

Getting access to on-premises resources with Microsoft Tunnel

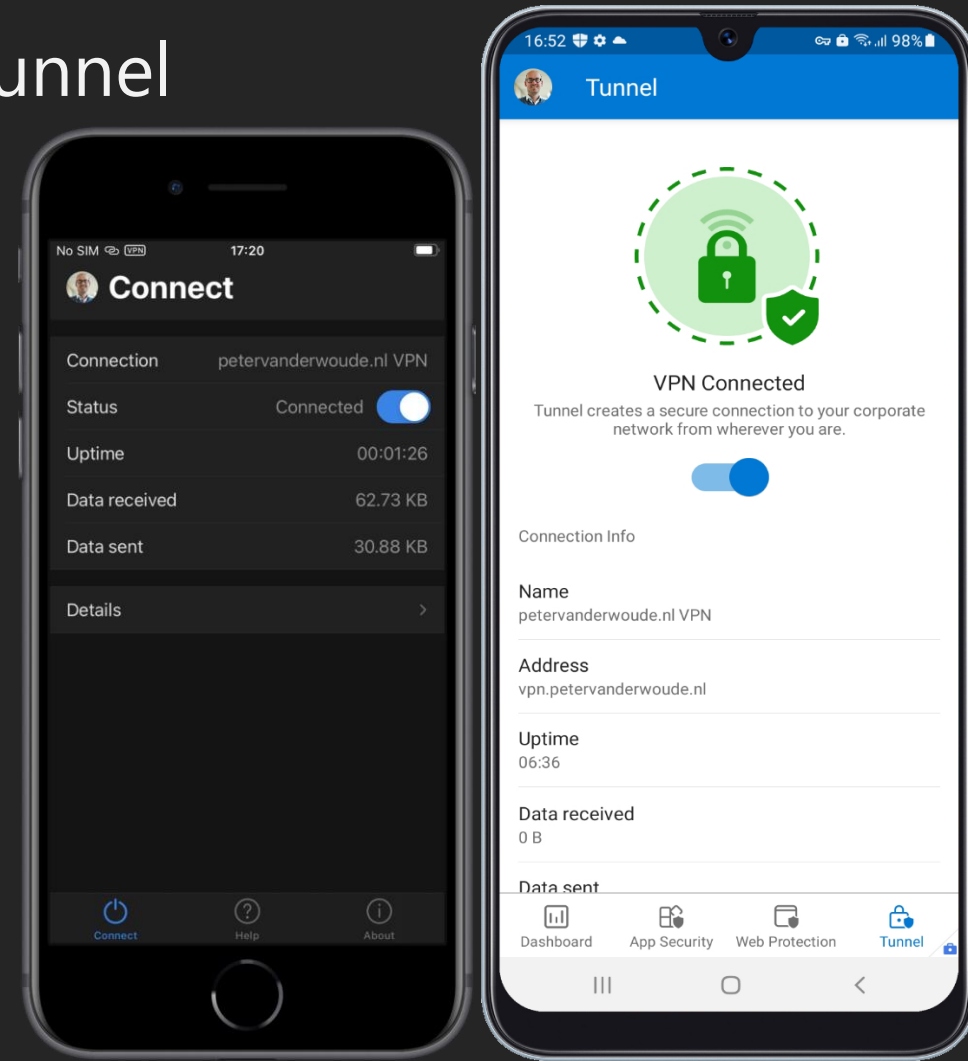
- Peter van der Woude
- Modern Workplace enthusiast
- [@pvanderwoude](https://twitter.com/pvanderwoude)
- <https://petervanderwoude.nl/>
- Enterprise Mobility MVP | Windows Insider MVP

Getting access to on-premises resources with Microsoft Tunnel

Get familiar with the capabilities of the Microsoft Tunnel Gateway that is available within your Microsoft Intune license

Agenda

- An introduction to Microsoft Tunnel
- The different components of Microsoft Tunnel
- How Microsoft Tunnel works
- Configuring Microsoft Tunnel
 - Creating the Server configuration
 - Creating the Site configuration
- Installing Microsoft Tunnel
- Configuring the iOS/Android device
 - Distributing the client app
 - Configuring the client app
- Interacting with Microsoft Tunnel



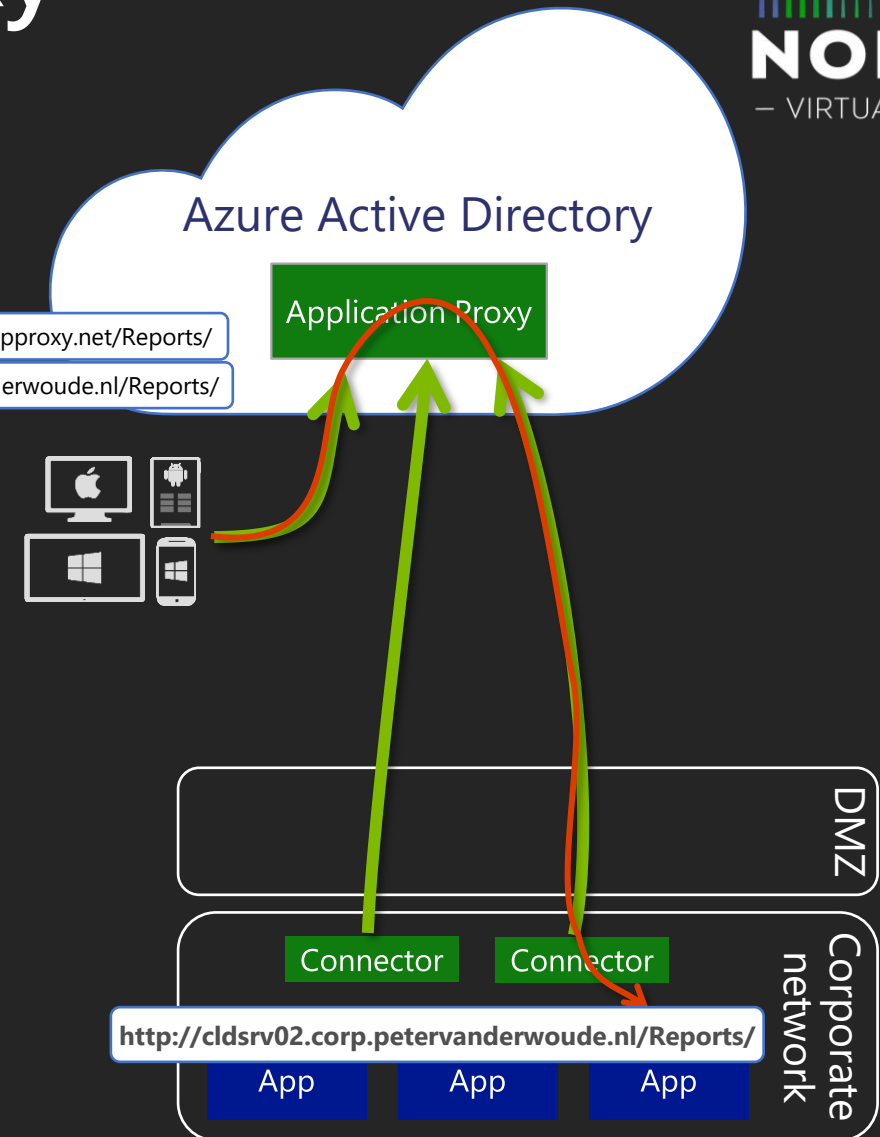
An introduction to Microsoft Tunnel

- A VPN gateway
- Provides access to internal apps and resources
- Seamless integration with Azure AD
- Access protected with Conditional Access
 - **How does it compare with Azure AD Application Proxy**
 - Web applications that use IWA for authentication
 - Web applications that use form-based or header-based access
 - Web APIs to expose to rich applications
 - Apps hosted behind a Remote Desktop Gateway
 - Rich client apps that are integrated with MSAL
 - **Replaces the need for a VPN or reverse proxy**

Azure AD Application Proxy

A quick look to refresh the memory

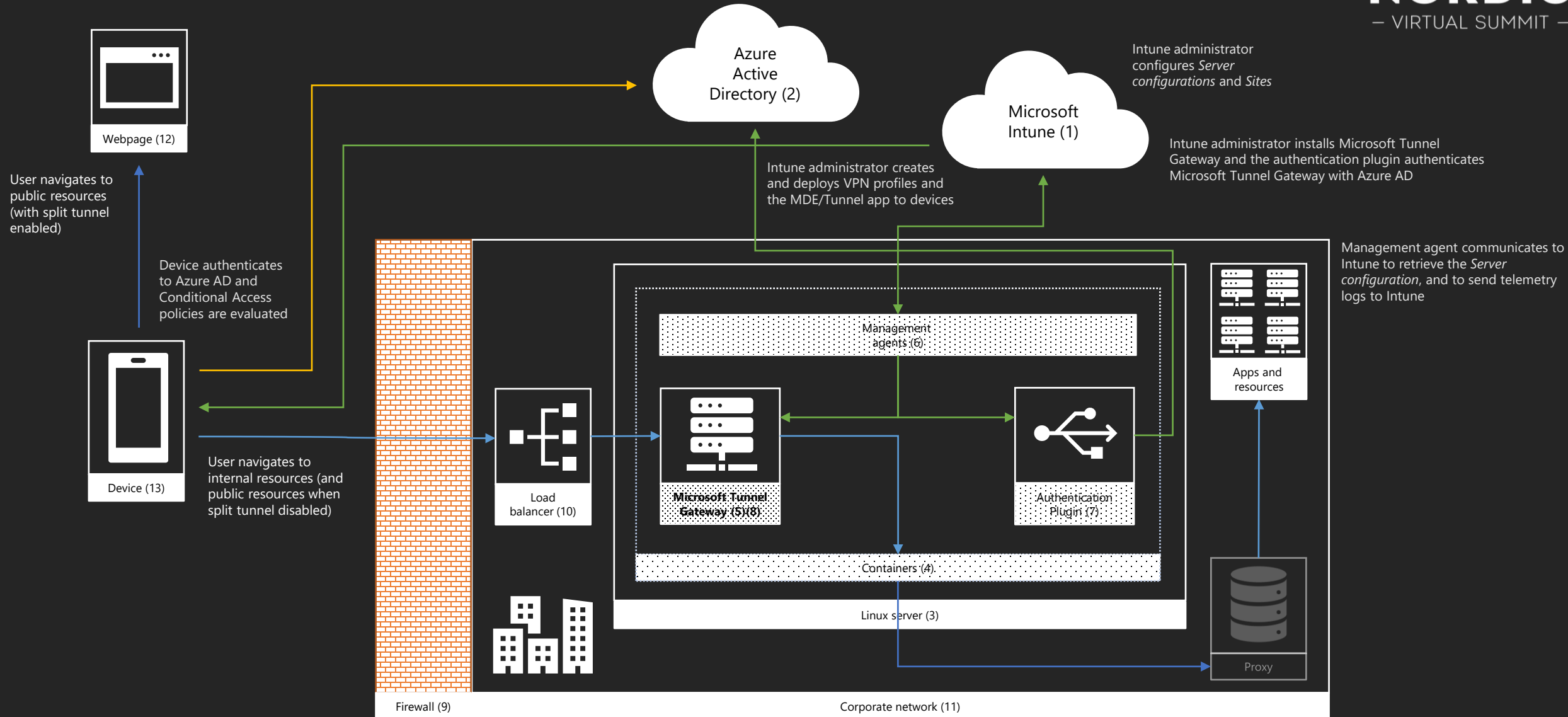
- *How does it work?*
 - Connectors are deployed on corporate network
 - Multiple connectors can be deployed for redundancy and scale
 - Connectors auto connect to the cloud service
 - User connects to the cloud service that routes their traffic to the resources via the connectors



Main components of Microsoft Tunnel

	Component	Usage
1	Microsoft Intune	The solution for managing the Tunnel Gateway and the device
2	Azure AD	The solution for authentication to the Tunnel Gateway
3	Linux server	The platform for running containers (Podman or Docker)
4	Containers	The engine for running containers of Tunnel Gateway and the management agent
5	Microsoft Tunnel	The VPN provider for access to on-premises resources
6	Management agent	The agent for applying the required configuration to the Tunnel Gateway
7	Authentication plugin	The authorization plugin for authentication with Azure AD
8	TLS certificate	The certificate for securing connections from devices to the Tunnel Gateway server
9	Firewall	The secure wall for protecting the on-premises resources
10	Public IP/FQDN	The public address for accessing the Tunnel Gateway
11	Corporate network	The location for the on-premises resources
12	Public Internet	The location for the mobile devices
13	Device	The device for connecting to the Tunnel Gateway server

How Microsoft Tunnel works



Configuring Microsoft Tunnel (Server)

- Server configuration
 - Configuration for servers
 - IP address range for clients
 - Port that server listens to
 - DNS servers for clients
 - DNS suffix for clients
 - Split tunnel rules (include or exclude ranges)

Microsoft Endpoint Manager admin center

Home > Tenant admin > Default server configuration >

Default server configuration


Microsoft Tunnel Gateway

1 Settings 2 Review + save


IP address range * ⓘ

Server port * ⓘ

DNS servers * ⓘ


Address	
192.168.20.1	
<input type="text"/>	

DNS suffix search ⓘ


Address	
<input type="text"/>	

Split tunneling rules

IP ranges to include ⓘ

 Upload .csv file

IP ranges to exclude ⓘ

 Upload .csv file

[Review + save](#) [Cancel](#)

Configuring Microsoft Tunnel (Site)

- Site configuration
 - Logically group servers
 - Public IP/FQDN as connection point
 - Configuration for all servers
 - URL for network access check
 - Automatically upgrade servers
 - (Optionally) Use maintenance windows for upgrade

Microsoft Endpoint Manager admin center

Home > Tenant admin > Default site configuration >

Default site configuration

Microsoft Tunnel Gateway

1 Settings 2 Review + save

Public IP address or FQDN *

Server configuration *

URL for internal network access check

Automatically upgrade servers at this site

Limit server upgrades to maintenance window

Time zone

Start time

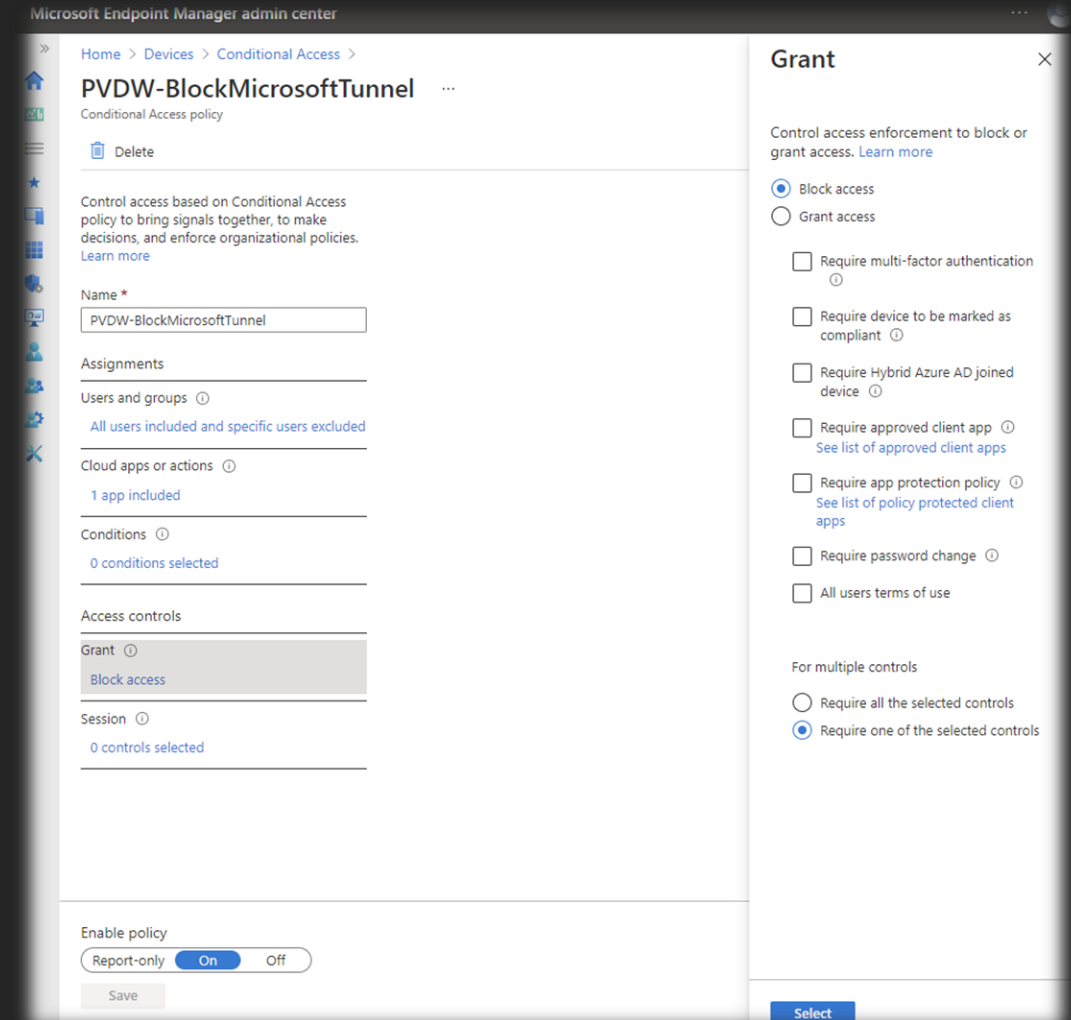
End time

i After you save your changes, all servers at this site will restart.

Review + save **Cancel**

Conditional Access for Microsoft Tunnel

- If needed, provision tenant using **st-CA-readiness.ps1** from aka.ms/mst-ca-provisioning (relies on Azure AD PowerShell module)
- Manage access to Microsoft Tunnel Gateway by introducing a block all traffic rule for Conditional Access



Installing Microsoft Tunnel

- download the installation script
- run the installation script
- When prompted, accept the license agreement (EULA)
- When prompted, copy the TLS certificate
- When prompted, sign in and authenticate with Intune (device login)
- `wget --output-document=mstunnel-setup https://aka.ms/microsofttunneldownload`
- `sudo chmod +x ./mstunnel-setup`

Configuring the device (VPN profile)

- VPN profile
 - The site configuration contains the public connection point
 - Configuration options slightly differ per platform
 - Use defendertoggle to only enable Microsoft Tunnel via the Microsoft Defender for Endpoint app

Microsoft Endpoint Manager admin center

Home > Devices > AE - Default VPN profile >

VPN

Android Enterprise

1 Configuration settings 2 Review + save

Connection type * ⓘ Microsoft Tunnel

Base VPN *

Connection name * ⓘ petervanderwoude.nl VPN

Microsoft Tunnel site * ⓘ

Default site configuration ⓘ

[Change the site](#)

Per-app VPN

Always-on VPN

Proxy

Custom settings

Configuration key	Value type	Configuration value
defendertoggle	Integer	0
Not configured		Not configured

Review + save Cancel

Configuring the device (VPN app)

- VPN app
 - Android
 - Microsoft Defender for Endpoint app
 - Available in (Managed) Google Play Store
 - iOS
 - Microsoft Tunnel app
 - Available in Apple App Store

Microsoft Endpoint Manager admin center

Home > Apps > Android > Microsoft Defender Endpoint >

Edit application

Managed Google Play store app

App information Review + save


Name Microsoft Defender Endpoint

Description Bescherm uw apparaat tegen beveiligingsrisico's; veilig toegang tot het bedrijfsnetwerk

Publisher Microsoft Corporation

Appstore URL <https://play.google.com/store/apps/details?id=com.microsoft.scmx&hl=nl-NL>

Logo Change image



Available licenses 0

Total licenses 0

Review + save Cancel

Interacting with Microsoft Tunnel

- /etc/mstunnel – directory that contains all configs
 - admin-settings.json – configuration as configured Intune
 - agent-info.json – agent information
 - ocserv.conf – VPN server configuration
 - version-info.json – version information
- journalctl – method to view logs
 - ocserv – displays the VPN server logs
 - mstunnel-agent – displays the Intune agent logs
 - msintune_monitor – displays the monitoring task logs
- mst-cli – command-line tool for local interaction
 - sudo mst-cli – displays the command-line options

Thank you!



MSEndPointMgr.com
#MSEndPointMgr

System Center User Group
Finland
#SCUGFI

System Center User Group
Denmark
#SCUGDK

System Center User Group
Sweden
#SCUGSE

Modern Management User Group
Norway
#MMUGNO