CITRIX

Citrix SSO for iOS

Contents

Overview

Citrix SSO provides best-in-class application access and data protection solution offered by Citrix Gateway. You can now securely access business critical applications, virtual desktops, and corporate data from anywhere at any time.

Citrix SSO is the next gen VPN client for Citrix Gateway built using Apple's Network Extension framework. It replaces the legacy Citrix VPN client on App Store.

Citrix SSO app provides complete Mobile Device Management (MDM) support on both MacOS and iOS. With an MDM server, an admin can now remotely configure and manage device level VPN profiles and per-app VPN profiles.

What's new

The legacy Citrix VPN client was built using Apple's private VPN APIs that have now been deprecated. VPN support in Citrix SSO has been rewritten from the ground up using Apple's public Network Extension framework.

Following are some of the major features introduced with Citrix SSO app:

- **Password Tokens** - A password token is a 6-digit code which is an alternative to Secondary Password Services such as VIP, OKTA etc. This code uses the Time-based One Time Password (T-OTP) protocol to generate the OTP code similar to services such as Google Authenticator, Microsoft Authenticator etc. Users are prompted for two passwords during authentication to Citrix Gateway for a given Active Directory user. The second factor is a changing six-digit code that users copy from a registered third-party service such as Google or Microsoft Authenticator into the desktop browser.

  Users need to first register for T-OTP on the Citrix ADC appliance. For registration steps, refer https://support.citrix.com/article/CTX228454. On the app, users can add the OTP feature by scanning the QR Code generated on Citrix ADC or manually entering the TOTP secret. OTP Tokens once added will show up on the Password Tokens segment on the user interface.

  To improve the experience, adding an OTP will prompt the user to create a VPN profile automatically. Users can take advantage of this VPN profile to connect to VPN directly from their iOS devices.

  Note

- Citrix SSO app can be used to scan the QR code while registering for Native OTP support. Citrix Gateway Push notification functionality is available only to the Citrix SSO app users.

- The **Password Tokens** feature is available on Citrix SSO for iOS users only.

- **Push notification** – Citrix Gateway sends Push notification on your registered mobile device for a simplified two-factor authentication experience. Instead of opening the Citrix SSO app to type in the second factor OTP on the Citrix ADC logon page, you can validate your identity by providing your Device PIN/Touch ID/ Face ID for the registered device.

  Note

  - Once you register your device for Push notification, you can also use the device for Native OTP support using the Citrix SSO app. Registration for Push Notifications is transparent to the user. When users register TOTP, device is also registered for Push Notifications if Citrix ADC supports it.

  - The **Push notification** feature is available on Citrix SSO for iOS users only.

Known issues and fixed issues

The following are the issues at this time.

Known issues

- **Issue description**: Tunneling for FQDN addresses that contain a ".local" domain in Per-App VPN or On-Demand VPN configurations. There is currently a bug in Apple's Network Extension framework which stops FQDN addresses containing .local in the domain part (ex: http://wwww.abc.local) from being tunneled over the system's TUN interface. The traffic for this address is sent out via the device's physical interface instead. The issue is observed only with Per-App VPN or On-Demand VPN configs and is not seen with system-wide VPN configurations. Citrix has filed a radar bug report with Apple, and Apple had noted that according to RFC-6762: https://tools.ietf.org/html/rfc6762, .local is a multicast DNS (mDNS) query and is hence not a bug. However, Apple has not closed the bug yet and it is not clear if the issue will be addressed in future iOS releases.
  Workaround: Assign a non .local domain name for such addresses as the workaround.

Feature Comparison between Citrix VPN and Citrix SSO

IMPORTANT: Citrix VPN cannot be used on iOS 12. It will be taken down by end of 2018. To continue to VPN, use the Citrix SSO app.

The following table compares the availability of various features between Citrix VPN and Citrix SSO.

Feature	Citrix VPN	Citrix SSO
Device level VPN	✓	✓
Per-App VPN (MDM only)	✓	✓
MDM configured VPN profiles	✓	✓
On-Demand VPN	✓	✓
Password Tokens (T-OTP based)	×	✓
Push Notifications based login (Second Factor from registered Phone)	×	✓
Certificate based Authentication	✓	✓
User Name/Password Authentication	✓	✓
Network Access Control Check with Citrix Endpoint Management (formerly XenMobile)	×	✓
Network Access Control Check with Microsoft Intune	✓	✓
DTLS support	×	✓
Block User Created VPN Profiles	✓	✓

Compatibility with MDM products

Citrix SSO works with most MDM providers such as Citrix **Endpoint Management (**formerly XenMobile**)**, Microsoft Intune etc. Citrix SSO also supports a feature called Network Access Control (NAC). For more on NAC, click here. With NAC, MDM administrators can enforce end user device compliance before connecting to Citrix ADC. NAC on Citrix SSO requires an MDM server such as Citrix Endpoint Management or Intune and Citrix ADC.

Configure an MDM managed VPN profile for Citrix SSO

The following section explains the step by step instructions to configure both device-wide and per-app VPN profiles for Citrix SSO using Citrix **Endpoint Management** (formerly XenMobile**)** as an example. Other MDM solutions can use this document as reference when working with Citrix SSO.

Note: This section explains the configuration steps for a basic Device-wide and Per-App VPN profile. Additionally you can configure On-Demand, Always-On, Proxies by following Citrix **Endpoint Management** (formerly XenMobile**)** documentation or Apple's MDM VPN payload configuration.

Device level VPN Profiles

Device level VPN profiles are used to setup a system wide VPN. Traffic from all apps and services is tunneled to Citrix Gateway based on the VPN policies (such as Full-tunnel, Split-tunnel, Reverse Split-tunnel etc.) defined in Citrix ADC.

Following are the steps to configure a device level VPN on Citrix **Endpoint Management** (formerly XenMobile**)**:

1. On the Citrix **Endpoint Management** MDM console, navigate to Configure > Device Policies > Add New Policy.

2. Select iOS and Mac OS on the left Policy Platform pane. Select VPN Policy on the right pane.

3. On the Policy Info page, type a valid Policy Name and Description and click next.

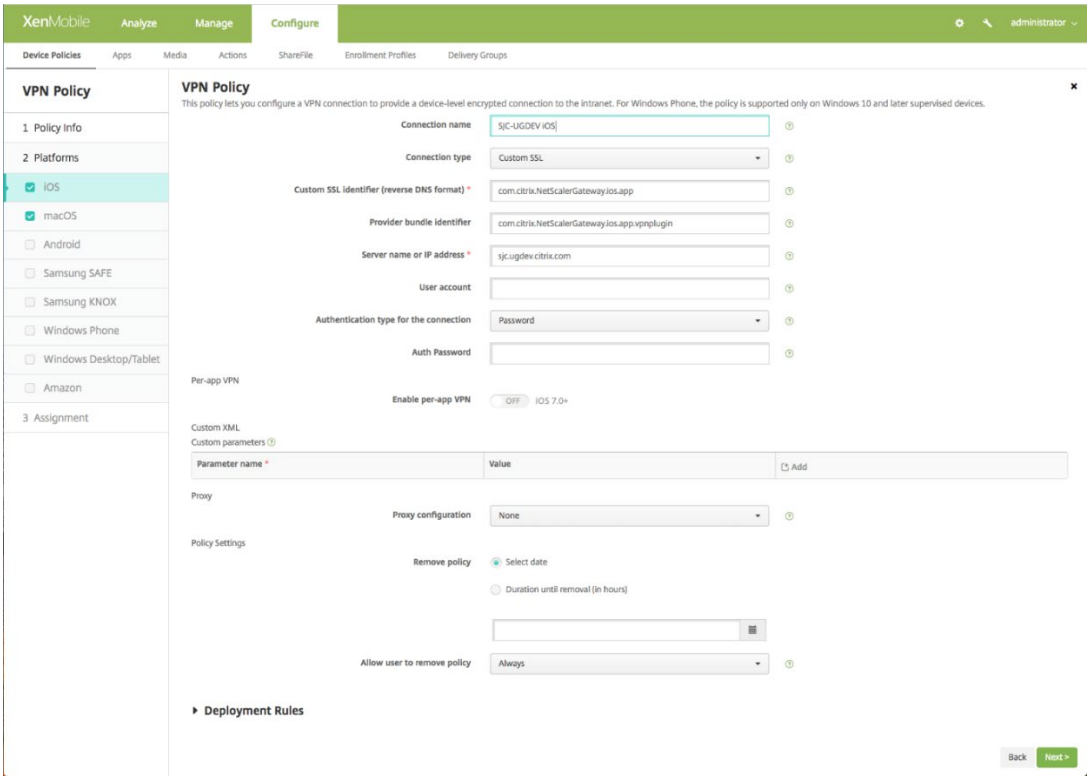
4. On the Policy detail page for iOS, type a valid Connection Name and choose "Custom SSL" from the Connection Type dropdown control.
   Note: In the MDM VPN payload, Connection Name corresponds to the "UserDefinedName" key and "VPN Type" Key must be set to value "VPN".

5. In the Custom SSL identifier (reverse DNS format) text field, type "com.citrix.NetScalerGateway.ios.app". This is the bundle identifier for the Citrix SSO App on iOS.
   Note: In the MDM VPN payload, Custom SSL identifier corresponds to the "VPNSubType" key.

6. In the Provider bundle identifier text field, type "com.citrix.NetScalerGateway.ios.app.vpnplugin". This is the bundle identifier of the Network Extension contained in the Citrix SSO iOS App binary.
   Note: In the MDM VPN payload, Provider bundle identifier corresponds to the "ProviderBundleIdentifier" key.

7. In the Server name or IP address text field, type the IP address or FQDN of the Citrix ADC associated with this Citrix Endpoint Management instance.

8. The remaining fields in the configuration page are optional. Configurations for these fields can be found in Citrix **Endpoint Management** (formerly XenMobile**)** documentation. The completed page should resemble the screenshot below. Click Next. You may go straight to point 13 from here if you do not need to configure VPN policy for MacOS. Proceed to the next step otherwise.

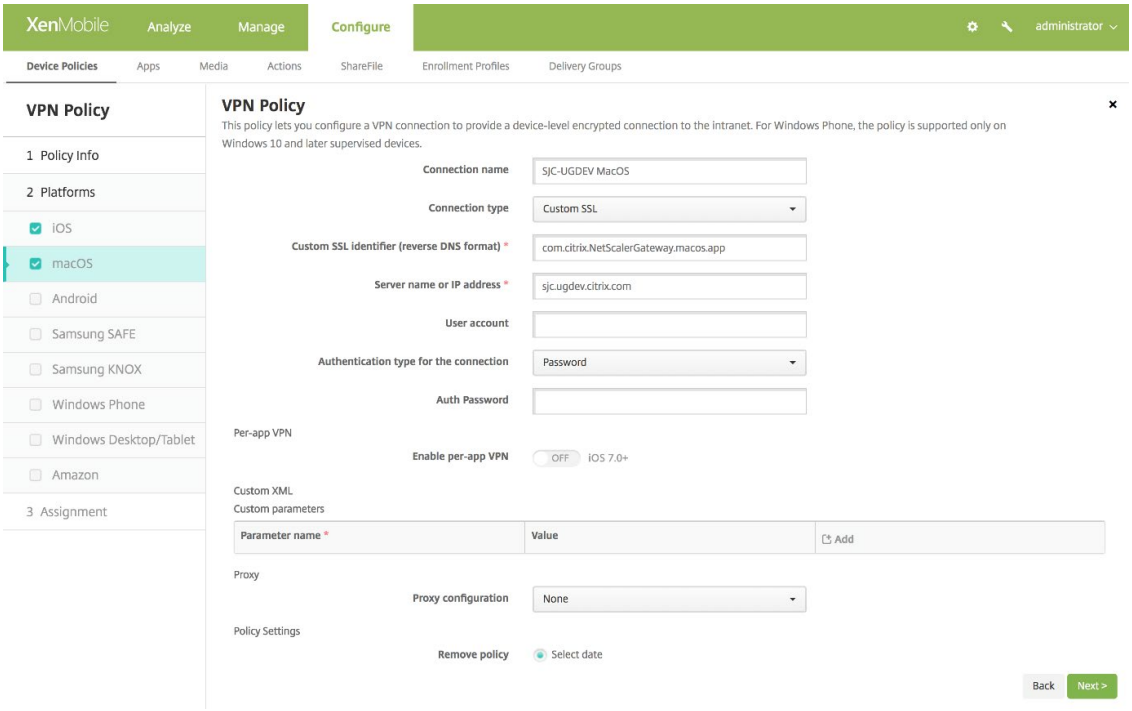


9. On the Policy detail page for MacOS, type a valid Connection Name and choose "Custom SSL" from the Connection Type dropdown control.

10. In the Custom SSL identifier (reverse DNS format) text field, type "com.citrix.NetScalerGateway.macos.app". This is the bundle identifier for the Citrix SSO App on Mac OS.

11. In the Server name or IP address text field, type the IP address or FQDN of the Citrix ADC associated with this Citrix Endpoint Management instance.

12. The remaining fields in the configuration page are optional. Configurations for these fields can be found in the Citrix **Endpoint Management** (formerly XenMobile**)** documentation. The completed page should resemble the screenshot below.



13. Click Next and choose a delivery group for this VPN profile. Click Save.

Per-App VPN Profiles

Per-App VPN profiles are used to setup VPN for a specific Application. Traffic from only the specific App is tunneled to Citrix Gateway. The Per-App VPN payload supports all of the keys for Device-wide VPN plus a few additional keys.

Following are the steps to configure a Per-App VPN on Citrix **Endpoint Management** (formerly XenMobile**)**:

1. Follow steps 1 to 7 as mentioned in configuring a Device-level VPN section.

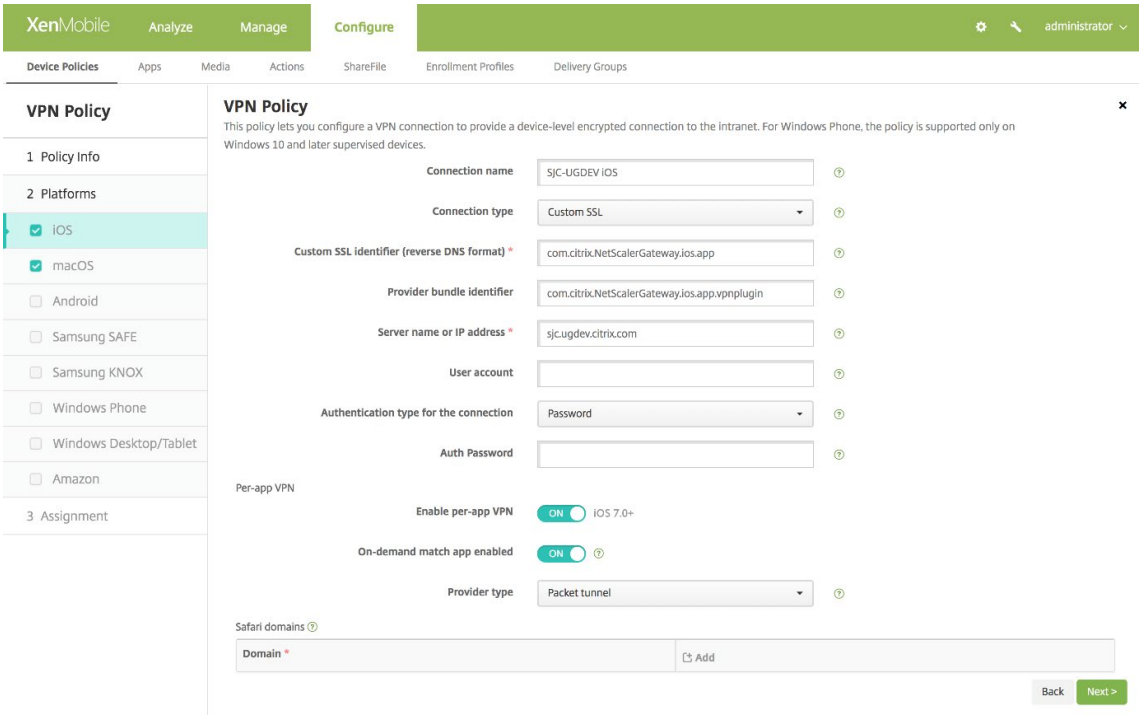
2. Turn the Enable Per-App VPN switch ON in the Per-App VPN section.

3. Turn the On-Demand Match App Enabled switch ON if Citrix SSO should be started automatically when the Match App is launched. This is recommended for most Per-App cases.
   Note: In the MDM VPN payload, this field corresponds to the key "OnDemandMatchAppEnabled".

4. Select "Packet Tunnel" in the Provider Type dropdown menu.
   Note: In the MDM VPN payload, this field corresponds to the key "ProviderType".

5. Safari Domain configuration is optional. Configuring this will start Citrix SSO automatically when users launch Safari and navigate to a URL that matches the one in Domain field. This is not recommended if you want to restrict VPN for a specific App.
   Note: In the MDM VPN payload, this field corresponds to the key "SafariDomains".

6. The remaining fields in the configuration page are optional. Configurations for these fields can be found in Citrix **Endpoint Management** (formerly XenMobile**)** documentation. The completed page should resemble the screenshot below. Click Next. You may go straight to point 13 from here if you do not need to configure the VPN policy for Mac OS. Proceed to the next step otherwise.



7. On the Policy detail page for MacOS, type a valid Connection Name and choose "Custom SSL" from the Connection Type dropdown control.

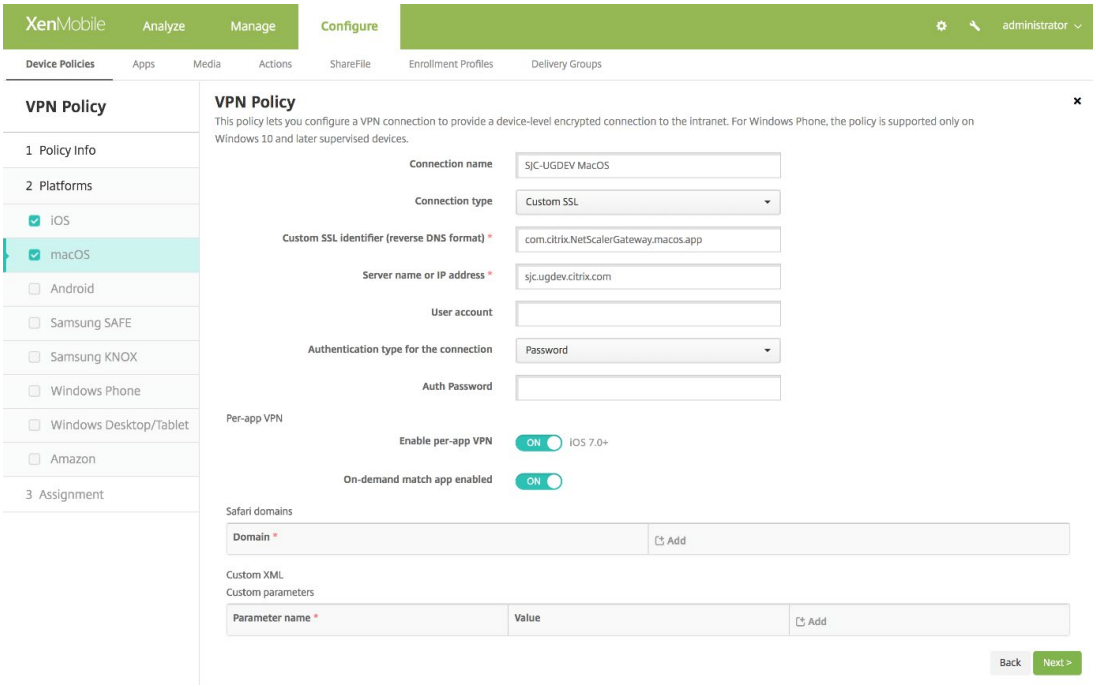
8. In the Custom SSL identifier (reverse DNS format) text field, type "com.citrix.NetScalerGateway.macos.app". This is the bundle identifier for the Citrix SSO App on Mac OS.

9. In the Server name or IP address text field, type the IP address or FQDN of the Citrix ADC associated with this Citrix Endpoint Management instance.

10. Turn the Enable Per-App VPN switch ON in the Per-App VPN section.

11. Turn the On-Demand Match App Enabled switch ON if Citrix SSO should be started automatically when the Match App is launched. This is recommended for most Per-App cases.

12. Safari Domain configuration is optional. Configuring this will start Citrix SSO automatically when users launch Safari and navigate to a URL that matches the one in Domain field. This is not recommended if you want restrict VPN for a specific App. The completed page should resemble the screenshot below.



13. Click **Next** and choose a delivery group for this VPN profile. Click **Save**.

14. Additionally, to associate this VPN profile to a specific App on the device, you need to create an App Inventory policy and a Credentials Provider policy by following this guide
    - https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/

Import Certificates into Citrix SSO for Client Authentication

Citrix SSO on iOS supports client certificate authentication with Citrix Gateway. On iOS, certificates can be delivered to the Citrix SSO app in one of two ways:

- **MDM server** - This is the preferred approach for MDM customers. Certificates are configured directly on the MDM managed VPN profile. Both VPN profiles and certificates are then pushed to enrolled devices when the device enrolls into the MDM server. Please follow MDM vendor specific documents for this approach.

- **Email** - Only approach for non-MDM customers. In this approach, administrators send an email with the User Certificate identity (Certificate and private key) attached as a PCKS#12 file to users. Users need to have their email accounts configured on their iOS device to receive the email with attachment. The file may then be imported to the Citrix SSO app on the iOS. The following section explains the configuration steps for this approach.

Prerequisites:

1. User Certificate - A PKCS#12 identity file with a .pfx or .p12 extension for a given user. This file contains both the certificate and the private key.

2. Email account configured on the iOS device.

3. Citrix SSO app installed on the iOS device.

Configuration Steps:

1. **Rename the Extension/MIME type of the User Certificate**

   File extensions most commonly used for user certificate are ".pfx", ".p12", and so forth. These file extensions are non-standard to the iOS platform unlike formats such as .pdf, .doc, and so forth. Both ".pfx" and ".p12" are claimed by the iOS System and cannot be claimed by 3rd party Apps such as Citrix SSO. Hence Citrix SSO has defined a new Extension/MIME type called ".citrixsso-pfx" and ".citrixsso-p12". Administrators must change the Extension/MIME type of the User Certificate, from standard ".pfx" or ".p12" to ".citrixsso-pfx" or ".citrixsso-p12" respectively. To rename the extension, admins can run the following command on Command Prompt or Terminal.

Windows 10

```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
rename <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-pfx
```

MacOS

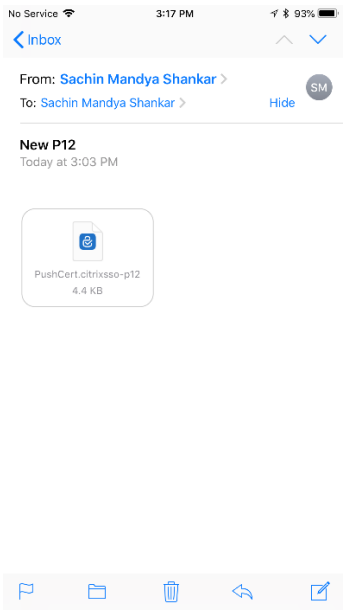
```
cd <DIRECTORY_PATH_TO_CERTIFICATE_FILE>
mv <CERTIFICATE_FILE_NAME>.pfx <CERTIFICATE_FILE_NAME>.citrixsso-pfx
```

2. **Send the file as an Email Attachment**

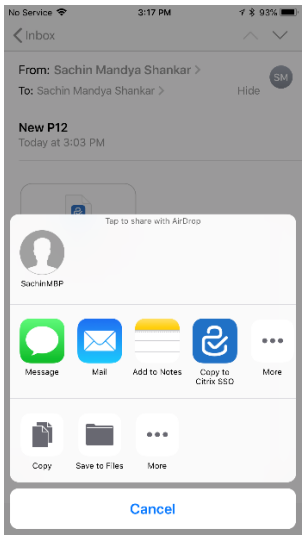
   The User Certificate file with the new extension can now be sent as an email attachment to the user.

3. **Open Email with Citrix SSO App**

   a. On receipt of the email, users must tap on the attachment to reveal the System "Open-In" menu.

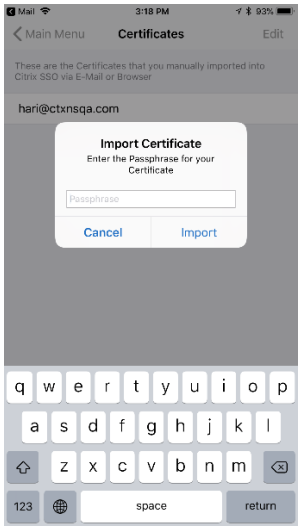


b. Tap **Copy to Citrix SSO**.

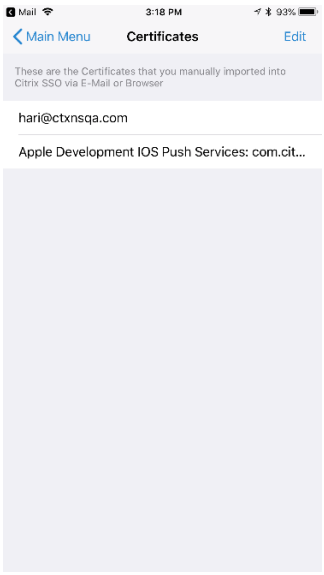


4. **Install Certificate in Citrix SSO App**

a. The App is now launched and a prompt for the Certificate Passphrase is shown to the user. User needs to enter the correct Passphrase for the certificate to be installed into the app's keychain.

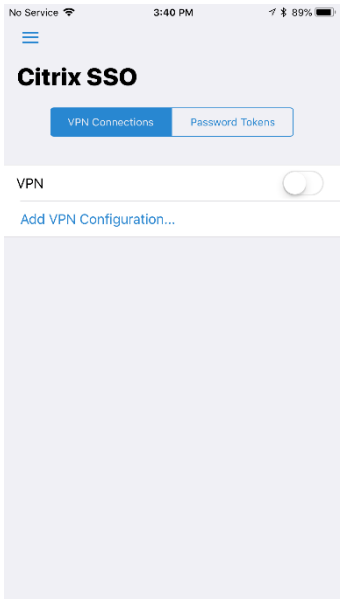


b. Upon successful validation, the certificate is imported.

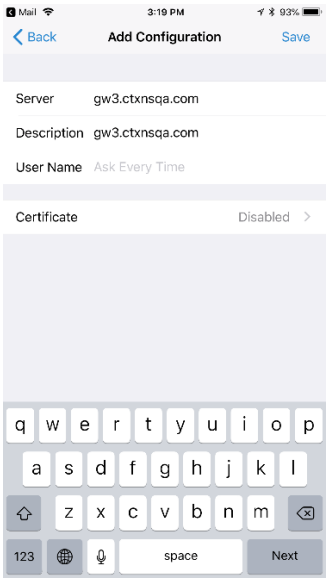


5. **Using Certificate based Authentication with VPN**

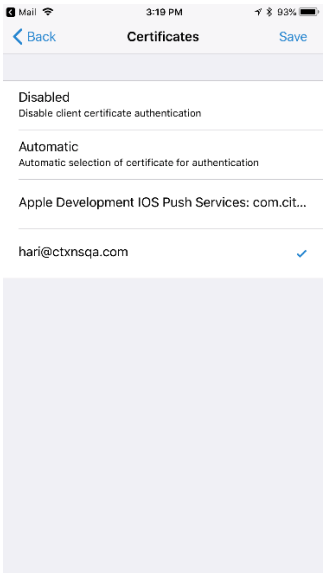
    a. To use the certificate for VPN authentication, users first need to create a new VPN Configuration/Profile on Citrix SSO. Navigate to the **VPN Connections** view and tap on **Add VPN Configuration**.



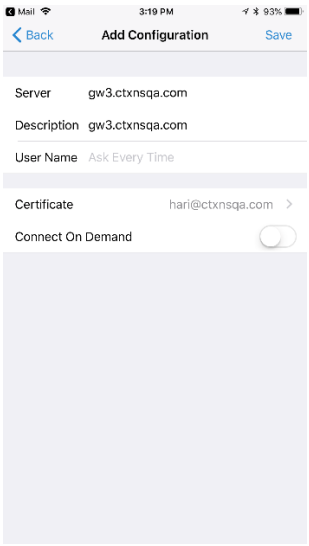
b. On the configuration view of the VPN profile, user can select the imported Certificate in the Certificates configuration section.



c. Tap **Save** to import the certificate.



d. Upon successful importing of certificate, the following screen appears.



6. **Managing Certificates**

   Certificates imported this way into Citrix SSO may be managed by the user by navigating to **App Settings > Certificates**.

FAQs

This section provides the frequently asked questions on the Citrix SSO app.

How is Citrix SSO app different from Citrix VPN app?

Citrix SSO is the next generation SSL VPN client for Citrix ADC. The App uses Apple's Network Extension framework to create and manage VPN connections on iOS and MacOS devices. Citrix VPN is the legacy VPN client that made use of Apple's private VPN APIs which is now deprecated. Support for Citrix VPN will be removed from the App Store in the months to come.

What is NE?

The Network Extension (NE) framework from Apple is a modern library which contains APIs that can be used to customize and extend the core networking features of iOS and macOS. Network Extension with support for SSL VPN is available on devices running iOS 9+ and MacOS 10.11+.

For which versions of Citrix ADC is the Citrix SSO compatible?

VPN features in Citrix SSO are supported on Citrix ADC versions 10.5 and above. The TOTP is available on Citrix ADC version 12.0 and above. Push Notification on Citrix ADC has not been publicly announced yet. The App requires iOS 9+ and MacOS 10.11+ versions.

How does Cert-based authentication for non-MDM customers work?

Customers who previously distributed Certificates via Email or Browser to perform Client Certificate Authentication in Citrix VPN should note this change when using Citrix SSO. This is mostly true for non-MDM customers who do not use an MDM Server to distribute User Certificates. Please refer, "Importing Certificates into Citrix SSO via Email" to be able to distribute Certificates.

What is Network Access Control (NAC)? How do I configure NAC with Citrix SSO and Citrix Gateway?

Microsoft Intune and Citrix Endpoint Management (formerly XenMobile) MDM customers can take advantage of Network Access Control (NAC) feature in Citrix SSO. With NAC, administrators can secure their enterprise internal network by adding an additional layer of authentication for mobile devices that are managed by an MDM server. Administrators can enforce a device compliancy check at the time of authentication in Citrix SSO.

To use NAC with Citrix SSO, you must enable it on both Citrix Gateway and the MDM server.

Perform the following steps:

- To enable NAC on Citrix ADC refer this link.
- If MDM vendor is Intune refer this link.
- If MDM vendor is Citrix **Endpoint Management** (formerly XenMobile**)** refer this link.

Note: The minimum supported Citrix SSO version is 1.1.6 and above.