Citrix SSO
Contents

Citrix SSO for iOS/macOS devices 3

Release Notes 3

Set up Citrix SSO for iOS users 5

Send user certificate identity as an email attachment to iOS users 13

Set up Citrix SSO for macOS users 14

FAQs 23

Citrix SSO for Android devices 24

Release Notes 24

Set up Citrix SSO app in a MDM environment 26
The legacy Citrix VPN client was built using Apple’s private VPN APIs that is now deprecated. VPN support in Citrix SSO is 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, and so on. 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 and so on. 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 must first register for T-OTP on the Citrix ADC appliance. For registration steps, refer [https://support.citrix.com/article/CTX228454](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 show up on the Password Tokens segment on the user interface.

To improve the experience, adding an OTP prompts 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.

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.

- **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.

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.

**Release Notes**

June 12, 2019

The Citrix SSO release notes describe the new features, enhancements to existing features, fixed issues, and known issues available in a service release. The release notes includes one or more of the
following sections:

**What’s new:** The new features and enhancements available in the current release.

**Fixed issues:** The issues that are fixed in the current release.

**Known issues:** The issues that exist in the current release and their workarounds, wherever applicable.

---

**Release Notes for 1.1.12 version of Citrix SSO iOS/Citrix SSO macOS client release**

**What’s new**

- **Telemetry data collection for macOS.** Citrix SSO collects custom analytics events related to VPN usage in the app.
  
  [CGOP-9789 - macOS]

- **Per-app split tunnel support.** Administrators can configure per-app split tunnel. Per-app traffic that matches the intranet routes for Citrix Gateway is tunneled to the Citrix Gateway appliance.
  
  [CGOP-657]

- **FQDN Split Tunnel tunnels traffic based on the FQDN of the system.** FQDN Split Tunnel tunnels traffic based on the FQDN of the system rather than the IP resolved by the DNS servers.
  
  [CGOP-316]

**Fixed issues**

- User interface elements such as buttons, text fields, labels and so forth are misaligned across iPad screens.
  
  [CGOP-10141 - iOS]

- Users are not notified for a remote login if they do not have a VPN profile added.
  
  [CGOP-9731 - iOS]

---

**Release Notes for 1.1.10 version of Citrix SSO iOS/Citrix SSO macOS client release**

**Fixed issues**

- Citrix SSO app doesn’t display proper error message upon reaching the when the maximum number of users.
  
  [CGOP-231]
Citrix SSO

- EULA checkbox is not unchecked by default.
  [CGOP-245]
- Add functionality is not supported for antiphishing “enabled” scan in EndPoint Analysis.
  [CGOP-249]
- Automatic selection of client/device certificate for authentication does not happen even if only one client/device is present in the keychain.
  [CGOP-251]
- Unable to add a ‘connection record’ after editing one in Citrix SSO app.
  [CGOP-7256]

Set up Citrix SSO for iOS users

June 14, 2019

**IMPORTANT:** Citrix VPN cannot be used on iOS 12 and later. To continue to VPN, use the Citrix SSO app.

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

<table>
<thead>
<tr>
<th>Feature</th>
<th>Citrix VPN</th>
<th>Citrix SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device level VPN</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Per-App VPN (MDM only)</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Per-App split tunnel</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>MDM configured VPN profiles</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>On-Demand VPN</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Password Tokens (T-OTP based)</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Push Notifications based login (Second Factor from registered Phone)</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Certificate based Authentication</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>User Name/Password Authentication</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>
Citrix SSO

<table>
<thead>
<tr>
<th>Feature</th>
<th>Citrix VPN</th>
<th>Citrix SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Access Control Check with Citrix Endpoint Management (formerly XenMobile)</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Network Access Control Check with Microsoft Intune</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>DTLS support</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Block User Created VPN Profiles</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Single Sign On for native apps managed by Citrix Cloud</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Supported OS version</td>
<td>iOS 9, 10, 11 (does not work from iOS 12+)</td>
<td>iOS 9+</td>
</tr>
</tbody>
</table>

**Compatibility with MDM products**

Citrix SSO is compatible with most MDM providers such as Citrix Endpoint Management (formerly XenMobile), Microsoft Intune and so on.

Citrix SSO also supports a feature called Network Access Control (NAC). For more information 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 captures 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. Also 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 set up 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) defined in Citrix ADC.

To configure a device level VPN on Citrix Endpoint Management

Perform the following steps to configure a device level VPN on Citrix Endpoint Management.
2. Select iOS on the left Policy Platform pane. Select VPN on the right pane.
3. On the Policy Info page, enter a valid policy name and description and click Next.
4. On the VPN Policy page for iOS, type a valid connection name and choose Custom SSL in Connection Type.

Note: In the MDM VPN payload, connection name corresponds to the UserDefinedName key and VPN Type Key must be set to VPN.

5. In Custom SSL identifier (reverse DNS format), enter 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 Provider bundle identifier enter 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 MDM VPN payload, provider bundle identifier corresponds to the ProviderBundleIdentifier key.

7. In Server name or IP address enter the IP address or FQDN (fully qualified domain name) of the Citrix ADC associated with this Citrix Endpoint Management instance.

The remaining fields in the configuration page are optional. Configurations for these fields can be found in Citrix Endpoint Management (formerly XenMobile) documentation.

8. Click Next.
Per-App VPN profiles

Per-App VPN profiles are used to set up 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.

To configure a per-App level VPN on Citrix Endpoint Management

Perform the following steps to configure a Per-App VPN:

1. Complete the device level VPN configuration on Citrix Endpoint Management.
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. In Provider Type, select Packet Tunnel.

   **Note:** In the MDM VPN payload, this field corresponds to the key `Provider Type`.

5. Safari Domain configuration is optional. When Safari domain is configured, Citrix SSO starts 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`.

The remaining fields in the configuration page are optional. Configurations for these fields can be found in Citrix Endpoint Management (formerly XenMobile) documentation.
14. Click **Next**.

15. Click **Save**.

To associate this VPN profile to a specific App on the device, you must 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/.

**Configuring split tunnel in Per-App VPN**

MDM customers can configure split tunnel in Per-App VPN for Citrix SSO. To do this, the following key/value pair must be added to the vendor configuration section of the VPN profile created on MDM server.

```
1. Key = "PerAppSplitTunnel"
2. Value = "true or 1 or yes"
```

The key is case sensitive and should be an exact match while value is not case sensitive.

**Note:** The user interface to configure vendor configuration is not standard across MDM vendors. You must contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.
The following is a sample screenshot of the configuration (vendor specific settings) in Microsoft Intune.

Disabling user created VPN profiles

MDM customers can prevent users from manually creating VPN profiles from within the Citrix SSO App. To do this, the following key/value pair must be added to the vendor configuration section of the VPN

© 1999-2019 Citrix Systems, Inc. All rights reserved.
profile created on MDM server.

1 - Key = "disableUserProfiles"
2 - Value = "true or 1 or yes"

The key is case sensitive and should be an exact match while value is not case sensitive.

**Note:** The user interface to configure vendor configuration is not standard across MDM vendors. You must contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.

The following is a sample screenshot of the configuration (vendor specific settings) in Microsoft Intune.
Known issues

**Issue description**: Tunneling for FQDN addresses that contain a “.local” domain in Per-App VPN or On-Demand VPN configurations. There is a bug in Apple’s Network Extension framework which stops FQDN addresses containing .local in the domain part (for example, http://www.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.

**Limitations**

- FQDN based split tunneling is not fully supported yet.
- Endpoint Analysis (EPA) is not supported on iOS.
- Split tunneling based on ports/protocols is not supported.
Send user certificate identity as an email attachment to iOS users

June 12, 2019

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 following 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**

- 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.

- Email account configured on the iOS device.

- 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. Both “.pfx” and “.p12” are claimed by the iOS System and cannot be claimed by third-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**
2. Send the file as an email attachment.
The User Certificate file with the new extension can be sent as an email attachment to the user.

On receipt of the email, users must install the certificate in Citrix SSO app.

## Set up Citrix SSO for macOS users

June 14, 2019

Citrix SSO app for macOS 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 generation VPN client for Citrix Gateway to create and manage VPN connections from macOS devices. Citrix SSO is built using Apple’s Network Extension (NE) framework. NE framework from Apple is a modern library which contains APIs that can be used to customize and extend core networking features of macOS. Network Extension with support for SSL VPN is available on devices running macOS 10.11+.

Citrix SSO app replaces the legacy Citrix Gateway plug-in that was based on Kernel Extensions (KE) which is going to be deprecated by Apple soon. Citrix SSO App supports advanced features like Server Initiated Connections and DTLS.

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

Citrix SSO app for macOS can be installed from a Mac App store.

### Feature comparison between Citrix VPN and Citrix SSO

The following table compares the availability of various features between Citrix VPN and Citrix SSO.
<table>
<thead>
<tr>
<th>Feature</th>
<th>Citrix VPN</th>
<th>Citrix SSO</th>
</tr>
</thead>
<tbody>
<tr>
<td>App distribution method</td>
<td>Citrix Downloads page</td>
<td>App Store</td>
</tr>
<tr>
<td>Number of tunneled connections</td>
<td>128</td>
<td>128</td>
</tr>
<tr>
<td>Access from browser</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Access from native app</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Split tunnel (OFF/ON/REVERSE)</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Split DNS (LOCAL/REMOTE/BOTH)</td>
<td>REMOTE</td>
<td>REMOTE</td>
</tr>
<tr>
<td>Local LAN access</td>
<td>Enable/Disable</td>
<td>Always enabled</td>
</tr>
<tr>
<td>Server Initiated Connections (SIC) support</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Transfer login</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Client side proxy</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Classic/Opswat EPA support</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Device certificate support</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Session timeout support</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Forced timeout support</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Idle timeout support</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>IPV6</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Network roaming (Switch between Wi-Fi, Ethernet, and so on)</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Intranet application support</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>DTLS support for UDP</td>
<td>Not supported</td>
<td>Supported</td>
</tr>
<tr>
<td>EULA support</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>App + Receiver integration</td>
<td>Supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Authentication – Local, LDAP, RADIUS</td>
<td>Supported</td>
<td>Supported</td>
</tr>
<tr>
<td>Client certificate authentication</td>
<td>Supported</td>
<td>Supported</td>
</tr>
</tbody>
</table>
### Compatibility with MDM products

Citrix SSO for macOS is compatible with most MDM providers such as Citrix XenMobile, Microsoft Intune and so on. It supports a feature called Network Access Control (NAC) using which, MDM administrators can enforce end user device compliance before connecting to Citrix Gateway. NAC on Citrix SSO requires an MDM server such as XenMobile or Intune and Citrix Gateway. For more on NAC, click [here](#).

### Configure an MDM managed VPN profile for Citrix SSO

The following section captures 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. Also 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 set up 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) defined in Citrix ADC.

#### To configure a device level VPN on Citrix Endpoint Management

Perform the following steps to configure a device level VPN.

3. On the Policy Info page, enter a valid policy name and description and click Next.
4. On the Policy detail page for macOS, type a valid connection name and choose **Custom SSL** in **Connection Type**.

**Note**: In the MDM VPN payload, connection name corresponds to the **UserDefinedName** key and **VPN Type Key** must be set to **VPN**.

5. In **Custom SSL identifier (reverse DNS format)**, enter `com.citrix.NetScalerGateway.macos.app`. This is the bundle identifier for the Citrix SSO App on macOS.

**Note**: In the MDM VPN payload, Custom SSL identifier corresponds to the **VPNSubType** key.

6. In **Provider bundle identifier** enter `com.citrix.NetScalerGateway.macos.app.vpnplugin`. This is the bundle identifier of the network extension contained in the Citrix SSO macOS app binary.

**Note**: In MDM VPN payload, provider bundle identifier corresponds to the **ProviderBundleIdentifier** key.

7. In **Server name or IP address** enter the IP address or FQDN of the Citrix ADC associated with this Citrix Endpoint Management instance.

The remaining fields in the configuration page are optional. Configurations for these fields can be found in Citrix Endpoint Management documentation.

8. Click **Next**.

9. Click **Save**.

**Per-App VPN profiles**

Per-App VPN profiles are used to set up 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.
To configure a per-App level VPN on Citrix Endpoint Management

Perform the following steps to configure a Per-App VPN on Citrix Endpoint Management:

1. Complete the device level VPN configuration on Citrix Endpoint Management.
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. Safari Domain configuration is optional. When Safari domain is configured, Citrix SSO starts 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**.

   The remaining fields in the configuration page are optional. Configurations for these fields can be found in Citrix Endpoint Management (formerly XenMobile) documentation.

13. Click **Next**.
14. Click **Save**.

To associate this VPN profile to a specific App on the device, you must 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/](https://www.citrix.com/blogs/2016/04/19/per-app-vpn-with-xenmobile-and-citrix-vpn/)

**Configuring split tunnel in Per-App VPN**

MDM customers can configure split tunnel in Per-App VPN for Citrix SSO. To do this, the following key/value pair must be added to the vendor configuration section of the VPN profile created on MDM
The key is case sensitive and should be an exact match while value is not case sensitive.

**Note:** The user interface to configure vendor configuration is not standard across MDM vendors. You must contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.

The following is a sample screenshot of the configuration (vendor specific settings) in Microsoft Intune.
Disabling user created VPN profiles

MDM customers can prevent users from manually creating VPN profiles from within the Citrix SSO App. To do this, the following key/value pair must be added to the vendor configuration section of the VPN profile created on MDM server.

1 - Key = "disableUserProfiles"
2 - Value = "true or 1 or yes"

The key is case sensitive and should be an exact match while value is not case sensitive.

**Note**: The user interface to configure vendor configuration is not standard across MDM vendors. You must contact the MDM vendor to find the vendor configuration section on your MDM user console.

The following is a sample screenshot of the configuration (vendor specific settings) in Citrix Endpoint Management.
Known issues

The following are the known issues currently.

- EPA login fails if the user is placed in quarantine group.
- Forced timeout warning message is not displayed.
SSO app allows login if split tunnel is ON and no intranet apps are configured.

Limitations

The following are the limitations currently.

- Some of the EPA scans (for example patch management scans, web browser scan, kill process) might fail because of restricted access to the SSO app due to sandboxing.
- Split tunneling based on ports/protocols is not supported.

FAQs

This section captures 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
Citrix SSO

can secure their enterprise internal network by adding an extra 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.

- 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.

FAQs

June 12, 2019

This section captures 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 extra layer of authentication for mobile devices that are managed by an MDM server. Administrators can enforce a device compliance 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.

- 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.

## Citrix SSO for Android devices

June 12, 2019

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.

## Release Notes

June 17, 2019

The Citrix SSO release notes describe the new features, enhancements to existing features, fixed issues, and known issues available in a service release. The release notes includes one or more of the following sections:

**What's new:** The new features and enhancements available in the current release.

**Fixed issues:** The issues that are fixed in the current release.

**Known issues:** The issues that exist in the current release and their workarounds, wherever applicable.

### V2.3.6

**What's new**

- **AlwaysON support for Citrix SSO**
The AlwaysON feature of Citrix SSO ensures that users are always connected to the enterprise network. This persistent VPN connectivity is achieved by automatic establishment of a VPN tunnel.

[CGOP-10015]

- **Notification to re-login is displayed if Athena token expiry causes a logout**

A notification prompting the users to re-login to Citrix workspace is displayed if the following conditions are met.

  - AlwaysON feature is enabled in the Citrix workspace provisioned VPN profile
  - Athena authentication is used for SSO
  - User is signed out of Citrix workspace app because of Athena token expiry

[CGOP-10016]

- **Registration for Push notification service is done using Citrix Gateway**

You can now register for push notification service using the Citrix Gateway appliance. Earlier the registration was done on the client device.

[CGOP-10542]

**Fixed issues**

In some cases, Citrix SSO crashes when a new token is scanned. For example, Citrix SSO crashes when an existing token is deleted and another one is scanned with the same token name.

[CGOP-10818]

**V2.3.1**

**What’s new**

- **Managed configurations are updated to include more user settings**

  Managed configurations are updated to include “BlockUntrustedServers”, “DefaultProfile-Name”, and “DisableUserProfiles” settings for Android Enterprise environments.

  [CGOP-10033]

- **Enhanced Push notification support**

  Upon configuring Citrix Gateway for Push Notification with type “OTP”, PIN/fingerprint is not asked after user selects “Allow” in response to Push Notification requesting user’s consent for allowing the authentication to proceed.

  [CGOP-9843]
• **Firebase Analytics support**
  Support for basic Firebase Analytics is added to provide usage information about the Citrix SSO app. The enhancement is applicable to coarse geolocations, screen usage, different versions of Android in use and so on.
  [CGOP-7523]

• **Support for Android Managed Configurations based VPN profile configuration**
  Citrix SSO app can be configured in Android Enterprise environment using an EMM/UEM vendor like Citrix Endpoint Management. The Android Enterprise Managed Configurations wizard in CEM can be used to deploy managed VPN configurations to the Citrix SSO app. For information on how to configure Citrix SSO app using Managed Configurations, refer [https://info.citrite.net/x/8TIFTw](https://info.citrite.net/x/8TIFTw)

**V2.2.9**

**What’s new**

• **Push Notification support**
  Citrix Gateway sends Push notification on your registered mobile device for a simplified two-factor authentication experience.
  [CGOP-9592]

**Fixed issues**

• Non-URL characters are allowed in server field under Add Connection screen.
  [CGOP-588]

**Set up Citrix SSO app in a MDM environment**

June 12, 2019

To set up Citrix SSO app in an MDM environment, see Configure Citrix SSO protocol for Android.

**Note:**

• In a Non-MDM environment, users create VPN profiles manually.
• You can also create an Android Enterprise managed configuration for Citrix SSO. For details, see Configure VPN profiles for Android Enterprise.