One Identity Manager 8.1

Konfigurationshandbuch für Webanwendungen

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, or VIDEO: Ein Informationssymbol weist auf Begleitinformationen hin.

One Identity Manager Konfigurationshandbuch für Webanwendungen
Aktualisiert - März 2019
Version - 8.1

Inhalt

Über dieses Handbuch **5**

Konfiguration des Web Portals **6**

IT Shop Konfiguration 6

Bestellung nach Referenzbenutzer 6

Nach Referenzbenutzern aktivieren oder deaktivieren 7

Anzeige der Referenzbenutzer einstellen 7

Einkaufswagen absenden 8

Priorität einstellen 8

Bestellung bestätigen 9

Erneute Authentifizierung erzwingen 9

Umgang mit Pflichtprodukten 10

Optionen für den Entscheider 11

Gültigkeit setzen 11

Anfrage stellen 12

Begründung einfordern 12

Entscheidungen über URL-Links 13

Anzeigen benutzerbezogener Prozesse im Web Portal 14

Starling Two-Factor Authentication **16**

Starling Two-Factor Authentication einrichten 16

Starling Two-Factor Authentication für bestimmte Personen 17

Anmeldung ohne Starling 2FA Token 18

Kennwortrücksetzungsportal **19**

Einrichten eines Kennwortrücksetzungsportal 19

Installation des Kennwortrücksetzungsportal 19

Authentifizierung 20

Setzbare Kennwörter 20

Kennwörter von Rücksetzung ausschließen 22

Zentrales Kennwort 22

Kennwortabhängigkeiten definieren 23

Setzen eines zentralen Kennwortes 23

Neues Anwendungstoken einrichten 24

Empfehlungen für einen sicheren Betrieb von Webanwendungen 25

Automatische Kennwortspeicherung abschalten 25

HTTP-Anfragemethode TRACE abschalten 26

HTTP Strict Transport Security (HSTS) verwenden 27

Unsichere Verschlüsselungsmechanismen abschalten 27

Transport Layer Security 1.1 und höher mit Microsoft .NET Framework verwenden 28

Same-site-Attribut für ASP.NET-Session-Cookies aktivieren 28

Über uns 30

Kontaktieren Sie uns 30

Technische Supportressourcen 30

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.

2

Konfiguration des Web Portals

Dieses Kapitel beschreibt die nötigen Konfigurationsschritte und -parameter im Web Designer, 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 auf Seite 6
- Anzeigen benutzerbezogener Prozesse im Web Portal auf Seite 14

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.

Einkaufswagen absenden

Der Einkaufswagen im Web Portal hat verschiedene Konfigurationsmöglichkeiten.

Detaillierte Informationen zum Thema

- Priorität einstellen auf Seite 8
- Bestellung bestätigen auf Seite 9
- Erneute Authentifizierung erzwingen auf Seite 9
- Umgang mit Pflichtprodukten auf Seite 10

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

Konfigurationsparameter	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 11
- Anfrage stellen auf Seite 12
- Begründung einfordern auf Seite 12

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	Entscheidung wird nicht direkt vorgenommen. Formular zur Bestätigung der Entscheidung wird angezeigt.
		Produkt erfüllt Filterbedingung nicht	Entscheidung erfolgt direkt 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.

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`.

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 22.

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 25
- HTTP-Anfragemethode TRACE abschalten auf Seite 26
- HTTP Strict Transport Security (HSTS) verwenden auf Seite 27
- Unsichere Verschlüsselungsmechanismen abschalten auf Seite 27
- Transport Layer Security 1.1 und höher mit Microsoft .NET Framework verwenden auf Seite 28
- Same-site-Attribut für ASP.NET-Session-Cookies aktivieren auf Seite 28

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.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 1.1 und höher mit Microsoft .NET Framework verwenden

Die One Identity Werkzeuge werden zum aktuellen Stand auf Basis von Microsoft .NET Framework 4.7.2 ausgeliefert. Für den Verbindungsaufbau verwendet Microsoft .NET Framework 4.7.2 standardmäßig maximal Transport Layer Security (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

Same-site-Attribut für ASP.NET-Session-Cookies aktivieren

Um eine Cross-Site-Request-Forgery (CSRF) zu vermeiden, können Sie in Ihren 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.

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

1. Laden Sie die Erweiterung **URL Rewrite** herunter: https://www.iis.net/downloads/microsoft/url-rewrite
2. Öffnen Sie die Konfigurationsdatei `web.config` der gewünschten Webanwendung.
3. Fügen Sie folgenden Code-Schnipsel innerhalb des Abschnitts `<system.webServer>` ein:

```
<rewrite>
  <outboundRules>
       <clear />
       <rule name="Add SameSite" preCondition="No SameSite">
         <match serverVariable="RESPONSE_Set_Cookie" pattern=".*" negate="false" />
         <action type="Rewrite" value="{R:0}; SameSite=lax" />
         <conditions>
         </conditions>
       </rule>
       <preConditions>
         <preCondition name="No SameSite">
               <add input="{RESPONSE_Set_Cookie}" pattern="." />
               <add input="{RESPONSE_Set_Cookie}" pattern="; SameSite=lax" negate="true" />
         </preCondition>
       </preConditions>
  </outboundRules>
</rewrite>
```

4. Speichern Sie die Datei.

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 besuchen Sie https://www.oneidentity.com/company/contact-us.aspx oder rufen Sie + 1-800-306-9329 an.

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