



Tunnel 1.2.3 for Windows Guide

Revised: May 2023

Contents

Revision history	4
New features summary	5
Overview of Tunnel for Windows 10	7
About this document	8
Deployment support	9
Use case support	9
Setting up Tunnel for Windows 10	11
Before you set up Tunnel for Windows 10	12
Configuring Tunnel VPN for Windows 10 (Core)	14
Configuring Tunnel VPN for Windows 10 (Cloud)	15
Tunnel for Windows 10 distribution	18
Tunnel VPN for Windows 10 field description	19
Key-value pairs for Access (Cloud)	23
Key-value pairs for custom data	26
What users see in Tunnel for Windows 10	37
Manually triggering Tunnel	38
Emailing debug logs	39

Revision history

TABLE 1. REVISION HISTORY

Date	Revision
May 12, 2023	Updated the " Key-value pairs for Access (Cloud) " on page 23.
December 16, 2022	Syntax correction for AppTriggerList/1/App/Id
April 22, 2022	Updated the template.
September 1, 2020	Corrected the case in some mentions of the key TrafficFilterList/0/App/Id.
July 25, 2019	Removed ATC limitation in the Limitation section.
March 14, 2019	Updated the formatting for keys in Key value pairs for Access.

New features summary

This release contains the following new features:

- Tunnel for Windows 10 support for Access as a service with Cloud deployments.

Overview of Tunnel for Windows 10

Tunnel for Windows 10 enables app VPN capability on Windows 10. Tunnel interacts with the Unified Endpoint Management (UEM) platform, Standalone Sentry, and Access to secure access to enterprise resources from outside the enterprise network. The enterprise resource can be on premise or in the cloud. The UEM platforms are: Core and Cloud.

About this document	8
Deployment support	9
Use case support	9

About this document

This document addresses the setup required for app VPN using Tunnel for Windows 10.

Deployment support

Tunnel is part of the following deployments for securing access to enterprise resources:

- UEM and Standalone Sentry.
- UEM and Access.

For Core deployments, only Access with Standalone Sentry deployment mode is supported.
For Cloud deployments, Access as a service deployment mode is also supported.

Use case support

The following use cases are supported:

- Tunnel VPN is automatically triggered when the user logs into the Windows 10 desktop. In this case, all traffic goes through Tunnel.
- Tunnel VPN is manually triggered. Once Tunnel is triggered, all traffic goes through Tunnel.
- The Tunnel VPN profile can be configured such that only designated apps trigger Tunnel. Once Tunnel is triggered, either all traffic from the designated apps can go through Tunnel or only designated traffic from the designated apps can go through Tunnel.

Setting up Tunnel for Windows 10

The following addresses the setup for app VPN using Tunnel for Windows 10 and contains the following:

Before you set up Tunnel for Windows 10	12
Configuring Tunnel VPN for Windows 10 (Core)	14
Configuring Tunnel VPN for Windows 10 (Cloud)	15
Tunnel for Windows 10 distribution	18
Tunnel VPN for Windows 10 field description	19
Key-value pairs for Access (Cloud)	23
Key-value pairs for custom data	26

Before you set up Tunnel for Windows 10

Review the following before proceeding with setting up Tunnel for Windows 10:

Required components for deploying Tunnel for Windows 10

The following components are required for a Tunnel deployment:

- Standalone Sentry with AppTunnel enabled or Access.
- Unified Endpoint Management (UEM):
 - Core
or
 - Cloud
- Windows 10 devices registered with a UEM.

For supported versions see the *Tunnel for Windows Release Notes*.

Requirements for configuring Tunnel for Windows 10

Ensure the following before configuring Tunnel for Windows 10:

- 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 the *MobileIron Sentry Guide* for your Unified Endpoint Management (UEM).
- If your deployment uses Access, you have set up Access.

For more information, see the [Access Guide](#).

- The appropriate ports are open.

Core: See the *On-Premise Installation Guide* for information on required ports and firewall rules associated with license activation, Standalone Sentry, and different content servers.

Cloud: See the *Cloud Architecture and Port Requirements* document for more information on ports and firewall rules.

- You cannot use an existing Tunnel for Windows Phone devices (WP8.1) setup. Create separate configurations for Tunnel for Windows 10 Desktop devices.
- A separate Standalone Sentry is not required for Tunnel for Windows 10 Desktop setup. However, you cannot use the Standalone Sentry that is being used for Tunnel for Windows Phone devices (WP8.1)

Recommendation for setting up Tunnel for Windows 10

- Ivanti, Inc recommends that Standalone Sentry use a trusted CA certificate.

If Standalone Sentry uses a self-signed certificate, do the following additional setup in Core:

- In the **Services > Sentry** page, for the Standalone Sentry, click the **View Certificate** link. This makes the Standalone Sentry's certificate known to Core.
- Follow the instructions in the *Using a Self-signed certificate with Standalone Sentry and Tunnel* knowledge base article in the Support and Knowledge Base portal at <https://forums.ivanti.com/s/article/Using-a-Self-signed-certificate-with-Standalone-Sentry-and-MobileIron-Tunnel-1713>.
- Ivanti, Inc recommends using Windows 10 TH2.

Limitations for Tunnel for Windows 10

- UDP functionality and scale will vary dependent on specific applications. Performance of real-time audio and video apps has not been tested.
- Windows 10 app behavior may vary. Some Windows 10 apps may not trigger Tunnel VPN.
- Trusted front-end deployments are not supported.
- Context headers are not supported.
- Domain names and IP addresses are not supported for triggering Tunnel VPN.
- Per app triggering does not work as expected with Windows 10 TH1.
- Windows Explorer triggers Tunnel only after a system restart.

Configuring Tunnel VPN for Windows 10 (Core)

Windows 10 devices use an IP_ANY tunnel service configured on Standalone Sentry to access backend resources.

Before you begin

- If you are configuring per app VPN, ensure that you have created an IP_ANY AppTunnel service in Standalone Sentry. For information on setting up an IP_ANY AppTunnel service see "Working with Standalone Sentry for AppTunnel" in the *Standalone Sentry Guide for Core*.
- If you are configuring Tunnel for securing authentication traffic with Access see the [Access Guide](#).

Procedure

1. In the Admin Portal, go to **Policies & Configs > Configurations**.
2. Click **Add New > VPN**.
3. For **Connection Type**, select **Tunnel (Windows)**.
4. Specify the following:
 - the Standalone Sentry on which you created the IP_ANY service
 - client certificates
 - how Tunnel is triggered
 - whether specified traffic or all traffic goes through Tunnel
 - Tunnel app behavior .
5. Click **Save**.
6. Apply the configuration to a label that contains the Windows 10 devices to which you want to distribute the configuration.

Related topics

- For a description of the configuration fields for Tunnel (Windows) VPN, see "[Tunnel VPN for Windows 10 field description](#)" on page 19.
 - For a description of the key-value pairs, see "[Key-value pairs for custom data](#)" on page 26.
 - For examples of custom data configuration, see "[Examples of custom data configurations](#)" on page 34.

Configuring Tunnel VPN for Windows 10 (Cloud)

Windows 10 devices use the Tunnel service for Windows configured on Standalone Sentry to access backend resources.

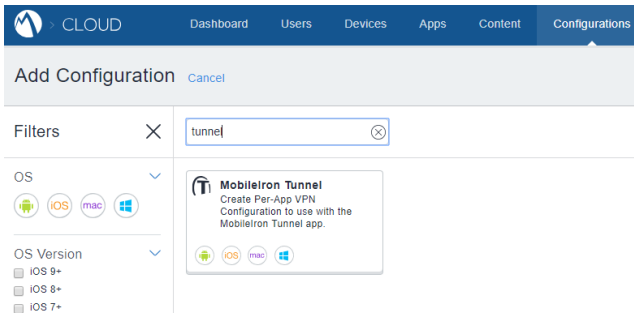
Before you begin

- If you are configuring per app VPN, ensure that you have created a Tunnel service for Windows in Standalone Sentry. For information on setting up Standalone Sentry with a Tunnel service, “Working with Standalone Sentry for AppTunnel” in the *Standalone Sentry Guide* for Cloud.
- If you are configuring Tunnel for securing authentication traffic with Access see the [Access Guide](#).

Procedure

1. In Cloud, go to **Configurations > +Add**.
2. Search for Tunnel.

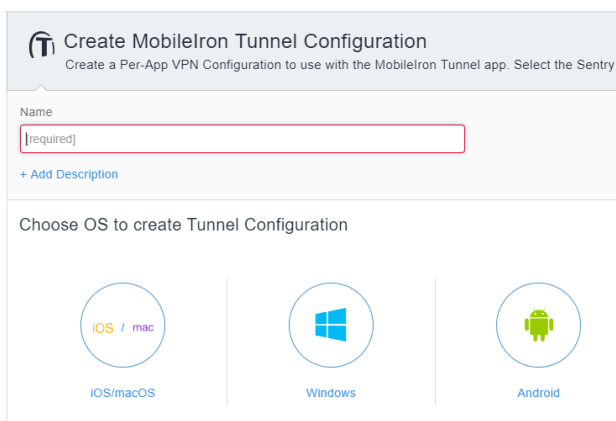
FIGURE 1. ADD TUNNEL CONFIGURATION



3. Click the **Tunnel** configuration.

The **Create Tunnel Configuration** page displays.

FIGURE 2. CREATE TUNNEL COFNIGURATION



4. Enter a name for the configuration and click **Windows**.

The configuration fields for Tunnel VPN for Windows display.

FIGURE 3. TUNNEL VPN FOR WINDOWS 10 COFIGURATION FIELDS

The screenshot shows the 'Configuration Setup' page for Tunnel VPN for Windows 10. It includes the following elements:

- Configuration Setup** header with a '10+' indicator and a Windows logo.
- Profile selection mode to use for this configuration:**
 - Sentry Profile Only
 - MobileIron Access Profile Only
- Note:** Changes to profile selection mode will clear any existing Sentry, Access and SCEP selections. This will result in needing to reconfigure the settings again.
- MobileIron Access Enabled:** A green checkmark icon.
- SCEP Identity:** A dropdown menu currently showing '-- Select --'.
- Debug Info Recipient:** A text input field containing 'name@example.com'.
- Define Tunnel App Settings:**
 - Text: 'Create App Groups and define VPN configuration route for just those groups. Or go to Advanced and enter Key Value Pairs.'
 - Radio buttons: Standard (Most Common) and Advanced (Enter Key Value Pairs only).
- Advanced Tunnel App Settings:**
 - Section: 'Enter Key Value Pairs'
 - Table with columns 'Key' and 'Value'.
 - Input fields for Key and Value, separated by a colon and a plus sign.
 - Link: '+ Add'

5. Specify the following:
 - the profile mode: Sentry only or Access only
 - client certificates
 - how Tunnel is triggered
 - whether specified traffic or all traffic goes through Tunnel
 - Tunnel app behavior .
6. Click **Next**.
7. 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 Tunnel for Android app.

Related topics

- For a description of the configuration fields for Tunnel (Windows) VPN, see ["Tunnel VPN for Windows 10 field description" on page 19](#).
- For a description of the key-value pairs, see ["Key-value pairs for custom data" on page 26](#).

- For examples of custom data configuration, see ["Examples of custom data configurations"](#) on [page 34](#).
- For an example of the custom data configuration for Access, see ["Key-value pairs for Access \(Cloud\)"](#) on [page 23](#)

Tunnel for Windows 10 distribution

Adding Tunnel to the App Catalog in UEM makes the app available for distribution to device users.

Tunnel is also available in the Windows Store. Device users can download the app directly from the Windows Store.

See the product documentation for your UEM for information on how to distribute Windows apps to device users.

For Cloud, see the *Cloud Administrator Guide*. For Core, see the *Core Apps@Work Guide*.

Tunnel VPN for Windows 10 field description

Use the following guidelines to configure Tunnel for Windows 10 VPN.


TABLE 2. TUNNEL (WINDOWS) CONFIGURATION FIELD DESCRIPTION

Item	Description
Name	Enter a name for the Tunnel for Windows VPN setting.
Description	Enter a description for the profile.
Connection Type (Core)	Select Tunnel (Windows) . Only fields relevant to Tunnel are displayed.
Profile selection mode to use for this configuration (Cloud)	Select one of the following: <ul style="list-style-type: none"> Sentry Profile Only: Select if Tunnel traffic goes only through Standalone Sentry. Access Profile Only: Select if Tunnel traffic goes to Access. This option is available only if an Access as a service deployment is set up.
Sentry (Profile)	Core: Select the Standalone Sentry on which you created the IP_ANY tunnel service for Windows 10 Desktop devices. Cloud: Select the Standalone Sentry profile on which you created the Tunnel service for Windows.
Sentry Service	Core: Select the IP_ANY service that Tunnel for Windows will use. Cloud: Select the Tunnel for Windows service.
SCEP Identity (Cloud)	Select the Identity Certificate configuration you created for Tunnel. This option is available only for Access Profile mode. If Sentry Profile Only is selected, the Identity Certificate is automatically selected, and the option is disabled.
Debug Info Recipient (Cloud) For Core, the setting is configured using key-value pairs in Custom Data.	Enter a valid email address. The device debug logs are sent to the configured email address. When users tap Email Debug Info , the To field is auto filled with the configured email address.
Identity Certificate (Core)	Select the Certificate Enrollment setting you created.
Send All Traffic (Core)	Not applicable to Windows 10 Desktop devices. Windows 10 Desktop devices will ignore this setting.
Windows Configuration (Core)	

TABLE 2. TUNNEL (WINDOWS) CONFIGURATION FIELD DESCRIPTION (CONT.)

Item	Description
Always On (Core)	Select to trigger Tunnel VPN when the user logs in to Windows 10 desktop. Do not select if you want to restrict which apps trigger Tunnel VPN. By default, Always On is not selected.
Secured Resources (Core)	Not applicable to Windows 10. Windows 10 will ignore this setting.
Define Tunnel App Settings (Cloud) Standard Tunnel App Settings: Create app groups and define route for the group.	
Always On (Cloud)	Select to trigger Tunnel VPN when the user logs in to Windows 10 desktop. Do not select if you want to restrict which apps trigger Tunnel VPN. By default, Always On is enabled.
Disable Certificate Pinning (Cloud)	Select to disable certificate pinning. By default, certificate pinning is enabled.
App Type (Cloud)	Select one of the following: <ul style="list-style-type: none"> • PFN Equals • EXE Path Equals
App Identifier (Cloud)	Depending on the App Type you selected, enter one of the following: <ul style="list-style-type: none"> • For PFN Equals, enter the package family name for Windows Store apps. Example: Microsoft.MicrosoftEdge_8wekyb3d8bbwe • For EXE Path Equals Enter the full path for legacy apps. Example: %PROGRAMFILES% (x86)\Google\Chrome\Application\chrome.exe
Traffic Filter (Cloud)	If a filter is not configured, all traffic is sent through Tunnel.

TABLE 2. TUNNEL (WINDOWS) CONFIGURATION FIELD DESCRIPTION (CONT.)

Item	Description
DNS Domain (Cloud)	(Optional) Enter the domain name for which traffic is sent through Tunnel. Use this option if you need to resolve the domain name.
DNS Server IP (Cloud)	Enter the IP address of the DNS to resolve the domain name entered in DNS Domain .
<p>Custom Data (Core) / Advanced (Cloud)</p> <p>Enter Key Value pairs to configure Tunnel behavior. You can use key-value pairs to control which apps trigger Tunnel, which traffic goes through Tunnel, idle session timeout, log levels, and viewing of debug diagnostic information.</p> <p>For Cloud deployments, if your profile mode is Access only, select Advanced to configure key-value pairs so that Tunnel VPN traffic goes to Access.</p> <hr/> <p> The Advanced option in Cloud is not automatically available. Please contact Customer Support to enable the Advanced feature for your tenant.</p> <hr/> <p>See "Key-value pairs for Access (Cloud)" on the next page.</p> <p>See "Key-value pairs for custom data" on page 26.</p>	

Key-value pairs for Access (Cloud)

If the profile mode for Tunnel VPN is Access only, select **Advanced** for **Define Tunnel App Settings** and enter the key-value pairs provided in the following table:

TABLE 3. KEY VALUE PAIRS FOR ACCESS

Key	Value
AppTriggerList/0/App/Id	App Id that will trigger Tunnel. Example: %PROGRAMFILES% (x86)\Google\Chrome\Application\chrome.exe
TrafficFilterList/0/App/Id	App Id that will tunnel traffic through Tunnel. Example: %PROGRAMFILES% (x86)\Google\Chrome\Application\chrome.exe
RouteList/0/Address	If your Cloud tenant is *.access-na1.mobileiron.com enter: 54.156.237.141 If your Cloud tenant is *.access-eu1.mobileiron.com enter: 18.158.157.61 If your Cloud tenant is *.ap2-sandbox.mobileiron.com enter: 3.105.254.35 If your Cloud tenant is *.access-sandbox.mobileiron.com enter: 184.73.234.161
RouteList/0/PrefixSize	32
TrafficFilterList/0/RoutingPolicyType	SplitTunnel
RouteList/1/Address	If your Cloud tenant is *.access-na1.mobileiron.com enter: 54.225.97.200 If your Cloud tenant is *.access-eu1.mobileiron.com enter: 18.159.128.208 If your Cloud tenant is *.ap2-sandbox.mobileiron.com enter: 3.104.98.59 If your Cloud tenant is *.access-sandbox.mobileiron.com enter: 23.23.171.60

TABLE 3. KEY VALUE PAIRS FOR ACCESS (CONT.)

Key	Value
RouteList/1/PrefixSize	32
RouteList/2/Address	If your Cloud tenant is *.access-na1.mobileiron.com enter: 18.235.224.5 If your Cloud tenant is *.access-eu1.mobileiron.com enter: 18.159.128.168 If your Cloud tenant is *.ap2-sandbox.mobileiron.com enter: 3.24.33.106 If your Cloud tenant is *.access-sandbox.mobileiron.com enter: 34.225.177.133
RouteList/2/PrefixSize	32

Key-value pairs for custom data

You use key-value pairs to define the following:

- ["Specify apps that will trigger Tunnel" on the next page](#)
- ["Traffic rules" on the next page](#)
- ["IPv4 network routes for Tunnel VPN" on page 28](#)
- ["DNS rules" on page 29](#)
- ["Network routes" on page 30](#)
- ["Pinning" on page 30](#)
- ["MTU" on page 31](#)
- ["Idle time out" on page 31](#)
- ["Debugging" on page 33](#)
- ["Examples of custom data configurations" on page 34](#)

The following table provides the key-value pairs supported for Tunnel for Windows 10.

TABLE 4. KEY-VALUE PAIRS FOR TUNNEL FOR WINDOWS 10

Key	Value	Description
Specify apps that will trigger Tunnel		
AppTriggerList/ AppTriggerId/App/Id trafficFilterID is 0 or an integer greater than zero. The trafficFilterId must start at 0. Enter a new row for each additional app and increment the trafficFilterId by 1. Do not skip a number	<ul style="list-style-type: none"> Package Family Name (PFN) Full path 	Package Family Name (PFN): Enter the package family name for Windows Store apps. Example: Microsoft.MicrosoftEdge_8wekyb3d8bbwe Full path: Enter the full path for legacy apps. Example: %PROGRAMFILES%(x86)\Google\Chrome\Application\chrome.exe
Specify apps that will route traffic through Tunnel		
TrafficFilterList/ trafficFilterId/App/Id trafficFilterID is 0 or an integer greater than zero. The trafficFilterId must start at 0. Enter a new row for each additional app and increment the trafficFilterId by 1. Do not skip a number.	<ul style="list-style-type: none"> Package Family Name (PFN) Full path 	Package Family Name (PFN): Enter the package family name for Windows Store apps. Example: Microsoft.MicrosoftEdge_8wekyb3d8bbwe Full path: Enter the full path for legacy apps. Example: %PROGRAMFILES%(x86)\Google\Chrome\Application\chrome.exe Ensure that Always On is not checked.
Traffic rules		
<ul style="list-style-type: none"> Defines which traffic is allowed through Tunnel. You configure traffic rules in conjunction with TrafficFilterList/trafficFilterId/App/Id. trafficFilterId in the traffic rule should match the trafficFilterId for the app to which this rule should apply. 		
TrafficFilterList/ trafficFilterId/Protocol	A number from 0-255	Only the IP protocols represented by the number are allowed. Example: 6. TCP = 6, UDP = 17

TABLE 4. KEY-VALUE PAIRS FOR TUNNEL FOR WINDOWS 10 (CONT.)



Key	Value	Description
TrafficFilterList/ trafficFilterId/LocalPortRanges	<i>A list of comma separated values specifying local port ranges</i>	Only the local port ranges listed are allowed. Example: 100-120, 200, 300-320.  Ports are only valid if the protocol is set to TCP=6 or UDP=17.
TrafficFilterList/ trafficFilterId /RemotePortRanges	<i>A list of comma separated values specifying remote port ranges</i>	Only the remote port ranges listed are allowed. Example: 100-120, 200, 300-320.  Ports are only valid if the protocol is set to TCP=6 or UDP=17.
TrafficFilterList/ trafficFilterId /LocalAddressRanges	<i>A list of comma separated values specifying local IP address ranges</i>	Only the IP addresses listed are allowed.
TrafficFilterList/ trafficFilterId /RemoteAddressRanges	<i>A list of comma separated values specifying remote IP address ranges</i>	Only the IP addresses listed are allowed.
TrafficFilterList/ trafficFilterId /RoutingPolicyType Specifies the routing policy for the app in the traffic filter list.	<ul style="list-style-type: none"> • ForceTunnel • SplitTunnel 	ForceTunnel: For this traffic rule all IP traffic from the app can go through Tunnel. SplitTunnel: For this traffic rule only designated traffic from the app, as determined by the networking stack, can go through Tunnel.
IPv4 network routes for Tunnel VPN		

TABLE 4. KEY-VALUE PAIRS FOR TUNNEL FOR WINDOWS 10 (CONT.)


Key	Value	Description
RouteList/ <i>routeRowId</i> /Address/PrefixSize <i>routeRowId</i> is 0 or an integer greater than zero. The <i>routeRowId</i> must start at 0. Enter a new row for each additional route and increment the <i>routeRowId</i> by 1. Do not skip a number.	<i>IPv4 network routes set aside for the VPN interface</i>	Specifies the IPv4 network routes for Tunnel VPN. The network routes are added to the device OS routing table.
<p>DNS rules</p> <p>Ivanti, Inc recommends configuring DNS rules. To configure DNS rules you must configure the following key-value pairs as a group:</p> <ul style="list-style-type: none"> • DomainNameInformationList/<i>dniRowId</i>/DomainName • DomainNameInformationList/<i>dniRowId</i>/DnsServers • DomainNameInformationList/<i>dniRowId</i>/DomainNameType <hr/> <p> Ensure that an explicit route to the DNS server is configured in the VPN profile. You can use IIPv4NetworkRoute key-value pair to configure the route to the DNS server.</p> <hr/>		
DomainNameInformationList/ <i>dniRowId</i> /DomainName <i>dniRowId</i> is 0 or an integer greater than zero. The <i>dniRowId</i> must start at 0. Enter a new row for each additional DNS server and increment the <i>dniRowId</i> by 1. Do not skip a number.	<ul style="list-style-type: none"> • <i>FQDN</i> • <i>Domain suffix</i> 	FQDN: Fully qualified domain name Domain suffix: A domain suffix that will be appended to the shortname query for DNS resolution. To specify a suffix, prepend a . to the DNS suffix. Example of domain suffix: .companyname.com
DomainNameInformationList/ <i>dniRowId</i> /DnsServers The <i>dniRowId</i> must match the <i>dniRowId</i> for the DomainName.	<i>List of comma separated DNS server IP addresses</i>	Ensure that there are no spaces between the listed IP addresses. Example: 10.10.15.6

TABLE 4. KEY-VALUE PAIRS FOR TUNNEL FOR WINDOWS 10 (CONT.)

Key	Value	Description
DomainNameInformationList/ <i>dniRowId</i> /DomainNameType The <i>dniRowId</i> must match the <i>dniRowId</i> for the DomainName.	<ul style="list-style-type: none"> FQDN Suffix 	Example: Suffix
Network routes Do not use these key-value pairs to configure Access routes.		
IPv4NetworkRoute	Valid IPv4 address range	Specifies the IPv4 network routes set aside for the VPN interface. Only traffic to the specified IP range will be allowed through Tunnel VPN. Enter an IPv4 address range. Ensure that the network routes are reachable and not overlapping. If an IPv4 address range is not specified, Tunnel sets the default route 0.0.0.0/0. You can enter multiple IPv4 address ranges. Each range must be separated by a semicolon. Example: 192.168.122.0/24
IPv4NetworkExcludedRoute	Valid IPv4 address range	These IPv4 routes will be excluded from going through Tunnel VPN. In the device routing table, the excluded routes are assigned to the non-VPN interfaces. Example: When a separate Standalone Sentry is set up for ActiveSync, access to the ActiveSync server does not need to go through Tunnel VPN, as ActiveSync traffic is secured by Standalone Sentry. In this case, you may want to exclude the specific route to the ActiveSync server. If the IP range is 192.0.0.0/24, and the IP address of the ActiveSync server is 192.0.1.1, the excluded route should be 192.0.1.1/32.
Pinning		

TABLE 4. KEY-VALUE PAIRS FOR TUNNEL FOR WINDOWS 10 (CONT.)

Key	Value	Description
DisablePinning	1	Disables certificate pinning. By default, certificate pinning is enabled.
MTU		
TunnelMTU	An integer greater than 0	Sets the Inner Tunnel MTU. The default is set for 1400 bytes. The maximum packet size that Windows 10 accepts is 1401 bytes. The Inner Tunnel Max Frame Size is set as 1500.
Idle time out		
TcpIdleTmoMs	An integer greater than 0	Controls the idle session timeout for the connection between the app and the backend resource. The timeout is measured in milliseconds. Example: For 70 seconds, enter 70000. The default idle timeout with Standalone Sentry for app VPN is 60 seconds.
DesktopIdleTmoMonitor	0, 1	Only for Windows 10 desktops. 1: DesktopSentIdleTmoMs is enabled. Tunnel monitors the idle time instead of Windows. This allow for faster and better response after a timeout. Tunnel uses the idle time out specified in DesktopSentIdleTmoMs and DesktopRecvIdleTmoMs. The default values are used if the key-value pairs are not configured. 0: The idle timeout management by Tunnel is disabled. The default value if the key-value pair is not configured: 1

TABLE 4. KEY-VALUE PAIRS FOR TUNNEL FOR WINDOWS 10 (CONT.)

Key	Value	Description
DesktopSentIdleTmoMs	<i>An integer greater than 0</i>	<p>Only for Windows 10 desktops.</p> <p>The timeout is measured in milliseconds.</p> <p>If a value is not configured or configured as 0, Standalone Sentry's timeout value, which is 60 seconds, or the value configured for TcpIdleTmoMs is used.</p> <p>The sent idle timeout is measured from the time of the last packet sent by Tunnel to Standalone Sentry.</p>
DesktopRecvIdleTmoMs	<i>An integer greater than 0</i>	<p>Only for Windows 10 desktops.</p> <p>The timeout is measured in milliseconds.</p> <p>If a value is not configured or configured as 0, received idled timeout is set to 30 seconds.</p> <p>The received idle timeout is measured from the time of the last packet received by Tunnel from Standalone Sentry.</p>
PhoneIdleTmoMonitor	0, 1	<p>Only for Windows 10 phones.</p> <p>1: DesktopSentIdleTmoMs is enabled. Tunnel monitors the idle time instead of Windows. This allow for faster and better response after a timeout. Tunnel uses the idle time out specified in DesktopSentIdleTmoMs and DesktopRecvIdleTmoMs. The default values are used if the key-value pairs are not configured.</p> <p>0: The idle timeout management by Tunnel is disabled.</p> <p>The default value if the key-value pair is not configured: 1</p>

TABLE 4. KEY-VALUE PAIRS FOR TUNNEL FOR WINDOWS 10 (CONT.)

Key	Value	Description
PhoneSentIdleTmoMs	<i>An integer greater than 0</i>	<p>Only for Windows 10 phones.</p> <p>The timeout is measured in milliseconds.</p> <p>If a value is not configured or configured as 0, Standalone Sentry's timeout value, which is 60 seconds, or the value configured for TcpIdleTmoMs is used.</p> <p>The sent idle timeout is measured from the time of the last packet sent by Tunnel to Standalone Sentry.</p>
PhoneRecvIdleTmoMs	<i>An integer greater than 0</i>	<p>Only for Windows 10 phones.</p> <p>The timeout is measured in milliseconds.</p> <p>If a value is not configured or configured as 0, received idled timeout is set to 30 seconds.</p> <p>The received idle timeout is measured from the time of the last packet received by Tunnel from Standalone Sentry.</p>
Debugging		
DebugLog	1	<p>Collects debug-level logs on the app connecting to the backend resource. By default, minimal-level logs are collected. If this key-value pair is configured, then the feature is grayed out in Tunnel and the user cannot change this setting on the device.</p>
ShowDebugUI	1	<p>Enables viewing of diagnostic information on the app connecting to the backend resource.</p> <p>After the key-value pair is pushed to the device, the app must try to connect to backend resource to get the value. If the app is already running, it will pick up the new key-value pair when it is restarted.</p>
debugInfoRecipient	A valid email address	<p>Auto populates the support email address to which the logs will be emailed.</p> <p>The log information is sent to the email address configured here.</p>

Examples of custom data configurations

The following are examples of custom data configurations:

- ["Trigger Tunnel VPN when the user logs in to Windows 10 desktop" below](#)
- ["Force tunneling with multiple DNS servers" below](#)
- ["Split tunneling with one route list and one DNS server" on the next page](#)
- ["Split tunneling with two route lists and one DNS server" on the next page](#)

Trigger Tunnel VPN when the user logs in to Windows 10 desktop

- **Always On** is checked.

Key	Value
IPv4NetworkRoute	0.0.0.0/0;10.10.15.6/32;
TrafficFilterList/0/RoutingPolicyType	ForceTunnel
TrafficFilterList/0/App/Id	C:\Program Files (x86)\Google\Chrome\Application\chrome.exe
DomainNameInformationList/0/DomainName	.companyname.com
DomainNameInformationList/0/DomainNameType	Suffix
DomainNameInformationList/0/DnsServers	10.10.15.6
TrafficFilterList/0/RemoteAddressRanges	10.0.0.0-10.255.255.25

Force tunneling with multiple DNS servers

- **Always On** is unchecked.

Key	Value
IPv4NetworkRoute	10.11.0.0/16;10.0.0.0/8;10.10.15.6/32;10.11.50.31/32;
TrafficFilterList/0/App/Id	%PROGRAMFILES% (x86)\Google\Chrome\Application\chrome.exe

Key	Value
TrafficFilterList/0/RoutingPolicyType	ForceTunnel
TrafficFilterList/0/RemoteAddressRanges	10.0.0.0-10.255.255.255
DomainNameInformationList/0/DomainName	.companyname.com
DomainNameInformationList/0/DnsServers	10.10.15.6
DomainNameInformationList/0/DomainNameType	Suffix
DomainNameInformationList/1/DomainName	.google.com
DomainNameInformationList/1/DnsServers	10.11.50.31
DomainNameInformationList/1/DomainNameType	Suffix

Split tunneling with one route list and one DNS server

- **Always On** is unchecked.

Key	Value
IPV4NetworkRoute	0.0.0.0/0;10.10.15.6/32;
TrafficFilterList/0/App/Id	%PROGRAMFILES% (x86)\Google\Chrome\Application\chrome.exe
RouteList/0/Address	10.0.0.0
RouteList/0/PrefixSize	8
TrafficFilterList/0/RoutingPolicyType	SplitTunnel
DomainNameInformationList/0/DomainName	.companyname.com
DomainNameInformationList/0/DnsServers	10.10.15.6
DomainNameInformationList/0/DomainNameType	Suffix

Split tunneling with two route lists and one DNS server

- **Always On** is unchecked.

Key	Value
IPV4NetworkRoute	10.10.15.6/32;10.11.50.31/32
TrafficFilterList/0/App/Id	%PROGRAMFILES% (x86)\Google\Chrome\Application\chrome.exe
RouteList/0/Address	10.10.0.0
RouteList/0/PrefixSize	16
RouteList/1/Address	10.11.0.0
RouteList/1/PrefixSize	16
TrafficFilterList/0/RoutingPolicyType	SplitTunnel
DomainNameInformationList/0/DomainName	.companyname.com
DomainNameInformationList/0/DnsServers	10.10.15.6
DomainNameInformationList/0/DomainNameType	Suffix

What users see in Tunnel for Windows 10

The following provide information about device user experience:

Manually triggering Tunnel	38
Emailing debug logs	39

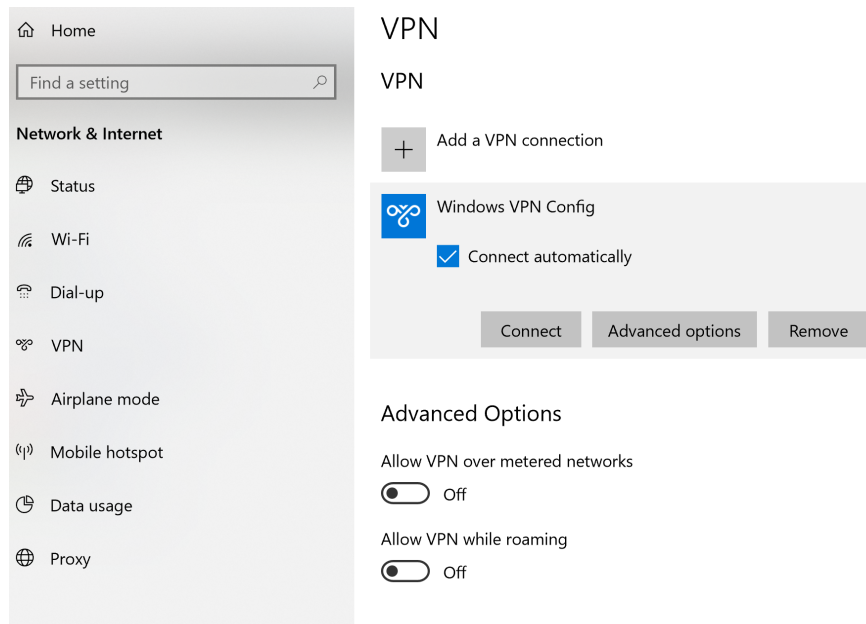
Manually triggering Tunnel

Device users can manually trigger Tunnel on their Windows 10 desktop.

Procedure

1. Go to **Setting > Network & Internet**.

FIGURE 1. CONNECT TUNNEL VPN



2. Click on **VPN**.
3. In the VPN pane, select the Tunnel VPN profile.

If there are multiple VPN profiles installed, Ivanti recommends also selecting **Connect automatically**.

4. Click **Connect**.

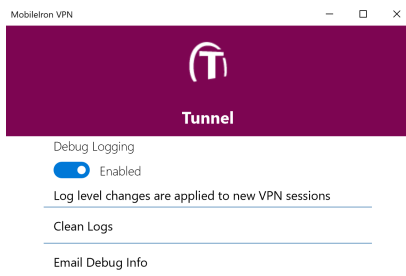
Emailing debug logs

To debug issues in the app you can email the debug logs from the app to a valid email address.

Procedure

1. Launch the Tunnel app.

FIGURE 1. LAUNCH TUNNEL APP

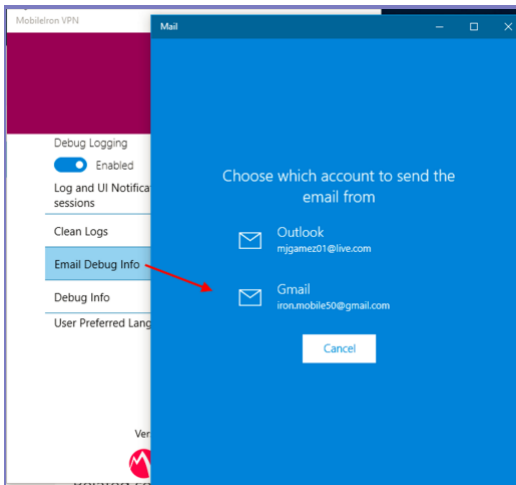


Version: 1.2.3.0



2. Click **Email Debug Info**.

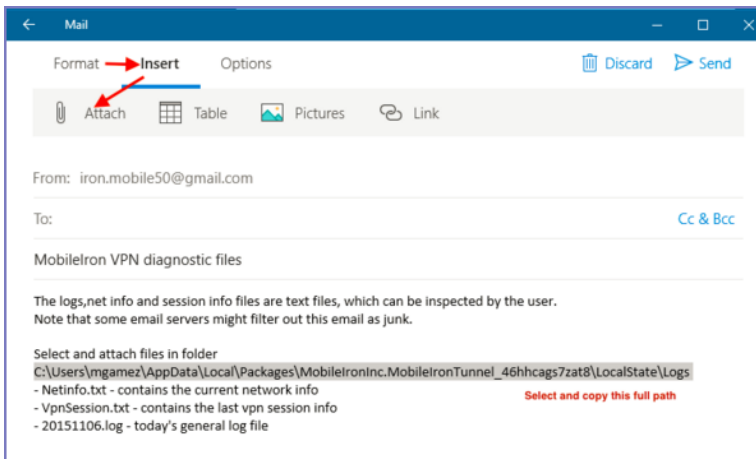
FIGURE 2. EMAIL DEBUG INFO



3. The default email app is launched. If a default app is not selected, you are asked to choose the email account you want to use.

The To address is auto populated if the support email address is configured in the Tunnel VPN profile. The email also contains the path to the log file on the Windows 10 desktop.

FIGURE 3. ATTACH TUNNEL DEBUG LOG FILE



4. Navigate to the path shown in the email to attach the log file to the email and send.