

Apple BYOD Einschreibung

Version 14.04.2026 – Aktualisiert 22.04.2026

Übersicht

1	1. BYOD-Einschreibung - Übersicht.....	3
2	Voraussetzungen.....	3
	2.1 Identitäts- und Integrationsmodell.....	3
	2.2 Domänenkonfiguration im Apple Business Manager.....	5
	2.3 Benutzererstellung (Verwaltete Apple-IDs).....	8
	2.3.1 Manuelle Erstellung.....	8
	2.3.2 Massenerstellung - Entra ID und ABM.....	9
3	Gerät mit dem Standard-Einschreibungsassistenten hinzufügen.....	12
4	Gerät mit der kontogesteuerten Einschreibung hinzufügen.....	15
	4.1 Verwaltete Apple-ID einem Benutzer zuweisen.....	15
	4.1.1 Manuelle Zuweisung.....	15
	4.1.2 Automatisch mit Entra ID (datomo MDM- und Entra-Integration).....	15
	4.2 Konfiguration und Domäne vorbereiten.....	16
	4.2.1 Domäne in datomo MDM hinzufügen.....	17
	4.3 Einschreibungsvorgang.....	18

1 1. BYOD-Einschreibung - Übersicht

Auf Apple-Geräten basiert die BYOD-Einschreibung auf dem User-Enrollment-Modell, das für private Geräte konzipiert wurde. Dieser Ansatz gewährleistet einen sicheren Zugriff auf Unternehmensressourcen und sorgt gleichzeitig für eine strikte Trennung zwischen organisationsbezogenen und persönlichen Daten.

Die Benutzereinschreibung erfordert eine Verwaltete Apple-ID, die die Unternehmensidentität auf dem Gerät etabliert. Während der Einschreibung werden verwaltete Daten kryptografisch von persönlichen Daten getrennt und automatisch gelöscht, wenn das Gerät aus der Verwaltung entfernt wird.

datomo MDM stellt einen Standard-Einschreibungsassistenten bereit, der eine schnelle Geräteregistrierung per E-Mail-Einladung, Telefonnummer oder QR-Code ermöglicht. Diese Einschreibungsmethode wird für Geräte mit iOS 13 bis iOS 17.x unterstützt.

Bei neueren Apple-Versionen ab iOS 17.x oder höher muss die BYOD-Einschreibung direkt auf dem Gerät gestartet werden. Die Einschreibung muss über

Einstellungen -> Allgemein mit der Option 'Bei Schul- oder Unternehmenskonto anmelden...' gestartet werden, wobei die entsprechende Domäne zuvor konfiguriert sein muss.

Für die Masseneinschreibung von Apple-Geräten finden Sie weitergehende Informationen in Apple-DEP-Dokumentation.

2 Voraussetzungen

2.1 Identitäts- und Integrationsmodell

Beim Standard-Einschreibungsassistenten werden die meisten dieser Abhängigkeiten innerhalb des Einschreibungsablaufs behandelt und sind für den Administrator möglicherweise nicht sichtbar, da der Prozess den Benutzer Schritt für Schritt durch den Assistenten führt.

Bei der kontogesteuerten Einschreibung (Account Driven Enrollment, ADE) müssen diese Beziehungen explizit konfiguriert werden, weshalb das Verständnis dieses Modells unerlässlich ist.

Die BYOD-ADE-Einschreibung umfasst drei unabhängige Systeme:

- o Apple Business Manager (Verwaltete Apple-IDs)
- o datomo MDM (Geräteverwaltung und Benutzerzuweisung)
- o (Optional) Identitätsanbieter wie Microsoft Entra ID oder Google Workspace

Diese Systeme können je nach Unternehmenskonfiguration unabhängig voneinander betrieben oder integriert werden.

Grundprinzipien:

- o Dieselbe Verwaltete Apple-ID muss einheitlich verwendet werden:
 - im Apple Business Manager (als Verwaltete Apple-ID) und
 - in datomo MDM (als Benutzer-E-Mail-Adresse).
- o Die Integration mit einem Identitätsanbieter ist optional.
- o Jede Integration kann unabhängig konfiguriert werden.
- o Die manuelle Benutzerverwaltung wird immer unterstützt.
- o Integrationen verbessern die Automatisierung und die Benutzererfahrung, sind jedoch für die Einschreibung nicht erforderlich.

Folgende verschiedene Konfigurationsszenarien für ADE werden unterstützt:

- o Manuelle Einrichtung (keine Integrationen):
 - Benutzer werden manuell im Apple Business Manager und in datomo MDM erstellt.
 - Die Verwaltete Apple-ID wird manuell in datomo MDM zugewiesen (entspricht der Benutzer-E-Mail-Adresse).
- o Apple Business Manager + Identitätsanbieter-Verbund:
 - Benutzer werden vom Identitätsanbieter (z. B. Microsoft Entra ID) mit dem Apple Business Manager synchronisiert.
 - Verwaltete Apple-IDs werden automatisch erstellt.

- Benutzer in datomo MDM können weiterhin manuell verwaltet werden.
- o datomo MDM + Identitätsanbieter-Integration:
 - Benutzer werden vom Identitätsanbieter mit datomo MDM synchronisiert.
 - Die Verwaltete Apple-ID muss weiterhin der Benutzer-E-Mail-Adresse entsprechen.
 - Apple Business Manager kann unabhängig bleiben.
- o Vollständige Integration (empfohlen):
 - Der Identitätsanbieter ist sowohl mit dem Apple Business Manager als auch mit datomo MDM integriert.
 - Benutzer und Authentifizierung werden zentral (SSO) verwaltet.

2.2 Domänenkonfiguration im Apple Business Manager

Die Erstellung einer Domäne im Apple Business Manager ermöglicht die Erstellung von Verwalteten Apple-IDs im Namensraum der Organisation. Dieser Schritt ist für die kontogesteuerte Einschreibung (ADE) erforderlich, kann aber auch optional für die Standardeinschreibung verwendet werden.

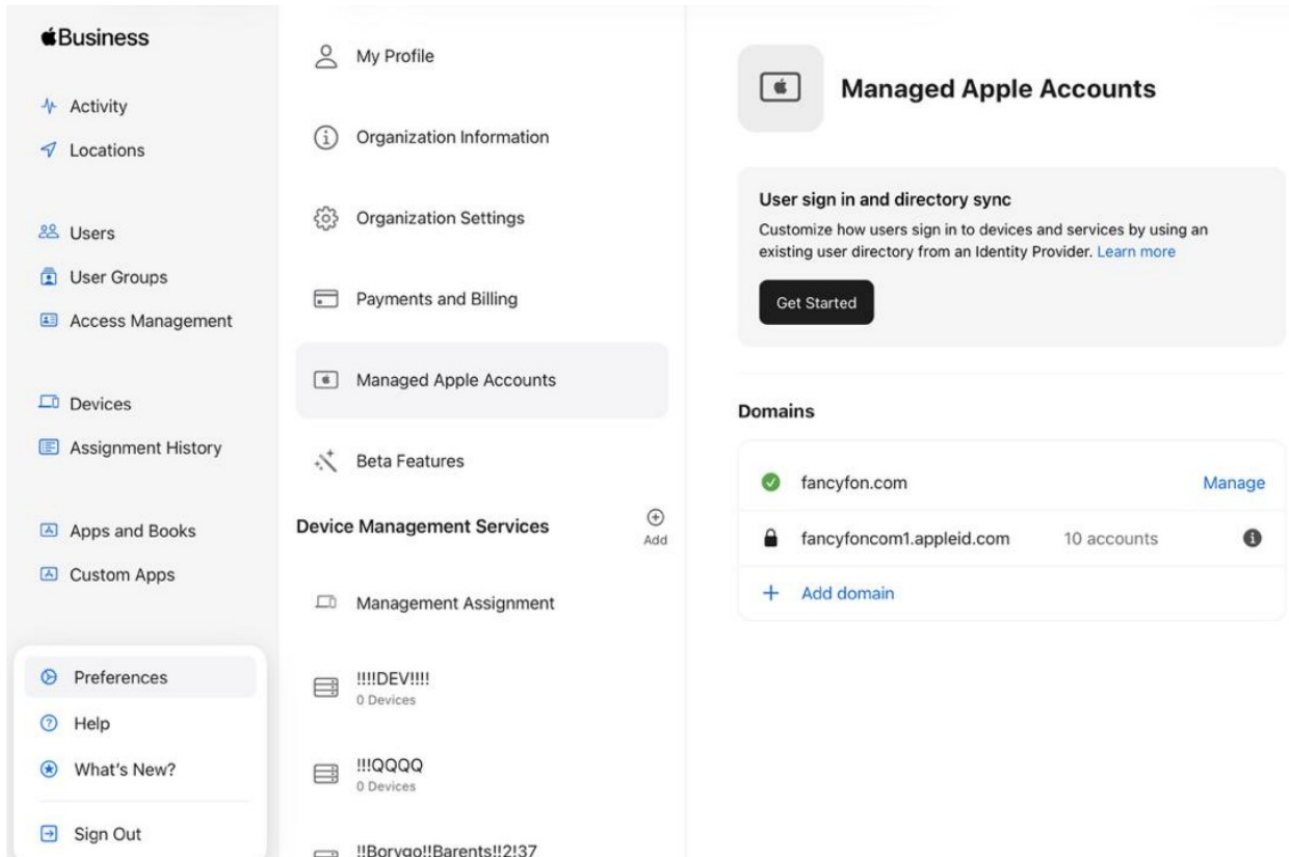
Beispiel: Domäne - beispieladresse.com

Verwaltete Apple-ID - vorname.nachname@beispieladresse.com

In dieser Dokumentation wird folgende Domäne verwendet: venice.fancyfon.com

Hinweis: Jede Domäne kann nur einer Apple-Business-Manager-Organisation zugewiesen werden.

Um eine Domäne zu erstellen, navigieren Sie im Apple Business Manager zum Kontoeintrag in der unteren linken Ecke und wählen dann Einstellungen -> Verwaltete Apple-Accounts:

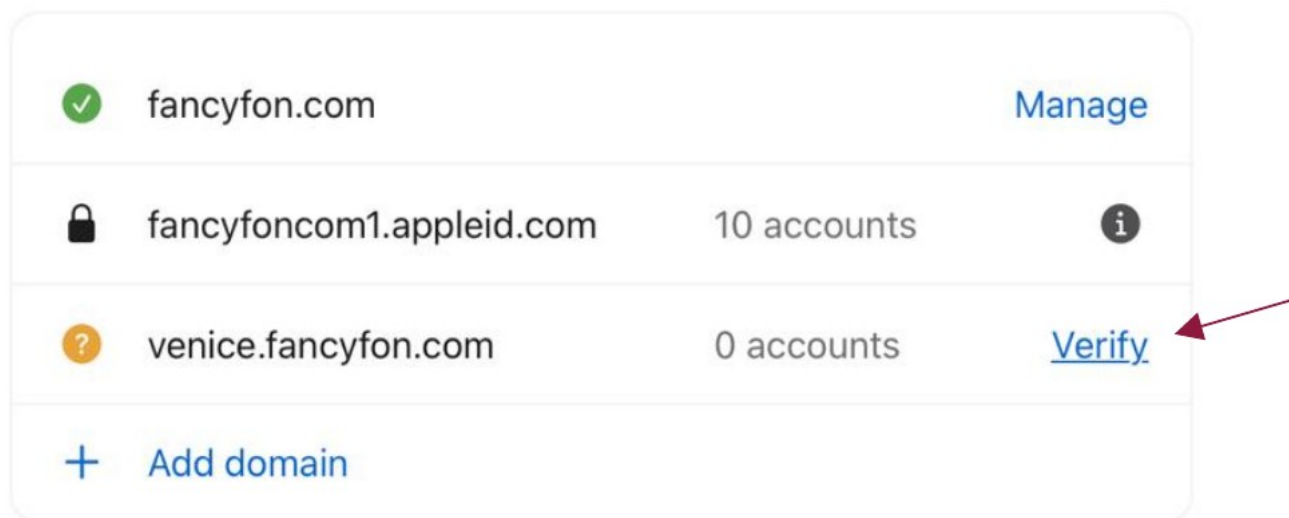


The screenshot shows the datomo MDM console interface. On the left is a sidebar with navigation options: Apple Business, Activity, Locations, Users, User Groups, Access Management, Devices, Assignment History, Apps and Books, Custom Apps, Preferences, Help, What's New?, and Sign Out. The main content area is divided into two columns. The left column contains 'My Profile', 'Organization Information', 'Organization Settings', 'Payments and Billing', 'Managed Apple Accounts' (highlighted), and 'Beta Features'. Below these are 'Device Management Services' with an 'Add' button and a list of services: 'Management Assignment', '!!!!DEV!!!!' (0 Devices), '!!!QQQQ' (0 Devices), and '!!Borygo!!Barents!!2!37'. The right column is titled 'Managed Apple Accounts' and features a 'User sign in and directory sync' section with a 'Get Started' button. Below this is a 'Domains' section with a table of domains.

Domain	Accounts	Actions
✓ fancyfon.com		Manage
🔒 fancyfoncom1.appleid.com	10 accounts	i
+ Add domain		

wählen Sie Domäne hinzufügen, geben Sie den Domänennamen ein und bestätigen Sie.

Nach der Erstellung muss die Domäne zur Bestätigung der Inhaberschaft verifiziert werden.



This is a close-up of the 'Domains' table from the previous screenshot. It shows three rows of domain information. The first row is 'fancyfon.com' with a green checkmark icon and a 'Manage' link. The second row is 'fancyfoncom1.appleid.com' with a lock icon, '10 accounts', and an information icon. The third row is 'venice.fancyfon.com' with a question mark icon, '0 accounts', and a 'Verify' link. A red arrow points to the 'Verify' link.

✓	fancyfon.com		Manage
🔒	fancyfoncom1.appleid.com	10 accounts	i
?	venice.fancyfon.com	0 accounts	Verify
+ Add domain			

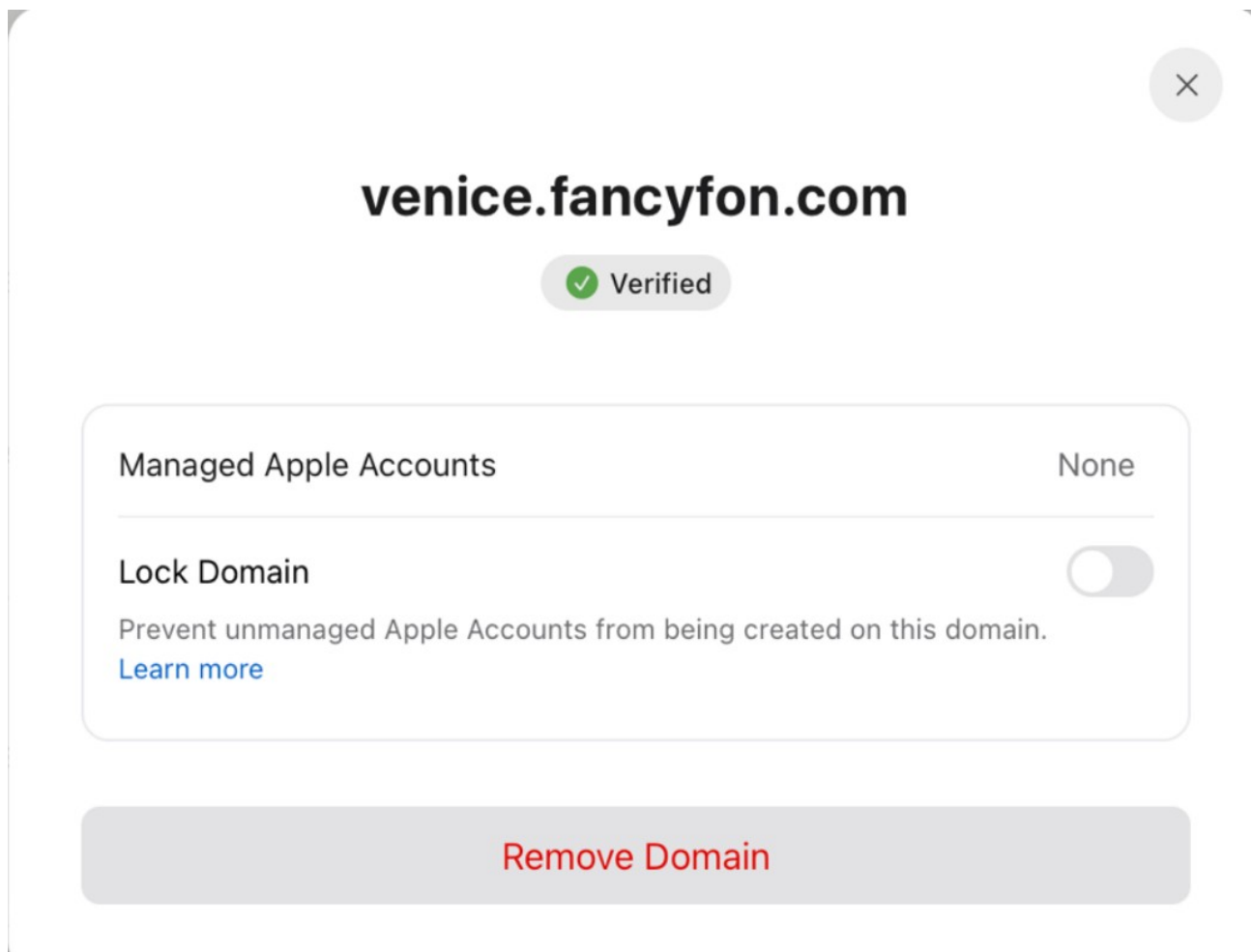
Wählen Sie in der Domänenliste „verify“.

Der Apple Business Manager stellt einen TXT-Eintrag bereit, der in der DNS-Konfiguration der Domäne hinzugefügt werden muss.

Nachdem Sie den Eintrag hinzugefügt haben, kehren Sie zurück und wählen Sie Verifizieren.

Die DNS-Weitergabe kann bis zu 72 Stunden dauern. Falls die Verifizierung fehlschlägt, versuchen Sie es zu einem späteren Zeitpunkt erneut. Die Inhaberschaft der Domäne muss innerhalb von 14 Tagen verifiziert werden.

Nach erfolgreicher Verifizierung ändert sich der Domänenstatus auf Verifiziert.



2.3 Benutzererstellung (Verwaltete Apple-IDs)

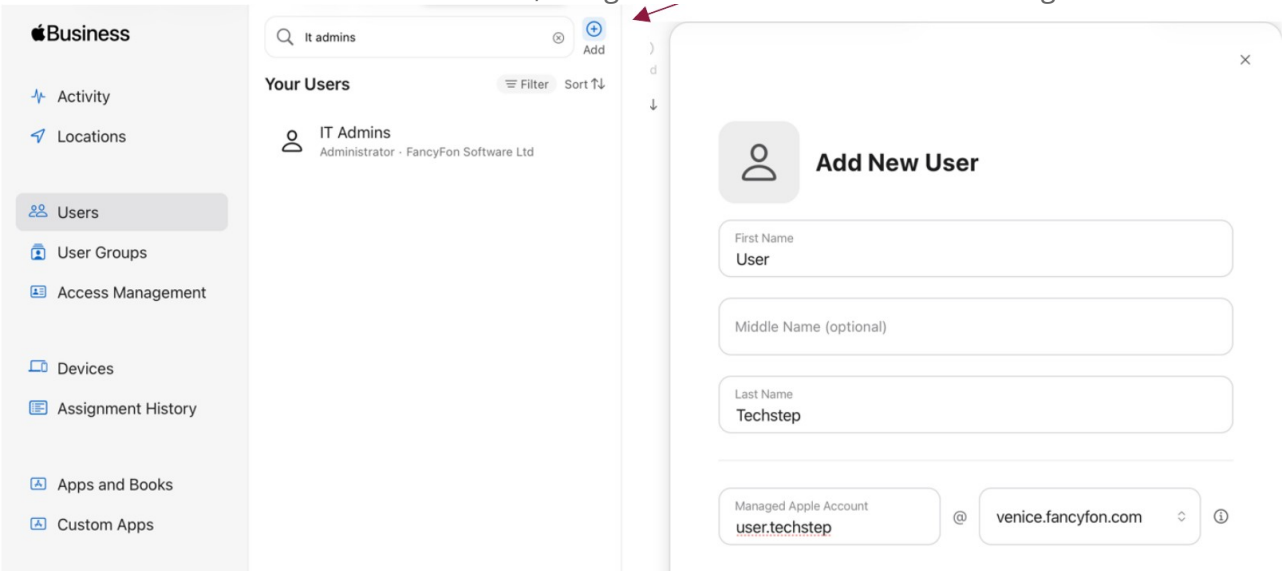
Nach der Erstellung der Domäne müssen Benutzer im Apple Business Manager erstellt werden. Die Benutzererstellung erzeugt automatisch die Verwaltete Apple-ID.

Zwei Methoden stehen zur Verfügung:

- o Manuelle Erstellung
- o Verbund mit einem Identitätsanbieter (Massenerstellung)

2.3.1 Manuelle Erstellung

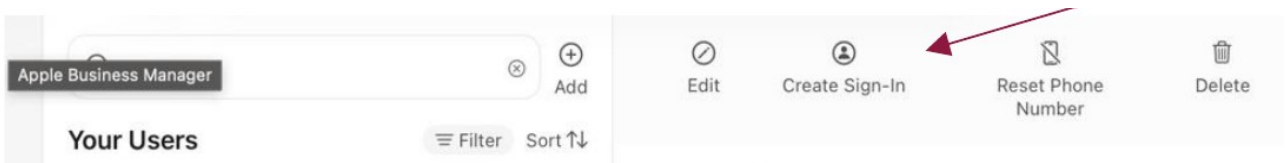
Um einen Benutzer manuell zu erstellen, navigieren Sie zu Benutzer -> Hinzufügen.



Geben Sie die erforderlichen Informationen ein und wählen Sie bei der Erstellung des Verwalteten Apple-Accounts die richtige Domäne aus.

Beispiel: benutzer@venice.fancyfon.com

Hinweis: Nach der Benutzererstellung müssen die Anmeldedaten in der Benutzerdetailsansicht generiert werden.

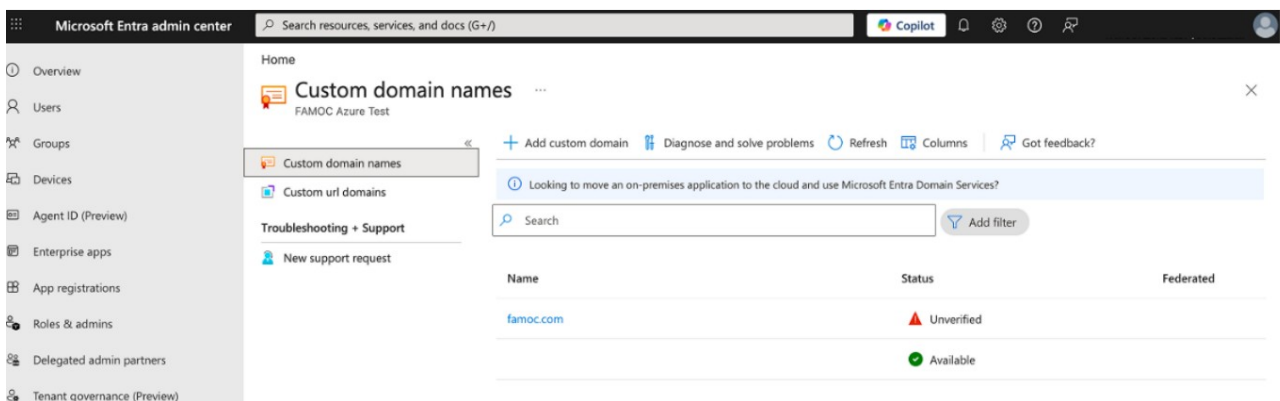


2.3.2 Massenerstellung - Entra ID und ABM

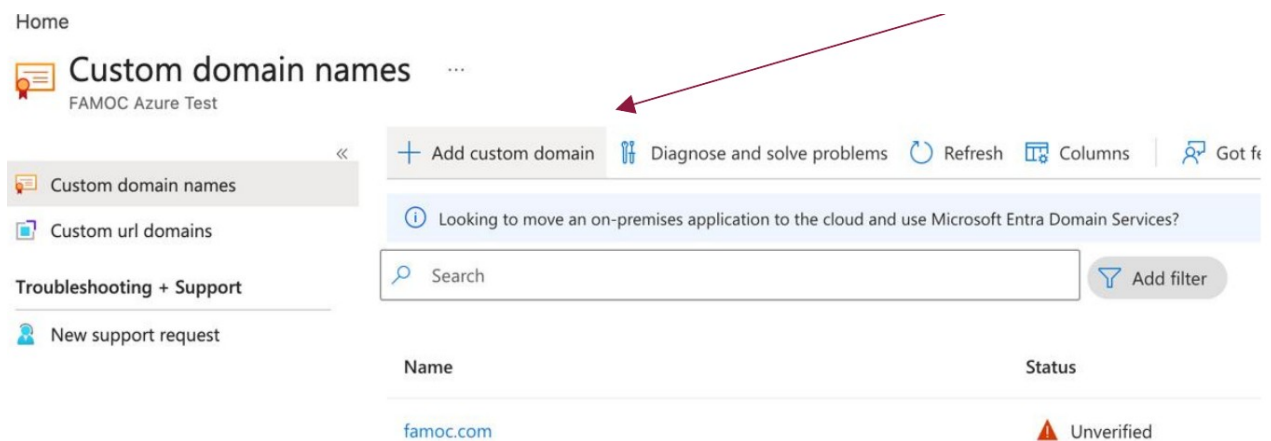
Benutzer können auch automatisch über einen Identitätsverbund erstellt werden. Diese Dokumentation beschreibt den Verbund mit Microsoft Entra ID. Die Konfiguration mit anderen Anbietern wie Google Workspace ist ähnlich.

Vor dem Verbund muss die Domäne in Entra ID verifiziert werden.

Navigieren Sie zu Entra ID -> Domänennamen -> Benutzerdefinierte Domäne hinzufügen:



Klicken Sie auf die Schaltfläche Benutzerdefinierte Domäne hinzufügen:



Geben Sie dann den Domänennamen ein und fügen Sie den von Entra bereitgestellten TXT-DNS-Eintrag hinzu.

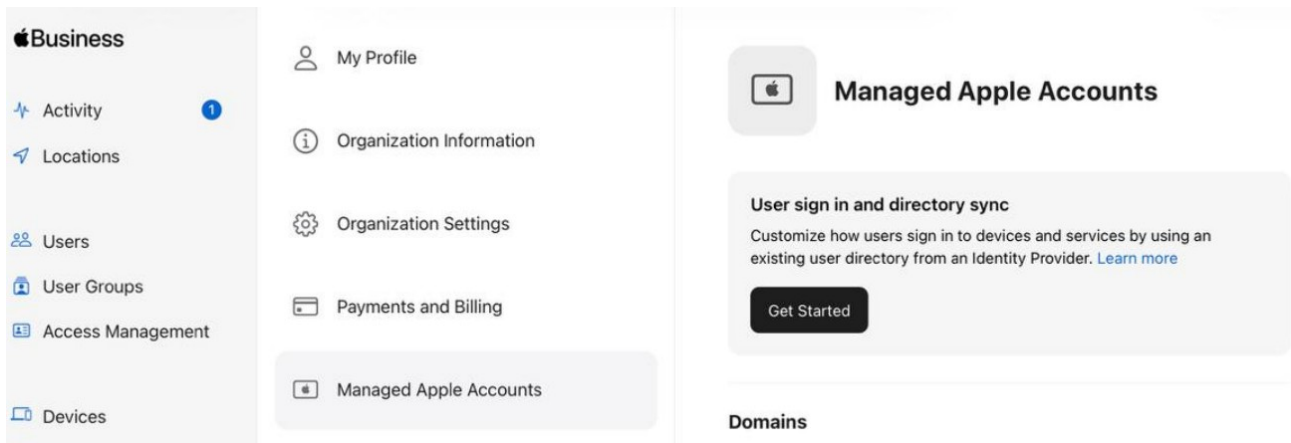
Verifizieren Sie die Domäne nach der DNS-Weitergabe; dies kann bis zu 72 Stunden dauern.

Sie finden die Dokumentation von Microsoft hier:

<https://learn.microsoft.com/en-us/entra/fundamentals/add-custom-domain>

Nach der Verifizierung in Entra ID kann der Verbund im Apple Business Manager konfiguriert werden.

Navigieren Sie zu Einstellungen -> Verwaltete Apple-Accounts -> Benutzeranmeldung und Verzeichnissynchronisierung.



wählen Sie dann „Get Started“.

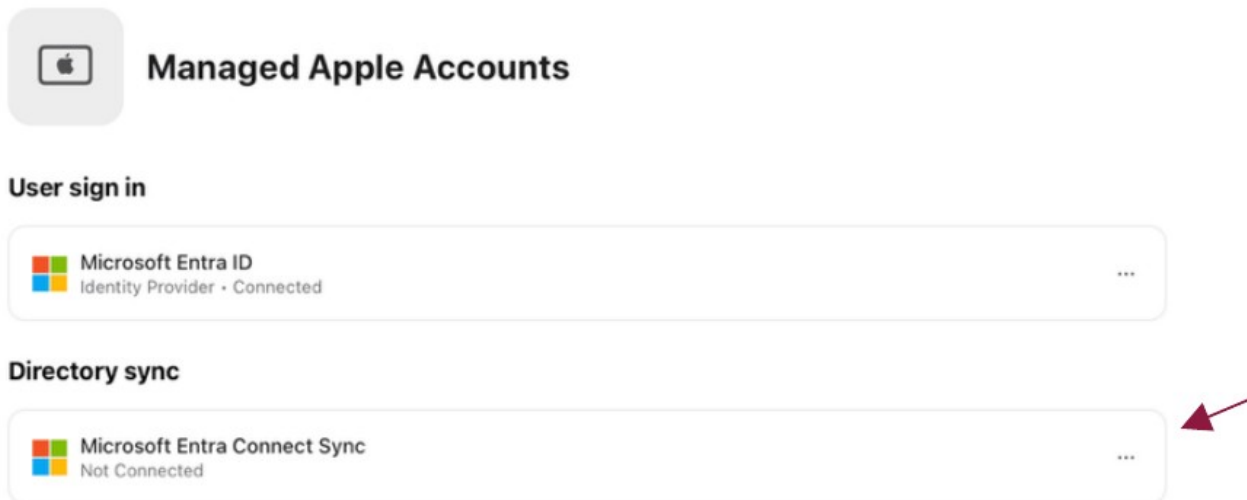
Wählen Sie Microsoft Entra ID aus der Liste aus und melden Sie sich bei Ihrem Konto an.

Erteilen Sie dann die erforderlichen Berechtigungen. Stellen Sie sicher, dass diese dem für die Integration verwendeten Konto in Entra zuvor zugewiesen wurden; das Konto muss die Rolle Globaler Leser, Anwendungsadministrator und Cloudanwendungsadministrator besitzen.

Hinweis:

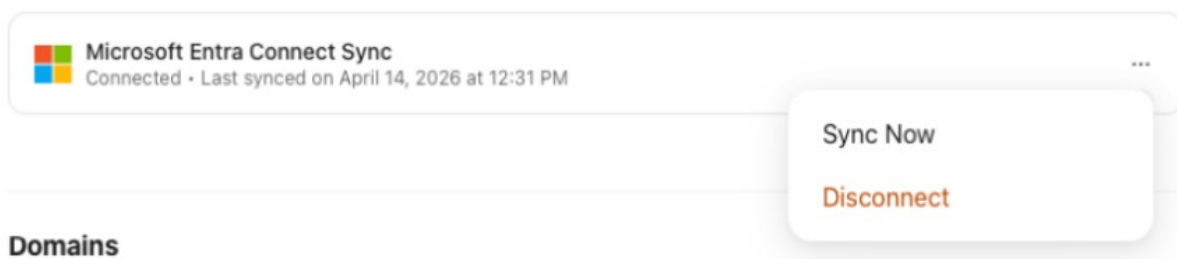
- o Der Apple Business Manager zeigt möglicherweise keine Fehler an, wenn der Verbund fehlschlägt, und leitet möglicherweise zum Startbildschirm weiter. Eine erfolgreiche Konfiguration wird nur Bestätigt, wenn der Verbund-Zusammenfassungsbildschirm erscheint.
- o Die Domäne muss auch im Apple Business Manager verifiziert werden (Abschnitt 2.1). Die automatische Verifizierung schlägt möglicherweise nicht immer erfolgreich durch.

Nach einem erfolgreichen Verbund und sobald der Identitätsanbieter verbunden ist, ist ein zusätzlicher Schritt erforderlich, um Benutzer automatisch zu erstellen und sie mit der verifizierten Domäne im Apple Business Manager zu verknüpfen. Der Status der Verzeichnissynchronisierung wird verfügbar und muss im Abschnitt Verwaltete Apple-Accounts konfiguriert werden.



Klicken Sie auf die drei Punkte und wählen Sie dann Jetzt synchronisieren, um alle Benutzer aus Entra innerhalb der ausgewählten Domäne abzurufen.

Directory sync



Nach erfolgreicher Synchronisierung erscheinen die Konten in der Liste. Der letzte Schritt besteht darin, die Anmeldung für diese Konten über die Option Verwalten im Domäneneintrag zu konfigurieren.

Domains

✓	Test.test.com	4 accounts	Manage
✓	Test.demo.com	17 User Name Conflicts	Manage
↗	17 unmanaged Apple Accounts found		Domain Capture
✓	test.com	0 accounts	Manage

Wählen Sie dann Mit Microsoft Entra ID anmelden. Ab diesem Zeitpunkt wird die Authentifizierung für Verwaltete Apple-IDs über den Identitätsanbieter Entra ID abgewickelt.

Weitere Informationen zum Verbund zwischen Entra ID und Apple Business Manager finden Sie in der offiziellen Dokumentation.

<https://support.apple.com/guide/apple-business-manager/federated-authentication-microsoft-entra-axm8c1cac980/web>

3 Gerät mit dem Standard-Einschreibungsassistenten hinzufügen

Der Standard-Einschreibungsassistent steht für Geräte mit iOS/iPadOS 13 bis 17.x zur Verfügung. Um ein einzelnes Gerät zum System hinzuzufügen, navigieren Sie zur Registerkarte Geräte, fahren Sie mit dem Mauszeiger über die Plus-Schaltfläche und wählen Sie die Option Gerät einschreiben. Das Einschreibungsverfahren für iPads folgt demselben Ablauf.

Ein schrittweises modales Fenster wird angezeigt, um den Einschreibungsprozess zu begleiten. Im ersten Schritt wählen Sie die Plattform aus. Verfügbare Optionen sind Android, Apple und andere Geräte (z. B. Windows). In diesem Beispiel wird die Plattform Apple ausgewählt.

Im zweiten Schritt wählen Sie die Einschreibungsmethode:

Benutzereingeschriebenes Gerät (BYOD)

Als Nächstes geben Sie die Verwaltete Apple-ID an, die dem Gerät zugeordnet wird, und wählen den dem Gerät zugewiesenen Benutzer aus. Weitere Informationen zur Verwalteten Apple-ID und deren Bezug finden Sie in den folgenden Abschnitten.

Nach der Auswahl des Gerätebenutzers können zusätzliche Informationen wie E-Mail-Adresse, Telefonnummer und Gerätebeschreibung angegeben werden.

Hinweis: Der ausgewählte Benutzer bestimmt die auf das Gerät angewendete Richtlinie. Weitere Informationen zu Richtlinien finden Sie in der detaillierten Beschreibung in der Wissensdatenbank: Richtlinien in datomo MDM.

Wählen Sie dann die Schaltfläche Weiter, um die Ansicht zur Richtlinienzuweisung anzuzeigen. Darunter können die Sicherheitseinstellungen, Anwendungen und Konfigurationen eingesehen werden, die auf das Gerät angewendet werden. Diese Einstellungen werden durch die zugewiesene Gerätegruppe oder Benutzergruppe bestimmt.

Im vorletzten Schritt kann die bevorzugte Einschreibungsmethode ausgewählt werden. für Apple-Geräte stehen zwei Optionen zur Verfügung: Einschreibungslink senden und QR-Code scannen.

Einschreibungslink senden

Ein Einschreibungslink wird dem Benutzer per E-Mail oder SMS zugesandt.

Hinweis: Die SMS-Option erfordert ein konfiguriertes SMS-Gateway.

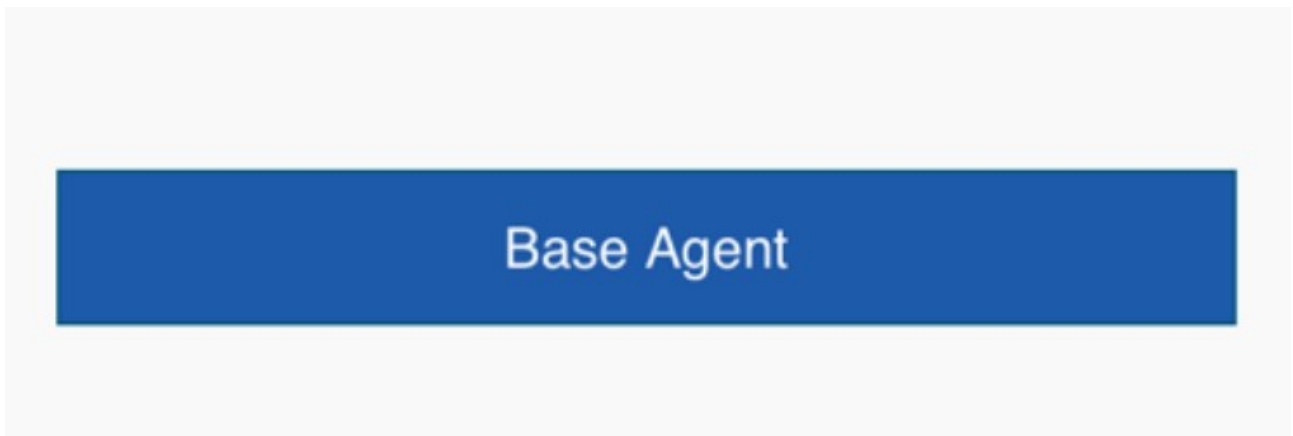
QR-Code scannen

Der QR-Code kann mit der Gerätekamera oder einer QR-Code-Reader-Anwendung gescannt werden.

Hinweis: Die QR-Reader-Anwendung sollte so konfiguriert sein, dass Links automatisch im Safari-Browser geöffnet werden. Andernfalls kann der QR-Code als verwendet markiert werden, bevor der Link geöffnet wird. Nach dem Scannen wird die Einschreibungsseite auf dem Gerät angezeigt.

Nach dem Scannen des QR-Codes und dem Öffnen des Links aus dem Popup-Fenster zeigt ein Bestätigungsmodal an, dass der Einschreibungsvorgang gestartet wurde.

Der nächste Schritt ist die Installation des Verwaltungsprofils auf dem Gerät. wählen Sie die Schaltfläche Basis-Agent.



Anschließend wird ein Bestätigungs-Popup angezeigt, das um Erlaubnis zur Installation des Profils bittet. Nach der Bestätigung erscheint ein Popup mit dem Titel Profil heruntergeladen.

Öffnen Sie als Nächstes die App Einstellungen und navigieren Sie zu Allgemein. Öffnen Sie dann den Abschnitt VPN & Geräteverwaltung und wählen Sie das heruntergeladene Profil aus.

Um das Profil zu installieren, wählen Sie die Schaltfläche Installieren in der oberen rechten Ecke des Bildschirms und geben Sie den Gerätecode ein, um den Vorgang zu bestätigen. Der letzte Schritt besteht darin, im Bestätigungs-Popup die Schaltfläche Vertrauen auszuwählen.

Nach erfolgreicher Installation ändert sich der Bildschirmtitel in „Profil installiert“, was bestätigt, dass das Gerät jetzt verwaltet wird.

Zusätzlich wird im Browser-Modal eine Bestätigungsnachricht angezeigt, die angibt, dass das Gerät einsatzbereit ist.

4 Gerät mit der kontogesteuerten Einschreibung hinzufügen

für iOS/iPadOS 17 und später hat Apple die kontogesteuerte Benutzereinschreibung eingeführt.

Im Gegensatz zum Standard-Einschreibungsassistenten beginnt dieser Vorgang direkt auf dem Gerät und erfordert eine zusätzliche Vorbereitung.

4.1 Verwaltete Apple-ID einem Benutzer zuweisen

Für die kontogesteuerte Einschreibung muss die Verwaltete Apple-ID mit dem Benutzer in datomo MDM verknüpft werden.

Dies geschieht durch Festlegen des Verwaltete-Apple-ID-Wertes im E-Mail-Feld des Benutzers.

Dies ermöglicht eine automatische Verknüpfung zwischen:

- o Verwalteter Apple-ID
- o datomo MDM-Benutzer
- o Eingeschriebenem Gerät

Nach der Einschreibung wird das Gerät dem Benutzer automatisch zugewiesen und Richtlinien werden gemaess dem Standard-Einschreibungsverhalten angewendet, einschliesslich Zuweisungen auf Basis von Benutzergruppen, intelligenten Gruppen und Gerätegruppen, die für die EinschreibungsDomäne konfiguriert sind (siehe Abschnitt 4.2).

4.1.1 Manuelle Zuweisung

Die Verwaltete Apple-ID kann manuell zugewiesen werden.

Navigieren Sie zu Benutzer -> Benutzerdetails, bearbeiten Sie dann das Feld E-Mail und geben Sie die Verwaltete Apple-ID ein.

4.1.2 Automatisch mit Entra ID (datomo MDM- und Entra-Integration)

Diese Lösung funktioniert gut zusammen mit dem Entra-Verbund mit dem Apple Business Manager. datomo MDM unterstützt die Entra-Synchronisierung und ermöglicht den Import derselben Benutzer.

Die Angabe der Verwalteten Apple-ID als E-Mail-Wert ermöglicht die Massenvorbereitung von Benutzern. Weitere Details sind in der dedizierten Dokumentation zur Verbindung zwischen datomo MDM und Microsoft Entra ID verfügbar.

<https://datomo.de/aktuelles/azure-active-directory-ad/>

Nach der Integration von datomo MDM mit Entra ID werden Benutzer aus Entra in datomo MDM verfügbar, können sich jedoch erst anmelden, wenn für jeden Benutzer manuell ein Passwort erstellt wurde. Um eine automatische Autorisierung über Entra ID zu ermöglichen, muss die SAML-Anmeldung in datomo MDM konfiguriert werden. Anweisungen hierzu finden Sie in der Dokumentation.

Sobald SAML aktiviert ist, können sich Benutzer während der Einschreibung über die Web-Ansicht mit ihrer Entra-Identität bei datomo MDM anmelden. Im nächsten Schritt, dank des Verbunds zwischen Apple Business Manager und Entra, können sie sich auch mit derselben Entra-Identität bei iCloud anmelden (weitere Details finden Sie im Abschnitt zum Einschreibungsvorgang).

Hinweis:

- o Die E-Mail-Adresse muss der Verwalteten Apple-ID entsprechen, um eine ordnungsgemäße Identitätsverknüpfung zu ermöglichen.
- o Stellen Sie sicher, dass der Benutzer sich vor der Einschreibung authentifizieren kann.
- o In den meisten Fällen entspricht der userPrincipalName der Verwalteten Apple-ID und sollte dem E-Mail-Feld in datomo MDM zugeordnet werden, was jedoch von der Entra- und Apple-Business-Manager-Verbundkonfiguration abhängt.

4.2 Konfiguration und Domäne vorbereiten

Bei der kontogesteuerten Einschreibung müssen Geräte wissen, woher sie die Einschreibungskonfiguration abrufen sollen. Dieser Vorgang ist automatisch und basiert auf der Domäne der Verwalteten Apple-ID.

während der Anmeldung leitet das Gerät die Domäne von der Verwalteten Apple-ID ab.

Beispiel:

Verwaltete Apple-ID: benutzer.dotoso@devman.datomo.de

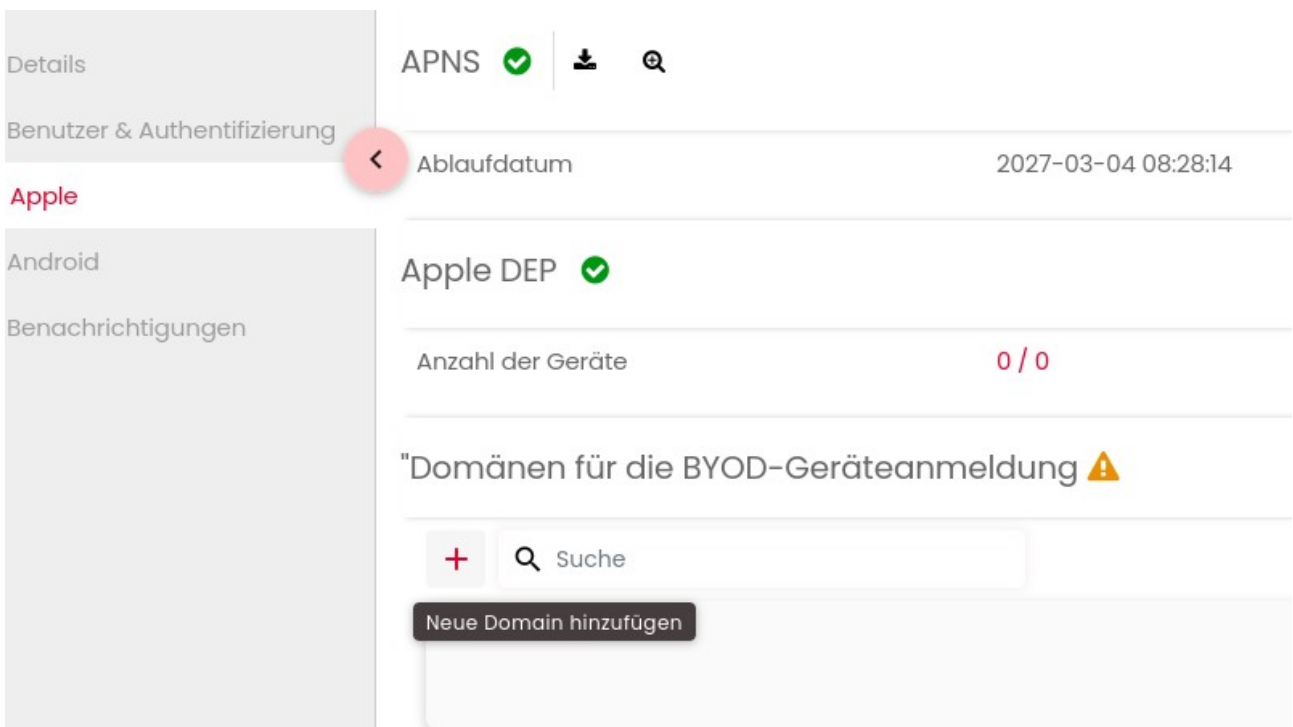
Abgeleitete Domäne: devman.datomo.de

Das Gerät versucht automatisch, die Konfiguration von folgender Adresse abzurufen:
devman.datomo.de/.well-known/com.apple.remotemanagement

Aufgrund dieses Mechanismus muss die Domäne in datomo MDM konfiguriert werden, um die Verfügbarkeit der Konfiguration zu validieren.

4.2.1 Domäne in datomo MDM hinzufügen

Um eine Domäne hinzuzufügen, navigieren Sie in die obere rechte Ecke und wählen Sie Konto -> Einstellungen -> Apple -> BYOD-Geräteeinschreibungs-Domänen:



wählen Sie dann Neue Domäne hinzufügen.

Geben Sie den erforderlichen Domänennamen sowie eine optionale Beschreibung und Gerätegruppen-Zuweisung an.

Die Gerätegruppen-Zuweisung ermöglicht die automatische Richtlinienzuweisung an Geräte, die aus dieser Domäne eingeschrieben werden.

Nach der Erstellung prüft das System automatisch, ob eine Einschreibungskonfiguration unter folgender Adresse vorhanden ist:

ihredomain/.well-known/com.apple.remotemanagement

Domain	Erstellt von	Erstellt am	Geändert am	Geändert von	Gerätegruppen	Beschreibung	Ist gültig
devman.datomo.de	Administrator System (admin)	vor einer Minute	vor ein paar Sekunden	Administrator System (admin)			Ja

Grundsätzlich sind zwei Szenarien möglich:

Domäne entspricht der datomo-MDM-Server-URL: Die Konfiguration wird automatisch generiert und bereitgestellt, und die Domäne wird automatisch als gültig markiert.

Domäne weicht von der datomo-MDM-Server-URL ab: Die Konfiguration muss heruntergeladen und manuell gehostet werden. Dazu kann die Konfiguration über das Domänen-Aktionsmenü heruntergeladen werden (drei Punkte -> Domänenkonfiguration herunterladen).

Domain	Erstellt von	Erstellt am	Geändert am	Geändert von	Gerätegruppen	Beschreibung	Aktionen
devman.datomo.de	Administrator System (admin)	vor 2 Minuten	vor einer Minute	Administrator System (admin)			Bearbeiten Löschen Domänenkonfiguration herunterladen

Die heruntergeladene JSON-Datei muss abgelegt werden unter:

ihredomain/.well-known/com.apple.remotemanagement

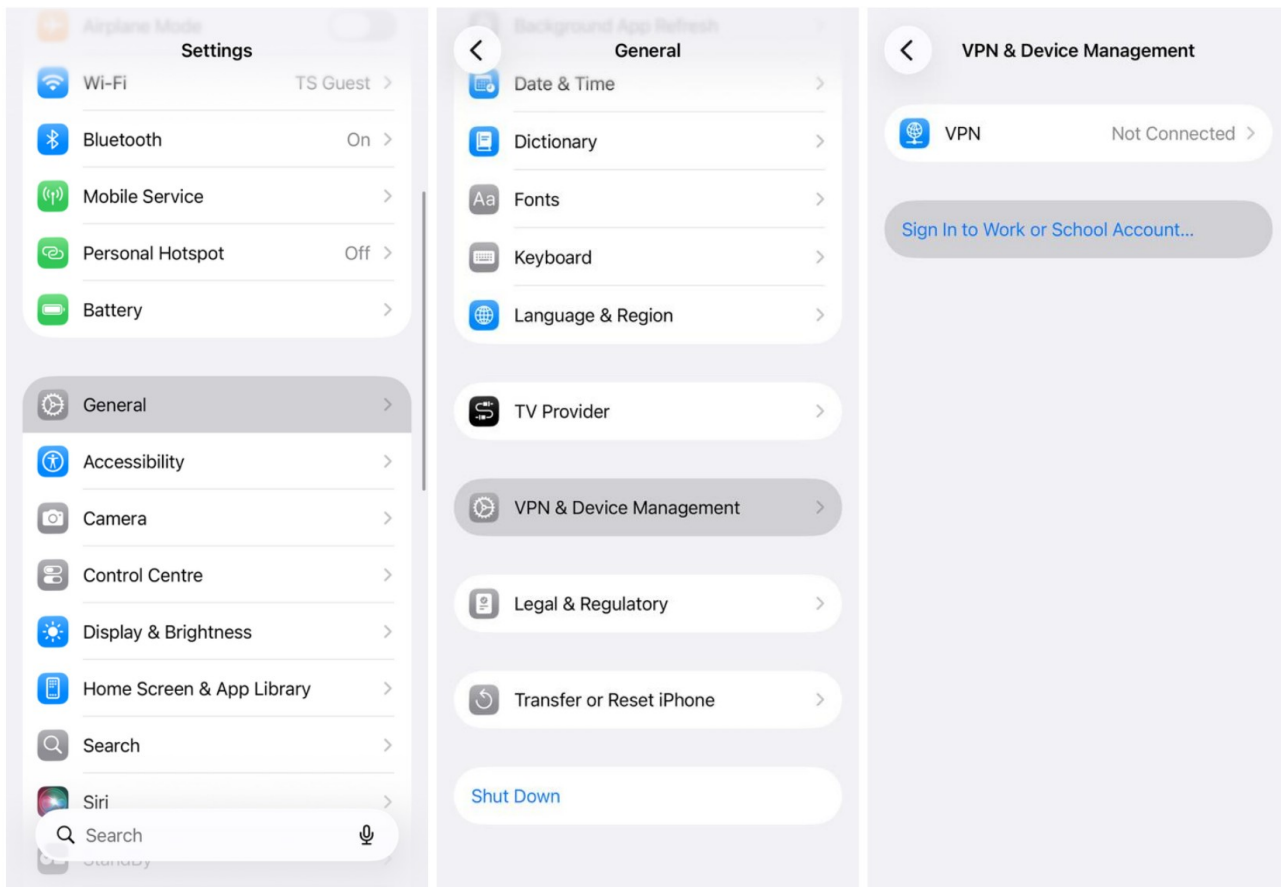
Nach der Veröffentlichung der Konfiguration sollte sich der Domänenstatus auf gültig ändern.

Die Konfiguration kann auch manuell überprüft werden, indem die URL geöffnet wird. Eine gültige Konfiguration gibt eine JSON-Antwort zurück.

Nach diesen Schritten ist die Umgebung für die Einschreibung bereit.

4.3 Einschreibungsvorgang

Um die Einschreibung zu starten, navigieren Sie auf dem Gerät zu: Einstellungen -> Allgemein -> VPN & Geräteverwaltung -> Bei Schul- oder Unternehmenskonto anmelden...



Geben Sie die Verwaltete Apple-ID ein und wählen Sie Weiter.

Die Web-Authentifizierungsansicht erscheint und fordert die mit dieser Identität verknüpften MDM-Zugangsdaten an.

In einem alternativen Szenario, wenn Entra ID integriert und die SAML-Authentifizierung aktiviert ist, ist eine zusätzliche Schaltfläche Mit SAML anmelden verfügbar. Diese Schaltfläche leitet Benutzer zur Microsoft-Anmeldung weiter, sodass sie sich in datomo MDM mit ihrer Entra-Identität authentifizieren können.

Anschließend erscheint der Microsoft-Autorisierungsbildschirm. Melden Sie sich mit Ihrem Passwort an und fahren Sie fort.

Nach der Authentifizierung wird der Benutzer in beiden Fällen aufgefordert, sich bei iCloud anzumelden. Es gibt ebenfalls zwei mögliche Szenarien. Ohne Verbund mit Entra: Der Benutzer

muss die Verwaltete Apple-ID und das Passwort eingeben und dann wie unten dargestellt fortfahren.

Und im zweiten Fall, wenn der Apple Business Manager mit Entra verbunden ist, kann die Identität von Entra bereitgestellt werden. In diesem Fall wird ein anderer Bildschirm mit einer Weiterleitung zur Microsoft-Anmeldeseite angezeigt, ähnlich dem Autorisierungsvorgang in datomo MDM.

Anschließend wird der standardmäßige Microsoft-Entra-Anmeldebildschirm angezeigt.

Nach einer erfolgreichen Anmeldung bei iCloud - unabhängig davon, ob die Anmeldung über den Identitätsanbieter oder die Standard-Apple-Methode erfolgte - erscheint der Bildschirm Remoteverwaltung mit folgenden Angaben:

- o Organisationsname
- o Serverinformationen
- o Verwaltungsbereich

wählen Sie Remoteverwaltung zulassen und bestätigen Sie mit dem Gerätecode.

Nach der Installation:

- o Das BYOD-Profil ist installiert.
- o Das Gerät wird verwaltet.
- o Das Gerät erscheint in der Administrator-Konsole.
- o Richtlinien werden automatisch angewendet.