One Identity Manager 9.2

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 - 29. September 2023, 03:00 Uhr

Die aktuellsten Versionen der Produktdokumentation finden Sie unter One Identity Manager Dokumentation.

Inhalt

1

Über dieses Handbuch

Dieses Handbuch liefert Administratoren und Webentwicklern Informationen zur Konfiguration und den Betrieb von Webanwendungen von 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 verwalten

Sie können den API Server sowie die dazugehörigen API-Projekte mithilfe des Administrationsportals konfigurieren und Informationen anzeigen.

Detaillierte Informationen zum Thema

Am Administrationsportal anmelden

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

Um sich am Administrationsportal anzumelden

1. In der Adresszeile Ihres Web-Browsers geben Sie die Web-Adresse (URL) des Administrationsportals ein.
2. Auf der Anmeldeseite des Administrationsportals 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**.

Informationen zum API Server anzeigen

Sie können verschiedenste Informationen des API Servers anzeigen. Sie können eine Übersicht zum API Server anzeigen, die allgemeine Informationen und eine Übersicht der Plugins enthält. Zusätzlich können Sie alle Pakete anzeigen, die der API Server enthält.

Um eine Übersicht des API Servers anzuzeigen

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
2. In der Navigation klicken Sie **Übersicht**.

Um alle Pakete des API Servers anzuzeigen

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
2. In der Navigation klicken Sie **Pakete**.

Konfiguration von API-Projekten einsehen und bearbeiten

Sobald Sie sich am Administrationsportal angemeldet haben, können Sie die Konfiguration der einzelnen API-Projekte einsehen und bearbeiten.

Detaillierte Informationen zum Thema

- Konfigurationsschlüssel bearbeiten auf Seite 7
- Kundenspezifische Einstellungen von API-Projekten anzeigen auf Seite 8
- Kundenspezifische Einstellungen von API-Projekten verwerfen auf Seite 9
- Lokale Änderungen in globale Änderungen umwandeln auf Seite 9

Verwandte Themen

- API-Projekte und Webanwendungen konfigurieren auf Seite 11

Konfigurationsschlüssel bearbeiten

Sie können die Konfiguration von API-Projekten mithilfe von Konfigurationsschlüsseln bearbeiten.

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 Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 nach einen Konfigurationsschlüssel zu suchen, 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**.

Kundenspezifische Einstellungen von API-Projekten anzeigen

Um sich einen Überblick über bereits erfolgte Anpassungen zu verschaffen, können Sie alle kundenspezifischen Einstellungen eins API-Projekts anzeigen.

Um alle kundenspezifischen Einstellungen eines API-Projekts anzuzeigen

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 ▼ (**Filtern**).
5. Im Kontextmenü aktivieren Sie das Kontrollkästchen **Kundenspezifische Einstellungen**.

Kundenspezifische Einstellungen von API-Projekten verwerfen

Sie können alle kundenspezifischen Einstellungen eins API-Projekts rückgängig machen.

Um alle kundenspezifischen Änderungen eines API-Projekts zu verwerfen

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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**.

Lokale Änderungen in globale Änderungen umwandeln

Um Änderungen, die bisher nur lokal für einen API Server angewendet werden, an alle API Server zu verteilen, können Sie lokale Änderungen in globale Änderungen umwandeln. Dabei werden die Änderungen in der globalen Konfigurationsdatei gespeichert.

Um lokale Änderungen in globale Änderungen umzuwandeln

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 lokale Änderungen Sie in globale Änderungen umwandeln möchten.
4. Klicken Sie ⋮ **Aktionen** > **Lokal angepasste Einstellungen in globale Einstellungen umwandeln**.
5. Im Bereich **Lokal angepasste Einstellungen in globale Einstellungen umwandeln** klicken Sie **Umwandeln**.

Verschlüsselung ändern

Sie können die verwendete Verschlüsselung von Daten ändern, indem Sie ein anderes Verschlüsselungszertifikat verwenden.

Um das Verschlüsselungszertifikat zu ändern

1. Im Installationsverzeichnis des API Servers öffnen Sie die Datei `web.config`.

   HINWEIS: Falls die Datei verschlüsselt ist, entschlüsseln Sie zuerst die Datei.

2. Ändern Sie den Wert der Eigenschaft `certificatethumbprint` auf den Thumbprint des Zertfikats, das Sie verwenden möchten.
3. Speichern Sie Ihre Änderungen an der Datei.

   HINWEIS: Falls die Datei vorher verschlüsselt war, verschlüsseln Sie die Datei erneut.

API-Projekte und Webanwendungen konfigurieren

Sie können Einstellungen für verschiedene API-Projekte (beziehungsweise Webanwendungen) vornehmen.

Detaillierte Informationen zum Thema

Authentifizierung konfigurieren

Die Authentifizierung von Benutzern am API Server erfolgt pro API-Projekt.

Die Authentifizierung erfolgt in zwei Schritten:

1. Erforderliche primäre Authentifizierung: Standard-Authentifizierung über ein Authentifizierungsmodul
2. Optionale sekundäre Authentifizierung: Multifaktor-Authentifizierung (über OneLogin)

Weitere Informationen zur Authentifizierung finden Sie im *One Identity Manager API-Entwicklungshandbuch* und im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Detaillierte Informationen zum Thema

- Primäre Authentifizierung mit Single Sign-on konfigurieren auf Seite 12
- Multifaktor-Authentifizierung konfigurieren auf Seite 13
- Authentifizierungstoken konfigurieren auf Seite 14

Primäre Authentifizierung mit Single Sign-on konfigurieren

Sie können für API-Projekte die Authentifizierung mit Single Sign-on über das Administrationsportal konfigurieren. In diesem Fall ist keine eigene Anfrage an die Methode **imx/login** erforderlich.

Benötigte Konfigurationsschlüssel:

- **Single-Sign-on-Authentifizierungsmodule** (**SsoAuthentifiers**): Legt fest, welche Authentifizierungsmodule für Single Sign-on verwendet werden.

Um die Authentifizierung mit Single Sign-on zu konfigurieren

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 Authentifizierung mit Single Sign-on konfigurieren möchten.
4. Klappen Sie den Konfigurationsschlüssel **Single-Sign-on-Authentifizierungsmodule** auf.
5. Klicken Sie **Neu**.
6. In der Auswahlliste wählen Sie das Authentifizierungsmodul aus, das Sie verwenden möchten.

   TIPP: Sie können weitere Authentifizierungsmodule festlegen. Klicken Sie dazu **Neu**.
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**.

Multifaktor-Authentifizierung konfigurieren

Für Attestierungen oder die Entscheidung von Bestellungen kann die Multifaktor-Authentifizierung mit OneLogin eingerichtet werden.

Voraussetzung

- Das OneLogin Modul ist vorhanden und die Synchronisation ist eingerichtet.

Ausführliche Informationen zum Einrichten der Multifaktor-Authentifizierung finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*. Ausführliche Informationen zum Einrichten und Starten der Synchronisation mit einer OneLogin Domäne finden Sie im *One Identity Manager Administrationshandbuch für die Integration mit OneLogin Cloud Directory*.

Um die Multifaktor-Authentifizierung mit OneLogin zu konfigurieren

1. Im Administrationsportal setzen Sie den Konfigurationsschlüssel `ServerConfig/ITShopConfig/StepUpAuthenticationProvider` auf den Wert **OneLogin MFA**.
    a. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
    b. In der Navigation klicken Sie **Konfiguration**.
    c. Auf der Seite **Konfiguration** wählen Sie in der Auswahlliste **Konfiguration für das folgende API-Projekt anzeigen** das API-Projekt aus, für das Sie die Multifaktor-Authentifizierung konfigurieren möchten.
    d. Klappen Sie den Konfigurationsschlüssel **Bestell-Konfiguration / Zusätzliche Authentifizierung für die Zustimmung zu Nutzungsbedingungen sowie Workflow-Entscheidungen** auf.
    e. In der Auswahlliste wählen Sie **OneLogin MFA**.
    f. Klicken Sie **Übernehmen**.
    g. 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**.
    h. Klicken Sie **Übernehmen**.
2. Stellen Sie sicher, dass die Authentifizierungsdaten zur Anmeldung an der OneLogin Domäne vorhanden sind. Die Authentifizierungsdaten können Sie bei der Installation des API Servers mit dem Web Installer einrichten oder nachträglich anpassen. Ausführliche Informationen finden Sie im *One Identity Manager Installationshandbuch*.

Authentifizierungstoken konfigurieren

Benutzer erhalten nach erfolgreicher Authentifizierung an einer Webanwendung ein Authentifizierungstoken. Solange dieses Token gültig ist, müssen sich Benutzer nicht erneut authentifizieren.

Benötigte Konfigurationsschlüssel:

- **Dauerhafte Authentifizierungstoken** (**AuthTokensEnabled**): Legt fest, ob dauerhafte Authentifizierungs-Tokens verwendet werden sollen, die zwischen Sitzungen aufbewahrt werden.
- **Gültigkeitsdauer von dauerhaften Authentifizierungstoken (in Minuten)** (**AuthTokensLifetimeMinutes**): Legt fest, wie lange dauerhafte Authentifizierungstoken gültig sind.

Um die Verwendung von Authentifizierungstoken zu konfigurieren

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 **API Server** aus.
4. Konfigurieren Sie die folgenden Konfigurationsschlüssel:
    - **Dauerhafte Authentifizierungstoken**: Legen Sie fest, ob dauerhafte Authentifizierungstoken verwendet werden soll. Aktivieren oder deaktivieren Sie dazu das entsprechende Kontrollkästchen.
    - **Gültigkeitsdauer von dauerhaften Authentifizierungstoken (in Minuten)**: Legen Sie fest, wie viele Minuten dauerhafte Authentifizierungstoken gültig sind. Nach Ablauf der Gültigkeit, muss sich der Benutzer wieder authentifizieren.
5. Klicken Sie **Übernehmen**.
6. 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**.
7. Klicken Sie **Übernehmen**.

Selbstregistrierung neuer Benutzer konfigurieren

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

HINWEIS: Um diese Funktion nutzen zu können, muss der neue Benutzer eine E-Mail-Adresse angeben (können), da ansonsten keine Bestätigungs-E-Mail versendet werden kann.

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

HINWEIS: Wie ein Benutzer sich selbst registriert beziehungsweise ein neues Benutzerkonto erstellt, erfahren Sie im *One Identity Manager Web Portal Anwenderhandbuch*.

Um die Selbstregistrierung zu konfigurieren

1. Starten Sie das Programm Designer.
2. Verbinden Sie sich mit der entsprechenden Datenbank.
3. Konfigurieren Sie die folgenden Konfigurationsparameter:

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

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

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

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

     TIPP: Die eigentliche Mail-Vorlage können Sie im Designer in der Kategorie **Mailvorlagen** > **Person** konfigurieren. Ausführliche Informationen zu Mail-Vorlagen finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.
   - **QER** | **Attestation** | **ApproveNewExternalUsers**: Legen Sie fest, ob selbstregistrierte Benutzer attestiert werden müssen, bevor sie aktiviert werden. Ein Manager entscheidet dann über die Registrierung des

neuen Benutzers.

- **QER** | **Attestation** | **NewExternalUserTimeoutInHours**: Legen Sie fest, wie viele Stunden der Bestätigungs-Link für neue selbstregistrierte Benutzer gültig ist.
- **QER** | **Attestation** | **NewExternalUserFinalTimeoutInHours**: Legen Sie fest, nach wie viele Stunden die Selbstregistrierung neuer Benutzer abgebrochen wird, sofern die Registrierung noch nicht erfolgreich abgeschlossen wurde.

4. Weisen Sie der Anwendungsrolle **Identity & Access Governance | Attestierung | Attestierer für externe Benutzer** mindestens eine Identität zu.
5. Stellen Sie sicher, dass ein Anwendungstoken vorhanden ist. Das Anwendungstoken setzen Sie bei der Installation des API Servers mit dem Web Installer. Ausführliche Informationen finden Sie im *One Identity Manager Installationshandbuch*.

   Das Anwendungstoken wird in der Datenbank im Konfigurationsparameter **QER | Person | PasswordResetAuthenticator | ApplicationToken** als Hashwert gespeichert und in der Datei `web.config` des API Servers verschlüsselt abgelegt.
6. Stellen Sie sicher, dass ein Benutzer konfiguriert ist, mit dem die neuen Benutzerkonten erstellt werden. Den Benutzer und die Authentifizierungsdaten können Sie bei der Installation des API Servers mit dem Web Installer einrichten oder nachträglich anpassen. Ausführliche Informationen finden Sie im *One Identity Manager Installationshandbuch*.

   HINWEIS: Es wird empfohlen, den Systembenutzer **IdentityRegistration** zu verwenden. Der Systembenutzer **IdentityRegistration** hat die vorgegebenen Berechtigungen, die für die Selbstregistrierung neuer Benutzer im Kennwortrücksetzungsportal benötigt werden. Wenn Sie einen benutzerdefinierten Systembenutzer benötigen, stellen Sie sicher, dass dieser die erforderlichen Berechtigungen besitzt. Ausführliche Informationen zu Systembenutzern und Berechtigungen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

Logo konfigurieren

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 zu konfigurieren

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 **API Server** 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 für HTML-Anwendungen** 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**.

Oberflächensprache für Benutzer konfigurieren

Sie können festlegen, welche Spracheinstellung für die Oberfläche von Webanwendungen für Benutzer verwendet werden soll.

Benötigte Konfigurationsschlüssel:

- **Sprache aus den Profil-Einstellungen als Oberflächensprache verwenden** (**UseProfileCulture**): Legt fest, ob die in den Profil-Einstellungen des Benutzers festgelegte Sprache als Oberflächensprache verwendet werden soll oder die Sprache des verwendeten Browsers.

Um die Oberflächensprache für Benutzer zu konfigurieren

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 Oberflächensprache konfigurieren möchten.
4. Klappen Sie den Konfigurationsschlüssel **Sprache aus den Profil-Einstellungen als Oberflächensprache verwenden** auf.
5. Nehmen Sie eine der folgenden Aktionen vor:
    - Um die in den Profil-Einstellungen des Benutzers festgelegte Sprache als Oberflächensprache zu verwenden, aktivieren Sie das Kontrollkästchen.
    - Um die Sprache des Browsers des Benutzers als Oberflächensprache zu verwenden, deaktivieren Sie das Kontrollkästchen.
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**.

Webanwendungen ohne Menüleiste verwenden

Der sogenannte "Headless"-Modus ermöglicht es Ihnen, Webanwendungen oder Teile davon ohne Menüleiste in Ihre eigenen Anwendungen einzubinden (beispielsweise in einem iFrame), sofern diese bereits die Navigation zur Verfügung stellen.

Um eine Webanwendung im Headless-Modus zu verwenden

Verwenden Sie für URLs, die Sie in Ihre Anwendung einbinden möchten, das Format https://<Server-Name>/<Applikationsname>/#/headless/.

Beispiel

```
https://ExampleServer/ApiServer/html/qer-app-portal/#/headless/dashboard
```

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 auf Seite 19
- Application Governance Modul konfigurieren auf Seite 20
- Helpdeskmodul/Tickets konfigurieren auf Seite 21
- Software konfigurieren auf Seite 24
- Leistungspositionen konfigurieren auf Seite 25
- Geräte konfigurieren auf Seite 26

Bestellfunktionen konfigurieren

Sie können Bestellfunktionen des Web Portals über das **Administrationsportal** konfigurieren.

Detaillierte Informationen zum Thema

- Bestellung nach Referenzbenutzer konfigurieren auf Seite 19

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 Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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**.

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 20
- Hyperviews von Anwendungen befüllen auf Seite 21

Berechtigungen konfigurieren

Um Identitäten zu ermöglichen, im Web Portal Anwendungen anzuzeigen, zu erstellen und zu verwalten sowie Bestellungen von Produkten von Anwendungen zu genehmigen, weisen Sie den entsprechenden Identitäten folgende Anwendungsrollen zu:

- **Application Governance** | **Administratoren**
- **Application Governance** | **Eigentümer**
- **Application Governance** | **Entscheider**

Weitere Informationen zu den Anwendungsrollen und wie Sie diese Identitäten zuweisen finden Sie im *One Identity Manager Handbuch zur Autorisierung und Authentifizierung*.

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

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. Sie können diesen Zeitplan starten und bearbeiten.

Weitere Informationen zu Zeitplänen und deren Eigenschaften finden Sie im *One Identity Manager Administrationshandbuch für betriebsunterstützende Aufgaben*.

Helpdeskmodul/Tickets konfigurieren

Sie können das Helpdeskmodul/Tickets über das **Administrationsportal** konfigurieren.

Weitere Informationen zum Helpdeskmodul/Tickets erhalten Sie im *One Identity Manager Web Portal Anwenderhandbuch* und im *One Identity Manager Anwenderhandbuch für das Helpdeskmodul*.

Detaillierte Informationen zum Thema

- Bearbeitbare Eigenschaften für das Erstellen von Tickets konfigurieren auf Seite 21
- Bearbeitbare Eigenschaften von Tickets konfigurieren auf Seite 22
- Dateitypen für Ticketanhänge konfigurieren auf Seite 23

Bearbeitbare Eigenschaften für das Erstellen von Tickets konfigurieren

Sie können festlegen, welche Eigenschaften Benutzer beim Erstellen von Tickets angeben können.

Benötigte Konfigurationsschlüssel:

- **Eigenschaften-Editoren / Primär bearbeitbare Eigenschaften / TroubleTicket** (

ServerConfig/OwnershipConfig/PrimaryFields/TroubleTicket): Legt fest, welche Eigenschaften Benutzer beim Erstellen von Tickets angeben können.

Um bearbeitbare Eigenschaften beim Erstellen von Tickets zu konfigurieren

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 **Web Portal** aus.
4. Klappen Sie den Konfigurationsschlüssel **Eigenschaften-Editoren / Primär bearbeitbare Eigenschaften / TroubleTicket** auf.
5. Sie können folgende Aktionen vornehmen:
    - Um eine Eigenschaft hinzuzufügen, klicken Sie **Neu** und wählen Sie in der Auswahlliste die entsprechende Eigenschaft aus.
    - Um eine bestehende Eigenschaft zu ändern, wählen Sie in der entsprechenden Auswahlliste eine Eigenschaft aus.
    - Um eine bestehende Eigenschaft zu entfernen, klicken Sie neben der entsprechenden Eigenschaft auf 🗑 (**Löschen**).
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**.

Bearbeitbare Eigenschaften von Tickets konfigurieren

Sie können festlegen, welche Eigenschaften Benutzer beim Bearbeiten von Tickets ändern können.

Benötigte Konfigurationsschlüssel:

- **Eigenschaften-Editoren / Bearbeitbare Eigenschaften / TroubleTicket** (**ServerConfig/OwnershipConfig/EditableFields/TroubleTicket**): Legt fest, welche Eigenschaften Benutzer beim Bearbeiten von Tickets bearbeiten können.

Um bearbeitbare Eigenschaften von Tickets zu konfigurieren

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 **Web Portal** aus.
4. Klappen Sie den Konfigurationsschlüssel **Eigenschaften-Editoren / Bearbeitbare Eigenschaften / TroubleTicket** auf.
5. Sie können folgende Aktionen vornehmen:
    - Um eine Eigenschaft hinzuzufügen, klicken Sie **Neu** und wählen Sie in der Auswahlliste die entsprechende Eigenschaft aus.
    - Um eine bestehende Eigenschaft zu ändern, wählen Sie in der entsprechenden Auswahlliste eine Eigenschaft aus.
    - Um eine bestehende Eigenschaft zu entfernen, klicken Sie neben der entsprechenden Eigenschaft auf 🗑 (**Löschen**).
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**.

Dateitypen für Ticketanhänge konfigurieren

Sie können festlegen, welche Dateitypen für Ticketanhänge zugelassen sind. Benutzer können nur Dateien dieser Typen an Tickets anhängen.

Benötigte Konfigurationsschlüssel:

- **Dateitypen für Ticketanhänge** (**AttachmentFileTypes**): Legt fest, welche Dateitypen für Ticketanhänge zugelassen sind.

Um Dateitypen für Ticketanhänge zu konfigurieren

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 **Web Portal** aus.
4. Klappen Sie den Konfigurationsschlüssel **Dateitypen für Ticketanhänge** auf.
5. Sie können folgende Aktionen vornehmen:
    - Um einen Dateitypen hinzuzufügen, klicken Sie **Neu** und geben Sie im Eingabefeld den Dateitypen im Format **.<Dateityp>** ein (beispielsweise **.png**)

- Um einen bestehenden Dateitypen zu ändern, klicken Sie in das entsprechende Eingabefeld und ändern Sie den Wert.
- Um einen bestehenden Dateitypen zu entfernen, klicken Sie neben dem entsprechenden Dateitypen auf 🗑 (**Löschen**).

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**.

Software konfigurieren

Sie können Software über das **Administrationsportal** konfigurieren.

Detaillierte Informationen zum Thema

- Bearbeitbare Eigenschaften von Software konfigurieren auf Seite 24

Bearbeitbare Eigenschaften von Software konfigurieren

Sie können festlegen, welche Eigenschaften Benutzer beim Bearbeiten von Software ändern können.

Benötigte Konfigurationsschlüssel:

- **Eigenschaften-Editoren / Bearbeitbare Eigenschaften / Application** (**Server-Config/OwnershipConfig/EditableFields/Application**): Legt fest, welche Eigenschaften von Software Benutzer bearbeiten können.

Um bearbeitbare Eigenschaften von Software zu konfigurieren

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 **Web Portal** aus.
4. Klappen Sie den Konfigurationsschlüssel **Eigenschaften-Editoren / Bearbeitbare Eigenschaften / Application** auf.
5. Sie können folgende Aktionen vornehmen:

- Um eine Eigenschaft hinzuzufügen, klicken Sie **Neu** und wählen Sie in der Auswahlliste die entsprechende Eigenschaft aus.
- Um eine bestehende Eigenschaft zu ändern, wählen Sie in der entsprechenden Auswahlliste eine Eigenschaft aus.
- Um eine bestehende Eigenschaft zu entfernen, klicken Sie neben der entsprechenden Eigenschaft auf (**Löschen**).

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**.

Leistungspositionen konfigurieren

Sie können Leistungspositionen über das **Administrationsportal** konfigurieren.

Detaillierte Informationen zum Thema

- Bearbeitbare Eigenschaften von Leistungspositionen konfigurieren auf Seite 25

Bearbeitbare Eigenschaften von Leistungspositionen konfigurieren

Sie können festlegen, welche Eigenschaften Benutzer beim Bearbeiten von Leistungspositionen ändern können.

Benötigte Konfigurationsschlüssel:

- **Eigenschaften-Editoren / Bearbeitbare Eigenschaften / AccProduct** (**Server-Config/OwnershipConfig/EditableFields/AccProduct**): Legt fest, welche Eigenschaften von Leistungspositionen Benutzer bearbeiten können.

Um bearbeitbare Eigenschaften von Leistungspositionen zu konfigurieren

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 **Web Portal** aus.

4. Klappen Sie den Konfigurationsschlüssel **Eigenschaften-Editoren / Bearbeitbare Eigenschaften / AccProduct** auf.
5. Sie können folgende Aktionen vornehmen:
    - Um eine Eigenschaft hinzuzufügen, klicken Sie **Neu** und wählen Sie in der Auswahlliste die entsprechende Eigenschaft aus.
    - Um eine bestehende Eigenschaft zu ändern, wählen Sie in der entsprechenden Auswahlliste eine Eigenschaft aus.
    - Um eine bestehende Eigenschaft zu entfernen, klicken Sie neben der entsprechenden Eigenschaft auf 🗑 (**Löschen**).
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**.

Geräte konfigurieren

Sie können Geräte über das **Administrationsportal** konfigurieren.

Detaillierte Informationen zum Thema

- Bearbeitbare Eigenschaften von Geräten konfigurieren auf Seite 26

Bearbeitbare Eigenschaften von Geräten konfigurieren

Sie können festlegen, welche Eigenschaften Benutzer beim Bearbeiten von Geräten ändern können.

Benötigte Konfigurationsschlüssel:

- **Bearbeitbare Eigenschaften für Geräte (Computer)** (**VI_Hardware_Fields_PC**): Legt fest, welche Eigenschaften von Computern Benutzer bearbeiten können.
- **Bearbeitbare Eigenschaften für Geräte (Server)** (**VI_Hardware_Fields_SRV**): Legt fest, welche Eigenschaften von Servern Benutzer bearbeiten können.
- **Bearbeitbare Eigenschaften für Geräte (Mobiltelefon)** (**VI_Hardware_Fields_MP**): Legt fest, welche Eigenschaften von Mobiltelefonen Benutzer bearbeiten können.

- **Bearbeitbare Eigenschaften für Geräte (Tablet)** (**VI_Hardware_Fields_TAB**): Legt fest, welche Eigenschaften von Tablets Benutzer bearbeiten können.
- **Bearbeitbare Eigenschaften für Geräte (Drucker)** (**VI_Hardware_Fields_PR**): Legt fest, welche Eigenschaften von Druckern Benutzer bearbeiten können.
- **Bearbeitbare Eigenschaften für Geräte (Bildschirm)** (**VI_Hardware_Fields_MO**): Legt fest, welche Eigenschaften von Bildschirmen Benutzer bearbeiten können.
- **Bearbeitbare Eigenschaften für Geräte (Standard)** (**VI_Hardware_Fields_Default**): Legt fest, welche Eigenschaften von Standardgeräten Benutzer bearbeiten können.

Um bearbeitbare Eigenschaften von Leistungspositionen zu konfigurieren

1. Melden Sie sich am Administrationsportal an (siehe Am Administrationsportal anmelden auf Seite 6).
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 **Web Portal** aus.
4. Klappen Sie einen der folgenden Konfigurationsschlüssel auf:
    - **Bearbeitbare Eigenschaften für Geräte (Computer)**
    - **Bearbeitbare Eigenschaften für Geräte (Server)**
    - **Bearbeitbare Eigenschaften für Geräte (Mobiltelefon)**
    - **Bearbeitbare Eigenschaften für Geräte (Tablet)**
    - **Bearbeitbare Eigenschaften für Geräte (Drucker)**
    - **Bearbeitbare Eigenschaften für Geräte (Bildschirm)**
    - **Bearbeitbare Eigenschaften für Geräte (Standard)**
5. Sie können folgende Aktionen vornehmen:
    - Um eine Eigenschaft hinzuzufügen, klicken Sie **Neu** und wählen Sie in der Auswahlliste die entsprechende Eigenschaft aus.
    - Um eine bestehende Eigenschaft zu ändern, wählen Sie in der entsprechenden Auswahlliste eine Eigenschaft aus.
    - Um eine bestehende Eigenschaft zu entfernen, klicken Sie neben der entsprechenden Eigenschaft auf 🗑 (**Löschen**).
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**.

Kennwortrücksetzungsportal konfigurieren

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

Detaillierte Informationen zum Thema

- Authentifizierung am Kennwortrücksetzungsportal konfigurieren auf Seite 28

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 28).
- Benutzer beantworten ihre persönlichen Kennwortfragen (siehe Anmeldung am Kennwortrücksetzungsportal mit Kennwortfragen konfigurieren auf Seite 29).
- Benutzer verwenden Ihren Benutzernamen und das persönliche Kennwort.

Detaillierte Informationen zum Thema

- Anmeldung am Kennwortrücksetzungsportal mit Zugangscode konfigurieren auf Seite 28
- Anmeldung am Kennwortrücksetzungsportal mit Kennwortfragen konfigurieren auf Seite 29

Anmeldung am Kennwortrücksetzungsportal mit Zugangscode konfigurieren

HINWEIS: Dieser Schritt ist nur erforderlich, wenn sie das ImxClient-Kommandozeilenprogramm nutzen, um einen API Server lokal zu hosten. Ausführliche Informationen zum ImxClient-Kommandozeilenprogramm finden Sie im *One Identity Manager API-Entwicklungshandbuch.*

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. Im Installationsverzeichnis des API Servers öffnen Sie die Datei `imxclient.exe.config`.

   HINWEIS: Falls die Datei verschlüsselt ist, entschlüsseln Sie zuerst die Datei.

2. Fügen Sie folgenden Eintrag hinzu:

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

3. Speichern Sie Ihre Änderungen an der Datei.

   HINWEIS: Falls die Datei vorher verschlüsselt war, verschlüsseln Sie die Datei erneut.

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:

   TIPP: 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 sich nicht mithilfe Ihrer Kennwortfragen am Kennwortrücksetzungsportal anmelden.

     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 sich am Kennwortrücksetzungsportal anmelden können.

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

- **QER** | **Person** | **PasswordResetAuthenticator** | **InvalidateUsedQuery**: Legen Sie fest, ob Benutzer neue Kennwortfragen und Antworten festlegen müssen, nachdem sie sich mithilfe Ihrer Kennwortfragen erfolgreich am Kennwortrücksetzungsportal angemeldet haben. Ist diese Option aktiviert, werden richtig beantwortete Kennwortfragen nach der Anmeldung am Kennwortrücksetzungsportal 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/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 hier.

Detaillierte Informationen zum Thema

- https://blogs.technet.microsoft.com/exchange/2015/07/27/exchange-tls-ssl-best-practices/
- https://support.microsoft.com/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 Kunden von One Identity 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