protokolldateien entfernen**.  
Solange auf der Arbeitsstation mehrere Starling CertAccess Agent-Installationen vorhanden sind, können die Konfigurationsdaten nicht entfernt werden.
  - b. Klicken Sie **Weiter**.
  - c. Bestätigen Sie die Sicherheitsabfrage mit **OK**.
4. Auf der letzten Seite klicken Sie **Ende**, um das Programm zu beenden.

### **Um den Starling CertAccess Agent vom Jobserver zu entfernen**

1. Öffnen Sie auf dem Jobserver die Dienstverwaltung und beenden Sie den Dienst **Starling CertAccess Service**.
2. Starten Sie die Deinstallation des Starling CertAccess Agent über die Windows Standardfunktionalität zur Deinstallation von Programmen.  
Der Starling CertAccess Assistent zur Deinstallation wird gestartet.
3. Auf der Startseite wählen Sie die Sprache für den Assistenten und klicken Sie **Weiter**.
4. Auf der Seite **Deinstallation** wird das Verzeichnis angezeigt, aus dem die Starling CertAccess Agent-Komponenten entfernt werden.
  - a. Um Protokolldateien und Konfigurationsdaten (beispielsweise Registry-Einträge) zu entfernen, aktivieren Sie **Alle Konfigurationsdaten und Protokolldateien entfernen**.
  - b. Klicken Sie **Weiter**.
  - c. Bestätigen Sie die Sicherheitsabfrage mit **OK**.
5. Auf der letzten Seite klicken Sie **Ende**, um das Programm zu beenden.

### **Verwandte Themen**

- [Starling CertAccess Agent auf einer Arbeitsstation installieren](#) auf Seite 27
- [Starling CertAccess Agent aktualisieren](#) auf Seite 29
- [Starling CertAccess Service installieren](#) auf Seite 35

# Arbeiten mit dem Starling CertAccess Agent

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

Mit dem Starling CertAccess Agent führen Sie folgende Arbeiten aus:

- Starling CertAccess Administratoren verwalten
- Starling CertAccess 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 CertAccess Service anzeigen
- Automatische Identitätenzuordnung konfigurieren
- Automatische Zuordnung von Systemberechtigungen zum IT Shop konfigurieren

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

## Detaillierte Informationen zum Thema

- [Starling CertAccess Launchpad starten](#) auf Seite 32
- [Starling CertAccess Administratoren verwalten](#) auf Seite 34
- [Starling CertAccess Service installieren](#) auf Seite 35
- [Automatische Zuordnung zu Identitäten konfigurieren](#) auf Seite 41
- [Automatische Zuordnung zum IT Shop konfigurieren](#) auf Seite 42
- [Active Roles ADSI Provider installieren](#) auf Seite 43
- [Synchronisation mit einer Active Directory Domäne einrichten](#) auf Seite 43

- [Synchronisationen verwalten](#) auf Seite 45
- [Protokolldatei des Starling CertAccess Service anzeigen](#) auf Seite 48

## Starling CertAccess Launchpad starten

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

### **Um das Launchpad zu starten**

1. Wählen Sie im Windows Startmenü **Starling CertAccess Launchpad**.
2. Wenn angefordert, geben Sie die Konfigurationsdaten zu Ihrer Starling CertAccess Instanz an.
  - a. Im Dialog **Starling CertAccess Konfigurationsdaten**, kopieren Sie Ihren Starling CertAccess Agent Schlüssel in das Textfeld.
  - b. Klicken Sie **OK**.
3. Wenn Ihre Starling CertAccess Instanz aktualisiert wurde, wird der Starling CertAccess Agent automatisch aktualisiert. Dabei wird die aktuellste Version des Starling CertAccess Agent geladen und installiert.
  - Im Meldungsfenster **Automatisches Update** klicken Sie **Ja**.
4. Melden Sie sich mit Ihren Starling Anmeldedaten an.
  - 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 CertAccess Agent](#) auf Seite 31
- [Konfigurationsdaten der Starling CertAccess Instanz laden](#) auf Seite 32
- [Aktualisieren der Starling CertAccess Instanz](#) auf Seite 11

## Konfigurationsdaten der Starling CertAccess Instanz laden

Für die Kommunikation mit Starling CertAccess benötigt der Starling CertAccess Agent den Schlüssel Ihrer Starling CertAccess 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 CertAccess Agent Schlüssel zu nutzen**

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

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

### **Um die Konfigurationsdaten zu laden**

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

### **Verwandte Themen**

- [Einrichten der Initialsynchronisation mit Active Roles](#) auf Seite 16
- [Arbeiten mit dem Starling CertAccess Agent](#) auf Seite 31
- [Starling CertAccess Launchpad starten](#) auf Seite 32
- [Starling CertAccess Service installieren](#) auf Seite 35
- [Synchronisation mit einer Active Directory Domäne einrichten](#) auf Seite 43

## **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 CertAccess 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 CertAccess Launchpad starten](#) auf Seite 32

# Starling CertAccess Administratoren verwalten

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

Starling CertAccess Administratoren konfigurieren Starling CertAccess über das Launchpad, sind Zielsystemverantwortliche für Active Directory, 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 CertAccess 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 CertAccess 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 CertAccess Administratoren verwalten** wird geöffnet.
3. Wählen Sie den Benutzer.
4. Klicken Sie  **Löschen**.
5. Klicken Sie **OK**.

### Verwandte Themen

- [Arbeiten mit dem Starling CertAccess Agent](#) auf Seite 31

## Starling CertAccess Service installieren

**WICHTIG:** Stellen Sie vor Beginn der Installation sicher, dass der Server alle Systemanforderungen erfüllt. Weitere Informationen finden Sie unter [Systemanforderungen des Starling CertAccess Agent](#) auf Seite 21.

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

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

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

### Um den Starling CertAccess 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 CertAccess Instanz an.
  - a. Im Dialog **Starling CertAccess Konfigurationsdaten**, kopieren Sie Ihren

Starling CertAccess 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:** Erfassen Sie den Namen oder die IP-Adresse des Servers, auf dem der Dienst installiert und gestartet wird.
  - **Dienstkonto:** Erfassen Sie die Angaben zum Benutzerkonto unter dem der Starling CertAccess Service läuft. Erfassen Sie das Benutzerkonto, das Kennwort zum Benutzerkonto und die Kennwortwiederholung.

Die Installation des Dienstes erfolgt mit dem Benutzerkonto, mit dem Sie an der administrativen Arbeitsstation angemeldet sind. Möchten Sie ein anderes Benutzerkonto für die Installation des Dienstes nutzen, können Sie dieses in den erweiterten Optionen eintragen. Angaben zum Starling CertAccess Service können Sie ebenfalls über die erweiterten Optionen ändern, beispielsweise das Installationsverzeichnis, den Namen, den Anzeigenamen und die Beschreibung für den Starling CertAccess Service.

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 CertAccess Service** in der Dienstverwaltung des Servers eingetragen.

## Verwandte Themen

- [Minimale Systemanforderungen für den Jobserver](#) auf Seite 22
- [Benötigte Berechtigungen für die Synchronisation mit One Identity Active Roles](#) auf Seite 26
- [Arbeiten mit dem Starling CertAccess Agent](#) auf Seite 31
- [Konfigurationsdaten der Starling CertAccess Instanz laden](#) auf Seite 32
- [Starling CertAccess Service als Docker-Container starten](#) auf Seite 49
- [Starling CertAccess Agent deinstallieren](#) auf Seite 29

# E-Mail-Versand konfigurieren

E-Mail-Benachrichtigungen werden beispielsweise bei der Entscheidung von Bestellungen oder bei Rezertifizierungen versendet. Um E-Mail-Benachrichtigungen nutzen zu können, konfigurieren Sie den E-Mail-Versand über das Launchpad. 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

**HINWEIS:** Erfassen Sie mindestens die Pflichtangaben, da sonst keine E-Mail-Benachrichtigungen versendet werden können.

### **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 von 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. Des Weiteren definieren Sie, 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>

- **Tägliche Benachrichtigungen über offene Entscheidungen:** Gibt an, ob Entscheider nur einmal täglich eine E-Mail-Benachrichtigung erhalten sollen, wenn für sie Bestellungen zur Entscheidung vorliegen.

Wenn die Funktion deaktiviert ist, erhalten Entscheider sofort eine E-Mail-Benachrichtigung, sobald eine Bestellung entschieden werden kann. Um die Anzahl der E-Mail-Benachrichtigungen zu verringern, aktivieren Sie die Funktion. Die Funktion **Entscheidung per E-Mail** kann dann nicht genutzt werden.

- **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. Die Funktion **Tägliche Benachrichtigungen über offene Entscheidungen** kann dann nicht genutzt werden.
- **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 **NTLM** verwendet.
8. Auf der Seite **E-Mail-Benachrichtigungen über Attestierungen** nehmen Sie allgemeine Einstellungen für E-Mail-Benachrichtigungen über Attestierungen vor. Attestierer erhalten einmal täglich eine E-Mail-Benachrichtigung, wenn für sie Attestierungsvorgänge zur Entscheidung vorliegen.

- **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>

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 CertAccess Agent](#) auf Seite 31

# 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 CertAccess Agent](#) auf Seite 31

## **Automatische Zuordnung zum IT Shop konfigurieren**

Die Synchronisation sorgt dafür, dass Active Directory Gruppen automatisch als Produkte in den IT Shop aufgenommen werden und so im Starling CertAccess Web Portal bestellt werden können. Bestimmte Gruppen können davon ausgeschlossen werden. Über eine Ausschlussliste legen Sie die Gruppen fest, die nicht automatisch in den IT Shop aufgenommen 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 IT Shop Zuordnung konfigurieren**.
2. Klicken Sie **Starten**.  
Der Dialog **Ausschlussliste für Active Directory Gruppen** 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 der Gruppe, die nicht automatisch in den IT Shop aufgenommen 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 CertAccess Agent](#) auf Seite 31

## Active Roles ADSI Provider installieren

Starling CertAccess Agent verwendet das Active Roles ADSI Interface für die Kommunikation mit einer Active Roles Instanz.

Um die Verbindung herzustellen, muss auf der administrativen Arbeitsstation der zur anzubindenden Active Roles Version passende Active Roles ADSI Provider installiert sein. Der Starling CertAccess Agent unterstützt die Synchronisation mit Active Roles in den Versionen 7.4.1, 7.4.3 und 7.4.4.

### *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 CertAccess Launchpad starten](#) auf Seite 32

## Synchronisation mit einer Active Directory Domäne einrichten

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

**Tabelle 5: Benötigte Informationen für die Einrichtung der Synchronisation**

<b>Angaben</b>	<b>Erläuterungen</b>
Definierter Name der Domäne	Definierter LDAP Name der Active Directory Domäne.
Benutzerkonto und Kennwort zur Anmeldung an Active Roles	Benutzerkonto und Kennwort zur Anmeldung an Active Roles. Stellen Sie ein Benutzerkonto mit ausreichend Berechtigungen bereit. Weitere Informationen finden Sie unter <a href="#">Benötigte Berechtigungen für die Synchronisation mit One Identity Active Roles</a> auf Seite 26.
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 über Active Roles einrichten**.
2. Klicken Sie **Starten**.  
Der Systemverbindungsassistent wird gestartet.
3. Wenn angefordert, geben Sie die Konfigurationsdaten zu Ihrer Starling CertAccess Instanz an.
  - a. Im Dialog **Starling CertAccess Konfigurationsdaten**, kopieren Sie Ihren Starling CertAccess Agent Schlüssel in das Textfeld.
  - b. Klicken Sie **OK**.
4. Auf der Startseite des Systemverbindungsassistenten klicken Sie **Weiter**.
5. Auf der Seite **Zielservers** 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 Zielservers 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 das Kennwort für den Zugriff auf Active Roles an.
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 CertAccess Agent](#) auf Seite 31
- [Synchronisationen verwalten](#) auf Seite 45
- [Konfigurationsdaten der Starling CertAccess Instanz laden](#) auf Seite 32
- [Minimale Systemanforderungen für die administrative Arbeitsstation](#) auf Seite 21

# 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 CertAccess Agent](#) auf Seite 31
- [Synchronisation mit einer Active Directory Domäne einrichten](#) auf Seite 43

# 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**.

Im Dialog **Synchronisationen verwalten** wird der aktuelle Status der Synchronisation angezeigt.

### Verwandte Themen

- [Synchronisationen verwalten](#) auf Seite 45
- [Protokolldatei des Starling CertAccess Service anzeigen](#) auf Seite 48

## 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 45
- [Synchronisation mit einer Active Directory Domäne einrichten](#) auf Seite 43

## Irregulären Abbruch einer Synchronisation behandeln

Solange die Synchronisation ausgeführt wird, werden einige Starling CertAccess-Prozesse angehalten. Ein weiterer Start der Synchronisation ist nicht möglich. Nach erfolgreicher Synchronisation werden die Prozesse automatisch freigegeben.

Wenn eine Synchronisation irregulär abgebrochen wurde, beispielsweise weil ein Server nicht erreichbar war, müssen Sie die Synchronisationsprozesse manuell freigeben. Erst danach können Sie die Synchronisation erneut starten.

**WICHTIG:** Die Synchronisation darf nicht zurückgesetzt werden, solange die Synchronisation regulär läuft!

Bevor Sie die Synchronisation zurücksetzen, stellen Sie sicher, dass die Synchronisation tatsächlich abgebrochen ist.

### **Um eine abgebrochene Synchronisation zurückzusetzen**

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 **Abgebrochene Synchronisation zurücksetzen**.
5. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

### **Verwandte Themen**

- [Synchronisationen verwalten](#) auf Seite 45
- [Protokolldatei des Starling CertAccess Service anzeigen](#) auf Seite 48

## **Systemverbindung löschen**

Wenn zu einem späteren Zeitpunkt keine Daten mehr zwischen einer Active Directory Domäne und Starling CertAccess ausgetauscht werden sollen, kann die entsprechende Systemverbindung entfernt werden. Ab diesem Zeitpunkt werden keine Daten zwischen dieser Domäne und Starling CertAccess synchronisiert. Bestehende Daten, die bis dahin über diese Systemverbindung synchronisiert wurden, bleiben in beiden Systemen erhalten. Ausführliche Informationen zum Löschen von Daten einer Domäne finden Sie im *One Identity Starling CertAccess Web Portal Anwenderhandbuch*.

### **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 45

# Protokolldatei des Starling CertAccess Service anzeigen

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

## Um die Protokolldatei des Starling CertAccess Service anzuzeigen

1. Wählen Sie im Launchpad **Administrative Aufgaben > Datensynchronisation > Protokolldatei des Dienstes anzeigen**.
2. Klicken Sie **Anzeigen**.  
Die verschiedenen Dienste des Starling CertAccess 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 farblich 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 CertAccess Agent](#) auf Seite 31
- [Einrichten der Berechtigung zum Erstellen eines HTTP Server](#) auf Seite 24
- [Anzeige der Starling CertAccess Service Protokolldatei über HTTPS konfigurieren](#) auf Seite 48

# Anzeige der Starling CertAccess Service Protokolldatei über HTTPS konfigurieren

Damit die Protokolldatei des Starling CertAccess Service mittels HTTPS erreichbar ist, sind zusätzliche Konfigurationseinstellungen erforderlich.

1. Konfigurieren Sie im Betriebssystem das Zertifikat.

Der Starling CertAccess Service nutzt System.Net.HttpListener für die Webschnittstelle. System.Net.HttpListener kann mittels HttpCfg.exe so konfiguriert werden, dass für bestimmte Ports ein Zertifikat verwendet wird. Ausführliche Informationen wie Sie Zertifikate konfigurieren finden Sie unter [How to: Configure a Port with an SSL Certificate](#).

2. Passen Sie die Konfiguration des Starling CertAccess Service an. Aktivieren Sie in der Konfigurationsdatei des Starling CertAccess Service den Parameter **SSL verwenden** (UseSSL). Verwenden Sie das Programm Job Service Configuration.

### **Um die Anzeige der Starling CertAccess Service Protokolldatei über HTTPS zu konfigurieren**

- a. Starten Sie Datei JobServiceConfigurator.exe aus dem Installationsverzeichnis des Starling CertAccess Service.

Die Konfigurationsdatei des Starling CertAccess Service (Jobservice.cfg) wird aus dem Installationsverzeichnis geladen. Der Pfad der geladenen Datei wird in der Titelzeile des Programms Job Service Configuration angezeigt.

- b. Wählen Sie im Job Service Configuration den Eintrag **Konfiguration** und aktivieren Sie die Option **SSL verwenden**.
- c. Um die Änderung zu speichern, wählen Sie **Datei > Speichern**.

Die Änderung wird im laufenden Betrieb des Starling CertAccess Service übernommen. Ein Neustart des Starling CertAccess Service ist nicht erforderlich.

## Starling CertAccess Service als Docker-Container starten

Der Starling CertAccess Service übernimmt die Synchronisation zwischen Starling CertAccess und der angebundenen Active Roles-Umgebung. Zusätzlich zur Installation des Starling CertAccess Service aus dem Launchpad stellt One Identity ein Docker-Image für eine einfache und standardisierte Installation und Ausführung des Starling CertAccess Service in Docker-Containern zur Verfügung. Da für die Verbindung des Starling CertAccess 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 CertAccess 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 CertAccess Instanz, welche auf der Starling CertAccess 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 "StarlingCertAccessService" `
--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 CertAccess Service installieren](#) auf Seite 35

## Abbildung der Active Roles Schematypen in Starling CertAccess

Um Active Directory Benutzerkonten und Gruppen mit Starling CertAccess zu verwalten, richten Sie die Synchronisation zwischen Active Roles und Starling CertAccess ein. Die Schematypen werden folgendermaßen aufeinander abgebildet.

**Tabelle 7: Abbildung der Schematypen**

<b>Schematyp im Active Roles</b>	<b>Schematyp im Starling CertAccess</b>
builtInDomain	ADSContainer
computer	ADSMachine
contact	ADSContact
container	ADSContainer
domainDNS	ADSDomain
group	ADSGroup
inetOrgPerson	ADSAccount
msDS-PasswordSettings	ADSPolicy
msExchSystemObjectsContainer	ADSContainer
organization	ADSContainer
organizationalUnit	ADSContainer
printQueue	ADSPrinter
rpcContainer	ADSContainer
user	ADSAccount

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](http://www.YouTube.com/OneIdentity)
- Engagement in der One Identity Community
- Chat mit Support-Ingenieuren
- Anzeigen von Diensten, die Sie bei Ihrem Produkt unterstützen

## A

- Abonnement 7
  - beenden 10
  - kostenpflichtig 7, 10
  - Produktion 10
  - Proof-of-Concept 7
  - starten 9-10
  - Test 7-8
- Active Directory Gruppe
  - automatisch an IT Shop zuordnen 42
- Active Roles ADSI Provider 43
- Administrator 25
  - bearbeiten 34
  - einfügen 34
  - löschen 34
  - verwalten 34
- ADSI Provider installieren 16, 43
- Arbeitsstation
  - installieren 27
  - Systemanforderungen 21

## B

- Benutzerkonto
  - Identität zuweisen 41
- Berechtigungen 24-25
- Betriebsunterstützung 12

## D

- Docker-Container 35, 49

## F

- Firewall Konfiguration 24

## I

- Identität
  - automatisch zuordnen 41
  - Zuordnung konfigurieren 41
- Installationsvoraussetzungen 21, 24
  - Arbeitsstation 21
  - Berechtigungen 25
  - Firewall 24
  - Jobserver 22
  - Ports 24
- IT Shop
  - automatische Zuordnung konfigurieren 42

## J

- Jobserver 13
  - Starling CertAccess Agent deinstallieren 29
  - Starling CertAccess Service deinstallieren 29
  - Starling CertAccess Service installieren 35
  - Systemanforderungen 22

## K

- Konfigurationsdaten laden 32

Kultur einstellen 33

## L

Launchpad 13, 32

## P

Ports 24

Proof-of-Concept 8

Protokolldatei 48

Prozess 12

    Ausführungsstatus 12

    Status Frozen 12

## R

Referenz

    nicht aufgelöst 12

## S

Sprache einstellen 33

Starling CertAccess

    Administrator 34

    aktualisieren 11

Starling CertAccess Agent

    aktualisieren 29, 32

    Architektur 13

    ausführen 31-32

    deinstallieren 29

    installieren 16, 27

Starling CertAccess Agent Schlüssel 16,  
32

Starling CertAccess Service 13

    Berechtigungen 25

    in Docker-Containern ausführen 35,  
49

Installationsvoraussetzungen 22, 24

installieren 16, 35, 49

Protokolldatei anzeigen 48

Synchronisation

    Abbruch behandeln 46

    Active Directory 43

    Benutzerkonto 26

    Berechtigungen 26

    einrichten 43

        initial 16

    starten 16, 45

    Systemverbindung bearbeiten 46

    Systemverbindung löschen 47

    weitere Domänen hinzufügen 43

    zurücksetzen 46

Systemanforderungen

    Arbeitsstation 21

    Benutzer 25

    Berechtigungen 25

    Browser 7

    Jobserver 22

    Starling CertAccess 7

    Starling CertAccess Service 22

Systemberechtigung

    automatisch an IT Shop zuordnen 42

## T

Test 8

## W

Web Portal 16