Konfigurieren des ISE 2.0-Zertifikatsbereitstellungsportals

Inhalt

Einführung

Dieses Dokument beschreibt die Konfiguration und die Funktionen des ISE-Portals (Identity Services Engine) für die Zertifikatsbereitstellung.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über grundlegende Kenntnisse in folgenden Bereichen zu verfügen:

- ISE
- Zertifizierungsstellen- und Zertifizierungsstellen-Server (Certificate Authority, CA).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Identity Service Engine 2.0
- Windows 7 - PC

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Das Portal für die Zertifikatsbereitstellung ist eine neue Funktion, die in ISE 2.0 eingeführt wurde und von Endgeräten zum Registrieren und Herunterladen von Identitätszertifikaten vom Server verwendet werden kann. Es werden Zertifikate für Geräte ausgegeben, die den Onboarding-Fluss nicht durchlaufen können.

Geräte wie Point-of-Sale-Terminals können beispielsweise nicht dem BYOD-Fluss (Bring Your Own Device) unterzogen werden und müssen manuell Zertifikate ausgestellt werden.

Über das Certificate Provisioning Portal können privilegierte Benutzer eine Zertifikatsanforderung (CSR) für diese Geräte hochladen. Generieren Sie Schlüsselpaare, und laden Sie dann das Zertifikat herunter.

Auf der ISE können Sie modifizierte Zertifikatsvorlagen erstellen, und Endbenutzer können eine geeignete Zertifikatsvorlage zum Herunterladen eines Zertifikats auswählen. Für diese Zertifikate fungiert die ISE als Zertifizierungsstellen-Server (Certificate Authority, CA), und das Zertifikat kann von der internen ISE-Zertifizierungsstelle signiert werden.

Das ISE 2.0-Portal für die Zertifikatsbereitstellung unterstützt den Zertifikatsdownload in folgenden Formaten:

- PKCS12-Format (einschließlich Zertifikatskette) eine Datei für Zertifikatskette und Schlüssel)
- PKCS12-Format (eine Datei für Zertifikat und Schlüssel)
- Zertifikat (einschließlich Kette) im Privacy Enhanced Electronic Mail (PEM)-Format, Schlüssel im PKCS8 PEM-Format.
- Zertifikat im PEM-Format, Schlüssel im PKCS8-PEM-Format:

Einschränkungen

Derzeit unterstützt die ISE nur diese Erweiterungen in einem CSR, um ein Zertifikat zu signieren.

- subjectDirectoryAttributes
- subjectAlternativeName
- Schlüsselverwendung
- subjectKeyIdentifier
- AuditIdentity
- ExtendedKeyUsage
- CERT_TEMPLATE_OID (Dies ist eine benutzerdefinierte OID, mit der die Vorlage angegeben wird, die normalerweise im BYOD-Fluss verwendet wird)

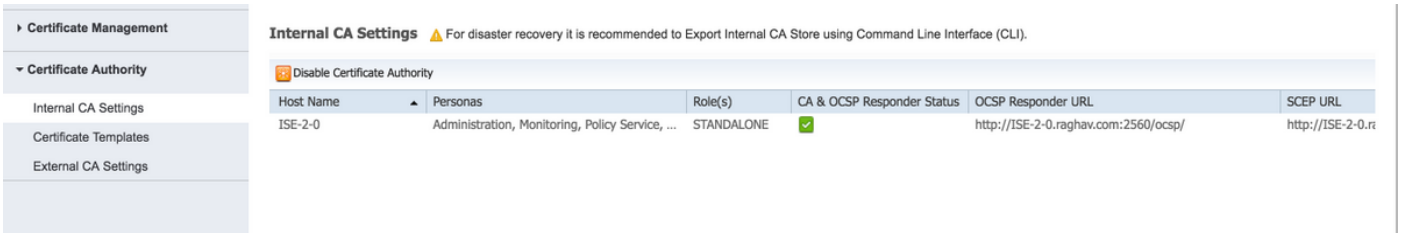
> **Hinweis**: Die interne Zertifizierungsstelle der ISE unterstützt Funktionen, die Zertifikate wie BYOD verwenden. Daher sind die Funktionen begrenzt. Die Verwendung der ISE als Enterprise CA wird von Cisco nicht empfohlen.

Konfigurieren

Um die Funktion der Zertifikatsbereitstellung im Netzwerk nutzen zu können, muss der interne

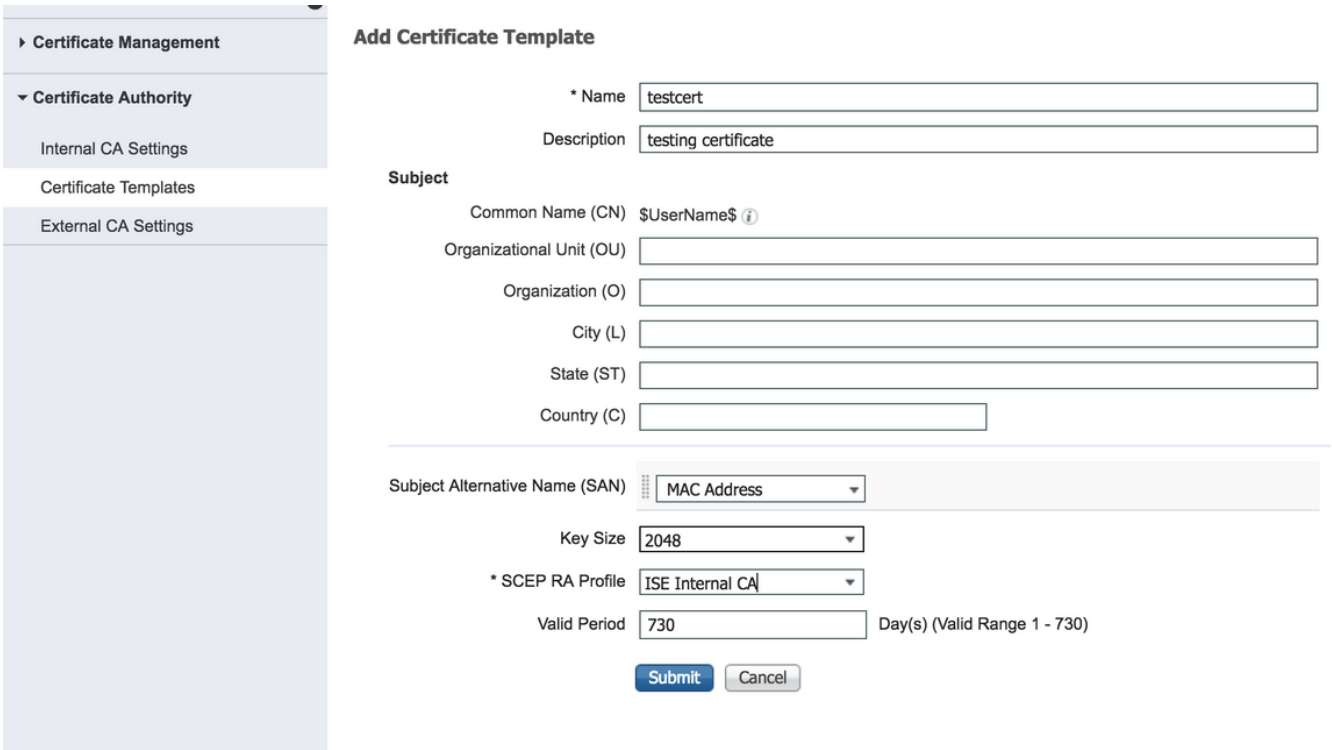
ISE-Zertifizierungsstellen-Service aktiviert und ein Portal für die Zertifikatsbereitstellung konfiguriert werden.

Schritt 1:Navigieren Sie in der ISE-GUI zu **Administration > System > Certificates > Certificate Authority > Internal CA**, und aktivieren Sie die internen CA-Einstellungen auf dem ISE-Knoten, und klicken Sie auf **Enable Certificate Authority**.

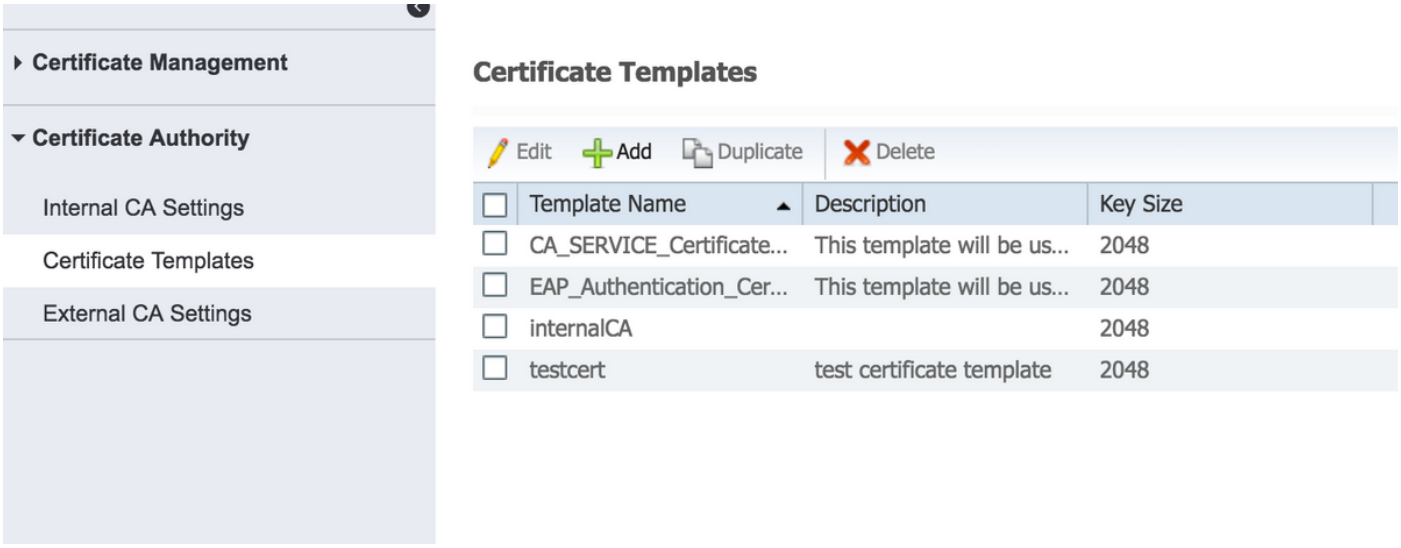


Schritt 2: Erstellen Sie Zertifikatsvorlagen unter **Administration > System > Certificates > Certificate Templates > Add**.

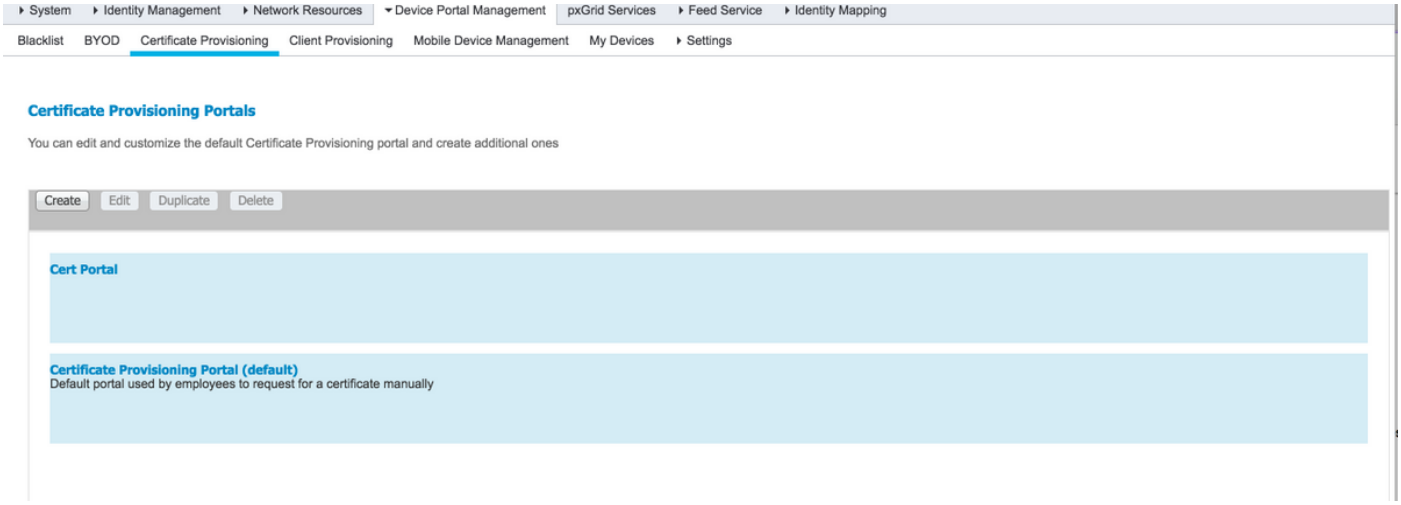
Geben Sie die Details gemäß den Anforderungen ein, und klicken Sie auf **Senden,** wie in diesem Bild gezeigt.



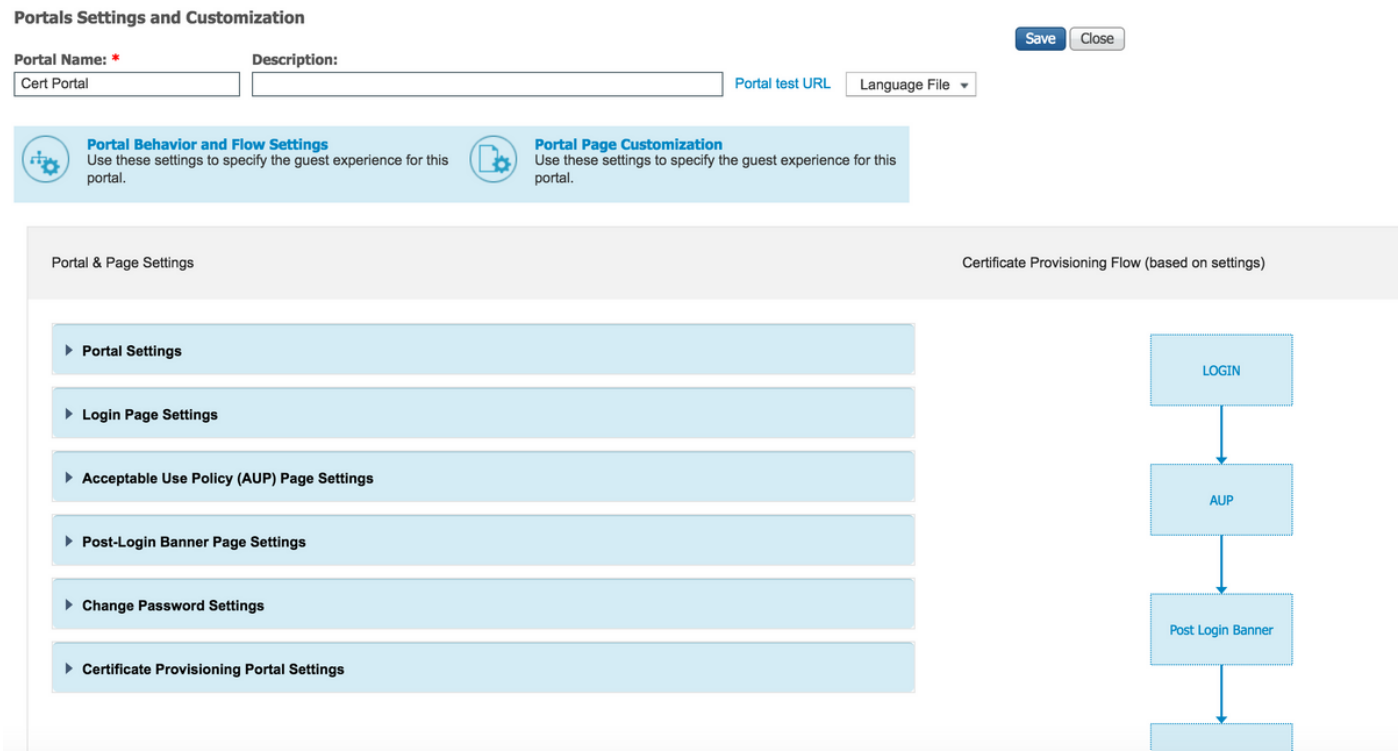
Hinweis: Sie können die Liste der erstellten Zertifikatsvorlagen unter **Administration > System > Certificates > Certificate Templates (Verwaltung > System > Zertifikate > Zertifikatsvorlagen) anzeigen**, wie in diesem Bild gezeigt.

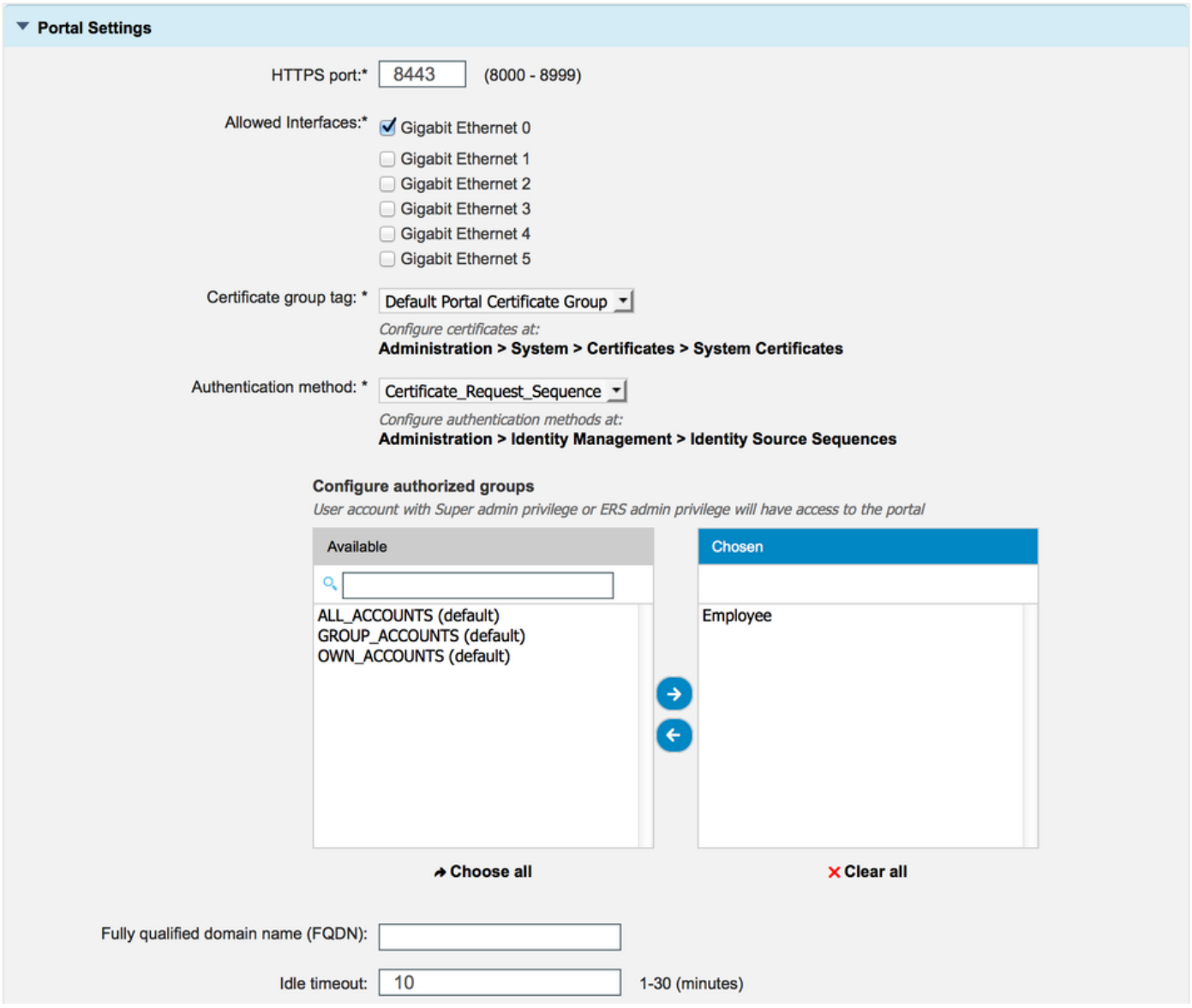


Schritt 3: Um das ISE-Portal für die Zertifikatsbereitstellung zu konfigurieren, gehen Sie zu **Administration > Device Portal Management > Certificate Provisioning > Create** (**Verwaltung > Geräteportal-Management > Zertifikatsbereitstellung > Erstellen**), wie im folgenden Bild gezeigt:



Schritt 4: Erweitern Sie im neuen Zertifikatsportal die Portaleinstellungen, wie im Bild gezeigt.





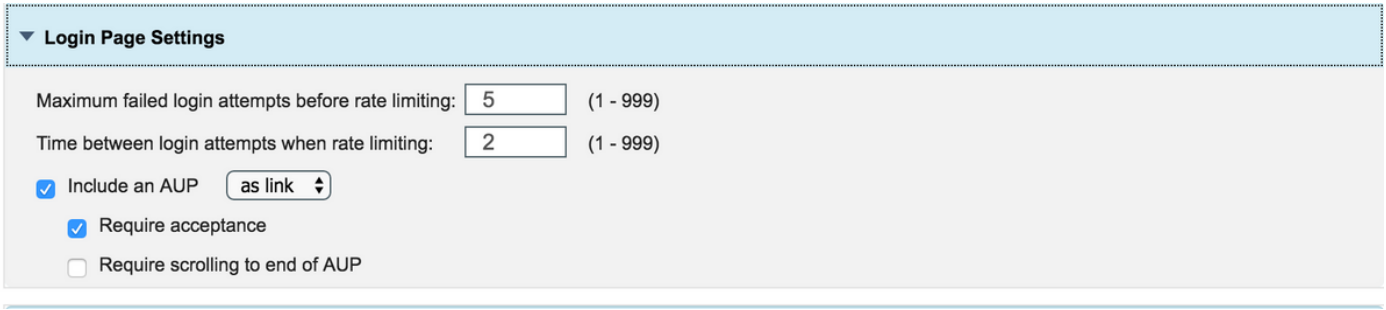
HTTPS-Port — Port, der vom Portal für die Zertifikatsbereitstellung für HTTPS v

Zugelassene Schnittstellen — Die Schnittstellen, auf denen die ISE auf dieses Portal hören so

Zertifikatgruppen-Tag	Das Zertifikat-Tag, das für das Zertifikatsbereitstellungsportal v
Authentifizierungsmethode	Wählen Sie die Identitätsspeichersequenz aus, die die Anmeld
Autorisierte Gruppen	Die Anzahl der Benutzer, die auf das Portal für die Zertifikatsbe
Vollqualifizierter Domänenname (FQDN)	Sie können diesem Portal auch einen bestimmten FQDN zuwei
Leerlaufzeitüberschreitung	Der Wert definiert das Leerlaufzeitlimit für das Portal.

> **Hinweis**: Die Konfiguration der Identitätsquelle kann unter **Administration > Identity Management > Identity Source Sequence** überprüft werden.

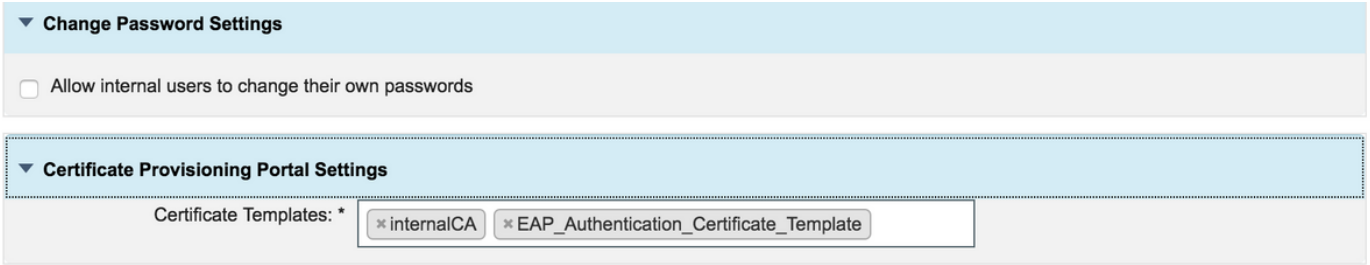
Schritt 5: Konfigurieren der Einstellungen für die Anmeldeseite



Schritt 6: Konfigurieren der Einstellungen für die AUP-Seite

Schritt 7: Sie können auch Banner nach der Anmeldung hinzufügen.

Schritt 8: Geben Sie unter Einstellungen für das Zertifikatsbereitstellungsportal die zulässigen Zertifikatsvorlagen an.



Schritt 9: Navigieren Sie zum oberen Seitenrand, und klicken Sie auf **Speichern**, um die Änderungen zu speichern.

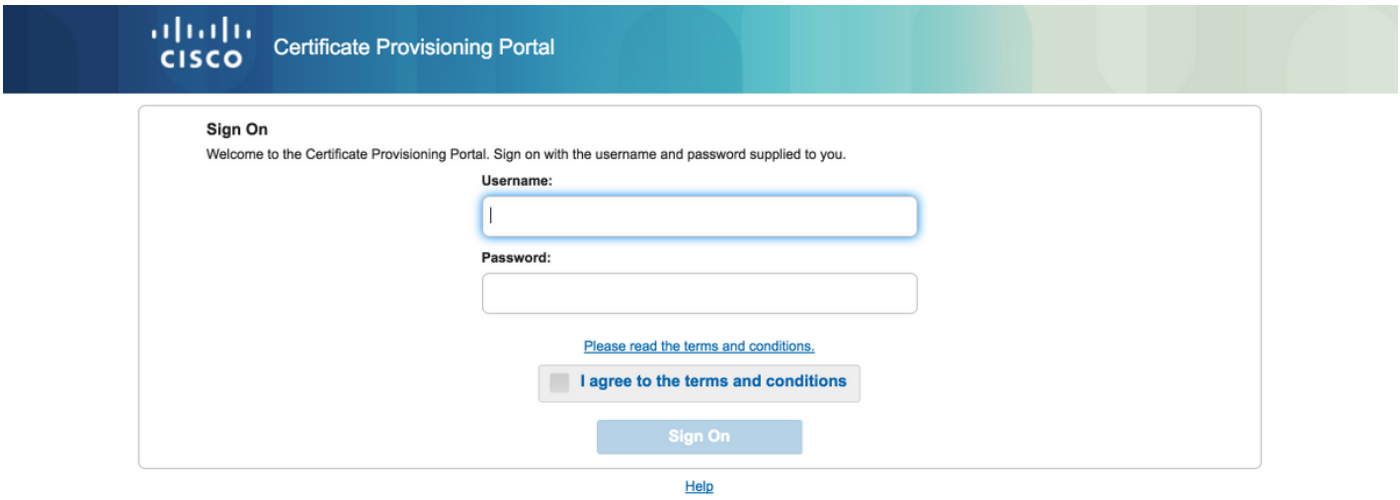
Zusätzlich kann das Portal durch Navigieren zur Registerkarte **für die Anpassung der Portalseite** weiter angepasst werden, auf der der AUP-Text, der Text des Anmeldebanners und andere Nachrichten entsprechend den Anforderungen geändert werden können.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Wenn die ISE für die Zertifikatsbereitstellung korrekt konfiguriert ist, kann ein Zertifikat mit diesen Schritten vom ISE-Zertifikatsbereitstellungsportal angefordert/heruntergeladen werden.

Schritt 1: Öffnen Sie den Browser, und rufen Sie das Portal für die Zertifikatsbereitstellung FQDN (wie oben konfiguriert) oder die URL für den Test zur Zertifikatsbereitstellung auf. Sie werden zum Portal umgeleitet, wie in diesem Bild gezeigt:



Schritt 2**:** Melden Sie sich mit Benutzername und Kennwort an.

Schritt 3: Akzeptieren Sie nach erfolgreicher Authentifizierung AUP, und es wird die Seite für die Zertifikatsbereitstellung angezeigt.

Schritt 4: Auf der Seite für die Zertifikatsbereitstellung stehen drei Möglichkeiten zum Herunterladen von Zertifikaten zur Verfügung:

- Einzelzertifikat (ohne Anforderung zur Signierung des Zertifikats)
- Einzelnes Zertifikat (mit Anforderung für Zertifikatssignierung)
- Massenzertifikate

Generieren eines einzelnen Zertifikats ohne Zertifikatssignierungsanforderung

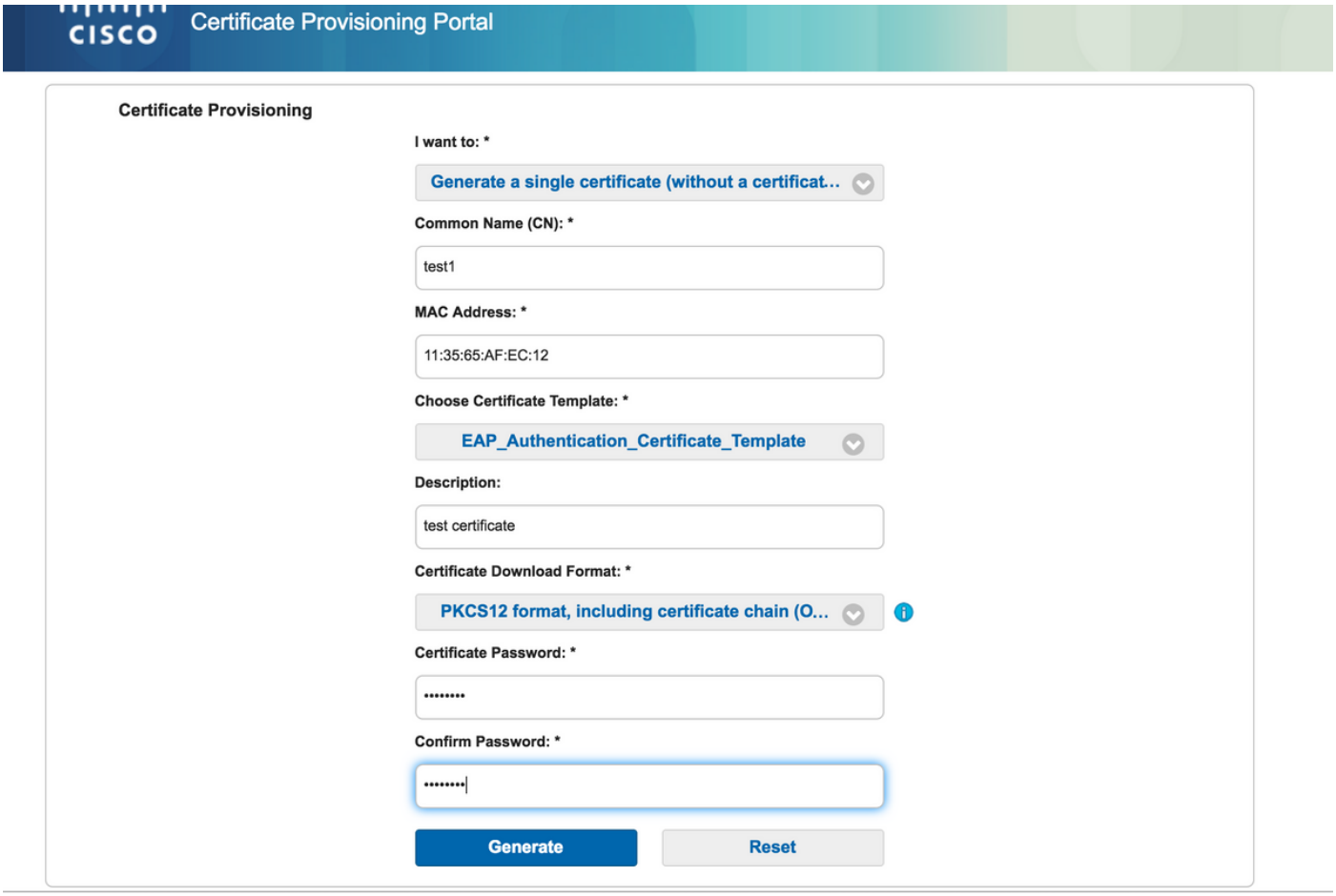
- Um ein einzelnes Zertifikat ohne CSR zu generieren, wählen Sie die Option **Einzelzertifikat generieren (ohne Zertifikatssignierungsanfrage) aus**.

- Geben Sie den allgemeinen Namen (CN) ein.

  Hinweis: Die angegebene CN muss mit dem Benutzernamen des Antragstellers übereinstimmen. Der Antragsteller bezieht sich auf den Benutzernamen, der für die Anmeldung beim Portal verwendet wird. Nur Admin-Benutzer können ein Zertifikat für einen anderen CN erstellen.

- Geben Sie die MAC-Adresse des Geräts ein, für das das Zertifikat generiert wird.

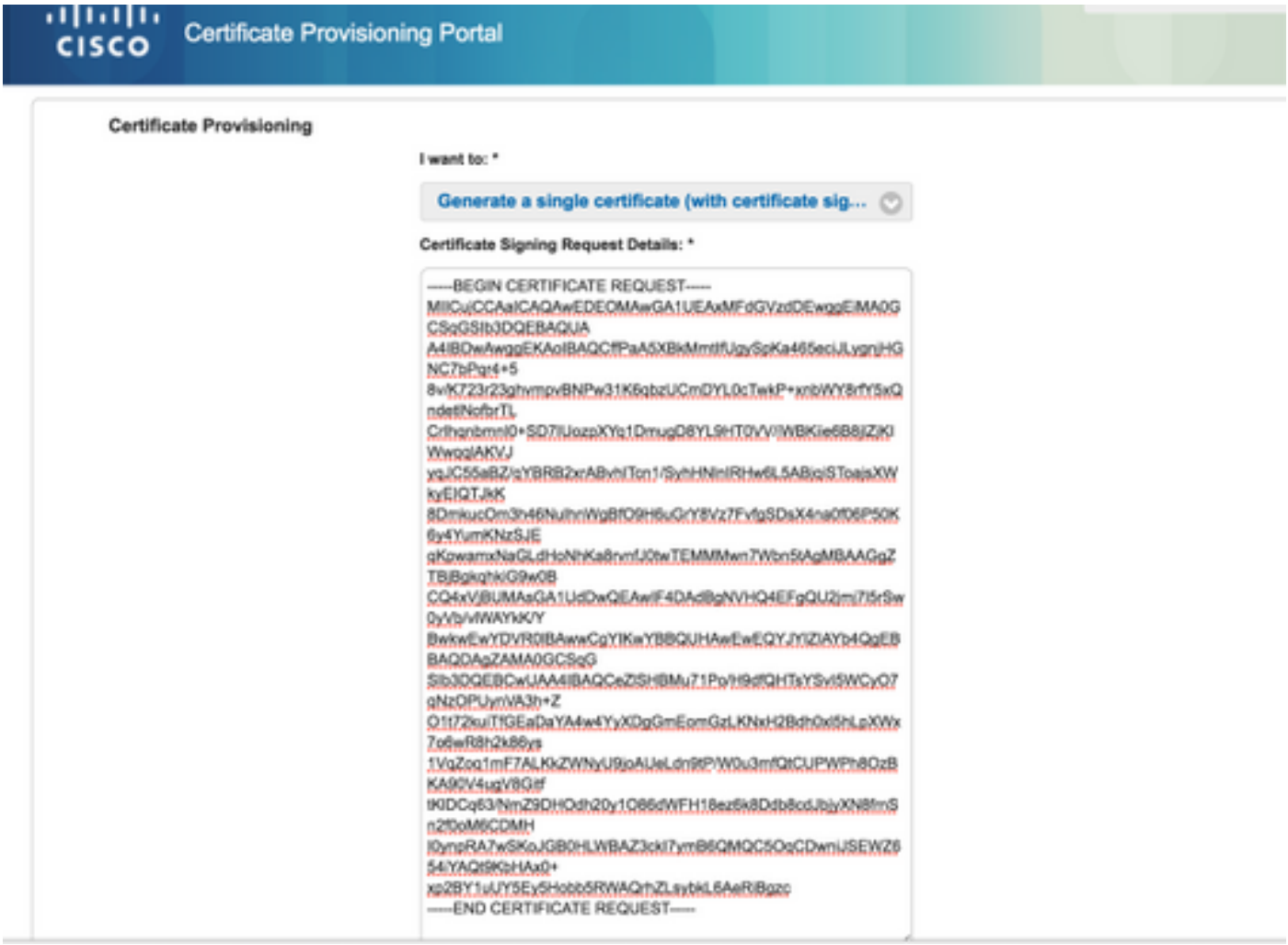
- Wählen Sie die entsprechende Zertifikatsvorlage aus.
- Wählen Sie das gewünschte Format aus, in dem das Zertifikat heruntergeladen werden soll.
- Geben Sie ein Zertifikatkennwort ein, und klicken Sie auf **G.Generieren.**
- Es wird ein einzelnes Zertifikat erstellt und erfolgreich heruntergeladen.

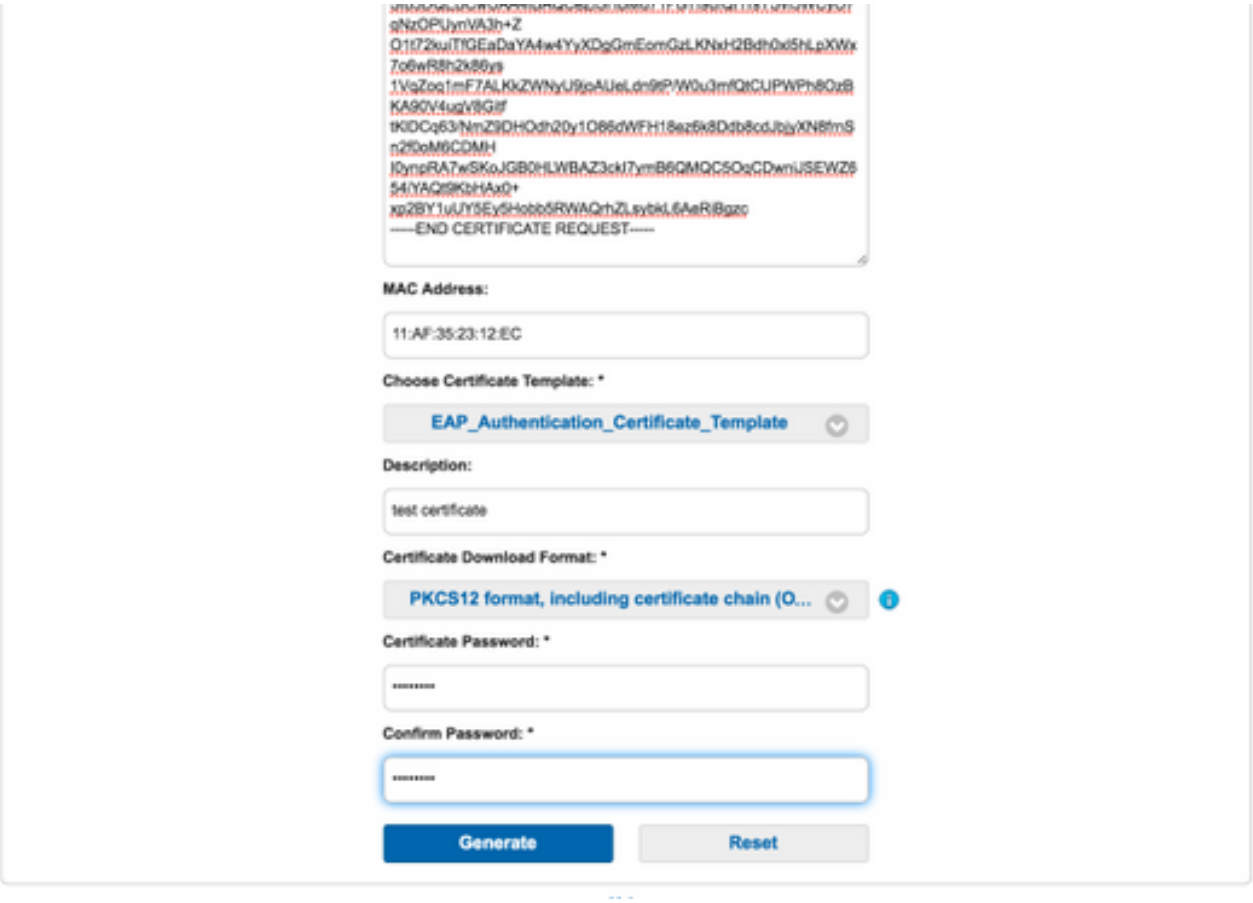


Generieren eines einzelnen Zertifikats mit Zertifikatssignierungsanforderung

- Um ein einzelnes Zertifikat ohne CSR zu generieren, wählen Sie die Option **Einzelzertifikat (mit Zertifikatssignierungsanfrage)** erstellen.
- Kopieren Sie den CSR-Inhalt aus der Notizblock-Datei unter **Details** der **Zertifikatsanforderung**.
- Geben Sie die MAC-Adresse des Geräts ein, für das das Zertifikat generiert wird.
- Wählen Sie die entsprechende Zertifikatsvorlage aus.
- Wählen Sie das gewünschte Format aus, in dem das Zertifikat heruntergeladen werden soll.
- Geben Sie ein Zertifikatskennwort ein, und klicken Sie auf **Generate (Generieren)**.

- Es wird ein einziges Zertifikat erstellt und erfolgreich heruntergeladen.



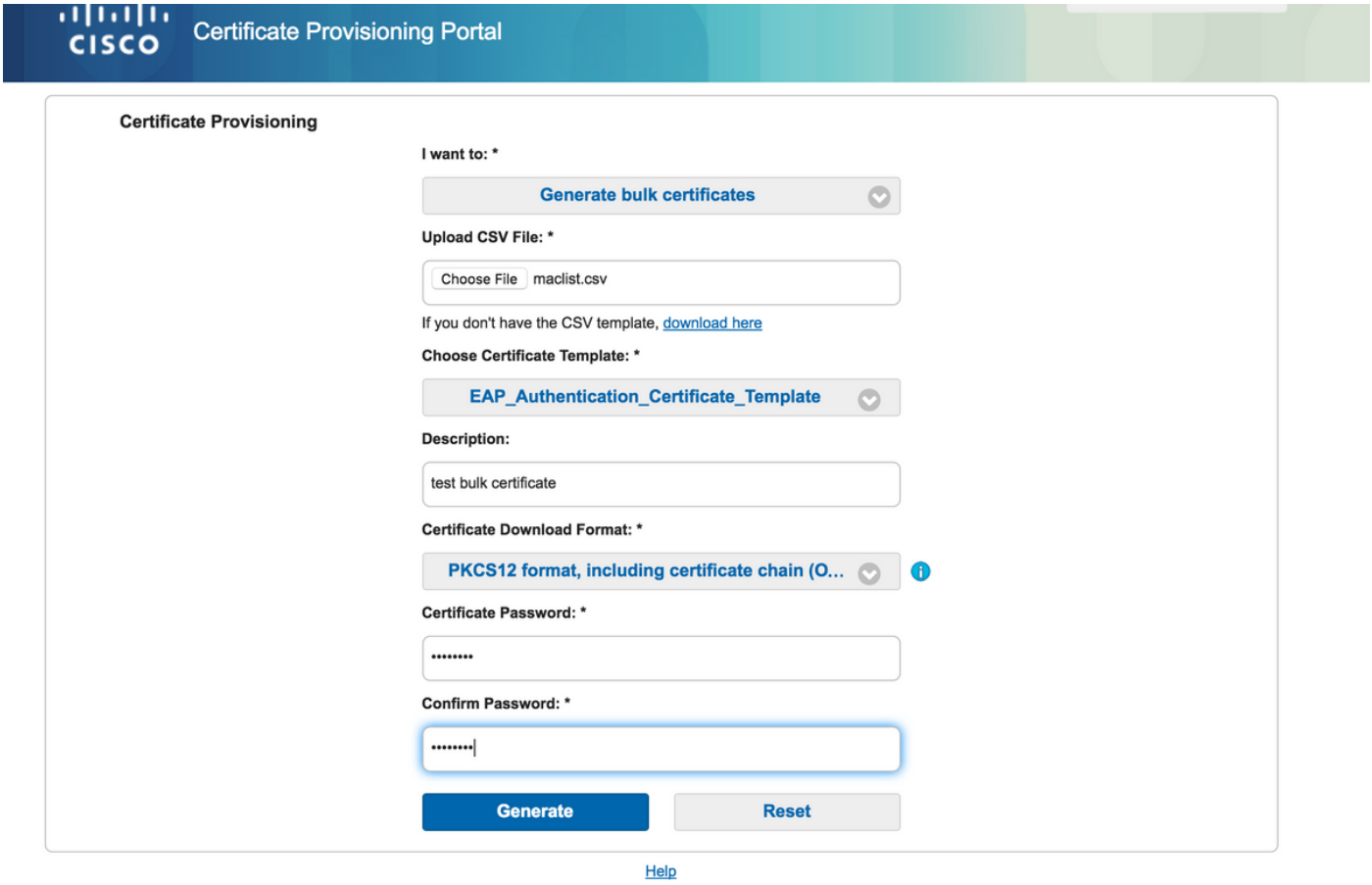


Generieren von Massenzertifikaten

Sie können Massenzertifikate für mehrere MAC-Adressen generieren, wenn Sie CSV-Dateien hochladen, die CN- und MAC-Adressfelder enthalten.

> **Hinweis**: Die angegebene CN muss mit dem Benutzernamen des Antragstellers übereinstimmen. Der Antragsteller bezieht sich auf den Benutzernamen, der für die Anmeldung beim Portal verwendet wird. Nur Admin-Benutzer können ein Zertifikat für einen anderen CN erstellen.

- Um ein einzelnes Zertifikat ohne CSR zu generieren, wählen Sie die Option **Einzelzertifikat generieren (mit Zertifikatssignierungsanfrage) aus**.
- Laden Sie die CSV-Datei für eine Massenanforderung hoch.
- Wählen Sie die entsprechende Zertifikatsvorlage aus.
- Wählen Sie das gewünschte Format aus, in dem das Zertifikat heruntergeladen werden soll.
- Geben Sie ein Zertifikatskennwort ein, und klicken Sie auf **Generate (Generieren)**.
- Eine ZIP-Datei für ein Massenzertifikat wird erstellt und heruntergeladen.



Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.