One Identity Manager 8.1.3

Konfigurationshandbuch für Webanwendungen

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.

One Identity Manager Konfigurationshandbuch für Webanwendungen
Aktualisiert - Juni 2020
Version - 8.1.3

Inhalt

1

Über dieses Handbuch

Dieses Handbuch liefert Administratoren und Webentwicklern Informationen zur Konfiguration und den Betrieb von Webanwendungen des One Identity Manager.

Verfügbare Dokumentation

Die Online Version der One Identity Manager Dokumentation finden Sie im Support-Portal unter Online-Dokumentation. Videos mit zusätzlichen Informationen finden Sie unter www.YouTube.com/OneIdentity.

Konfiguration des Web Portals

Dieses Kapitel beschreibt die nötigen Konfigurationsschritte und -parameter, die Sie für die Konfiguration einiger Features des Web Portals vornehmen müssen.

Ausführliche Informationen zum Web Designer finden Sie im *One Identity Manager Referenzhandbuch für den Web Designer*.

Detaillierte Informationen zum Thema

IT Shop Konfiguration

Sie können den IT Shop des Web Portal im Web Designer konfigurieren.

Bestellung nach Referenzbenutzer

Tabelle 1: Konfigurationsparameter für die Bestellung nach Referenzbenutzer

Konfigurationsparameter	Beschreibung
VI_ITShop_ProductSelectionByReferenceUser	Stellt für Bestellungen die Funktion "nach Referenzbenutzer" im Web Portal zur Verfügung.
VI_ITShop_Filter_PersonReference	Stellt Anzahl der angezeigten Referenzbenutzer ein. Dieser Konfigurationsparameter ist eine SQL_ Filterbediung auf der Tabelle "Person".

Um das Bestellen nach Referenzbenutzern im Web Portal nutzen zu können oder nicht, oder die Menge der angezeigten Referenzbenutzer zu bestimmen, sind Einstellungen an diesen Konfigurationsparametern erforderlich.

Detaillierte Informationen zum Thema

- Nach Referenzbenutzern aktivieren oder deaktivieren auf Seite 7
- Anzeige der Referenzbenutzer einstellen auf Seite 7

Nach Referenzbenutzern aktivieren oder deaktivieren

Sie können im Web Designer einstellen, ob das Bestellen von Bestellungen anderer Benutzer möglich sein soll oder nicht. Diese Funktion heißt Bestellungen nach Referenzbenutzer. Hierzu muss der Konfigurationsparameter "VI_ITShop_ ProductSelectionByReferenceUser" im Web Designer bearbeitet werden.

Um das Bestellen nach Referenzbenutzern zu aktivieren- oder deaktivieren

1. Öffnen Sie den Web Designer.
2. Öffnen Sie das Modul "VI_ITShop_ProduCtSelection" und suchen Sie über das Definitionsbaumfenster nach "VI_ITShop_ProductSelectionByReferenceUser".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_ITShop_ ProductSelectionByReferenceUser".
4. Wechseln Sie im Definitionsbaumfenster über in die Ansicht **Konfiguration (kundenspezifisch)**. Hier können Sie den Wert des Konfigurationsparameter bearbeiten.
5. Nehmen Sie eine der folgenden Aktionen vor.
    a. Sie möchten das Bestellen nach Referenzbenutzern abstellen: Setzen Sie im Fenster **Knotenbearbeitung** den Wert `True`.
    b. Sie möchten das Bestellen nach Referenzbenutzern einstellen: Setzen Sie im Fenster **Knotenbearbeitung** den Wert `false`.

Anzeige der Referenzbenutzer einstellen

Um bei der Auswahl eines Referenzbenutzers die Menge der angezeigten Referenzbenutzer im Web Portal einzustellen, muss dieser Konfigurationsparameter im Web Designer bearbeitet werden.

HINWEIS: Möchten Sie auf den angemeldeten Benutzer verweisen, können Sie eine Variable `%useruid%` einbauen.

Um die Menge der angezeigten Referenzbenutzer einzustellen

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_VI_ITShop_Filter_PersonReference".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_VI_ITShop_Filter_PersonReference".
4. Erfassen Sie im Fenster **Knotenbearbeitung** im Eingabefeld **Wert** den gewünschten Wert.

Bestellungen über Peer-Gruppen aktivieren

Benutzer des Web Portals können Produkte anzeigen und bestellen, die andere Mitarbeiter aus ihrem Umfeld bereits bestellt haben. Zusätzlich können Manager diese Informationen auch für einzelne Mitarbeiter anzeigen, für die sie verantwortlich sind. So erhalten Benutzer eine schnelle Möglichkeit, Produkte zu bestellen, die für sie oder Ihre Mitarbeiter ebenfalls wichtig sein könnten.

TIPP: Als Peer-Gruppe werden alle Personen zusammengefasst, die denselben Manager haben oder der derselben primären oder sekundären Abteilung angehören, wie der Bestellempfänger.

HINWEIS: Bevor Sie Bestellungen über Peer-Gruppen aktivieren können, müssen Sie die Peer-Gruppen-Analyse konfigurieren und aktivieren. Weitere Informationen zur Peer-Gruppen-Analyse und deren Konfiguration finden Sie im *One Identity Manager Administrationshandbuch für IT Shop*.

Um Bestellungen über Peer-Gruppen zu aktivieren

1. Starten Sie den Web Designer.
2. Konfigurieren Sie die folgenden Konfigurationsschlüssel:
   - **VI_ITShop_Find_Products_By_Peer_Group**: Aktivieren Sie diesen Konfigurationsschlüssel, um Bestellungen über Peer-Gruppen zu aktivieren. Wenn Sie diesen Konfigurationsschlüssel aktivieren, können alle Benutzer Produkte ihrer eigenen Peer-Gruppe anzeigen und bestellen.
   - **VI_ITShop_Manager_Find_Products_By_Peer_Group**: Aktivieren Sie diesen Konfigurationsschlüssel, um Bestellungen über Peer-Gruppen zu aktivieren. Wenn Sie diesen Konfigurationsschlüssel aktivieren, können Manager Produkte der Peer-Gruppe eines Mitarbeiters anzeigen und bestellen, für den sie verantwortlich sind.

   TIPP: Wenn Manager Bestellungen über Peer-Gruppen für sich selbst UND Mitarbeiter, für die sie verantwortlich sind, durchführen sollen, aktivieren Sie beide Konfigurationsschlüssel.

Einkaufswagen absenden

Der Einkaufswagen im Web Portal hat verschiedene Konfigurationsmöglichkeiten.

Detaillierte Informationen zum Thema

Priorität einstellen

Tabelle 2: Konfigurationsparameter für Priorität an Bestellungen

Konfigurationsparameter	Beschreibung
VI_ITShop_DisablePWOPriorityChange	Deaktiviert die Einstellung einer Prioriät an einer Bestellung durch den Benutzer am Web Portal.

Standardmäßig kann ein Benutzer eine Priorität an seiner Bestellung einstellen.

Um die Einstellung einer Priorität zu deaktivieren

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_ITShop_DisablePWOPriorityChange".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_ITShop_DisablePWOPriorityChange".
4. Setzen Sie im Fenster **Knotenbearbeitung** den Wert `True`.

Bestellung bestätigen

Tabelle 3: Konfigurationsparameter für Bestätigung von Bestellungen

Konfigurationsparameter	Beschreibung
VI_ITShop_SubmitOrderImmediately	Erzwingt die Bestätigung einer Bestellung im Web Portal.

Der Benutzer kann im Web Portal standardmäßig eine Bestellung ohne zusätzliche Bestätigung absenden. Jedoch wird eine zusätzliche Bestätigung gefordert, wenn die Prüfung der Bestellung mindestens eine Warnung ergibt.

Möchten Sie zusätzliche Bestätigungen an Bestellungen ohne Warnungen einfordern, können Sie den Konfigurationsparameter "VI_ITShop_SubmitOrderImmediately" bearbeiten.

Um die Bestätigung einer Bestellung einzufordern

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_ITShop_SubmitOrderImmediately".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_ITShop_SubmitOrderImmediately".
4. Setzen Sie im Fenster **Knotenbearbeitung** den Wert `False`.

Erneute Authentifizierung erzwingen

Tabelle 4: Konfigurationsparameter für Active Directory Authentifizierung bei Bestellung

Konfigurations-parameter	Beschreibung	Einstellung	
		False	**True**
VI_ITShop_TermsOf UseRequireAD Authentication	Erzwingt eine erneute Active Directory Authentifizierung bei der Durchführung einer Bestellung.	Abgelehnte und abbestellte Bestellungen können nicht direkt als neue Bestellung eingestellt werden.	Abgelehnte und abbestellte Bestellungen können vom Empfänger oder Auftraggeber der Bestellung wiedereingestellt werden.

Um beim Bestellen eine erneute Authentifizierung zu erzwingen

1. Weisen Sie der Nutzungsbedingung die Leistungsposition zu.

   Ausführliche Informationen zu Leistungspositionen zuweisen finden Sie im One Identity Manager Administrationshandbuch für IT Shop.
2. Öffnen Sie den Web Designer.
3. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_ITShop_TermsOfUseRequireADAuthentication".
4. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_ITShop_TermsOfUseRequireADAuthentication".
5. Setzen Sie im Fenster **Knotenbearbeitung** den Wert `True`.

Umgang mit Pflichtprodukten

Im Web Portal ist der unterschiedliche Umgang mit Pflichtprodukten möglich. Die erforderlichen Einstellungen am Konfigurationsparameter unternehmen Sie im Web Designer.

Tabelle 5: Konfigurationsparameter zum Umgang mit Pflichtprodukten

Konfigurationsparameter	Beschreibung
VI_ITShop_AllowRequestWithMissingDependencies	Der aktivierte Konfigurationsparameter erlaubt das Absenden einer Bestellung, trotz nicht bestellbarem Pflichtprodukt wegen bereits vorhandener Zuweisung.

Standardmäßig ist der Konfigurationsparameter "VI_ITShop_ AllowRequestWithMissingDependencies" deaktiviert. Das heißt, eine Bestellung kann nicht abgesendet werden, wenn das Pflichtprodukt nicht bestellt werden kann.

Um den Umgang mit Pflichtprodukten zu konfigurieren

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_ ITShop_AllowRequestWithMissingDependencies".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_ITShop_ AllowRequestWithMissingDependencies".
4. Bearbeiten Sie den Konfigurationsknoten im Tabreiter **Konfiguration**, in dem Sie im Fenster **Knotenbearbeitung** den Wert `true` einstellen, wenn Sie die Standardeinstellung aufheben möchten.

Optionen für den Entscheider

Für den Entscheider von Bestellungen im Web Portal sind verschiedene Konfigurationseinstellungen möglich.

Detaillierte Informationen zum Thema

- Gültigkeit setzen auf Seite 12
- Anfrage senden auf Seite 12
- Begründung einfordern auf Seite 13

Gültigkeit setzen

Tabelle 6: Konfigurationsparameter für Gültigkeit

Konfigurationsparameter	Beschreibung
VI_ITShop_ApproverCanSetValidFrom	Erlaubt dem Entscheider das Setzen eines neuen Gültigkeitsbeginn einer Bestellung.
VI_ITShop_ApproverCanSetValidUntil	Erlaubt dem Entscheider das Setzen eines neuen Gültigkeitsende einer Bestellung.

Mit den Einstellungen an den Konfigurationsparameter `VI_ITShop_ApproverCanSetValidFrom` und `VI_ITShop_ApproverCanSetValidUntil` erlauben Sie dem Entscheider der Bestellung einen neue Gültigkeit zu setzen.

Um die Gültigkeit zu setzen

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_ ITShop_ApproverCanSetValidFrom".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_ITShop_ ApproverCanSetValidFrom".
4. Setzen Sie im Fenster **Knotenbearbeitung** den Wert `True`.
5. Suchen Sie über das Definitionsbaumfenster nach "VI_ITShop_ ApproverCanSetValidUntil".
6. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_ITShop_ ApproverCanSetValidUntil".
7. Setzen Sie im Fenster **Knotenbearbeitung** den Wert `True`.

Anfrage senden

Tabelle 7: Konfigurationsparameter für Anfrage

Konfigurationsparameter	Beschreibung
VI_ITShop_WantSeeQueryToPerson	Erlaubt dem Entscheider eine Anfrage an andere Mitarbeiter im Rahmen des Entscheidungsworkflows zu senden.

Um Anfragen senden zu können

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_ITShop_WantSeeQueryToPerson".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_ITShop_WantSeeQueryToPerson".
4. Setzen Sie im Fenster **Knotenbearbeitung** den Wert `True`.

Begründung einfordern

Tabelle 8: Konfigurationsparameter für Begründung

Konfigurationsparameter	Beschreibung
VI_ITShop_ApproverReasonMandatoryOnDeny	Fordert eine Begründung vom Entscheider ein, wenn er die Bestellung ablehnt.

Um Anfragen stellen zu können

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_ITShop_ApproverReasonMandatoryOnDeny".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_ITShop_ApproverReasonMandatoryOnDeny".
4. Setzen Sie im Fenster **Knotenbearbeitung** den Wert `True`.

Entscheidungen über URL-Links

Tabelle 9: Konfigurationsparameter für Entscheidungen über URL-Link

Konfigurationsparameter	Beschreibung	Bedeutung	
VI_ITShop_Approvals_InteractiveApproval	Fordert Rücksprache mit Benutzer vor Entscheidung. Dieser Schlüssel ist eine SQL-Filterbedingung auf der Tabelle "AccProduct".	Produkt erfüllt Filterbedingung	Entscheidung wird nicht direkt vorgenommen. Formular zur Bestätigung der Entscheidung wird angezeigt.
		Produkt erfüllt Filterbedingung nicht	Entscheidung erfolgt direkt

Konfigurationsparameter	Beschreibung	Bedeutung
		beim Aufruf der Seite. Entscheider erhält Rückmeldung, dass Entscheidung im System eingetragen wurde.

Eine (positive oder negative) Entscheidung zu einer Bestellung kann durch den Aufruf einer URL erfolgen, die beispielsweise in einer E-Mail übermittelt wurde.

Fälle, in denen diese Art der Übermittlung zu Entscheidungen erforderlich ist, sind bestimmte Leistungspositionen, die zur Entscheidung den Austausch mit dem Benutzer fordern. Entscheidungen über diese Leistungspositionen sind ohne Rückfrage nicht zulässig.

Um eine Entscheidung über URL-Link zu verhindern

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_ITShop_Approvals_InteractiveApproval".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_ITShop_Approvals_InteractiveApproval".
4. Setzen Sie im Fenster **Knotenbearbeitung** den Wert.

Anzeigen benutzerbezogener Prozesse im Web Portal

Ein benutzerbezogener Prozess ist ein Prozess, der speziell für die Nachverfolgung durch den Benutzer konfiguriert wird. Er ermöglicht die Statusverfolgung und die Rückmeldung eines Verarbeitungsergebnisses in das Web Portal.

Ein am Web Portal angemeldeter Benutzer sieht alle Prozesse, die von ihm ausgelöst wurden. Der Wert der Spalte `XUserInserted` entspricht dem angemeldeten Benutzer. Ein Prozess kann nur aus einer angemeldeten Sitzung des Benutzers selbst generiert werden, wenn er als benutzerbezogener Prozess erkannt werden soll.

Die benutzerbezogenen Prozesse werden im Web Portal in der Ansicht **Meine Vorgänge** angezeigt. Ausführliche Informationen finden Sie im *One Identity Manager Anwenderhandbuch für das Web Portal*.

An dieser Stelle wird nur auf die Konfiguration für die Anzeige der Prozessinformationen im Web Portal eingegangen. Ausführliche Informationen zur Prozessüberwachung, zum Aufzeichnen von Prozessinformationen und zur Konfiguration der Prozesse und Prozessschritte finden Sie im *One Identity Manager Konfigurationshandbuch*.

Empfehlungen für die Konfiguration zur Aufzeichnung benutzerbezogener Prozesse

- Prüfen Sie im Designer den Konfigurationsparameter **Common | ProcessState**. Der Konfigurationsparameter muss aktiviert sein.
- Prüfen Sie im Designer den Konfigurationsparameter **Common | ProcessState | JobHistory**. Der Konfigurationsparameter muss aktiviert sein. Wählen Sie als Wert des Konfigurationsparameter **ERRORorSELECTED** oder **SELECTED**.

  HINWEIS: Der Wert **ALL** berücksichtigt ebenfalls die Meldungen der Prozesshistorie. Diese Einstellung kann jedoch zu einem sehr großem Datenvolumen führen.
- Prüfen Sie im Designer den Konfigurationsparameter **Common | ProcessState | ProgressView**. Der Konfigurationsparameter muss aktiviert sein und sollte den Wert **2** haben.
- Prüfen Sie im Designer die Konfigurationsparameter **Common | ProcessState | ProgressView | LifeTime** und **Common | ProcessState | JobHistory | LifeTime**. Die Konfigurationsparameter bestimmen die Aufbewahrungszeit der Prozessinformationen und der Meldungen in der Prozesshistorie. Die Konfigurationsparameter müssen aktiviert sein. Passen Sie bei Bedarf die Aufbewahrungszeiten an. Im Standard werden die Informationen 30 Tage aufbewahrt, bevor Sie aus der One Identity Manager Datenbank entfernt werden.
- Konfigurieren Sie im Designer die Prozesse und Prozessschritte zur Aufzeichnung von Prozessinformationen.
  - Für einen Prozess wählen Sie in der Eigenschaft **Prozessinformation** den Wert **Web Portal Verfolgung**.
  - Für die Prozessschritte wählen Sie in der Eigenschaft **Prozessinformation** den Wert **Web Portal Verfolgung**. Aktivieren Sie die Option **Prozesshistorie**.
  - Verwenden Sie für die Prozesse und Prozessschritte benutzerfreundliche Anzeigewerte für die Prozesse und Prozessschritte. Erfassen Sie dazu die Bildungsvorschriften für die Prozessinformationen der Prozesse und Prozessschritte.

Selbstregistrierung neuer Benutzer konfigurieren

Noch nicht registrierte Benutzer haben die Möglichkeit sich für die Verwendung des Web Portals selbst zu registrieren. Nachdem sich ein Benutzer registriert hat erhält er eine Bestätigungs-E-Mail mit einem Link auf eine Bestätigungsseite. Auf dieser Seite kann der Benutzer die Registrierung selbstständig abschließen und anschließend das Kennwort zur Anmeldung initial setzen.

HINWEIS: Um diese Funktion nutzen zu können, muss der neue Benutzer eine E-Mail-

Adresse angeben (können), da ansonsten keine Bestätigungs-E-Mail versendet werden kann.

HINWEIS: Ausführliche Informationen zur Selbstregistrierung neuer Benutzer im Web Portal und des zugehörigen Attestierungsprozesses finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

Um die Selbstregistrierung zu konfigurieren

1. Starten Sie den Designer.
2. Konfigurieren Sie die folgenden Konfigurationsparameter:

   HINWEIS: Wie Sie Konfigurationsparameter im Designer bearbeiten, erfahren Sie im *One Identity Manager Konfigurationshandbuch*.

   - **QER** | **WebPortal** | **PasswordResetURL**: Legen Sie die Web-Adresse des Kennwortrücksetzungsportals fest. Diese URL wird beispielsweise in der E-Mail-Benachrichtigung an den neuen Benutzer verwendet.
   - **QER** | **Attestation** | **MailTemplateIdents** | **NewExternalUserVerification**:

     Standardmäßig wird die Bestätigungsmeldung und der Bestätigungs-Link mit der Mail-Vorlage **Bestätigungslink für neuen externen Benutzer** versendet.

     Um eine andere Vorlage für diese Benachrichtigung zu verwenden, ändern Sie den Wert des Konfigurationsparameters.

     TIPP: Die eigentliche Mail-Vorlage können Sie im Designer in der Kategorie **Mailvorlagen** | **Person** konfigurieren. Ausführliche Informationen zu Mail-Vorlagen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.
   - **QER** | **Attestation** | **ApproveNewExternalUsers**: Legen Sie fest, ob selbstregistrierte Benutzer attestiert werden müssen, bevor sie aktiviert werden. Ein Manager entscheidet dann über die Registrierung des neuen Benutzers.
   - **QER** | **Attestation** | **NewExternalUserTimeoutInHours**: Legen Sie fest, wie viele Stunden der Bestätigungs-Link für neue selbstregistrierte Benutzer gültig ist.
   - **QER** | **Attestation** | **NewExternalUserFinalTimeoutInHours**: Legen Sie fest, nach wie viele Stunden die Selbstregistrierung neuer Benutzer abgebrochen wird, sofern die Registrierung noch nicht erfolgreich abgeschlossen wurde.
3. Weisen Sie der Anwendungsrolle **Identity & Access Governance | Attestierung | Attestierer für externe Benutzer** mindestens eine Person zu.

Vier-Augen-Prinzip für die Vergabe des Zugangscodes konfigurieren

Sie können festlegen, ob ein durch den Helpdesk generierter Zugangscode in zwei Bestandteile aufgeteilt wird. Eine Hälfte des Zugangscode wird dem Helpdesk-Mitarbeiter mitgeteilt und die zweite Hälfte wird dem zuständigen Manager der Person zugeschickt. Die Person muss dann die zweite Hälfte des Zugangscodes bei seinem Manager erfragen. Dieses Verfahren erhöht die Sicherheit bei der Vergabe des Zugangscodes.

Um das Vier-Augen-Prinzip für die Vergabe des Zugangscodes zu konfigurieren

1. Starten Sie den Designer.
2. Aktivieren Sie den Konfigurationsparameter **QER** | **Person** | **PasswordResetAuthenticator** | **PasscodeSplit**.

   HINWEIS: Wie Sie Konfigurationsparameter im Designer bearbeiten, erfahren Sie im *One Identity Manager Konfigurationshandbuch*.
3. Aktivieren Sie den Konfigurationsparameter **QER** | **WebPortal** | **MailTemplateIdents** | **InformManagerAboutSecondHalfOfPasscode**.

   Standardmäßig wird die zweite Hälfte des Sicherheitscodes mit der Mail-Vorlage **Teil des Zugangscodes für Kennwortzurücksetzung** versendet.

   Um eine andere Vorlage für diese Benachrichtigung zu verwenden, ändern Sie den Wert des Konfigurationsparameters.

   TIPP: Die eigentliche Mail-Vorlage können Sie im Designer in der Kategorie **Mailvorlagen** | **Person** konfigurieren. Ausführliche Informationen zu Mail-Vorlagen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

Kennwortfragen konfigurieren

Sollten Benutzer des Web Portals ihr Kennwort vergessen, so können Sie mithilfe selbst festgelegter Kennwortfragen ein neues Kennwort setzen.

Um die Verwendung von Kennwortfragen zu konfigurieren

1. Starten Sie den Designer.
2. Konfigurieren Sie die folgenden Konfigurationsparameter:

   HINWEIS: Wie Sie Konfigurationsparameter im Designer bearbeiten, erfahren Sie im *One Identity Manager Konfigurationshandbuch*.

   - **QER** | **Person** | **PasswordResetAuthenticator** | **QueryAnswerDefinitions**: Legen Sie fest, wie viele Kennwortfragen und zugehörige Antworten Benutzer festlegen müssen. Benutzer die keine oder

nicht genug Kennwortfragen und Antworten festgelegt haben, können ihre Kennwörter nicht neu setzen.

HINWEIS: Der Wert darf nicht niedriger sein, als der Wert des Konfigurationsparameters **QueryAnswerRequests**.

- **QER** | **Person** | **PasswordResetAuthenticator** | **QueryAnswerRequests**: Legen Sie fest, wie viele Kennwortfragen Benutzer beantworten müssen, damit sie ihre Kennwörter neu setzen können.

  HINWEIS: Der Wert darf nicht höher sein, als der Wert des Konfigurationsparameters **QueryAnswerDefinitions**.

- **QER** | **Person** | **PasswordResetAuthenticator** | **InvalidateUsedQuery**: Legen Sie fest, ob Benutzer nach erfolgreicher Kennwortrücksetzung neue Kennwortfragen und Antworten festlegen müssen. Dabei werden die richtig beantworteten Kennwortfragen gelöscht.

Webauthn-Sicherheitsschlüssel

One Identity bietet Benutzern die Möglichkeit, sich mithilfe von (physischen) Sicherheitsschlüsseln bequem und sicher an den Webanwendungen des One Identity Managers anzumelden. Diese Sicherheitsschlüssel unterstützen den W3C-Standard **Webauthn**.

Die Nutzung von Sicherheitsschlüsseln gewährleistet eine höhere Sicherheit beim Anmelden.

Hinweise

- Sie können Starling Two-Factor Authentication und Webauthn parallel für eine Webanwendung laufen lassen. Benutzer, die mindestens einen gültigen Sicherheitsschlüssel besitzen, müssen nicht zusätzlich den Starling 2FA-Prozess durchlaufen. Benutzer, die keinen Sicherheitsschlüssel besitzen, verwenden weiterhin Starling 2FA.
- Personen-Administratoren haben im Manager die Möglichkeit, alle Sicherheitsschlüssel einer Person einzusehen und zu löschen. Weitere Informationen finden Sie im *One Identity Manager Administrationshandbuch für das Identity Management Basismodul*.
- Der Webauthn-Standard wird im Internet Explorer NICHT unterstützt. Benutzer müssen einen anderen Browser verwenden.

Verwandte Themen

- Webauthn-Konfiguration auf Seite 19

Webauthn-Konfiguration

Die Konfiguration von Webauthn für eine Webanwendung führen Sie in vier Schritten durch:

1. Konfigurieren Sie das OAuth-Zertifikat, um die sichere Kommunikation zwischen dem RSTS und One Identity Manager zu ermöglichen.
2. Konfigurieren Sie den RSTS.

3. Konfigurieren Sie den Anwendungsserver.
4. Konfigurieren Sie die Webanwendung.

Verwandte Themen

- Webauthn-Sicherheitsschlüssel auf Seite 19
- Schritt 1: OAuth-Zertifikat konfigurieren auf Seite 20
- Schritt 2: RSTS konfigurieren auf Seite 21
- Schritt 3: Anwendungsserver konfigurieren auf Seite 23
- Schritt 4: Webanwendung konfigurieren auf Seite 23

Schritt 1: OAuth-Zertifikat konfigurieren

Die Kommunikation zwischen dem RSTS und One Identity Manager findet mithilfe von Tokens statt, die mit dem privaten Schlüssel eines Zertifikats signiert werden. Dieses Zertifikat muss gültig und vertrauenswürdig sein, da der RSTS dieses Zertifikat auch zur Client-Zertifikatsanmeldung am Anwendungsserver verwendet. One Identity empfiehlt Ihnen, entweder eine bereits existierende Public-Key-Infrastruktur (PKI) oder eine neue Zertifizierungskette aus Root-Zertifikat und damit signiertem OAuth-Signatur-Zertifikat zu verwenden.

Um das OAuth-Signatur-Zertifikat zu konfigurieren

1. Erstellen Sie ein neues gültiges und vertrauenswürdiges OAuth-Signatur-Zertifikat.
2. Stellen Sie Folgendes sicher:
    - Der RSTS muss Zugriff auf das OAuth-Signatur-Zertifikat mit privatem Schlüssel haben.
    - Der Anwendungsserver, von dem der RSTS die Webauthn-Sicherheitsschlüssel abfragt, muss der Zertifizierungskette des OAuth-Signatur-Zertifikats vertrauen.
    - Die Webanwendung, die eine Anmeldung per RSTS erlaubt, muss Zugriff auf das OAuth-Signatur-Zertifikat mit privatem Schlüssel haben.
    - Die Webanwendung, über welche die Webauthn-Sicherheitsschlüssel verwaltet werden sollen, muss Zugriff auf das OAuth-Signatur-Zertifikat mit privatem Schlüssel haben.

Verwandte Themen

- Webauthn-Sicherheitsschlüssel auf Seite 19
- Schritt 2: RSTS konfigurieren auf Seite 21
- Schritt 3: Anwendungsserver konfigurieren auf Seite 23
- Schritt 4: Webanwendung konfigurieren auf Seite 23

Schritt 2: RSTS konfigurieren

HINWEIS: Bevor Sie den RSTS konfigurieren können, müssen Sie das OAuth-Signatur-Zertifikat konfigurieren. Weitere Informationen finden Sie unter Schritt 1: OAuth-Zertifikat konfigurieren auf Seite 20.

Um Webauthn am RSTS zu konfigurieren

1. Nehmen Sie eine der folgenden Aktionen vor:
   - Wenn Sie den RSTS installieren: Bei der Installation des RSTS wählen Sie das vorherig erstellte OAuth-Signatur-Zertifikat, damit der entsprechende Eintrag am Identitätsanbieter im One Identity Manager entsprechend gesetzt wird.
   - Wenn der RSTS bereits installiert ist: Beenden Sie den entsprechenden Dienst und tauschen Sie die Datei `RSTS.exe` durch die aktuelle Version aus und starten Sie den RSTS neu.

     Die aktuelle Version der Datei `RSTS.exe` finden Sie im Installationsmedium im Verzeichnis `Modules\QBM\dvd\AddOn\Redistributable STS`.
2. In Ihrem Web-Browser rufen Sie die URL der Administrationsoberfläche des RSTS' auf: https://<Webanwendung>/RSTS/admin.
3. Auf der Startseite klicken Sie **Applications**.
4. Auf der Seite **Applications** klicken sie **Add Application**.
5. Auf der Seite **Edit** vervollständigen Sie die Angaben in den verschiedenen Tabreitern.

   HINWEIS: Die Weiterleitungs-URLs (**Redirect Url**) im Tabreiter **General Settings** werden nach folgenden Formaten gebildet:
   - Für den API Server:

     https://<Server-Name>/<Anwendungsserver-Pfad>/html/<Webanwendung>/?Module=OAuthRoleBased
   - Für das Web Portal:

     https://<Server-Name>/<Webanwendung>/
6. Wechseln Sie zum Tabreiter **Two Factor Authentication**.
7. Im Tabreiter **Two Factor Authentication** im Bereich **Required By** in der Liste klicken Sie auf:
   - **All Users**: Alle Benutzer müssen sich per Zwei-Faktor-Authentifizierung anmelden.
   - **Specific Users/Groups**: Bestimmte Benutzer müssen sich per Zwei-Faktor-Authentifizierung anmelden. Diese können Sie hinzufügen, indem Sie **Add** klicken.
   - **Not Required**: Der Anwendungsserver entscheidet, welche Benutzer sich per Zwei-Faktor-Authentifizierung anmelden müssen.
8. In der Navigation klicken Sie **Home**.
9. Auf der Startseite klicken Sie **Authentication Providers**.

10. Auf der Seite **Authentication Providers** bearbeiten Sie den Eintrag in der Liste.
11. Auf der Seite **Edit** wechseln Sie zum Tabreiter **Two Factor Authentication**.
12. Im Bereich **Two Factor Authentication Settings** klicken Sie **FIDO2/WebAuthn**.
13. Bearbeiten Sie die folgenden Eingabefelder:
    - **Relying Party Name**: Geben Sie einen beliebigen Namen ein.
    - **Domain Suffix**: Geben Sie das Suffix Ihrer Active Directory-Domäne ein, auf welcher der RSTS gehostet wird.
    - **API URL Format**: Geben Sie die URL des Anwendungsservers ein. Die eingegebene URL muss einen Platzhalter in der Form `{0}` enthalten, der die eindeutige Kennung des Benutzers angibt.

      Das **API URL Format** wird vom RSTS genutzt, um die Liste der Webauthn-Sicherheitsschlüssel eines bestimmten Benutzers abzurufen. Geben Sie die URL in folgendem Format an:

      https://<Server-Name>/<Anwendungsserver-Pfad>/appServer/webauthn/<Identitätsanbieter>/Users/{0}

      - `<Server-Name>` – Vollqualifizierter Host-Name des Webservers, der den Anwendungsserver hostet
      - `<Anwendungsserver-Pfad>` – Pfad zur Webanwendung des Anwendungsserver (Standard: `AppServer`)
      - `<Identitätsanbieter>` – Name des Identitätsanbieters

        TIPP: Den Namen des Identitätsanbieters können Sie im Designer ermitteln:

        Basisdaten | **Sicherheitseinstellungen** | **OAuth 2.0/OpenId Connect Konfiguration**

    Beispiel:
    https://www.example.com/AppServer/appServer/webauthn/OneIdentity/Users/{0}

14. Klicken Sie **Finish**.

Verwandte Themen

- Webauthn-Sicherheitsschlüssel auf Seite 19
- Schritt 1: OAuth-Zertifikat konfigurieren auf Seite 20
- Schritt 3: Anwendungsserver konfigurieren auf Seite 23
- Schritt 4: Webanwendung konfigurieren auf Seite 23

Schritt 3: Anwendungsserver konfigurieren

Der RSTS ruft die Webauthn-Sicherheitsschlüssel für Active Directory-Benutzer über eine Schnittstelle ab. Da diese Informationen sensibel sind und nicht von Unbefugten abgerufen werden dürfen, muss der Zugriff über eine Client-Zertifikat-Anmeldung abgesichert werden.

Damit dies funktionieren kann, müssen die Zertifikate gültig sein und die Client-Zertifikat-Anmeldung am IIS aktiv sein.

Der Anwendungsserver prüft bei der Anmeldung den Fingerabdruck des Zertifikats, mit dem sich der Client angemeldet hat. Nur wenn der Fingerabdruck mit dem hinterlegten Fingerabdruck übereinstimmt, werden die Informationen geliefert.

Falls Sie den Anwendungsserver auch als Backend für Webanwendungen verwenden, vergeben Sie für den Anwendungspool-Benutzer Zugriffsrechte auf den privaten Schlüssel des OAuth-Signatur-Zertifikat.

Um die Client-Zertifikat-Anmeldung am IIS zu aktivieren

1. Starten Sie den Internet Information Services Manager.
2. Öffnen Sie für den entsprechenden Anwendungsserver das Menü **SSL Settings**.
3. Ändern den Wert der Option **Client certificates** auf **Accept**.

Verwandte Themen

- Webauthn-Sicherheitsschlüssel auf Seite 19
- Schritt 1: OAuth-Zertifikat konfigurieren auf Seite 20
- Schritt 2: RSTS konfigurieren auf Seite 21
- Schritt 4: Webanwendung konfigurieren auf Seite 23

Schritt 4: Webanwendung konfigurieren

HINWEIS: Die Webanwendung, die Webauthn verwenden soll, muss das sichere Kommunikationsprotokoll HTTPS verwenden (siehe HTTPS verwenden auf Seite 38).

Um Webauthn in der Webanwendung zu konfigurieren

1. Starten Sie den Web Designer.
2. In der Menüleiste klicken Sie **Ansicht** | **Startseite**.
3. Auf der Startseite klicken Sie **Webanwendung auswählen** und wählen Sie die gewünschte Webanwendung aus.
4. Klicken Sie **Einstellungen der Webanwendung bearbeiten**.
5. Im Dialogfenster **Einstellungen der Webanwendung bearbeiten** in der Auswahlliste **Authentifizierungsmodul** klicken Sie **OAuth 2.0/OpenID Connect**.

6. Im Bereich **OAuth** in der Auswahlliste **OAuth 2.0/OpenID Connect Konfiguration** klicken Sie den entsprechenden Identitätsanbieter.
7. Klicken Sie **OK**.
8. In der Menüleiste klicken Sie **Bearbeiten** | **Projekt konfigurieren** | **Webprojekt**.
9. Konfigurieren Sie die folgenden Konfigurationsschlüssel:
    - **VI_Common_RequiresAccessControl**: Aktivieren Sie diesen Parameter, um die Zwei-Faktor-Authentifizierung zu aktivieren.
    - **VI_Common_AccessControl_Webauthn_2FA**: Legen Sie fest, ob Sie die Webauthn-Zwei-Faktor-Authentifizierung für die Webanwendung aktivieren möchten.

      Sie können die Webauthn-Zwei-Faktor-Authentifizierung und die Verwaltung der Sicherheitsschlüssel voneinander getrennt konfigurieren. Wenn Sie beispielsweise nur die Verwaltung der Sicherheitsschlüssel, nicht aber die Zwei-Faktor-Authentifizierung mithilfe der Sicherheitsschlüssel in der Webanwendung aktivieren möchten, deaktivieren Sie diesen Konfigurationsschlüssel und aktivieren Sie den nachfolgend beschriebenen Konfigurationsschlüssel **VI_Common_AccessControl_Webauthn_2FA_VisibleControls**.
    - **VI_Common_AccessControl_Webauthn_2FA_VisibleControls**: Legen Sie fest, ob Benutzer in der Webanwendung Sicherheitsschlüssel verwalten können.
    - **VI_Employee_QERWebAuthnKey_Filter**: Legen Sie fest, welche Mitarbeiter Sicherheitsschlüssel in der Webanwendung verwalten können. Wenn Sie hier nichts angeben, können alle Benutzer der Webanwendung Sicherheitsschlüssel verwalten (vorausgesetzt der Konfigurationsschlüssel **VI_Common_AccessControl_Webauthn_2FA_VisibleControls** ist aktiviert).
    - **VI_Common_AccessControl_Webauthn_2FAID**: Geben Sie die eindeutige Kennung des sekundären Authentifizierungsanbieters für die Webauthn-Zwei-Faktor-Authentifizierung ein. Diese Kennung finden Sie in Ihrer RSTS-Konfiguration:
        a. In Ihrem Web-Browser rufen Sie die URL der Administrationsoberfläche des RSTS auf: https://<Webanwendung>/RSTS/admin
        b. Auf der Hauptseite klicken Sie **Authentication Providers**.
        c. Auf der Seite **Authentication Providers** klicken Sie den entsprechenden Eintrag.
        d. Auf der Seite **Edit** wechseln Sie zum Tabreiter **Two Factor Authentication**.
        e. Entnehmen Sie dem Feld **Provider ID** die entsprechende Kennung.

Verwandte Themen

- Webauthn-Sicherheitsschlüssel auf Seite 19
- Schritt 1: OAuth-Zertifikat konfigurieren auf Seite 20

- Schritt 2: RSTS konfigurieren auf Seite 21
- Schritt 3: Anwendungsserver konfigurieren auf Seite 23

Starling Two-Factor Authentication

Eine höhere Sicherheit beim Anmelden an einer Webanwendung gewährleistet die Multifaktor-Authentifizierung. Für die Multifaktor-Authentifizierung nutzen die Werkzeuge des One Identity Manager die Starling Two-Factor Authentication.

Zur Nutzung der Starling Two-Factor Authentication müssen folgende Voraussetzungen erfüllt sein:

- Benutzer müssen über ein registriertes Starling 2FA Token verfügen.
- Verwendung eines personenbezogenes Authentifizierungsmodul, zum Beispiel "Person (rollenbasiert)".

Die Starling Two-Factor Authentication erfolgt nach der primären Anmeldung an der Datenbank und ist von dieser unabhängig. Auf Ebene der Webanwendung wird jeder Zugriff auf andere Seiten verhindert, solange keine Starling Two-Factor Authentication durchgeführt wurde.

Starling Two-Factor Authentication einrichten

Tabelle 10: Konfigurationsparameter für Multifaktor-Authentifizierung

Konfigurationsparameter	Beschreibung
VI_Common_RequiresAccessControl	Fordert die Authentifizierung an der Webanwendung ein.
VI_Common_AccessControl_StarlingEnabled	Aktiviert die Nutzung der Starling Two-Factor Authentication.

Die Einrichtung der Multifaktor-Authentifizierung wird am Webprojekt im Web Designer vorgenommen.

Um Starling Two-Factor Authentication einzurichten

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach"VI_Common_RequiresAccessControl".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_Common_RequiresAccessControl" und setzen Sie im Knotenbearbeitungsfenster den Wertauf `true`.
4. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_Common_AccessControl_StarlingEnabled" und setzen Sie im Knotenbearbeitungsfenster den Wertauf `true`.

Starling Two-Factor Authentication für bestimmte Personen

Tabelle 11: Konfigurationsparameter für Multifaktor-Authentifizierung für bestimmte Prersonen

Konfigurationsparameter	Beschreibung
VI_Common_AccessControl_Filter	Richtet die Multifaktor-Authentifizierung für bestimmte Personen ein.

An Ihrem Webprojekt können Sie einstellen, welche Personen die Multifaktor-Authentifizierung nutzen sollen.

Um Starling Two-Factor Authentication nur für bestimmte Personen einzurichten

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_Common_AccessControl_Filter".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter "VI_Common_AccessControl_Filter".
4. Erfassen Sie im Knotenbearbeitungsfenster eine Filterbedingung, die nur Personen trifft, die für die Multifaktor-Authentifizierung erforderlich ist.

Anmeldung ohne Starling 2FA Token

Tabelle 12: Konfigurationsparameter für Anmeldung ohne Multifaktor-Authentifizierung

Konfigurationsparameter	Beschreibung	Einstellung	
		True	False
VI_Common_ AccessControl_Starling_ AllowUnregistered	Erlaubt dem Benutzer eine Anmeldung an der Webanwendung ohne Multifaktor-Authentifizierung.	Benutzer, die keinen registrierten Starling 2FA Token besitzen, können sich ohne Starling Two-Factor Authentication an der Webanwendung anmelden.	Benutzer, die keinen registrierten Starling 2FA Token besitzen, können sich nicht an der Webanwendung anmelden.

Sie können an Ihrem Webprojekt festlegen, dass Benutzer ohne Multifaktor-Authentifizierung sich an der Webanwendung anmelden können.

Um eine Anmeldung ohne Starling 2FA Token einzustellen

1. Öffnen Sie den Web Designer.
2. Öffnen Sie ein Modul und suchen Sie über das Definitionsbaumfenster nach "VI_ Common_AccessControl_Starling_AllowUnregistered".
3. Markieren Sie im Definitionsbaumfenster den Konfigurationsparameter VI_Common_ AccessControl_Starling_AllowUnregistered".
4. Setzen Sie den Wert im Knotenbearbeitungsfenster auf `true`.

Starling Two-Factor Authentication für das Web Portal für Betriebsunterstützung aktivieren

Sie können für das Web Portal für Betriebsunterstützung auf dem API Server Starling 2FA aktivieren.

Um Starling Two-Factor Authentication für das Web Portal für Betriebsunterstützung zu aktivieren

1. Starten Sie den API Designer.
2. In der Menüleiste klicken Sie **Ansicht** | **Navigation**.
3. In der Navigation klicken Sie **API-Projekte**.
4. In der Baumstruktur doppelklicken Sie das API-Projekt **QBM_OperationsSupport**.
5. Im Definitionsbaumfenster rechtsklicken Sie den Knoten **Authentifizierung**.
6. Im Kontextmenü klicken Sie **Element in Erweiterung** | **In Erweiterung <Name der Erweiterung> anlegen** | **Authentifizierungsmodul**.
7. In der Menüleiste klicken Sie **Ansicht** | **Knotenbearbeitung**.
8. Im Definitionsbaumfenster klicken Sie den neu erstellten Knoten **Zweiter Authentifizierungs-Faktor**.
9. Im Knotenbearbeitungsfenster aktivieren Sie das Kontrollkästchen **Zweiter Authentifizierungs-Faktor**.
10. In der Auswahlliste klicken Sie **Starling 2FA**.

Kennwortrücksetzungsportal

Das Kennwortrücksetzungsportal ermöglicht den Benutzern das sichere Zurücksetzen von Kennwörtern für die von ihnen verwalteten Benutzerkonten.

Einrichten eines Kennwortrücksetzungsportal

Um das Kennwortrücksetzungsportal nutzen zu können, muss es als eigene Webanwendung installiert sein. Die erforderliche Sicherheit wird durch die Multifaktor-Authentifizierung gewährleistet.

Installation des Kennwortrücksetzungsportal

Tabelle 13: Konfigurationsparameter für Anwendungstoken

Konfigurationsparameter	Beschreibung
QER\Person\PasswordResetAuthenticator\ApplicationToken	Setzt einen Anwendungstoken für das Kennwortrücksetzungsportal.

Während der Installation werden Sie aufgefordert, ein Anwendungstoken einzugeben. Dieses Anwendungstoken funktioniert wie ein Kennwort, mit dem sich die Webanwendung an der Datenbank authentifiziert. Damit wird sicher gestellt, dass Kennwortrücksetzungen nur von einer dafür vorgesehenen Webanwendung vorgenommen werden können.

Um das Kennwortrücksetzungsportal zu installieren

1. Folgen Sie der Schrittanleitung "Um das Web Portal zu installieren" aus "Installieren des Web Portal" im One Identity Manager Installationshandbuch.
2. Wählen Sie im Auswahlfeld **Webprojekt** das Projekt **QER_PasswordWeb** aus.

   Nach Auswahl des Webprojektes werden Sie aufgefordert einen Anwendungstoken einzugeben.
3. Wählen Sie ein ausreichend sicheres Anwendungstoken und erfassen Sie es im vorgesehenen Eingabefeld.

   Das Anwendungstoken wird in der Datenbank im Konfigurationsparameter "QER\Person\PasswordResetAuthenticator\ApplicationToken" als Hashwert gespeichert und in der Datei `web.config` der Webanwendung verschlüsselt abgelegt.

Authentifizierung

Die Authentifizierung am Kennwortrücksetzungsportal unterscheidet sich von der Authentifizierung am Web Portal. Der Benutzer hat drei Möglichkeiten zur Auswahl.

Tabelle 14: Möglichkeiten der Authentifizierung

Art der Anmeldung	Verwendetes Authentifizierungsmodul	Anwendung (QBMProduct)
Anmeldung über einen Zugangscode.	Kennwortrücksetzung (rollenbasiert), nicht änderbar.	PasswordReset, nicht änderbar.
Anmeldung über die Bearbeitung der persönlichen Kennwortfrage.	Kennwortrücksetzung (rollenbasiert), nicht änderbar.	PasswordReset, nicht änderbar.
Anmeldung über Benutzername und Kennwort.	Wird in der Konfiguration der Webanwendung festgelegt.	Wird in der Konfiguration der Webanwendung festgelegt.

Setzbare Kennwörter

Ein Benutzer kann standardmäßig folgende Kennwörter setzen.

Tabelle 15: Übersicht der Kennwörter

Benutzer	Kennwort	Tabelle / Spalte
Jeder	Persönliches Kennwort	Person.DialogUserPassword
Jeder	Kennwort eines Benutzerkontos, welches a. direkt dem angemeldeten Mitarbeiter zugewiesen ist. - oder - b. einer Subidentität des angemeldeten Mitarbeiters zugewiesen ist. - oder - c. einer Zusatzidentität, Dienstidentität oder Gruppenidentität des angemeldeten Mitarbeiters zugewiesen ist. - oder - d. eines dem angemeldeten Mitarbeiter gemeinsam genutztes Benutzerkonto zugewiesen ist.	AADUser.Password ADSAccount.UserPassword CSMUser.Password EBSUser.Password GAPUser.Password LDAPAccount.UserPassword NDOUser.Password SAPUser.Password UNSAccountB.Password UNXAccount.UserPassword
Mitglieder der Anwendungsrollen **Basisrollen | Administratoren**	Kennwort einzelner Systembenutzer	DialogUser.Password

HINWEIS: In folgenden Fällen wird der Systembenutzer nicht zur Kennwortrücksetzung angeboten:

- Wenn die externe Kennwortverwaltung für den Systembenutzer aktiviert ist.
- Wenn der Systembenutzer als Dienstkonto aktiviert ist.
- Wenn für die automatische Softwareaktualisierung der Webanwendungen des One Identity Manager der Systembenutzer verwendet wird.

Diese Fälle sind im Skript `QER_PasswordWeb_IsAllowSet` implementiert, das überschreibbar ist.

- Wenn der Systembenutzer für die rollenbasierte Anmeldung verwendet wird.

In diesem Fall wird der Systembenutzer vom Kennwortrücksetzungsportal nicht akzeptiert.

Kennwörter von Rücksetzung ausschließen

Tabelle 16: Skript für das Rücksetzen von Kennwörtern

Skript	Beschreibung
QER_PasswordReset_IsAllowSet	Bestimmt, ob das Rücksetzen eines Kennwortes im Kennwortrücksetzungsportal erlaubt ist.

Um den Benutzer am Setzen ungewollter Kennwörter zu hindern, können Sie bestimmte Kennwörter von der Rücksetzung ausschließen.

Anwendungsfälle hierfür können Kennwörter sein, die aus anderen Werten berechnet werden oder Kennwörter für Zielsysteme, die nur lesend angebunden sind.

HINWEIS: Im Skript "QER_PasswordWeb_IsAllowSet" wird der Systembenutzer standardmäßig in folgenden Fällen am Zurücksetzen des Kennwortes gehindert.

- Wenn die externe Kennwortverwaltung aktiviert ist.
- Wenn der Systembenutzer als Dienstkonto aktiviert ist.
- Wenn für die automatische Softwareaktualisierung der Webanwendungen des One Identity Manager der Systembenutzer verwendet wird.

Um Kennwörter von der Rücksetzung auszuschließen

1. Öffnen Sie den Designer.
2. Suchen Sie das Skript "QER_PasswordReset_IsAllowSet".
3. Definieren Sie ein überschreibendes Skript anhand der Vorlage "QER_PasswordReset_IsAllowSet" mit folgenden Eingabeparametern.
    a. UID_Person des angemeldeten Benutzers.
    b. Schlüssel (ObjectKey) des Objekts, für das die Kennwortrücksetzung angeboten wird.
    c. Spaltennamen des Kennworts.
4. Speichern Sie die Einstellungen im Designer.
5. Kompilieren Sie das Kennwortrücksetzungsportal.

Zentrales Kennwort

Im Kennwortrücksetzungsportal kann, neben dem Setzen von individuellen Kennwörtern, ebenfalls das zentrale Kennwort gesetzt werden. Jeder Benutzer hat ein zentrales Kennwort, mit dem - abhängig von der Konfiguration der Zielsysteme - andere Kennwörter verwaltet werden können.

Kennwortabhängigkeiten definieren

Beim Definieren von Kennwortabhängigkeiten, legen Sie fest, welche Kennwörter durch das zentrale Kennwort verwaltet werden.

Tabelle 17: Skript zur Deklaration von Kennwörtern

Skript	Beschreibung
QER_PasswordWeb_IsByCentralPwd	Standardmäßig prüft das Skript, ob der Konfigurationsparameter "QER\Person\UseCentralPassword" aktiviert ist. Ist der Konfigurationsparameter aktiviert, wird die Kennwortspalte des Benutzerkontos auf den Empfang von Daten aus dem zentralen Kennwort der verknüpften Person geprüft. Ein Benutzerkonto muss mit dem angemeldeten Benutzer verknüpft sein, es darf sich nicht um ein privilegiertes Konto handeln. Das Skript kann überschrieben werden.

Um Kennwortabhängigkeiten zu definieren

1. Öffnen Sie den Designer.
2. Suchen Sie das Skript QER_PasswordWeb_IsByCentralPwd.
3. Definieren Sie ein überschreibendes Skript anhand der Vorlage "QER_PasswordWeb_IsByCentralPwd" mit folgenden Eingabeparametern.
   a. UID_Person des angemeldeten Benutzers.
   b. Schlüssel (ObjectKey) des Objekts, für das die Kennwortrücksetzung angeboten wird.
   c. Spaltennamen des Kennwortes.

   Anhand dieser Eingabeparameter muss das Skript die Information zurückliefern, ob ein Kennwort vom zentralen Kennwort verwaltet wird.
4. Speichern Sie die Einstellungen im Designer.
5. Kompilieren Sie das Kennwortrücksetzungsportal.

Setzen eines zentralen Kennwortes

Das zentrale Kennwort wird getrennt von anderen Kennwörtern gesetzt, um Probleme zu vermeiden.

Wenn mindestens ein Kennwort des angemeldeten Benutzers vom zentralen Kennwort verwaltet wird, werden nach der Authentifizierung zwei Möglichkeiten angeboten.

a. Setzen des zentralen Kennwortes

b. Setzen eines oder mehrerer Kennwörter

Beim Setzen eines oder mehrerer Kennwörter ist es möglich, ein vom zentralen Kennwort verwaltetes Kennwort zu setzen. Möchten Sie das verhindern, können Sie das Kennwort von der Kennwortrücksetzung ausschließen.

Weitere Informationen finden Sie unter Kennwörter von Rücksetzung ausschließen auf Seite 33.

Prüfung aller Kennwortrichtlinien aktivieren

Sobald ein Benutzer sein zentrales Kennwort ändert und das Benutzerkonto mit weiteren Zielsystemkonten verknüpft ist, kann das Kennwort gegen alle Kennwortrichtlinien der verknüpften Zielsysteme geprüft werden.

Um die Prüfung aller Kennwortrichtlinien zu aktivieren

1. Starten Sie den Designer.
2. Aktivieren Sie den Konfigurationsparameter **QER** | **Person** | **UseCentralPassword** | **CheckAllPolicies**:

   HINWEIS: Wie Sie Konfigurationsparameter im Designer bearbeiten, erfahren Sie im *One Identity Manager Konfigurationshandbuch*.

Neues Anwendungstoken einrichten

Über die Datei `WebDesigner.ConfigFileEditor.exe` können Sie einen neuen Anwendungstoken setzen.

Um einen neuen Anwendungstoken zu setzen

1. Öffnen Sie die Datei `WebDesigner.ConfigFileEditor.exe`.
2. Stellen Sie sicher, dass als Webprojekt **QER_PasswordWeb** ausgewählt ist.
3. Klicken Sie bei **Applikationstoken ist eingetragen** auf .

Anmeldung am Kennwortrücksetzungsportal über Zielsystembenutzerkonten konfigurieren

Standardmäßig ist die Anmeldung am Kennwortrücksetzungsportal mithilfe von Kennwortfragen oder einem Zugangscode nur mit dem zentralen Benutzerkonto möglich. Sie können das Authentifizierungsmodul des Kennwortrücksetzungsportals so konfigurieren, dass die Anmeldung mithilfe der Kennwortfragen oder einem Zugangscode auch über Zielsystembenutzerkonten möglich ist (beispielsweise über Active Directory-Benutzerkonten). Dazu geben Sie die Datenbanktabelle und -spalte an, welche die Benutzernamen der Benutzerkonten enthält, die sich am Kennwortrücksetzungsportal anmelden dürfen. Weitere Informationen zum Authentifizierungsmodul des Kennwortrücksetzungsportals finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Um die Anmeldung über Zielsystembenutzerkonten zu konfigurieren

1. Starten Sie den Designer.
2. Aktivieren und konfigurieren Sie die folgenden Konfigurationsparameter:

   HINWEIS: Wie Sie Konfigurationsparameter im Designer bearbeiten, erfahren Sie im *One Identity Manager Konfigurationshandbuch*.

   - **QER** | **Person** | **PasswordResetAuthenticator** | **SearchTable**: Geben Sie den Namen der Datenbanktabelle ein, in der die Benutzernamen der Benutzerkonten enthalten sind, die sich am Kennwortrücksetzungsportal anmelden dürfen.
     Versucht ein Benutzer sich am Kennwortrücksetzungsportal anzumelden, wird diese Tabelle und die unter **SearchColumn** angegebene Spalte nach dem verwendeten Benutzernamen durchsucht.

     Beispiel: `ADSAccount`

     HINWEIS: Diese Datenbanktabelle muss einen Fremdschlüssel namens **UID_Person** enthalten, der auf die Tabelle **Person** zeigt, damit die Benutzernamen den One Identity Manager-Benutzerkonten zugeordnet werden können.
   - **QER** | **Person** | **PasswordResetAuthenticator** | **SearchColumn**: Geben Sie den Namen der Tabellenspalte ein, welche die Benutzernamen der Benutzerkonten enthält, die sich am Kennwortrücksetzungsportal anmelden dürfen.
     Versucht ein Benutzer sich am Kennwortrücksetzungsportal anzumelden, wird diese Spalte in der unter **SearchTable** angegebenen Tabelle nach dem verwendeten Benutzernamen durchsucht.

     Beispiel: `CN`

- **QER** | **Person** | **PasswordResetAuthenticator** | **DisabledBy**: (Optional) Geben Sie den Namen der booleschen Tabellenspalte ein, die festlegt, ob ein Benutzerkonto gesperrt ist. Benutzerkonten, die hier als gesperrt markiert sind (Wert in der Spalte: `true`), können sich NICHT am Kennwortrücksetzungsportal anmelden.

  TIPP: Um mehrere Spalten anzugeben, trennen Sie die einzelnen Werte mit dem Pipe-Zeichen (**|**).

  Beispiel: `Locked|Disabled`
- **QER** | **Person** | **PasswordResetAuthenticator** | **EnabledBy**: (Optional) Geben Sie den Namen der booleschen Tabellenspalte ein, die festlegt, ob ein Benutzerkonto aktiviert ist. Benutzerkonten, die hier als deaktiviert markiert sind (Wert in der Spalte: `false`), können sich NICHT am Kennwortrücksetzungsportal anmelden.

  TIPP: Um mehrere Spalten anzugeben, trennen Sie die einzelnen Werte mit dem Pipe-Zeichen (**|**).

  Beispiel: `Active|Enabled`

6

Empfehlungen für einen sicheren Betrieb von Webanwendungen

Um den sicheren Betrieb Ihrer One Identity Manager Webanwendungen zu gewährleisten, werden hier einige Empfehlungen vorgestellt, die sich im Zusammenspiel mit den One Identity-Werkzeugen als bewährte Lösungen erwiesen haben. Welche empfohlene oder alternative Sicherheitslösung für Ihre individuell angepassten Webanwendungen die geeignetste ist, bleibt Ihnen selbst überlassen.

Detaillierte Informationen zum Thema

HTTPS verwenden

Betreiben Sie die Webanwendungen des One Identity Managers immer über das sichere Kommunikationsprotokoll "Hypertext Transfer Protocol Secure" (HTTPS).

Damit Webanwendungen das sichere Kommunikationprotokoll verwenden, können Sie bei der Installation der Anwendungen die Nutzung von "Secure Sockets Layer" (SSL)

erzwingen. Weitere Informationen zur Nutzung von HTTPS/SSL finden Sie im *One Identity Manager Installationshandbuch*.

Automatische Kennwortspeicherung abschalten

Mit dieser Einstellung können Sie das automatische Vervollständigen Ihrer Benutzerdaten auf der Anmeldeseite unterbinden. Diese Einstellung wird im Web Designer vorgenommen und kann zur Sicherheit des Betriebs der Webanwendung beitragen.

Tabelle 18: Konfigurationsparameter zum Abschalten der automatischen Kennwortspeicherung

Konfigurationsparameter	Beschreibung
VI_Common_Login_PrefillLoginData	Unterbindet die Vervollständigung der Benutzerdaten auf der Anmeldeseite.

Um die automatische Kennwortspeicherung zu deaktivieren

1. Öffnen Sie den Web Designer.
2. Öffnen Sie in der Menüleiste den Menüeintrag **Bearbeiten | Projekt konfigurieren | Webprojekt**.
3. Suchen Sie im Tabreiter **Projekt konfigurieren** den Konfigurationsparameter "VI_Common_Login_PrefillLoginData".
4. Klicken Sie am Schlüssel **Vorausfüllen der Anmeldedaten erlauben** in der Spalte **Wert (kundenspezifisch)** +.

   Der Standardwert wird auf "False" gesetzt. Die automatische Kennwortspeicherung ist deaktiviert.

HTTP-Anfragemethode TRACE abschalten

Über die Anfrage TRACE kann der Weg zum Webserver verfolgt und die korrekte Datenübermittlung dorthin überprüft werden. Somit wird ein traceroute auf Anwendungsebene, also der Weg zum Webserver über die verschiedenen Proxys hinweg, ermittelt. Diese Methode ist besonders für das Debugging von Verbindungen sinnvoll.

WICHTIG: TRACE sollte nicht auf einer produktiven Umgebung aktiviert sein, da es zu Leistungseinbußen führen kann.

Um die HTTP-Anfragemethode TRACE über Internet Information Services zu deaktivieren

- Lesen Sie die Anweisungen, die Sie über folgenden Link aufrufen können.

  https://docs.microsoft.com/en-us/iis/configuration/system.webserver/tracing/

HTTP Strict Transport Security (HSTS) verwenden

HTTP Strict Transport Security (HSTS) ist ein Sicherheitsmechanismus für HTTPS-Verbindungen. Dieser Mechanismus schützt vor Aushebelung der Verbindungsverschlüsselung durch Downgrade-Attacke und Session Hijacking. Hierbei kann ein Server mithilfe des HTTP Response Header "Strict-Transport-Security" dem Browser des Benutzer mitteilen, zukünftig eine definierte Zeit (max-age) ausschließlich verschlüsselte Verbindungen für diese Domain zu verwenden. Wahlweise lässt sich diese Einstellung über den Parameter `includeSubDomains` auf alle Subdomains ausweiten. Das heißt, es wird nicht nur `https://example.org` berücksichtigt, sondern auch `https://subdomains.example.org`.

Um HSTS zu aktivieren

1. Öffnen Sie die Konfigurationsdatei `web.config` der gewünschten Webanwendung.
2. Setzen Sie den HTTP Response Header `Strict-Transport-Security` und den Wert `maxage = expireTime`.

   Ausführliche Informationen wie Sie den HTTP Response Header setzen, finden Sie unter folgendem Link https://docs.microsoft.com/en-us/iis/configuration/system.applicationhost/sites/site/hsts.

Unsichere Verschlüsselungsmechanismen abschalten

Aus Sicherheitsgründen wird empfohlen alte, nicht benötigte Verschlüsselungsmethoden und Protokolle zu deaktivieren. Durch das Deaktivieren von alten Protokollen und Methoden können ältere Plattformen und Systeme unter Umständen keine Verbindung mehr mit der Webanwendung aufbauen. Es ist daher notwendig, anhand der benötigten Plattformen zu entscheiden, welche Protokolle und Methoden notwendig sind.

HINWEIS: Zur Deaktivierung der Verschlüsselungsmethoden und Protokolle wird die Software "IIS Crypto" von Nartac Software empfohlen.

Ausführliche Informationen zur Deaktivierung finden Sie unter https://www.nartac.com/Products/IISCrypto.

Detaillierte Informationen zum Thema

- https://blogs.technet.microsoft.com/exchange/2015/07/27/exchange-tls-ssl-best-practices/
- https://support.microsoft.com/en-us/help/245030/how-to-restrict-the-use-of-certain-cryptographic-algorithms-and-protoc

"HttpOnly"-Attribut für ASP.NET-Session-Cookies setzen

Um zu verhindern, dass Cookies mit JavaScript manipuliert werden können und um das Risiko von Cross-Site-Scripting-Angriffen und Cookie-Diebstahl zu reduzieren, können Sie das sogenannte "HttpOnly"-Attribut für Ihre ASP.NET-Session-Cookies setzen. Dadurch können Cookies nicht mehr durch Client-seitige Skripte verwendet werden.

Um das "HttpOnly"-Attribut für die ASP.NET-Session-Cookies zu setzen

1. Öffnen Sie die Konfigurationsdatei `web.config` der gewünschten Webanwendung.
2. Fügen Sie folgenden Code-Schnipsel innerhalb des Abschnitts `<configuration>` ein:

```
<system.web>
    <httpCookies httpOnlyCookies="true"/>
</system.web>
```

3. Speichern Sie die Datei.

Verwandte Themen

- "Secure"-Attribut für ASP.NET-Session-Cookies setzen auf Seite 42
- "Same-site"-Attribut für ASP.NET-Session-Cookies setzen auf Seite 41

"Same-site"-Attribut für ASP.NET-Session-Cookies setzen

Um eine Cross-Site-Request-Forgery (CSRF) zu vermeiden, können Sie für Ihre ASP.NET-Session-Cookies das Same-site-Attribut setzen.

Um das Same-site-Attribut für alle .NET-Versionen ab 4.7.2 zu setzen

1. Öffnen Sie die Konfigurationsdatei `web.config` der gewünschten Webanwendung.
2. Fügen Sie folgenden Code-Schnipsel innerhalb des Abschnitts `<configuration>` ein:

```
<system.web>
    <httpCookies sameSite="Strict" />
</system.web>
```

3. Speichern Sie die Datei.

Verwandte Themen

- "HttpOnly"-Attribut für ASP.NET-Session-Cookies setzen auf Seite 41
- "Secure"-Attribut für ASP.NET-Session-Cookies setzen auf Seite 42

"Secure"-Attribut für ASP.NET-Session-Cookies setzen

Um zu verhindern, dass Cookies von Unbefugten ausgelesen werden können, können Sie das sogenannte "Secure"-Attribut für Ihre ASP.NET-Session-Cookies setzen. Dadurch werden Cookies nur noch über gesicherte SSL-Verbindungen übertragen.

Um das "Secure"-Attribut für die ASP.NET-Session-Cookies zu setzen

1. Öffnen Sie die Konfigurationsdatei `web.config` der gewünschten Webanwendung.
2. Fügen Sie folgenden Code-Schnipsel innerhalb des Abschnitts `<configuration>` ein:

```
<system.web>
    <httpCookies requireSSL="true"/>
</system.web>
```

3. Speichern Sie die Datei.

Verwandte Themen

- "Same-site"-Attribut für ASP.NET-Session-Cookies setzen auf Seite 41
- "HttpOnly"-Attribut für ASP.NET-Session-Cookies setzen auf Seite 41

Windows-IIS-8.3-Kurznamen deaktivieren

Der URL-Parser in den Microsoft Internet Information Services (IIS) ermöglicht einem Remote-Angreifer, Datei- und Ordnernamen der Webanwendungen (die nicht zugänglich sein sollen) durch Verwenden der IIS-8.3-Kurznamen offen zu legen.

Die Ausnutzung dieser Schwachstelle kann dazu führen, dass Dateien mit sensiblen Informationen wie Anmeldeinformationen, Konfigurationsdateien, Wartungsskripte und anderen Daten weitergegeben werden.

Um dies zu verhindern, können Sie die Erstellung von Kurznamen in Windows IIS 8.3 deaktivieren.

Um die Erstellung von Windows-IIS-8.3-Kurznamen zu deaktivieren

1. Auf dem System, auf dem die Webanwendung installiert ist, erstellen Sie den folgenden Registry-Eintrag:
    - Pfad: `HKLM\SYSTEM\CurrentControlSet\Control\FileSystem`
    - Name: `NtfsDisable8dot3NameCreation`
    - Wert: `1`
2. Führen Sie eine Neuinstallation der Webanwendung durch.

Detaillierte Informationen zum Thema

- https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-2000-server/cc959352(v=technet.10)

HTTP-Response-Header in Windows IIS entfernen

Angreifer können viele Informationen über Ihren Server und Ihr Netzwerk erhalten, indem sie sich die Response-Header ansehen, die Ihr Webserver zurückgibt.

Um Angreifern so wenig Informationen wie möglich zu geben, können Sie die HTTP-Response-Header in Windows IIS entfernen.

Um die HTTP-Response-Header in WindowsIIS zu entfernen

- Lesen Sie die Anweisungen unter folgenden Links:
    - https://github.com/dionach/stripheaders
    - https://www.saotn.org/remove-iis-server-version-http-response-header/

X-Frame-Options-HTTP-Response-Header erstellen

Angreifer können eine eigene Webseite erstellen, um den Inhalt Ihrer Website innerhalb eines Iframes zu laden. Dies kann einen Clickjacking-Angriff ermöglichen, bei dem der Angreifer auf Benutzereingaben abzielt, oder Benutzer dazu veranlassen, unbeabsichtigt Aktionen innerhalb der gefälschten Anwendung durchzuführen.

Um dies zu verhindern, können Sie einen X-Frame-Options-HTTP-Response-Header erstellen. Damit können Inhalte der Seite nicht mehr auf anderen Websites eingebunden werden.

Um einen X-Frame-Options-HTTP-Response-Header zu erstellen

1. Öffnen Sie die Konfigurationsdatei `web.config` der gewünschten Webanwendung.
2. Fügen Sie folgenden Code-Schnipsel innerhalb des Abschnitts `<configuration>` ein:

```
<httpProtocol>
    <customHeaders>
        <add name="X-Frame-Options" value="SAMEORIGIN" />
    </customHeaders>
</httpProtocol>
```

3. Speichern Sie die Datei.

Webanwendungen im Release-Modus laufen lassen

Um zu verhindern, dass Sitzungen von Benutzern gestohlen werden können, lassen Sie Ihre Webanwendungen im Release-Modus laufen. Dadurch wird die Session ID im HTML-Code nicht mehr ausgegeben.

Um die Web-Anwendung im Release-Modus laufen zu lassen

1. Starten Sie den Web Designer.
2. In der Menüleiste klicken Sie **Ansicht** | **Startseite**.
3. Auf der Startseite klicken Sie **Webanwendung auswählen** und wählen Sie die gewünschte Webanwendung aus.
4. Klicken Sie **Einstellungen der Webanwendung bearbeiten**.
5. Deaktivieren Sie das Kontrollkästchen **Debugging**.

   TIPP: Wenn das Kontrollkästchen bereits deaktiviert ist, müssen Sie nichts weiter

tun. Ihre Webanwendung läuft bereits im Release-Modus.

6. Klicken Sie **OK**.
7. Starten Sie den Web Designer neu.
8. Auf der Startseite wählen Sie wieder die gewünschte Webanwendung aus und klicken **Release** (**Kompilieren zur Freigabe**).

Über uns

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

Kontaktieren Sie uns

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

Technische Supportressourcen

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

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

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