CITRIX

Citrix SSO for Mac OS X

User Guide

Contents

Overview

Citrix SSO app for Mac OS X 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, built using Apple's Network Extension (NE) framework to create and manage VPN connections from Mac OS X devices. NE framework from Apple is a modern library which contains APIs that can be used to customize and extend the core networking features of Mac OS. 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 in the near future. Citrix SSO App supports advanced features like Server Initiated Connections and DTLS.

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.

Citrix SSO app for Mac OS X can be installed from 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.

Feature	Citrix VPN	Citrix SSO
App distribution method	**Citrix Downloads page**	**App Store**
Number of tunnelled connections	**128**	**128**
Access from browser	✓	✗
Access from native app	✓	✓
Split tunnel (OFF/ON/REVERSE)	✓	✓
Split DNS (LOCAL/REMOTE/BOTH)	**REMOTE**	**REMOTE**
Local Lan Access	**Enable/Disable**	**Always enabled**
Server Initiated Connections (SIC) support	✗	✓
Transfer login	✓	✓
Client side proxy	✓	✗
Classic/Opswat EPA support	✓	✓
Device certificate support	✓	✓
Session timeout support	✓	✓
Forced timeout support	✓	✓
Idle timeout support	✓	✗
IPV6	✗	✓
Network roaming (Switch between Wifi, Ethernet etc)	✓	✓
Intranet application support	✓	✓
DTLS support for UDP	✗	✓

Feature	Citrix VPN	Citrix SSO
EULA support	✓	✓
App + Receiver integration	✓	✗
Authentication – Local, LDAP, Radius	✓	✓
Client certificate authentication	✓	✗
TLS support (TLS1, TLS1.1 and TLS1.2)	✓	✓
Two factor authentication	✓	✓

Compatibility with MDM products

Citrix SSO for Mac OS X works with most MDM providers such as Citrix XenMobile, Microsoft Intune etc. 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 explains the step by step instructions to configure both device-wide and per-app VPN profiles for Citrix SSO using Citrix 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 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 NetScaler Gateway based on the VPN policies (such as Full-tunnel, Split-tunnel, Reverse Split-tunnel etc.) defined in NetScaler.

Following are the steps to configure a device level VPN on Citrix XenMobile:

1. On the XenMobile 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.

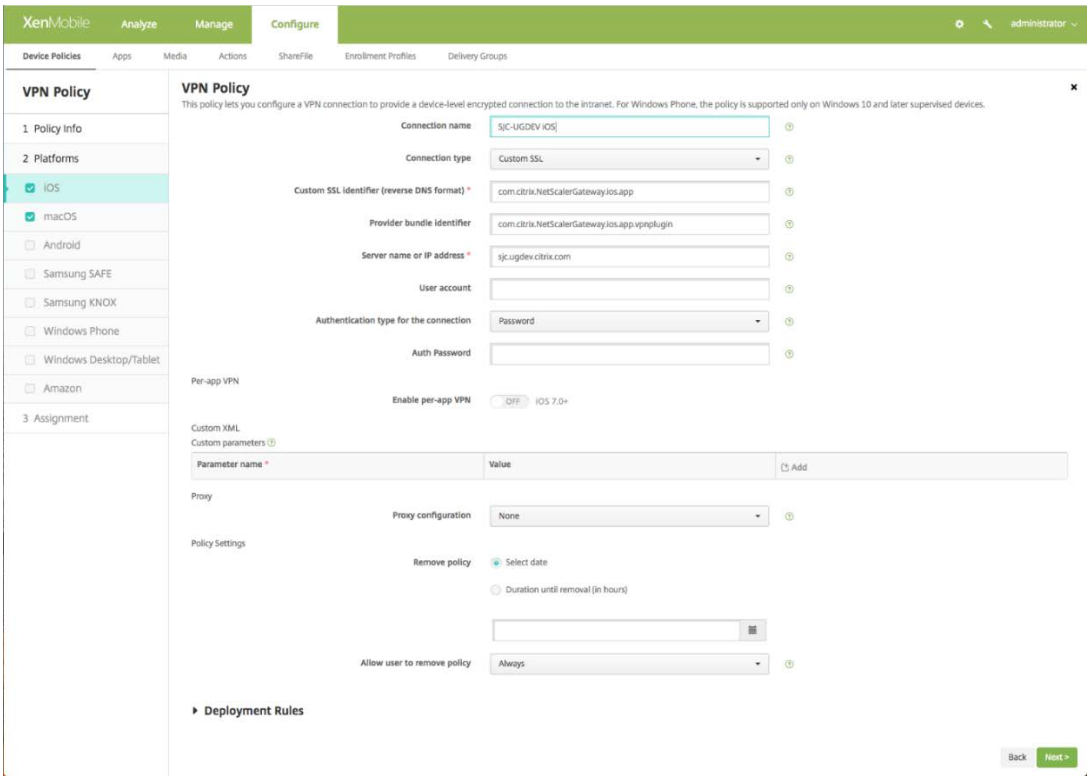
4. On the Policy detail page for iOS, type a valid Connection Name and choose "Custom SSL" from the Connection Type dropdown control.
   Note: In the MDM VPN payload, Connection Name corresponds to the "UserDefinedName" key and "VPN Type" Key must be set to value "VPN".

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 NetScaler associated with this XenMobile instance.

8. The remaining fields in the configuration page are optional. Configurations for these fields can be found in 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.

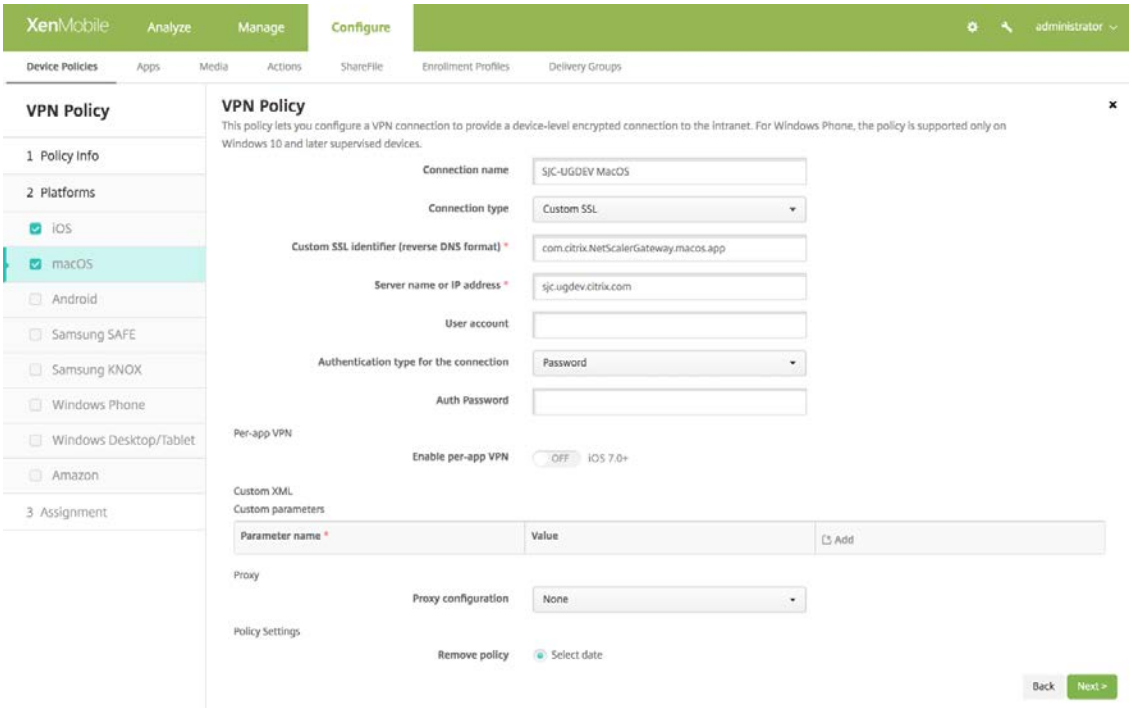


9. On the Policy detail page for MacOS, type a valid Connection Name and choose "Custom SSL" from the Connection Type dropdown control.

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 NetScaler associated with this XenMobile instance.

12. The remaining fields in the configuration page are optional. Configurations for these fields can be found in the 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 tunnelled to NetScaler 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 XenMobile:

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

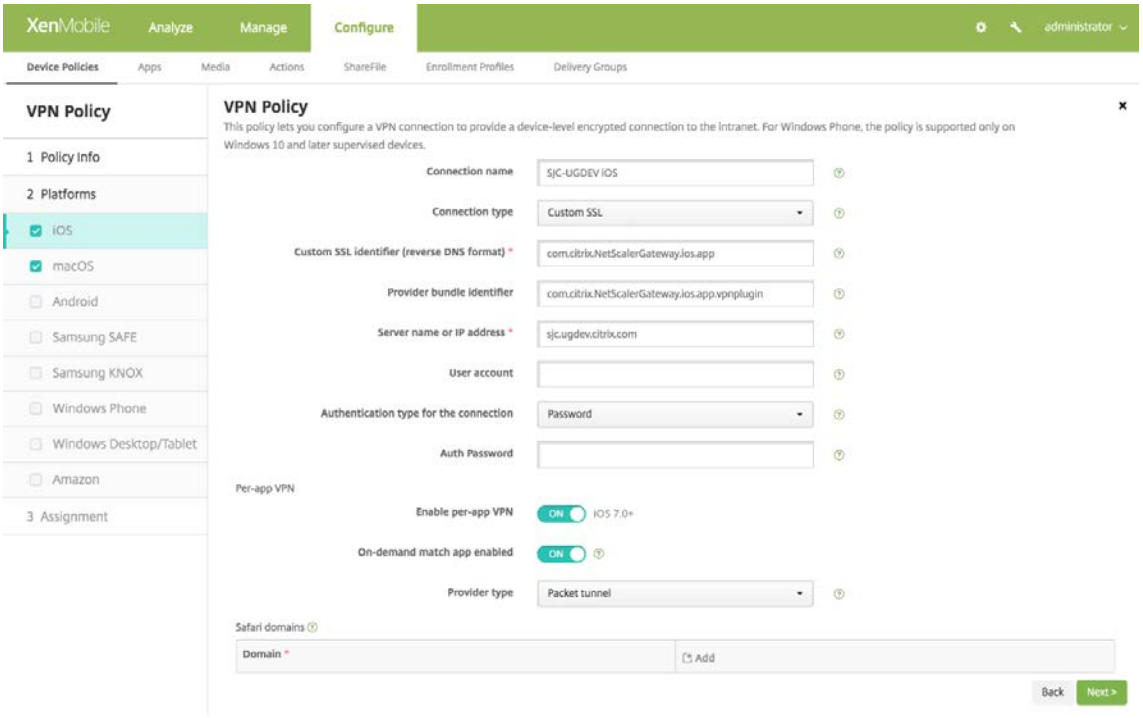
2. Turn the Enable Per-App VPN switch ON in the Per-App VPN section.

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 recomended 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 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.

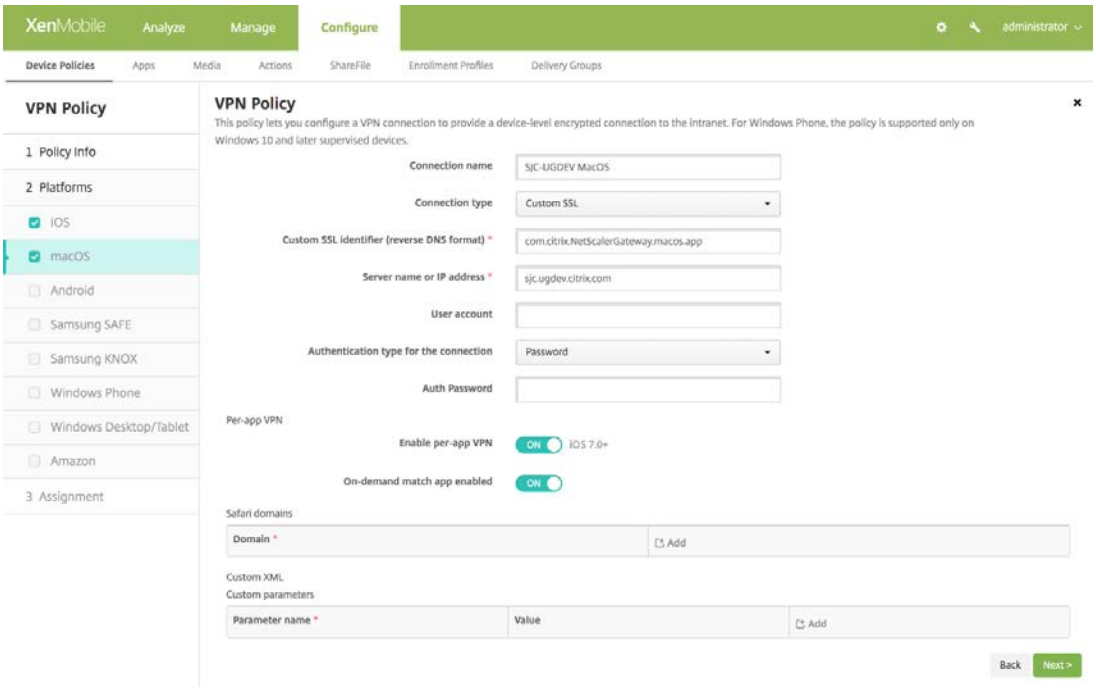
8. In the Custom SSL identifier (reverse DNS format) text field, type "com.citrix.NetScalerGateway.macos.app". This is the bundle identifier for the Citrix SSO App on Mac OS.

9. In the Server name or IP address text field, type the IP address or FQDN of the NetScaler associated with this XenMobile 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 recomended 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/

Known issues

The following are the known issues at this time.

- Network Access Control (NAC) with Citrix SSO and Microsoft Intune isn't supported yet. Both Microsoft and Citrix are currently working on it at the time of this writing.
- User must automatically select the certificate if only one device cert is present in the keychain.
- In case of EPA failure logon fails if the user is placed in quarantine group.
- Forced timeout warning message is not displayed.
- SSO app allows logon if split tunnel is ON and no intranet apps are configured.

Limitations

The following are the limitations at this time.

- In case of EPA Some of the EPA scans (e.g Patch Management scans, web browser scan, kill process) might fail because of restricted access for SSO app due to sandboxing.
- Split tunnelling based on ports/protocols isn't supported.