One Identity Manager

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 - 27. April 2022, 00:49 Uhr

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.

API Server konfigurieren

Sie können den API Server sowie die dazugehörigen API-Projekte mithilfe des Administration Portals konfigurieren.

Detaillierte Informationen zum Thema

Am Administration Portal anmelden

Um den API Server sowie die dazugehörigen API-Projekte zu konfigurieren, müssen Sie sich am Administration Portal anmelden.

Um sich am Administration Portal anzumelden

1. In der Adresszeile Ihres Web-Browsers geben Sie die Web-Adresse (URL) des Administration Portals ein.
2. Auf der Anmeldeseite des Administration Portals wählen Sie in der Auswahlliste **Authentifizierung** die Authentifizierungsart aus, mit der Sie sich anmelden möchten.
3. Im Eingabefeld **Benutzer** geben Sie Ihren vollständigen Benutzernamen ein.
4. Im Eingabefeld **Kennwort** geben Sie Ihr persönliches Kennwort ein.
5. Klicken Sie **Anmelden**.

Konfiguration von API-Projekten einsehen und bearbeiten

Sobald Sie sich am Administration Portal angemeldet haben, können Sie die Konfiguration der einzelnen API-Projekte einsehen und mithilfe von Konfigurationsschlüsseln bearbeiten.

Zusätzlich können Sie alle kundenspezifischen Änderungen anzeigen und gegebenenfalls rückgängig machen.

TIPP: Möchten Sie Änderungen auf einem Server ausprobieren, können Sie die Änderungen lokal übernehmen. Möchten Sie Änderungen für alle API Server übernehmen, können Sie die Änderungen global übernehmen.

Um einen Konfigurationsschlüssel eines API-Projekts zu bearbeiten

1. Melden Sie sich am Administration Portal an (siehe Am Administration Portal anmelden auf Seite 5).
2. In der Navigation klicken Sie **Konfiguration**.
3. Auf der Seite **Konfiguration** wählen Sie in der Auswahlliste **Konfiguration für das folgende API-Projekt anzeigen** das API-Projekt aus, das Sie konfigurieren möchten.
4. (Optional) Um die angezeigten Konfigurationsschlüssel weiter einzuschränken, geben Sie im Suchfeld den Namen des Konfigurationsschlüssels ein.
5. Klicken Sie auf den Namen des Konfigurationsschlüssels, um diesen auszuklappen.
6. Bearbeiten Sie den Wert des Konfigurationsschlüssels.
7. Klicken Sie **Übernehmen**.
8. Nehmen Sie eine der folgenden Aktionen vor:
   - Wenn Sie die Änderungen nur lokal übernehmen möchten, klicken Sie **Lokal übernehmen**.
   - Wenn Sie die Änderungen global übernehmen möchten, klicken Sie **Global übernehmen**.
9. Klicken Sie **Übernehmen**.

Um alle kundenspezifischen Änderungen eines API-Projekts anzuzeigen

1. Melden Sie sich am Administration Portal an (siehe Am Administration Portal anmelden auf Seite 5).
2. In der Navigation klicken Sie **Konfiguration**.
3. Auf der Seite **Konfiguration** wählen Sie in der Auswahlliste **Konfiguration für das folgende API-Projekt anzeigen** das API-Projekt aus, dessen Änderungen Sie anzeigen möchten.
4. Klicken Sie ▼ (**Filter**).

5. Im Kontextmenü aktivieren Sie das Kontrollkästchen **Kundenspezifische Einstellungen**.

Um alle kundenspezifischen Änderungen eines API-Projekts zu verwerfen

1. Melden Sie sich am Administration Portal an (siehe Am Administration Portal anmelden auf Seite 5).
2. In der Navigation klicken Sie **Konfiguration**.
3. Auf der Seite **Konfiguration** wählen Sie in der Auswahlliste **Konfiguration für das folgende API-Projekt anzeigen** das API-Projekt aus, dessen Änderungen Sie verwerfen möchten.
4. Klicken Sie ⋮ **Aktionen**.
5. Nehmen Sie eine der folgenden Aktionen vor:
   - Um alle global angepassten Einstellungen zu verwerfen, klicken Sie **Alle global angepassten Einstellungen verwerfen**.
   - Um alle lokal angepassten Einstellungen zu verwerfen, klicken Sie **Alle lokal angepassten Einstellungen verwerfen**.
6. Im Dialogfenster **Konfiguration zurücksetzen** bestätigen Sie die Abfrage mit **Ja**.

Allgemeine Konfiguration von Webanwendungen

Sie können einige Einstellungen vornehmen, die sich auf alle Webanwendungen auswirken.

Detaillierte Informationen zum Thema

- Logo anpassen auf Seite 8

Logo anpassen

Sie können festlegen, welches Logo in den Webanwendungen verwendet werden soll. Das Logo wird auf den Anmeldeseiten und in den Kopfleisten der Webanwendungen angezeigt. Wenn Sie kein Logo festlegen, wird das One Identity-Firmenlogo verwendet.

Benötigte Konfigurationsschlüssel:

- **Firmenlogo** (**CompanyLogoUrl**): URL unter der die Bilddatei des Firmenlogos zu finden ist.

Um das Logo anzupassen

1. Melden Sie sich am Administration Portal an (siehe Am Administration Portal anmelden auf Seite 5).
2. In der Navigation klicken Sie **Konfiguration**.
3. Auf der Seite **Konfiguration** wählen Sie in der Auswahlliste **Konfiguration für das folgende API-Projekt anzeigen** das API-Projekt **imx** aus.
4. Klappen Sie den Konfigurationsschlüssel **Firmenlogo** auf.
5. Im Eingabefeld **Wert** geben Sie URL des Logos ein. Geben Sie die URL in einem der folgenden Formate ein:
   - **https://www.example.com/logos/company-logo.png**
   - **http://www.example.com/logos/company-logo.png**

- **/logos/company-logo.png** (relativ zum Basisverzeichnis des API Servers)

TIPP: Wenn das Logo nicht angezeigt wird, prüfen Sie die Konfiguration der Content Security Policy mithilfe des Konfigurationsschlüssels **Content security policy for HTML applications** im API-Projekt **imx**.

6. Klicken Sie **Übernehmen**.
7. Nehmen Sie eine der folgenden Aktionen vor:
   - Wenn Sie die Änderungen nur lokal übernehmen möchten, klicken Sie **Lokal übernehmen**.
   - Wenn Sie die Änderungen global übernehmen möchten, klicken Sie **Global übernehmen**.
8. Klicken Sie **Übernehmen**.

Web Portal konfigurieren

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

Bestellfunktionen konfigurieren

Sie können Bestellfunktionen des Web Portals über das **Administration Portal** konfigurieren.

Bestellung nach Referenzbenutzer konfigurieren

Benutzer des Web Portals können Produkte bestellen, die eine bestimmte Identität bereits besitzt. Dies wird als Bestellung über einen Referenzbenutzer bezeichnet.

Benötigte Konfigurationsschlüssel:

- **Produkte können über den Referenzbenutzer bestellt werden** (**VI_ITShop_ProductSelectionByReferenceUser**): Aktiviert oder deaktiviert die Funktion "Bestellung über Referenzbenutzer" im Web Portal.

Um das Bestellen nach Referenzbenutzern zu konfigurieren

1. Melden Sie sich am Administration Portal an (siehe Am Administration Portal anmelden auf Seite 5).
2. In der Navigation klicken Sie **Konfiguration**.
3. Auf der Seite **Konfiguration** wählen Sie in der Auswahlliste **Konfiguration für das folgende API-Projekt anzeigen** das API-Projekt aus, für das Sie das Bestellen nach Referenzbenutzern konfigurieren möchten.
4. Klappen Sie den Konfigurationsschlüssel **Produkte können über den Referenzbenutzer bestellt werden** auf.
5. Nehmen Sie eine der folgenden Aktionen vor:
   - Um die Funktion "Bestellung über Referenzbenutzer" zu aktivieren, aktivieren Sie das Kontrollkästchen **Produkte können über den Referenzbenutzer bestellt werden**.
   - Um die Funktion "Bestellung über Referenzbenutzer" zu deaktivieren, deaktivieren Sie das Kontrollkästchen **Produkte können über den Referenzbenutzer bestellt werden**.
6. Klicken Sie **Übernehmen**.
7. Nehmen Sie eine der folgenden Aktionen vor:
   - Wenn Sie die Änderungen nur lokal übernehmen möchten, klicken Sie **Lokal übernehmen**.
   - Wenn Sie die Änderungen global übernehmen möchten, klicken Sie **Global übernehmen**.
8. Klicken Sie **Übernehmen**.

Multi-Faktor-Authentifizierung

Eine höhere Sicherheit beim Anmelden an einer Webanwendung gewährleistet die Multi-Faktor-Authentifizierung. Für die Multi-Faktor-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.

Multi-Faktor-Authentifizierung konfigurieren

Sie können die Multi-Faktor-Authentifizierung für Webanwendungen konfigurieren.

Benötigte Konfigurationsschlüssel:

- **Multi-Faktor-Authentifizierung** (**MfaAuthenticationProvider**): Legt fest, welche Multi-Faktor-Authentifizierung verwendet wird.

Um Multi-Faktor-Authentifizierung einzurichten

1. Melden Sie sich am Administration Portal an (siehe Am Administration Portal anmelden auf Seite 5).
2. In der Navigation klicken Sie **Konfiguration**.
3. Auf der Seite **Konfiguration** wählen Sie in der Auswahlliste **Konfiguration für das folgende API-Projekt anzeigen** das API-Projekt aus, für das Sie die Multi-Faktor-Authentifizierung einrichten möchten.

4. Klappen Sie den Konfigurationsschlüssel **Multifaktor-Authentifizierung** auf.
5. In der Auswahlliste wählen Sie das Authentifizierungsmodul aus, das Sie verwenden möchten.
6. Klicken Sie **Übernehmen**.
7. Nehmen Sie eine der folgenden Aktionen vor:
    - Wenn Sie die Änderungen nur lokal übernehmen möchten, klicken Sie **Lokal übernehmen**.
    - Wenn Sie die Änderungen global übernehmen möchten, klicken Sie **Global übernehmen**.
8. Klicken Sie **Übernehmen**.

Anmeldung ohne Multi-Faktor-Authentifizierung

Sie können festlegen, welche Benutzer sich ohne Multi-Faktor-Authentifizierung an der Webanwendung anmelden können:

- Alle Benutzer können sich ohne Multi-Faktor-Authentifizierung an der Webanwendung anmelden.
- Benutzer mit IP-Adressen aus einem bestimmten IP-Adressbereich können sich ohne Multi-Faktor-Authentifizierung an der Webanwendung anmelden.

Benötigte Konfigurationsschlüssel:

- **Zugriff für Benutzer zulassen, die nicht für die Multi-Faktor-Authentifizierung registriert sind** (**VI_Common_AccessControl_AllowUnregistered**): Legt fest, ob Benutzer, die nicht für die Multi-Faktor-Authentifizierung registriert sind, auf die Webanwendung zugreifen dürfen.
- **MFA bypass IP address range** (**MfaAllowListIpAddressRange**): Benutzer mit den hier festgelegten IP-Adressen können sich ohne Multi-Faktor-Authentifizierung an der Webanwendung anmelden.

Um eine Anmeldung ohne Multi-Faktor-Authentifizierung für alle Benutzer zuzulassen

1. Melden Sie sich am Administration Portal an (siehe Am Administration Portal anmelden auf Seite 5).
2. In der Navigation klicken Sie **Konfiguration**.
3. In der Navigation klicken Sie **Konfiguration**.
4. Auf der Seite **Konfiguration** wählen Sie in der Auswahlliste **Konfiguration für das folgende API-Projekt anzeigen** das API-Projekt aus, für das Sie die Anmeldung ohne Multi-Faktor-Authentifizierung zulassen möchten.

5. Klappen Sie den Konfigurationsschlüssel **Zugriff für Benutzer zulassen, die nicht für die Multi-Faktor-Authentifizierung registriert sind** auf.
6. Aktivieren Sie das Kontrollkästchen **Zugriff für Benutzer zulassen, die nicht für die Multi-Faktor-Authentifizierung registriert sind**.
7. Klicken Sie **Übernehmen**.
8. Nehmen Sie eine der folgenden Aktionen vor:
   - Wenn Sie die Änderungen nur lokal übernehmen möchten, klicken Sie **Lokal übernehmen**.
   - Wenn Sie die Änderungen global übernehmen möchten, klicken Sie **Global übernehmen**.
9. Klicken Sie **Übernehmen**.

Um eine Anmeldung ohne Multi-Faktor-Authentifizierung für bestimmte IP-Adressen zuzulassen

1. Melden Sie sich am Administration Portal an (siehe Am Administration Portal anmelden auf Seite 5).
2. In der Navigation klicken Sie **Konfiguration**.
3. In der Navigation klicken Sie **Konfiguration**.
4. Auf der Seite **Konfiguration** wählen Sie in der Auswahlliste **Konfiguration für das folgende API-Projekt anzeigen** das API-Projekt **imx** aus.
5. Klappen Sie den Konfigurationsschlüssel **MFA bypass IP address range** auf.
6. Im Eingabefeld **Wert** geben Sie die entsprechenden IP-Adressen/Adressbereiche ein.

   Beispiel:

   ```
   192.168.0.10 -
   192.168.10.20,192.168.0.*,192.168.0.0/255.255.255.0,192.168.0.0/16,fe80:
   :/10,192.168.0.0
   ```

   TIPP: Sie können IP-Adressen auch als Classless Inter-Domain Routing (CIDR)-Notation angeben.
7. Klicken Sie **Übernehmen**.
8. Nehmen Sie eine der folgenden Aktionen vor:
   - Wenn Sie die Änderungen nur lokal übernehmen möchten, klicken Sie **Lokal übernehmen**.
   - Wenn Sie die Änderungen global übernehmen möchten, klicken Sie **Global übernehmen**.
9. Klicken Sie **Übernehmen**.

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

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

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

1. Starten Sie das Programm 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**.

Application Governance Modul konfigurieren

Mithilfe des Application Governance Moduls können Sie schnell und einfach den Onboarding-Prozess für neue Anwendungen zentral mit einem Tool durchführen. Eine mit dem Application Governance Modul erstellte Anwendung vereint alle Berechtigungen, die Benutzer der Anwendung für ihre tägliche Arbeit benötigen. So können Sie Ihrer Anwendung Berechtigungen und Rollen zuweisen und planen, ab wann diese als Leistungsposition zur Verfügung stehen (beispielsweise im Web Portal).

Verwandte Themen

- Berechtigungen konfigurieren auf Seite 16
- Hyperviews von Anwendungen befüllen auf Seite 17

Berechtigungen konfigurieren

Um Mitarbeitern zu ermöglichen, im Web PortalAnwendungen anzuzeigen, zu erstellen und zu verwalten sowie Bestellungen von Produkten von Anwendungen zu genehmigen, müssen Sie den Mitarbeitern bestimmte Anwendungsrollen zuweisen.

HINWEIS: Das Verwalten einer Anwendung umfasst Folgendes:

- Bearbeiten der Stammdaten der Anwendung und der zugewiesenen Berechtigungen und Rollen
- Zuweisen von Berechtigungen und Rollen zur Anwendung
- Aufheben der Zuweisungen von Berechtigungen und Rollen zur Anwendung
- Bereitstellen der Anwendung und der zugehörigen Berechtigungen und Rollen
- Aufheben der Bereitstellungen der Anwendung und der zugehörigen Berechtigungen und Rollen

Um Mitarbeitern eine Anwendungsrolle für Application Governance zuzuweisen

1. Starten Sie das Programm Manager.
2. Verbinden Sie sich mit der entsprechenden Datenbank.
3. Im unteren Bereich der Navigation klicken Sie die Kategorie **One Identity Manager Administration**.
4. Im oberen Bereich der Navigation klicken Sie die Anwendungsrolle, die Sie Mitarbeitern zuweisen möchten:
   - **Application Governance** | **Administratoren**: Mitglieder dieser Anwendungsrolle können im Web Portal neue Anwendungen erstellen und sämtliche Anwendungen verwalten.
   - **Application Governance** | **Eigentümer**: Wird diese Anwendungsrolle einer Anwendung als Eigentümer-Anwendungsrolle zugeordnet, können die Mitglieder diese Anwendung im Web Portal verwalten.
   - **Application Governance** | **Entscheider**: Wird diese Anwendungsrolle einer Anwendung als Entscheider-Anwendungsrolle zugeordnet, können die Mitglieder über Bestellungen von Produkten dieser Anwendung entscheiden (wenn das Entscheidungsverfahren **BE - Genehmiger einer Anwendung** verwendet wird).
5. Im Bereich **Aufgaben** klicken Sie die Aufgabe **Personen zuweisen**.
6. Im Bereich **Zuordnungen hinzufügen** doppelklicken Sie die Mitarbeiter, denen Sie die Anwendungsrolle zuweisen möchten.
7. Klicken Sie (**Speichern**).

Hyperviews von Anwendungen befüllen

Im Web Portal steht Benutzern für jede Anwendung eine Übersicht in Form eines Hyperviews zur Verfügung. Der Zeitplan **Befüllen der Anwendungsübersicht** sammelt alle Daten für dieses Hyperview und befüllt es damit.

Um den Zeitplan zum Befüllen des Hyperviews zu starten

1. Starten Sie das Programm Designer.
2. Verbinden Sie sich mit der entsprechenden Datenbank.
3. Im Designer in der Navigation klicken Sie die Kategorie **Basisdaten** > **Allgemein** > **Zeitpläne**.
4. In der Liste wählen Sie den Zeitplan **Befüllen der Anwendungsübersicht**.
5. Unter der Liste im Detailbereich des Zeitplans klicken Sie **Start**.
6. Bestätigen Sie die Sicherheitsabfrage mit **Ja**.

Um den Zeitplan zum Befüllen des Hyperviews zu bearbeiten

1. Starten Sie das Programm Designer.
2. Verbinden Sie sich mit der entsprechenden Datenbank.
3. Im Designer in der Navigation klicken Sie die Kategorie **Basisdaten** > **Allgemein** > **Zeitpläne**.
4. In der Liste wählen Sie den Zeitplan **Befüllen der Anwendungsübersicht**.
5. Unter der Liste im Detailbereich des Zeitplans bearbeiten Sie die Stammdaten des Zeitplans.

   Weitere Informationen zu Zeitplänen und deren Eigenschaften finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.
6. Wählen Sie den Menüeintrag **Datenbank** > **Übernahme in Datenbank** und klicken Sie **Speichern**.

Kennwortrücksetzungsportal konfigurieren

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

Authentifizierung am Kennwortrücksetzungsportal konfigurieren

Die Authentifizierung am Kennwortrücksetzungsportal unterscheidet sich von der Authentifizierung am Web Portal. Benutzer können sich über folgende Möglichkeiten am Kennwortrücksetzungsportal anmelden:

- Benutzer verwenden einen Zugangscode, den sie von Ihrem Manager erhalten haben (siehe Anmeldung am Kennwortrücksetzungsportal mit Zugangscode konfigurieren auf Seite 19).
- Benutzer beantworten ihre persönlichen Kennwortfragen (siehe Anmeldung am Kennwortrücksetzungsportal mit Kennwortfragen konfigurieren auf Seite 20).
- Benutzer verwenden Ihren Benutzernamen und das persönliche Kennwort.

Anmeldung am Kennwortrücksetzungsportal mit Zugangscode konfigurieren

Benutzer können einen Zugangscode verwenden, den sie von Ihrem Manager erhalten haben, um sich am Kennwortrücksetzungsportal anzumelden.

Um die Anmeldung mit einem Zugangscode zu konfigurieren

1. Verbinden Sie sich auf Ihren API Server.
2. Öffnen Sie die Datei `imxclient.exe.config` mit einem Texteditor.
3. Fügen Sie folgenden Eintrag hinzu:

```
<add name="QER\Person\PasswordResetAuthenticator\ApplicationToken"
connectionString="<API Server-Anwendungstoken>"/>
```

4. Speichern Sie Ihre Änderungen an der Datei.
5. (Optional) Verschlüsseln Sie die Datei.

Anmeldung am Kennwortrücksetzungsportal mit Kennwortfragen konfigurieren

Sollten Benutzer des Web Portals ihr Kennwort vergessen, so können sie sich mithilfe selbst festgelegter Kennwortfragen am Kennwortrücksetzungsportal anmelden und ein neues Kennwort setzen.

Um die Verwendung von Kennwortfragen zu konfigurieren

1. Starten Sie das Programm Designer.
2. Verbinden Sie sich mit der entsprechenden Datenbank.
3. 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.

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*.

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/

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

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/

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