



One Identity Manager 8.0.5

Konfigurationshandbuch für  
Webanwendungen

**Copyright 2020 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 JEDLICHE 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 JEDLICHE 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 mögliche Personen- oder Sachschäden oder Schaden mit Todesfolge hin.
-  **VORSICHT:** Das Symbol **VORSICHT** weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.
-  **WICHTIG, HINWEIS, TIPP, MOBIL, oder VIDEO:** Ein Informationssymbol weist auf Begleitinformationen hin.

One Identity Manager Konfigurationshandbuch für Webanwendungen  
Aktualisiert - Mai 2020  
Version - 8.0.5

# Inhalt

<b>Konfiguration von Webanwendungen</b> .....	<b>1</b>
<b>Konfiguration des Web Portal</b> .....	<b>2</b>
IT Shop Konfiguration .....	2
Bestellung nach Referenzbenutzer .....	2
Nach Referenzbenutzern aktivieren oder deaktivieren .....	3
Anzeige der Referenzbenutzer einstellen .....	3
Einkaufswagen absenden .....	4
Priorität einstellen .....	4
Bestellung bestätigen .....	4
Erneute Authentifizierung erzwingen .....	5
Umgang mit Pflichtprodukten .....	6
Optionen für den Entscheider .....	6
Gültigkeit setzen .....	7
Anfrage stellen .....	7
Begründung einfordern .....	8
Entscheidungen über URL-Links .....	8
<b>Starling Two-Factor Authentication</b> .....	<b>10</b>
Starling Two-Factor Authentication einrichten .....	10
Starling Two-Factor Authentication für bestimmte Personen .....	11
Anmeldung ohne Starling 2FA Token .....	12
<b>Kennworrücksetzungsportal</b> .....	<b>13</b>
Einrichten eines Kennworrücksetzungsportal .....	13
Installation des Kennworrücksetzungsportal .....	13
Authentifizierung .....	14
Setzbare Kennwörter .....	14
Kennwörter von Rücksetzung ausschließen .....	16
Zentrales Kennwort .....	16
Kennwortabhängigkeiten definieren .....	17
Setzen eines zentralen Kennwortes .....	18
Neues Anwendungstoken einrichten .....	18

<b>Empfehlungen für einen sicheren Betrieb von Webanwendungen</b> .....	<b>19</b>
Automatische Kennwortspeicherung abschalten .....	19
HTTP-Anfragemethode TRACE abschalten .....	20
HTTP Strict Transport Security (HSTS) verwenden .....	20
Unsichere Verschlüsselungsmechanismen abschalten .....	21
Transport Layer Security (TLS) 1.1 und höher mit Microsoft .NET Framework verwenden .....	21
<b>Über uns</b> .....	<b>23</b>
Kontaktieren Sie uns .....	23
Technische Supportressourcen .....	23

# Konfiguration von Webanwendungen

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

Unter anderem erfahren Sie wie der IT Shop im Web Portal konfiguriert oder eine Starling Two-Factor Authentication eingerichtet werden kann. Des Weiteren wird das Einrichten des Kennwortrücksetzungsportal Schritt für Schritt beschrieben.

# Konfiguration des Web Portal

Das Web Portal ist über den Web Designer konfigurierbar. Im nächsten Abschnitt soll es zunächst um die Konfiguration des IT Shop gehen.

## 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_Filterbedingung 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 3
- [Anzeige der Referenzbenutzer einstellen](#) auf Seite 3

# 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 %userid% 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.

# Einkaufswagen absenden

Der Einkaufswagen im Web Portal hat verschiedene Konfigurationsmöglichkeiten.

## Detaillierte Informationen zum Thema

- [Priorität einstellen](#) auf Seite 4
- [Bestellung bestätigen](#) auf Seite 4
- [Erneute Authentifizierung erzwingen](#) auf Seite 5
- [Umgang mit Pflichtprodukten](#) auf Seite 6

## Priorität einstellen

**Tabelle 2: Konfigurationsparameter für Priorität an Bestellungen**

Konfigurationsparameter	Beschreibung
VI_ITShop_DisablePWOPriorityChange	Deaktiviert die Einstellung einer Priorität 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**

<b>Konfigurationsparameter</b>	<b>Beschreibung</b>	<b>Einstellung</b>	
		<b>False</b>	<b>True</b>
VI_ITShop_TermsOfUseRequireADAuthentication	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 wieder eingestellt 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 7
- [Anfrage stellen](#) auf Seite 7
- [Begründung einfordern](#) auf Seite 8

## 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 stellen

**Tabelle 7: Konfigurationsparameter für Anfrage**

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

### 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\_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 Produkt erfüllt Filterbedingung nicht
		Entscheidung wird nicht direkt vorgenommen. Formular zur Bestätigung der Entscheidung wird angezeigt. 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.

## 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 Personen**

<b>Konfigurationsparameter</b>	<b>Beschreibung</b>
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.



# Kennworrücksetzungsportal

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

## Einrichten eines Kennworrücksetzungsportal

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

## Installation des Kennworrücksetzungsportal

**Tabelle 13: Konfigurationsparameter für Anwendungstoken**

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

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 Kennworrücksetzungen nur von einer dafür vorgesehenen Webanwendung vorgenommen werden können.

## Um das Kennworrücksetzungsportal 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 Kennworrücksetzungsportal unterscheidet sich von der Authentifizierung am Web Portal. Der Benutzer hat drei Möglichkeiten zur Auswahl.

**Tabelle 14: Möglichkeiten der Authentifizierung**

<b>Art der Anmeldung</b>	<b>Verwendetes Authentifizierungsmodul</b>	<b>Anwendung (QBMPProduct)</b>
Anmeldung über einen Zugangscode.	Kennworrücksetzung (rollenbasiert), nicht änderbar.	PasswordReset, nicht änderbar.
Anmeldung über die Bearbeitung der persönlichen Kennwortfrage.	Kennworrücksetzung (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**

<b>Benutzer</b>	<b>Kennwort</b>	<b>Tabelle / Spalte</b>
Jeder	Persönliches Kennwort	Person.DialogUserPassword
Jeder	Kennwort eines Benutzerkontos, welches <ul style="list-style-type: none"> <li>a. direkt dem angemeldeten Mitarbeiter zugewiesen ist.</li> <li>- oder -</li> <li>b. einer Subidentität des angemeldeten Mitarbeiters zugewiesen ist.</li> <li>- oder -</li> <li>c. einer Zusatzidentität, Dienstidentität oder Gruppenidentität des angemeldeten Mitarbeiters zugewiesen ist.</li> <li>- oder -</li> <li>d. eines dem angemeldeten Mitarbeiter gemeinsam genutztes Benutzerkonto zugewiesen ist.</li> </ul>	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 von Systembenutzern	DialogUser.Password

**HINWEIS:** In folgenden Fällen wird der Systembenutzer nicht zur Kennwörterücksetzung 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 Kennwörterücksetzungsportal 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 Kennwörterücksetzungsportal 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 Kennwörterücksetzung angeboten wird.
  - c. Spaltennamen des Kennworts.
4. Speichern Sie die Einstellungen im Designer.
5. Kompilieren Sie das Kennwörterücksetzungsportal.

# Zentrales Kennwort

Im Kennwörterücksetzungsportal 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 16.

# 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 .

# 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

- [Automatische Kennwortspeicherung abschalten](#) auf Seite 19
- [HTTP-Anfragemethode TRACE abschalten](#) auf Seite 20
- [HTTP Strict Transport Security \(HSTS\) verwenden](#) auf Seite 20
- [Unsichere Verschlüsselungsmechanismen abschalten](#) auf Seite 21
- [Transport Layer Security \(TLS\) 1.1 und höher mit Microsoft .NET Framework verwenden](#) auf Seite 21

## 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**

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".

### Detaillierte Informationen zum Thema

- <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.com 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>

## Transport Layer Security (TLS) 1.1 und höher mit Microsoft .NET Framework verwenden

Die One Identity Werkzeuge werden zum aktuellen Stand auf Basis von Microsoft .NET Framework 4.5 ausgeliefert. Für den Verbindungsaufbau verwendet Microsoft .NET

Framework 4.5 standardmäßig maximal TLS 1.0. Um höhere Versionen als TLS 1.0 zu verwenden, müssen Registrierungsunterschlüssel in Windows angepasst werden.

**Setzen Sie im Windows Registrierungs-Editor folgende Registrierungsunterschlüssel**

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ .NETFramework\v4.0.30319]
```

```
"SchUseStrongCrypto"=dword:00000001
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\ .NETFramework\v4.0.30319]
```

```
"SchUseStrongCrypto"=dword:00000001
```

**Detaillierte Informationen zum Thema**

- <https://docs.microsoft.com/en-us/officeonlineserver/enable-tls-1-1-and-tls-1-2-support-in-office-online-server>

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 Geschäftssagilität 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