



One Identity Manager

Konfigurationshandbuch für Webanwendungen

Copyright 2022 One Identity LLC.

ALLE RECHTE VORBEHALTEN.

Diese Anleitung enthält urheberrechtlich geschützte Informationen. Die in dieser Anleitung beschriebene Software wird unter einer Softwarelizenz oder einer Geheimhaltungsvereinbarung bereitgestellt. Diese Software darf nur in Übereinstimmung mit den Bestimmungen der geltenden Vereinbarung verwendet oder kopiert werden. Kein Teil dieser Anleitung darf ohne die schriftliche Erlaubnis von One Identity LLC in irgendeiner Form oder mit irgendwelchen Mitteln, elektronisch oder mechanisch reproduziert oder übertragen werden, einschließlich Fotokopien und Aufzeichnungen für irgendeinen anderen Zweck als den persönlichen Gebrauch des Erwerbers.

Die Informationen in diesem Dokument werden in Verbindung mit One Identity Produkten bereitgestellt. Durch dieses Dokument oder im Zusammenhang mit dem Verkauf von One Identity LLC Produkten wird keine Lizenz, weder ausdrücklich oder stillschweigend, noch durch Duldung oder anderweitig, an jeglichem geistigen Eigentumsrecht eingeräumt. MIT AUSNAHME DER IN DER LIZENZVEREINBARUNG FÜR DIESES PRODUKT GENANNTEN BEDINGUNGEN ÜBERNIMMT ONE IDENTITY KEINERLEI HAFTUNG UND SCHLIESST JEGLICHE AUSDRÜCKLICHE, IMPLIZIERTE ODER GESETZLICHE GEWÄHRLEISTUNG ODER GARANTIE IN BEZUG AUF IHRE PRODUKTE AUS, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF DIE IMPLIZITE GEWÄHRLEISTUNG DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG VON RECHTEN. IN KEINEM FALL HAFTET ONE IDENTITY FÜR JEGLICHE DIREKTE, INDIREKTE, FOLGE-, STÖRUNGS-, SPEZIELLE ODER ZUFÄLLIGE SCHÄDEN (EINSCHLIESSLICH, OHNE EINSCHRÄNKUNG, SCHÄDEN FÜR VERLUST VON GEWINNEN, GESCHÄFTSUNTERBRECHUNGEN ODER VERLUST VON INFORMATIONEN), DIE AUS DER NUTZUNG ODER UNMÖGLICHKEIT DER NUTZUNG DIESES DOKUMENTS RESULTIEREN, SELBST WENN ONE IDENTITY AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN HAT. One Identity übernimmt keinerlei Zusicherungen oder Garantien hinsichtlich der Richtigkeit und Vollständigkeit des Inhalts dieses Dokuments und behält sich das Recht vor, Änderungen an Spezifikationen und Produktbeschreibungen jederzeit ohne vorherige Ankündigung vorzunehmen. One Identity verpflichtet sich nicht, die in diesem Dokument enthaltenen Informationen zu aktualisieren.

Wenn Sie Fragen zu Ihrer potenziellen Nutzung dieses Materials haben, wenden Sie sich bitte an:

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Besuchen Sie unsere Website (<http://www.OneIdentity.com>) für regionale und internationale Büro-Adressen.


Patente

One Identity ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente und anhängige Patente gelten. Für die aktuellsten Informationen über die geltenden Patente für dieses Produkt besuchen Sie bitte unsere Website unter <http://www.OneIdentity.com/legal/patents.aspx>.

Marken

One Identity und das One Identity Logo sind Marken und eingetragene Marken von One Identity LLC. in den USA und anderen Ländern. Für eine vollständige Liste der One Identity Marken besuchen Sie bitte unsere Website unter www.OneIdentity.com/legal. Alle anderen Marken sind Eigentum der jeweiligen Besitzer.

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.

Inhalt

Über dieses Handbuch	5
API Server konfigurieren	6
Am Administration Portal anmelden	6
Konfiguration von API-Projekten einsehen und bearbeiten	7
Authentifizierung konfigurieren	8
Primäre Authentifizierung mit Single Sign-on konfigurieren	9
Multifaktor-Authentifizierung konfigurieren	10
Authentifizierungstoken konfigurieren	11
Verschlüsselung ändern	12
Allgemeine Konfiguration von Webanwendungen	13
Logo anpassen	13
Web Portal konfigurieren	15
Bestellfunktionen konfigurieren	15
Bestellung nach Referenzbenutzer konfigurieren	15
Selbstregistrierung neuer Benutzer konfigurieren	16
Application Governance Modul konfigurieren	19
Berechtigungen konfigurieren	19
Hyperviews von Anwendungen befüllen	20
Kennworrücksetzungsportal konfigurieren	22
Authentifizierung am Kennworrücksetzungsportal konfigurieren	22
Anmeldung am Kennworrücksetzungsportal mit Zugangscode konfigurieren	22
Anmeldung am Kennworrücksetzungsportal mit Kennwortfragen konfigurieren	23
Empfehlungen für einen sicheren Betrieb von Webanwendungen	25
HTTPS verwenden	25
HTTP-Anfragemethode TRACE abschalten	26
Unsichere Verschlüsselungsmechanismen abschalten	26
HTTP-Response-Header in Windows IIS entfernen	27
Über uns	28
Kontaktieren Sie uns	28

Technische Supportressourcen 28

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 konfigurieren

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

Detaillierte Informationen zum Thema

- [Am Administration Portal anmelden](#) auf Seite 6
- [Konfiguration von API-Projekten einsehen und bearbeiten](#) auf Seite 7

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](#) sowie lokale Änderungen in globale Änderungen [umwandeln](#).

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 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 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 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 ▼ (**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 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**.

Um lokale Änderungen in globale Änderungen umzuwandeln

1. Melden Sie sich am Administration Portal an (siehe [Am Administration Portal 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**.

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 9
- [Multifaktor-Authentifizierung konfigurieren](#) auf Seite 10

Primäre Authentifizierung mit Single Sign-on konfigurieren

Sie können für API-Projekte die Authentifizierung mit Single Sign-on über das Administration Portal 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 Administration Portal an (siehe [Am Administration Portal 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*.

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 Administration Portal an (siehe [Am Administration Portal 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. In der Konfigurationsdatei des API Servers fügen Sie die Verbindungsparameter zu Ihrer OneLogin Domäne hinzu.
 - a. Im Installationsverzeichnis des API Servers öffnen Sie die Datei `web.config`.
| **HINWEIS:** Falls die Datei verschlüsselt ist, entschlüsseln Sie zuerst die Datei.
 - b. Im Abschnitt `<connectionStrings>` fügen Sie folgenden Eintrag hinzu:

```
<add name="OneLogin"
connectionString="Domain=<domain>;ClientId=<clientid>;ClientSecret=<clientSecret>" />
```

- <domain> steht für den DNS Namen der synchronisierten OneLogin Domäne (OLGAPIDomain.DNSName).
 - <clientid> steht für die Client-ID der OneLogin Anwendung.
 - <clientSecret> steht für den Sicherheitstoken der OneLogin Anwendung.
- c. Speichern Sie Ihre Änderungen an der Datei.

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

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 Administration Portal an (siehe [Am Administration Portal 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 **imx** 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**.

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 Zertifikats, das Sie verwenden möchten.
3. Speichern Sie Ihre Änderungen an der Datei.
| **HINWEIS:** Falls die Datei vorher verschlüsselt war, verschlüsseln Sie die Datei erneut.

Allgemeine Konfiguration von Webanwendungen

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

Detaillierte Informationen zum Thema

- [Logo anpassen](#) auf Seite 13

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 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 **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 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**.

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 15
- [Selbstregistrierung neuer Benutzer konfigurieren](#) auf Seite 16

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 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**.

Selbstregistrierung neuer Benutzer konfigurieren

Noch nicht registrierte Benutzer haben im Kennworrücksetzungsportal die Möglichkeit sich für die Verwendung des Web Portals selbst zu registrieren und neue Konten 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 im Web Portal und des zugehörigen Attestierungsprozesses finden Sie im *One Identity Manager Administrationshandbuch für Attestierungen*.

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:

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

- **QER | WebPortal | PasswordResetURL:** Legen Sie die Web-Adresse des Kennworrücksetzungsportals 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. Im Installationsverzeichnis des API Servers öffnen Sie die Datei `web.config`.

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

6. Im Abschnitt `<connectionStrings>` fügen Sie folgenden Eintrag hinzu:

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

`<Anwendungstoken>` steht für das Anwendungstoken, das bei der Installation des API Servers gesetzt wurde.

7. Im Abschnitt <connectionStrings> fügen Sie folgenden Eintrag hinzu:

```
<add name="sub:register"
connectionString="Module=DialogUser;User=<BENUTZER>;
(Password)Password=<KENNWORT>" />
```

- <BENUTZER> steht für den Anmeldenamen des Benutzers, mit dem die neuen Benutzerkonten erstellt werden
- <KENNWORT> steht für das Kennwort des Benutzers

8. Speichern Sie Ihre Änderungen an der Datei.

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

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 19
- [Hyperviews von Anwendungen befüllen](#) auf Seite 20

Berechtigungen konfigurieren

Um Mitarbeitern zu ermöglichen, im Web Portal Anwendungen 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**.

Kennworrücksetzungsportal konfigurieren

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

Authentifizierung am Kennworrücksetzungsportal konfigurieren

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

- Benutzer verwenden einen Zugangscode, den sie von Ihrem Manager erhalten haben (siehe [Anmeldung am Kennworrücksetzungsportal mit Zugangscode konfigurieren](#) auf Seite 22).
- Benutzer beantworten ihre persönlichen Kennwortfragen (siehe [Anmeldung am Kennworrücksetzungsportal mit Kennwortfragen konfigurieren](#) auf Seite 23).
- Benutzer verwenden Ihren Benutzernamen und das persönliche Kennwort.

Anmeldung am Kennworrücksetzungsportal mit Zugangscode konfigurieren

Benutzer können einen Zugangscode verwenden, den sie von Ihrem Manager erhalten haben, um sich am Kennworrücksetzungsportal 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 Kennworrücksetzungsportal mit Kennwortfragen konfigurieren

Sollten Benutzer des Web Portals ihr Kennwort vergessen, so können sie sich mithilfe selbst festgelegter Kennwortfragen am Kennworrücksetzungsportal 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 Kennworrücksetzung 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](#) auf Seite 25
- [HTTP-Anfragemethode TRACE abschalten](#) auf Seite 26
- [Unsichere Verschlüsselungsmechanismen abschalten](#) auf Seite 26
- [HTTP-Response-Header in Windows IIS entfernen](#) auf Seite 27

HTTPS verwenden

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

Damit Webanwendungen das sichere Kommunikationsprotokoll 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 Windows IIS 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/>

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