MobileIron Tunnel 4.1.0 for macOS Guide for Administrators

for MobileIron Core and MobileIron Cloud

Revised: March 8, 2021

For complete product documentation, see:
MobileIron Tunnel for macOS Documentation Home Page.

Revision history

Date	Revision
March 8, 2021	• Updated the description for Match Domain List: Tunnel VPN configuration field description • Added note to the description for IP routes: Key-value pairs for Tunnel for macOS

Contents

New features and enhancements

This guide documents the following new features and enhancements:

- **Rebranding**: Rebranding: MobileIron has updated the Tunnel for iOS icons and user interface color scheme. For more information, see the Coming Soon - MobileIron UX changes MobileIron Tunnel Android and iOS App. See also What users see in MobileIron Tunnel for macOS.
- **User experience updates**: The MobileIron Tunnel logo is seen on the top menu bar. Users can click on the icon to view the Tunnel status and to access additional options. For more information, see What users see in MobileIron Tunnel for macOS.

  These updates also resolve the issue where users saw multiple prompts to authorize the keychain for Tunnel.

About MobileIron Tunnel for macOS

The following provide an overview of MobileIron Tunnel for macOS devices:

Overview of MobileIron Tunnel for macOS

MobileIron Tunnel enables VPN capability on iOS devices. MobileIron Tunnel interacts with the MobileIron enterprise mobility management (UEM) platform, MobileIron Standalone Sentry, and MobileIron Access to secure access to enterprise resources from outside the enterprise network. The enterprise resource can be on premise or in the cloud. The MobileIron UEM platforms are: MobileIron Core and MobileIron Cloud.

About MobileIron Tunnel configuration

Configurations for MobileIron Tunnel are created in a MobileIron unified endpoint management (UEM) platform. MobileIron Tunnel receives the configuration from the MobileIron UEM client. The MobileIron client for MobileIron Core is Mobile@Work, and the client for MobileIron Cloud is MobileIron Go.

Deployment use cases with MobileIron Tunnel for macOS

MobileIron Tunnel enables native per app VPN on macOS devices. MobileIron Tunnel is part of the following MobileIron deployments for securing access to enterprise resources:

- MobileIron UEM and Standalone Sentry.
- MobileIron UEM and MobileIron Access.

The following use cases are enabled with these deployments:

- access to internal corporate URLs from the Safari browser.
- per-app VPN for managed apps (managed apps do not need AppConnect wrapping or SDK).
- device-level VPN.
- single sign-on.

Setting up MobileIron Tunnel for macOS

The following addresses the setup required for app VPN using MobileIron Tunnel for macOS and contains the following:

IMPORTANT: The bundle IDs for Tunnel for iOS and for macOS are different. Therefore, create a separate MobileIron Tunnel configuration for macOS. DO NOT use the same configuration for iOS and macOS.

Before you set up MobileIron Tunnel for macOS

Before you set up MobileIron Tunnel for macOS, see the following:

Required components for deploying MobileIron Tunnel for macOS

The following components are required for a MobileIron Tunnel for macOS deployment:

- Standalone Sentry with AppTunnel enabled or MobileIron Access.
- MobileIron unified endpoint management (UEM) platform:
  - MobileIron Core

  or
  - MobileIron Cloud
- macOS devices registered with a MobileIron UEM.

MobileIron Core: For information about registering macOS devices, see “Registering iOS and macOS devices through the web” in the *MobileIron Core Device Management Guide* for iOS and macOS Devices.

MobileIron Cloud: For information about registering macOS devices on MobileIron Cloud, see the *MobileIron Cloud Administrator Guide* or the **Help** on MobileIron Cloud.

For supported versions see the *MobileIron Tunnel for macOS Release Notes*.

Requirements for setting up MobileIron Tunnel for macOS

The following are requirements for setting up MobileIron Tunnel for macOS:

- If your deployment uses Standalone Sentry:
  - You have installed Standalone Sentry. See the *Standalone Sentry Installation Guide*.
  - Standalone Sentry is set up for AppTunnel using identity certificates for device authentication. For information about setting up a Standalone Sentry for AppTunnel, see *MobileIron Sentry Guide for MobileIron Core* for your MobileIron unified endpoint management (UEM) platform.
  - The Standalone Sentry IP address is publicly accessible.
  - The Standalone Sentry name is registered in DNS.
  - To tunnel IP traffic, ensure that you have created an IP_ANY service.
  - For documentation, see Standalone Sentry product documentation.
- Standalone Sentry is required for packet tunnel provider with per-app VPN.
- If your deployment uses MobileIron Access, ensure that MobileIron Access is set up. See the *MobileIron Access Guide* for information on how to set up MobileIron Access. For documentation, see MobileIron Access product documentation.
- The appropriate ports are open.
  See the *MobileIron Tunnel for macOS Release Notes*.

Recommendations for setting up MobileIron Tunnel for macOS (Core)

Standalone Sentry: MobileIron recommends that Standalone Sentry use a trusted CA certificate. If Standalone Sentry uses a self-signed certificate, you must do the following additional setup in MobileIron Core:

- In the **Services > Sentry** page, for the Standalone Sentry, click the **View Certificate** link. This makes the Standalone Sentry's certificate known to MobileIron Core.
- Follow the instructions in the Using a Self-signed certificate with Standalone Sentry and MobileIron Tunnel knowledge base article.

  If the self-signed certificate is changed at any time, you must push the changed certificate to the device, otherwise there may be a disruption in service. Therefore, MobileIron **recommends using a certificate from a trusted certificate authority for the Standalone Sentry**.

UDP traffic: If you want to limit the UDP traffic through Standalone Sentry, gather a list of destination UDP ports that should be tunneled through Tunnel VPN. All other UDP traffic is, therefore, not tunneled. Configure the **SplitUDPPortList** key-value pair to limit the UDP traffic through Tunnel.

Limitations for MobileIron Tunnel for macOS

MobileIron Tunnel for macOS has the following limitations:

- Single sign on with Kerberos is not supported.

Main tasks for configuring MobileIron Tunnel for macOS (Core)

Following are the main steps for configuring MobileIron Tunnel for macOS:

1. Configuring MobileIron Tunnel VPN (Core)
2. Applying the MobileIron Tunnel VPN setting to managed apps (Core)
3. Distribute MobileIron Tunnel for macOS as a VPP app (Core)

Configuring MobileIron Tunnel VPN (Core)

Tunnel supports per-app and device-level VPN. Choose the appropriate configuration depending on whether you are creating a per-app VPN or a device-level VPN.

You can create multiple Tunnel configurations to push to a device. The VPN profiles pushed to a device are listed in **Settings > General > VPN**, and in **Settings > General > Device Management**. Depending on the app in use, macOS automatically switches to use the VPN profile applied to the app.

You can apply both per-app VPN and device-level VPN to a device. However, per-app VPN takes priority over device-level VPN. The device-level VPN is used for apps that are not associated with a per-app VPN.

Before you begin

- If you are configuring app proxy VPN, ensure that you have created a TCP AppTunnel service in Standalone Sentry.
- If you are configuring packet tunnel provider type, ensure that you have created an IP AppTunnel service in Standalone Sentry.
- For information on setting up a TCP or IP AppTunnel service see “Working with Standalone Sentry for AppTunnel” in the *Standalone Sentry Guide* for MobileIron Core.
- If you are configuring MobileIron Tunnel for securing authentication traffic with MobileIron Access see the *MobileIron Access Guide*.

IMPORTANT: MobileIron strongly recommends creating separate Tunnel VPN configurations for iOS and macOS. Using the same Tunnel VPN configuration for iOS and macOS may cause issues with how Tunnel operates and how traffic through Tunnel is handled.

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Click **Add New > VPN**.
3. For **Connection Type**, select **MobileIron Tunnel**.
4. Add the necessary configurations.
5. Click **Save**.
6. Apply the configuration to a label containing the macOS devices.

Next steps

Go to Applying the MobileIron Tunnel VPN setting to managed apps (Core).

Related topics

- For a description of the configuration fields for MobileIron Tunnel VPN, see Tunnel VPN configuration field description.
- For a description of the key-value pairs, see Key-value pairs for Tunnel for macOS.

Applying the MobileIron Tunnel VPN setting to managed apps (Core)

When you Add or Edit an app in the App Catalog, you have the option to select the per app VPN setting to apply to the app. For this workflow, select the **MobileIron Tunnel** VPN setting for macOS that you created.

Before you begin

Ensure that the apps to which you will apply the Tunnel VPN setting are available in the App Catalog on Core. See the *MobileIron Core Apps@Work Guide* for your release for more information.

NOTE: macOS apps can be deployed either as VPP apps or as in-house apps. Ensure that the VPP apps are assigned to a VPP label and a macOS label, and in-house apps are assigned to a macOS label.

Procedure

1. In the Admin Portal, go to **Apps > App Catalog**.
2. Select **macOS** from the **Platform** list.
3. Select an app and click the edit icon next to the app.
4. In the form, for **Per App VPN Settings**, select the MobileIron Tunnel (iOS) VPN you created.

Related topics

For more information about adding and editing apps for distribution, see the following sections in the *MobileIron Core Apps@Work Guide*:

- “Populating the iOS and macOS App Catalogs.”
- “Using the wizard to add an in-house iOS or macOS app to the App Catalog.”

- "Using the Apple Volume Purchase Program (VPP)."
- MobileIron Core product documentation.

Distribute MobileIron Tunnel for macOS as a VPP app (Core)

MobileIron Tunnel is available in the Mac App Store. Device users can download the app directly from the Mac App Store.

MobileIron Tunnel can also be distributed as a Volume Purchase Program (VPP) app from MobileIron Core. Apple provides VPP to facilitate app purchase and distribution within an organization. The App Store Volume Purchase Program (VPP) allows participating organizations to purchase iOS and macOS apps in volume and distribute the apps to their users.

IMPORTANT: While Apple supports user-based licensing for macOS VPP apps, currently there is an Apple issue with the installation of user-based licensed VPP apps through MDM. As a result, MobileIron does not recommend applying user-based licenses to macOS VPP apps.

For information on how to distribute MobileIron Tunnel for macOS as a VPP app, see "Using the Apple Volume Purchase Program (VPP) in the *MobileIron Core Apps@Work Guide.*

NOTE: For countries for which a VPP program is not available, device users can download and install MobileIron Tunnel directly from the Mac App Store.

Main tasks for configuring MobileIron Tunnel for macOS (Cloud)

Following are the main steps for configuring MobileIron Tunnel for macOS:

1. Adding a MobileIron Tunnel configuration in MobileIron Cloud
2. Applying the MobileIron Tunnel VPN setting to managed apps (Cloud)
3. Distribute MobileIron Tunnel for macOS as a VPP app (Cloud)

Adding a MobileIron Tunnel configuration in MobileIron Cloud

You create the configuration for MobileIron Tunnel in **Configurations**. Tunnel supports per-app as well as device-level VPN. Choose the appropriate Tunnel configuration depending on whether you are creating a per-app VPN or a device-level VPN.

Before you begin

- If you are configuring per app VPN, create a MobileIron Tunnel service for iOS in Standalone Sentry. For information on setting up Standalone Sentry with a MobileIron Tunnel service, see "Working with Standalone Sentry for AppTunnel" in the *Standalone Sentry Guide* for MobileIron Cloud.

- If you are configuring MobileIron Tunnel for securing authentication traffic with MobileIron Access see the *MobileIron Access Guide*.

IMPORTANT: MobileIron strongly recommends creating separate Tunnel VPN configurations for iOS and macOS. Using the same Tunnel VPN configuration for iOS and macOS may cause issues with how Tunnel operates and how traffic through Tunnel is handled.

Procedure

1. In MobileIron Cloud, go to **Configurations > +Add**.
2. Search for MobileIron Tunnel.
3. Click one of the following:
   - **MobileIron Tunnel**: Use this configuration to create a per-app VPN configuration for MobileIron Tunnel.
   - **MobileIron Tunnel (On Demand)**: Use this configuration to create a per-device VPN configuration for MobileIron Tunnel.

   The MobileIron Tunnel configuration page displays.
4. If you selected the **MobileIron Tunnel** configuration, click **iOS/macOS**.
   The configuration options display.
5. Add the necessary configurations and click **Next**.
6. Choose a distribution option for the configuration and click **Done.**
   The configuration is distributed to the subset of the devices to which the app is distributed. Select the same distribution option that you selected for the MobileIron Tunnel for macOS app.

Next steps

Go to Applying the MobileIron Tunnel VPN setting to managed apps (Cloud).

Related topics

- For a description of the configuration fields for MobileIron Tunnel VPN, see Tunnel VPN configuration field description.
- For a description of the key-value pairs, see Key-value pairs for Tunnel for macOS.

Applying the MobileIron Tunnel VPN setting to managed apps (Cloud)

When you Add or Edit an app in the App Catalog, you have the option to select the per app VPN setting to apply to the app. For this workflow, select the MobileIron Tunnel VPN setting you created for macOS. This procedure is not needed if you configured per-device VPN using **MobileIron Tunnel (On Demand)**.

Procedure

1. In **Apps > App Catalog**, add or edit an app.
2. In **App Configuration** for the app, for **Per App VPN** click **+**.
3. Enter a name for the configuration.

4. Check **Enable Per-App VPN for this app.**
5. Select the Tunnel for macOS configuration to apply to the app.
6. Select a distribution option and click **Next**.
7. Click **Done**

Related topics

For more information about adding and editing apps for distribution, see the following sections in the *MobileIron Cloud Guide*:

- "Adding an app from a public store."
- "Adding an In-house app."

Distribute MobileIron Tunnel for macOS as a VPP app (Cloud)

MobileIron Tunnel is available in the Mac App Store. Device users can download the app directly from the Mac App Store.

MobileIron Tunnel can also be distributed as a Volume Purchase Program (VPP) app from MobileIron Cloud. Apple provides VPP to facilitate app purchase and distribution within an organization. The App Store Volume Purchase Program (VPP) allows participating organizations to purchase iOS and macOS apps in volume and distribute the apps to their users.

IMPORTANT: While Apple supports user-based licensing for macOS VPP apps, currently there is an Apple issue with the installation of user-based licensed VPP apps through MDM. As a result, MobileIron does not recommend applying user-based licenses to macOS VPP apps.

For information on how to distribute MobileIron Tunnel for macOS as a VPP app, see "Licenses" in the *MobileIron Cloud Administrator Guide* or by clicking **Help** in MobileIron Cloud.

NOTE: For countries for which a VPP program is not available, device users can download and install MobileIron Tunnel directly from the Mac App Store.

Tunnel VPN configuration field description

The following table provides field descriptions for the Tunnel configuration. There are some variations in field names between MobileIron Core and MobileIron Cloud.

TABLE 1. TUNNEL CONFIGURATION FIELD DESCRIPTION

Item	Description
Name	Enter a name for the MobileIron Tunnel VPN profile.
Description	Enter a description for the profile.
Connection Type	Select **MobileIron Tunnel**.

TABLE 1. TUNNEL CONFIGURATION FIELD DESCRIPTION (CONT.)

Item	Description
(MobileIron Core)	Only fields relevant to MobileIron Tunnel are displayed.
Choose OS to create Tunnel Configuration (MobileIron Cloud)	Select **iOS/macOS.**
Profile selection mode to use for this configuration (MobileIron Cloud)	Select one of the following: • **Sentry Profile Only**: Select if Tunnel traffic goes only through Standalone Sentry only. • **MobileIron Access Profile Only**: Select if Tunnel traffic goes to Access only. Only authentication traffic is tunneled to Access. This option is available only if a MobileIron Access deployment is set up. NOTE: If **MobileIron Access Profile Only** is configured with per-app VPN packet tunnel provider type, only authentication traffic is tunneled to Access. All other traffic is dropped. If **MobileIron Access Profile Only** is configured with device-level VPN packet tunnel provider type, only authentication traffic is tunneled to Access. All other traffic goes directly to the destination. • **MobileIron Sentry + Access Profile**: Select if Tunnel VPN supports both traffic to Access for authentication to enterprise cloud resources and through Standalone Sentry to on-premise enterprise resources. This option is available only if a MobileIron Access as a service deployment is set up.
Legacy App Support (iOS only)	Not applicable for Tunnel for macOS.
VPN Sub Type (MobileIron Cloud)	(Optional) Overrides the bundle identifier for a customized MobileIron Tunnel app.
Enable Access (MobileIron Core)	This option is not supported for macOS.
Provider Type	**app-proxy**: This is the default setting. Use this setting for TCP tunneling only. **packet-tunnel**: Select to allow Tunnel to also handle IP traffic. NOTE: Per-device VPN automatically uses the packet-tunnel provider type.
Per-app VPN (MobileIron Core)	The options are available if **Provider Type** is **packet-tunnel**. Otherwise, the options are grayed out. Device-level VPN is not available for app-proxy tunnel.

TABLE 1. TUNNEL CONFIGURATION FIELD DESCRIPTION (CONT.)

Item	Description
	Yes: This is the default setting. Connectivity is established for an app, rather than the device. **No**: Select to establish connectivity for the device, rather than just an app.
Sentry (Profile)	**Core:** Select the Standalone Sentry on which you created the TCP tunnel service. **Cloud**: If you are configuring per app VPN, select the Standalone Sentry profile.
Sentry Service	**Core:** Select the TCP or IP service that the Safari browser or managed app will use. **Cloud**: Select the Tunnel for iOS service that the Safari browser or managed app will use. The field is not available if the profile mode is **MobileIron Access Profile Only.** Only TCP services are available for selection if the provider type is app-proxy. Only IP services are available for selection for the following: • The provider type is packet-tunnel. • The VPN is per device.
SCEP Identity (MobileIron Cloud)	Select the Identity Certificate configuration you created for Tunnel. The Identity Certificate is automatically selected if **Sentry Profile Only** or **MobileIron Sentry + Access Profile** is enabled.
Debug Info Recipient (MobileIron Cloud)	Enter an email address for emailing debug logs.
Identity Certificate (MobileIron Core)	Select the certificate setting you created. If you are using user-provided certificates, select the user provided certificate you created for MobileIron Tunnel.
On Demand Rules (iOS 9 and later; macOS 10.13 and later) (MobileIron Core) VPN On Demand rules are applied when the device's primary network interface changes, for example when the device switches to a different Wi-Fi network. Devices will drop the Tunnel VPN connection if an enterprise Wi-Fi is detected. If the network is not a Wi-Fi network or if its SSID does not appear in the list, the device will continue to use Tunnel VPN. Note The Following: • A matching rule is not required. The Default Rule is applied if a matching rule is not defined. • If you select Evaluate Connection, a matching rule is not required.	

TABLE 1. TUNNEL CONFIGURATION FIELD DESCRIPTION (CONT.)

Item	Description
• You can create up to 10 On Demand matching rules. • For each matching rule you can create up to 50 Type and Value pairs. IMPORTANT: An Ethernet on-demand rule is only applicable to macOS devices. If the rule is pushed to iOS device, the rule may cause issues with Tunnel behavior and how traffic through Tunnel is handled. Therefore, MobileIron strongly recommends using separate Tunnel VPN configurations for iOS and macOS.	
Add +	Click to add a new On Demand matching rule.
On Demand Action	Select one of the following actions to apply to the matching rule: • Connect • Disconnect
Matching Rules For each On Demand matching rule to which the action is applied enter the type and value pair.	
Add +	Click to add a new On Demand matching rule. A dialog box appears.
Type	Select the following key type: • **SSID**
Value	Enter a list of SSIDs to match the enterprise Wi-Fi. If the network is not a Wi-Fi network or if its SSID does not appear in the list, the match will fail. TIP: To add multiple SSIDs, create a separate SSID Type-Value pair for each SSID.
Description	Enter additional information about this matching rule.
OK	Click to add the On Demand Action and the associated Matching Rules.
Default Rule The default rule (action) is applied to a connection that does not match any of the matching rules.	
On Demand Action	From the drop down list, select **Connect**.
Safari Domains The device user can access servers ending with these domains in Safari. A MobileIron Tunnel configuration is only applied to a managed app. Therefore, a managed app with the MobileIron Tunnel configuration must be installed on the device for the device user to access the domains from Safari.	

TABLE 1. TUNNEL CONFIGURATION FIELD DESCRIPTION (CONT.)

Item	Description
NOTE: If the device resolves the destination domain, then Tunnel is not launched.	
Safari Domain	Enter a domain name. Only alphanumeric characters and periods (.) are supported.
Description	Enter a description for the domain.
Add New	Click to add a domain.
Calendar Domains (iOS 13 and later; macOS 10.15 and later) A Tunnel VPN connection is automatically established for these domains. Only available for per-app VPN.	
Calendar Domain	Enter a domain name. Only alphanumeric characters and periods (.) are supported.
Description	Enter a description for the domain.
Add New	Click to add a domain.
Contact Domains (iOS 13 and later; macOS 10.15 and later) A Tunnel VPN connection is automatically established for these domains. Only available for per-app VPN.	
Contact Domain	Enter a domain name. Only alphanumeric characters and periods (.) are supported.
Description	Enter a description for the domain.
Add New	Click to add a domain.
Mail Domains (iOS 13 and later; macOS 10.15 and later) A Tunnel VPN connection is automatically established for these domains. Only available for per-app VPN.	
Mail Domain	Enter a domain name. Only alphanumeric characters and periods (.) are supported.
Description	Enter a description for the domain.
Add New	Click to add a domain.
Included Routes (Added Routes) Only available for device-level VPN. Configured routes are set to the TUN interface. If routes are not configured, Tunnel uses 0.0.0.0/0.	

TABLE 1. TUNNEL CONFIGURATION FIELD DESCRIPTION (CONT.)

Item	Description
Enter list of IPv4 addresses in CIDR format. For multiple values, enter a semicolon separated list.	
DNS Resolver IPs Only for packet-tunnel provider type. Enter a domain name server (DNS) to resolve the IP address. IPv4 only. For multiple values, enter a semicolon separated list. Ensure that the DNS is routable if the default route in not used. If DNS is not configured, the Sentry DNS is used.	
DNS Search Domain List Only for packet-tunnel provider type. Enter DNS search domains for resolving the domain names. IPv4 only. For multiple values, enter a semicolon separated list.	
Match Domain List Only for packet-tunnel provider type. Enter domains for which a proxy connection is used. IPv4 only. For multiple values, enter a semicolon separated list. Only for the domains configured here, Tunnel checks the DNS configured in **DNS Resolver IPs** to resolve the domains. DNS look up for all other domains goes directly to the device network's DNS server. If no domains are configured here, Tunnel checks the VPN's DNS to resolve all domains.	
Custom Data Enter Key Value pair to configure the MobileIron Tunnel VPN disconnect, debug, and timeout behavior. See Key-value pairs for Tunnel for macOS.	

Additional configurations using key-value pairs for MobileIron Tunnel

Key-value pairs are used to customize Tunnel for macOS app behavior. These key-value pairs define app behavior such as idle timeout, email address for sending debug information, and level of log detail that is collected.

Key-value pairs for Tunnel for macOS

The following table provides the key-value pairs for customizing Tunnel for macOS.

TABLE 2. KEY-VALUE PAIRS FOR TUNNEL FOR MACOS

Key	Value
Manage Tunnel timeout	
disconnectTimeoutInSeconds (MobileIron Core)	Enter 0 or a number between 5 - 18000. If the value is 0, then MobileIron Tunnel VPN never disconnects itself. You have to manually disconnect the VPN in the MobileIron Tunnel. If the value is > 0, the MobileIron Tunnel VPN is disconnected after number entered. Default value if the key-value pair is not configured: 60 seconds.
TcpIdleTmoMs	Enter an integer between 5000 - 1800000. The timeout is measured in milliseconds. Configuring idle timeout allows you to control the idle session timeout for the TCP connection between the app and the backend server. You may want to configure idle timeout if the backend server takes more than 60 seconds to respond to a request. The default idle timeout with Standalone Sentry for per app VPN if the key-value pair is not configured: 60 seconds.
Troubleshooting	
debugInfoRecipient (Available as field value in MobileIron Cloud)	Enter an email address to forward the debug information.
LogLevel	Enter debug <*Log Level*> Use one of the following log level options. The options are listed from the least to the most verbose level. • error: Captures error logs if the Tunnel app errors out while performing

TABLE 2. KEY-VALUE PAIRS FOR TUNNEL FOR MACOS (CONT.)

Key	Value
	an action. • warning: Captures warning messages logged if there is missing or incorrect information that might cause an error. This log level is rarely used. • info: Captures informational level details such as, log prints inputs, metadata, parameter values. • debug: Captures debug level information such as, actions, operations, values of critical data, and information that is helpful in debugging. • session: Captures everything that occurs during a tunnel session. • packet: Captures packet level information, such as, length in bytes. Used for troubleshooting DNS queries and responses to and from Tunnel. Default if the key-value pair is not configured: info
DNS and network	
IPv6NetworkPrefix	IPv6 ULA network prefix to use for internal NAT table.
Certificates	
DisablePinning	false: Default, if the key-value pair is not configured. Certificate pinning is enabled. true: Certificate pinning is disabled. Disabling certificate pinning is not recommended for security reasons. NOTE: The Standalone Sentry server certificate is automatically pushed to the device.
Packet-tunnel	
IPRoutes	IP routes of the iOS or macOS device VPN. Enter list separated by semicolon. The default value if the key-value is not configured is 0.0.0.0/0 **Example** 10.0.0.0/8;172.16.0.0/16 NOTE: MobileIron recommends configuring IP routes for better Tunnel performance.
ExcRoutes	IP routes that will be excluded from **IPRoutes.** **Example**

TABLE 2. KEY-VALUE PAIRS FOR TUNNEL FOR MACOS (CONT.)

Key	Value
	10.10.10.10/32.
SplitUDPPortList	List the destination UDP ports of the UDP packets that want to be sent through VPN. All other UDP packets are sent directly to destination from Tunnel client. If the key-value pair is not configured all UDP packets from the VPN interface go through VPN. **Example** 53;161-162;200-1024
MTU	Tunnel MTU. The default value if the key-value is not configured is 1400.
TunIP	IP address of the VPN network interface. Configure only if the customer network is in the same range. **Example** 192.168.13.10
AtpProbeIdleSec	Sets the minimum idle time, in seconds, after which probe packets are sent out with outbound Tunnel traffic. If Tunnel does not receive a response for at least one of the probes sent, the existing connection is dropped and a new connection is established with the server. The minimum idle time is based on the last inbound response received by Tunnel. For example, if the value is 60 seconds, if Tunnel does not receive any inbound traffic for 60 seconds, probe packets are sent with the next outbound Tunnel traffic. Default value if the key-value pair is not configured: 60 seconds
AtpProbeIntervalSec	Sets the interval, in seconds, between probe packets sent after the minimum idle time specified in AtpProbeIdleSec. Default value if the key-value pair is not configured: 1 second

TABLE 2. KEY-VALUE PAIRS FOR TUNNEL FOR MACOS (CONT.)

Key	Value
AtpProbeCount	Sets the total count of the probe packets sent after the minimum idle time specified in AtpProbeIdleSec. Default value if the key-value pair is not configured: 5
App proxy	
DirectLocalhost	Enter `true`. Configure if using app proxy Tunnel. The key-value pair is required for Tunnel to handle app proxy localhost traffic from apps. true: If an app uses localhost, ::1, or 127.0.0.1, the localhost app proxy (TCP) traffic is redirected to the device itself.

What users see in MobileIron Tunnel for macOS

The following provide information about device user experience:

MobileIron Tunnel installation on macOS

MobileIron Tunnel is distributed to macOS devices from MobileIron Core using Apple Volume Purchase Plan (VPP). For information on distributing MobileIron Tunnel for macOS, see

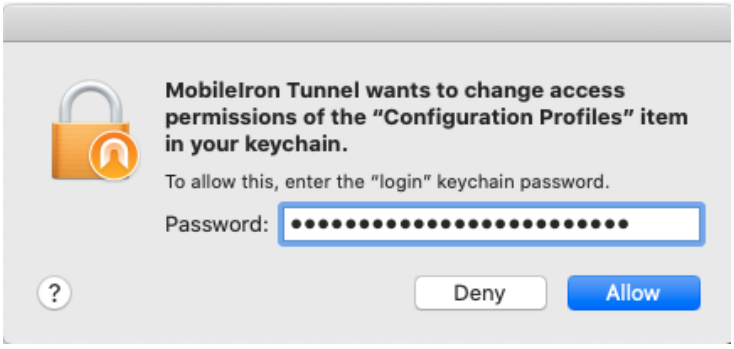
- MobileIron Core deployments: Distribute MobileIron Tunnel for macOS as a VPP app (Core).
- MobileIron Cloud deployments: Distribute MobileIron Tunnel for macOS as a VPP app (Cloud)

No user action is required for installing MobileIron Tunnel on macOS. The app is automatically installed on macOS devices when the administrator applies the VPP label to the app in the app catalog in MobileIron Core. Users see the Tunnel icon on the top menu bar. The Tunnel icon is also seen on the Launchpad. However, Tunnel cannot be launched from the Launchpad.

Allow keychain

When users access enterprise resources from a Safari browser or a managed app to which the Tunnel VPN configuration is applied, MobileIron Tunnel is automatically used to secure access to the enterprise resource. The experience is seamless to the end user. However, when the Tunnel is first pushed to the device or when the Tunnel configuration is re-pushed to the device, macOS prompts users to authorize the key. When prompted to authorize, click **Allow**.

FIGURE 1. ALLOW KEYCHAIN



IMPORTANT: . If users either click **Deny** or ignore the prompt, the dialog is presented the next time Tunnel tries to connect.

Note The Following:

- If Tunnel is in use, the app cannot be removed from the device. Users will see the following message: The item MITunnel can't be moved to the Trash because some of its extensions are in use.
- Per app VPN connection status is not provided on macOS.
- For countries for which a VPP program is not available, device users can download and install MobileIron Tunnel directly from the Mac App Store.
- Users cannot launch Tunnel from the Launchpad.

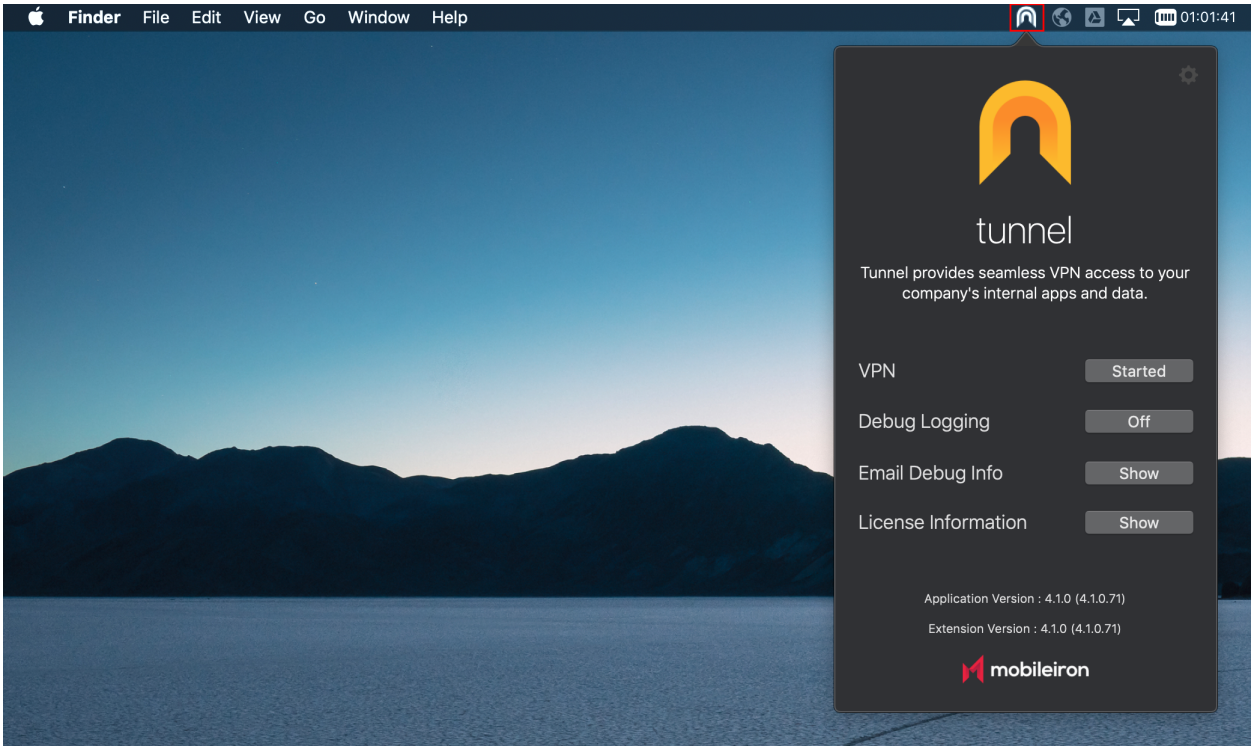
MobileIron Tunnel icon on macOS devices

If Tunnel is deployed to macOS devices, users see the Tunnel icon in the top menu bar.

The icon is highlighted if Tunnel VPN is actively connected. The icon is grayed out if Tunnel is not in use. However, the Tunnel application is always running in the background.

If users click on the Tunnel icon, the icon expands to display the Tunnel status and additional options.

FIGURE 2. TUNNEL ICON AND EXPANDED OPTIONS



The following table describes the options in the Tunnel window.

TABLE 3. TUNNEL OPTIONS

Option	Description
VPN	Click to change the status of the VPN connection. Displays one of the following status. • Started: The VPN connection is active. • Stopped: The VPN connection is inactive.
Debug Logging	Click to turn on debug logging. The default is Off. Enabling debug logging saves the Tunnel logs to a file so that it can be emailed.
Email Debug Info	Click to email the log file. NOTE: Log information is included only if there has been activity using the Tunnel app.
License Information	Click to view the license information.

Exiting MobileIron Tunnel on macOS devices

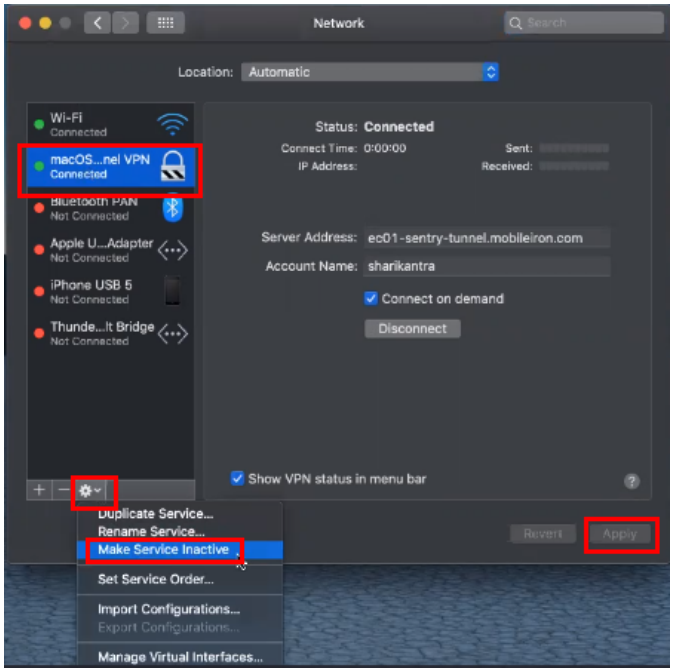
Once Tunnel is deployed, the application is always running in the background. However, if needed, users have the option to exit the Tunnel application. To exit the application, users must first deactivate Tunnel.

NOTE: If the macOS device is not registered or a Tunnel VPN setting has not been pushed to the device, MobileIron Tunnel will not be activated.

Procedure

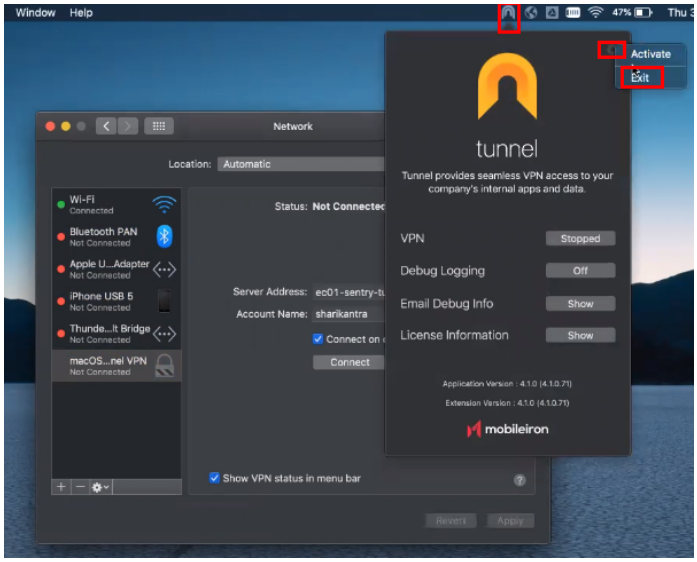
1. On the macOS device, go to System **Preferences > Network Preferences**.
2. Select the MobileIron VPN from the list of connected networks.

FIGURE 3. MAKE SERVICE INACTIVE



3. Click the **gear icon > Make Service Inactive**.
4. Click **Apply**.
5. Click the Tunnel icon in the menu bar.

FIGURE 4. EXIT APPLICATION



6. On the top right corner, click the **gear icon > Exit**.
   The Tunnel icon is no longer seen on the menu bar.

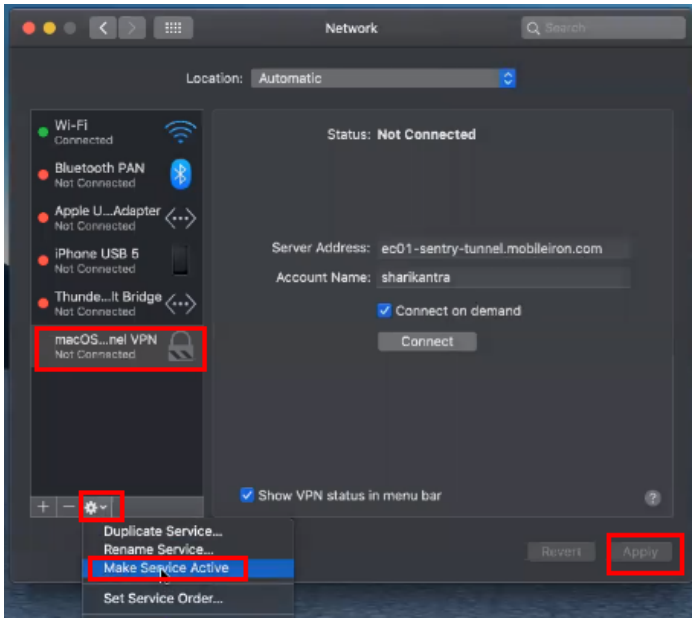
Activating MobileIron Tunnel on macOS devices

To active Tunnel from the Tunnel menu, users must first activate the service in **System Preference > Network Preferences**.

Procedure

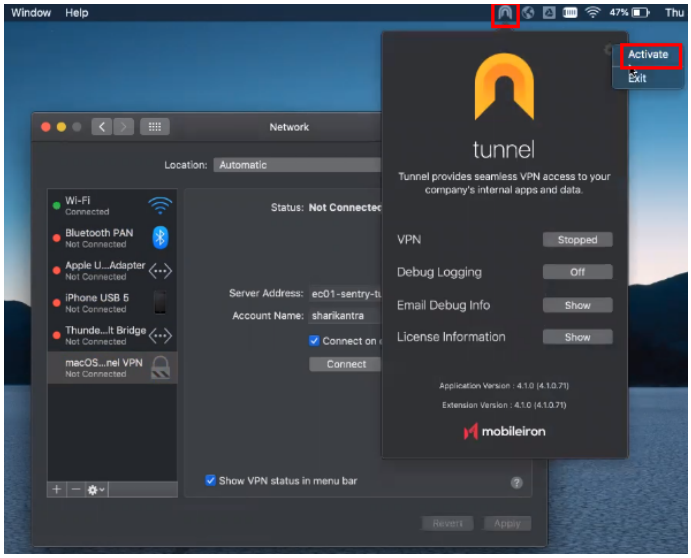
1. On the macOS device, go to **System Preferences > Network Preferences**.
2. Select the MobileIron Tunnel VPN from the list of networks.

FIGURE 5. MAKE SERVICE INACTIVE



3. Click the **gear icon > Make Service Active**.
4. Click **Apply**.
5. Click the Tunnel icon in the menu bar.

FIGURE 6. EXIT APPLICATION



6. On the top right corner, click the **gear icon > Activate**.

Emailing debug log information

IT administrators may require Tunnel debug and log data for troubleshooting purposes. Users can email the Tunnel debug and log file to the IT administrator.

Procedure

1. In the Tunnel app, turn on **Debug Logging**.
   Enabling debug logging saves the Tunnel logs to a file so that it can be emailed.
2. Redo the steps that resulted in the error so that the logs can be captured.
3. Click **Email Debug Info**.

   NOTE: Log information is included only if there has been activity using the Tunnel app.
4. Enter the email address provided by your administrator.
5. Click **Send**.