Enhancing remote access in Windows 10 with an automatic VPN profile

Microsoft IT manages a remote access infrastructure that enables mobile productivity, security, and convenience for Microsoft employees. Every weekday, 35,000 to 45,000 employees use a virtual private network (VPN) connection to remotely connect to the corporate network. That number dips only slightly to 25,000 to 35,000 on weekends and during non-peak hours. We leveraged new capabilities in Windows 10 Anniversary Update that made it possible for us to roll out a new VPN connection profile. The VPN connection profile uses Always-On functionality to simplify how employees connect when they're away from the office, and it helps improve the remote access experience for employees running Windows 10 Anniversary Update, or later, by providing a seamless, secure network connection to Microsoft resources from their Windows 10 desktop or mobile device.

Some benefits of this feature include:

- Improving employee experience by automatically connecting to the corporate network using VPN.
- Minimizing user touch points, leveraging a single sign-in and certificate check to provide ongoing connectivity.
- Enabling VPN compliance policy enforcement through system health checks.

Providing an Always-On remote access experience

Employees running Windows 10 Anniversary Update—with the new VPN connection profile installed—are automatically connected when they try to open a website or resource that needs a VPN connection. Employees don't have to do anything to connect after their initial sign-in. By default, the Always-On VPN connection profile chooses the best entry point based on an employee's geographic location.

We didn't phase out the VPN solution that was used in the environment before we implemented the Always-On VPN connection profile. The VPN solution relies on a client connection manager app, based on Windows Connection Manager, that's installed on employees' computers that employees use to initiate a connection to the remote access infrastructure. We still use VPN with client connection manager for computers that haven't installed the Windows 10 Anniversary Update.

Both the VPN with client connection manager and the Always-On VPN connection profile connect to the same VPN infrastructure using the same strong authentication methods and employee sign-in with multi-factor authentication. The only difference is that with the VPN connection profile, employees need to sign in only once and a certificate is issued that makes all future connections automated—up to the time-bound expiration date that we configure for the certificate. We configured certificates to expire so that we can validate employees' credentials and devices on a regular basis.

Securely accessing the corporate network on domain-joined or managed devices

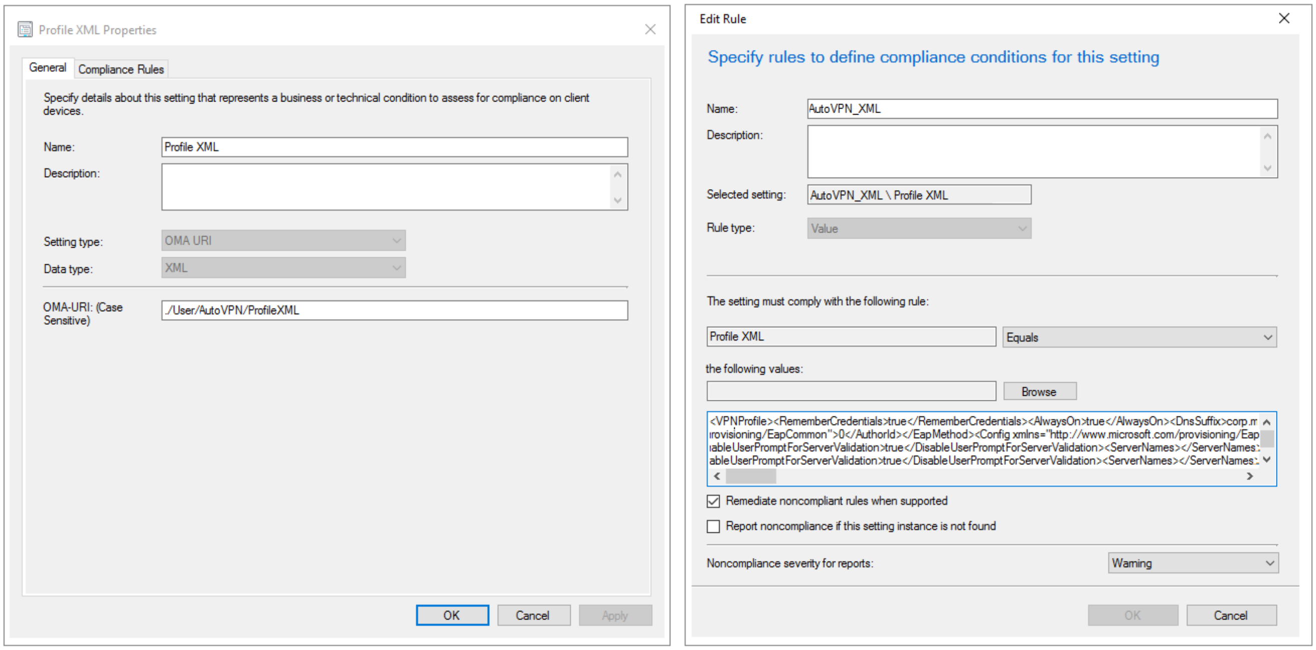
We use System Center Configuration Manager to manage all our domain-joined computers, and Microsoft Intune provides enterprise mobility management support for Microsoft Azure Active Directory (Azure AD) domain–joined computers and mobile devices that have enrolled in the service. In our hybrid configuration, VPN policies are replicated into Microsoft Intune and applied to enrolled devices; these include certificate issuance that we create in Configuration Manager for Windows 10 devices.

For more information about how we use Microsoft Intune as part of our mobile device management strategy, see Mobile device management at Microsoft.

Configuring a VPN connection profile

VPN profiles contain all the information a device requires to connect to the corporate network, including the authentication methods that are supported and the VPN server that the device should connect to. Changes in Windows 10 Anniversary Update, including Conditional Access and single sign-on, made it possible for us to create our Always-On VPN connection profile. We created the connection profile for domain-joined and Microsoft Intune–managed devices using System Center Configuration Manager console.

The Microsoft Intune custom profile for Intune-managed devices uses Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings with XML data type. Figure 1 shows an example.



Profile XML Properties

General | Compliance Rules

Specify details about this setting that represents a business or technical condition to assess for compliance on client devices.

Name: Profile XML

Description:

Setting type: OMA URI

Data type: XML

OMA-URI: (Case Sensitive) ./User/AutoVPN/ProfileXML

Edit Rule

Specify rules to define compliance conditions for this setting

Name: AutoVPN_XML

Description:

Selected setting: AutoVPN_XML \ Profile XML

Rule type: Value

The setting must comply with the following rule:

Profile XML | Equals

the following values:

```
<VPNProfile><RememberCredentials>true</RememberCredentials><AlwaysOn>true</AlwaysOn><DnsSuffix>corp.m
rovisioning/EapCommon">0</AuthorId></EapMethod><Config xmlns="http://www.microsoft.com/provisioning/Eap
iableUserPromptForServerValidation>true</DisableUserPromptForServerValidation><ServerNames></ServerNames:
ableUserPromptForServerValidation>true</DisableUserPromptForServerValidation><ServerNames></ServerNames:
```

☑ Remediate noncompliant rules when supported

□ Report noncompliance if this setting instance is not found

Noncompliance severity for reports: Warning

Figure 1. Creating a Profile XML and editing the OMA-URI settings to create a connection profile in System Center Configuration Manager

For more information about creating VPN profiles, see How to Create VPN Profiles in Configuration Manager and VPN profile options.

Installing the VPN connection profile

The new VPN connection profile was installed using a script on domain-joined computers, running Windows 10 Anniversary Update, through a policy in System Center Configuration Manager.

For mobile devices running Windows 10 Anniversary Update or Windows 10 Mobile that are managed through Microsoft Intune, after the device is enrolled, the user policy for the connection profile is available at the gateway and a policy is loaded on the device that includes the connection profile. After the profile is installed on Windows 10 (the 64-bit version) and Windows 10 Mobile devices that are enrolled in Mobile Device Management, and if all the required certificates are also installed on the devices, employees can connect using the custom profile.

For more information about how we use Microsoft Intune as part of our mobile device management strategy, see Mobile device management at Microsoft.

VPN client connection flow

We use an optional feature that checks the device health and corporate policies before allowing it to connect. Conditional Access is supported with connection profiles, and we've started using the feature in our environment. Rather than just relying on the managed device certificate for a "pass" or "fail" for VPN connection, Conditional Access places machines in a quarantined state while checking for the latest required security updates and antivirus definitions to help ensure that the system isn't introducing risk. On every connection attempt, the system health check looks for a certificate that the device is still compliant with corporate policy.

Figure 2 illustrates how the VPN client-side connection flow works.

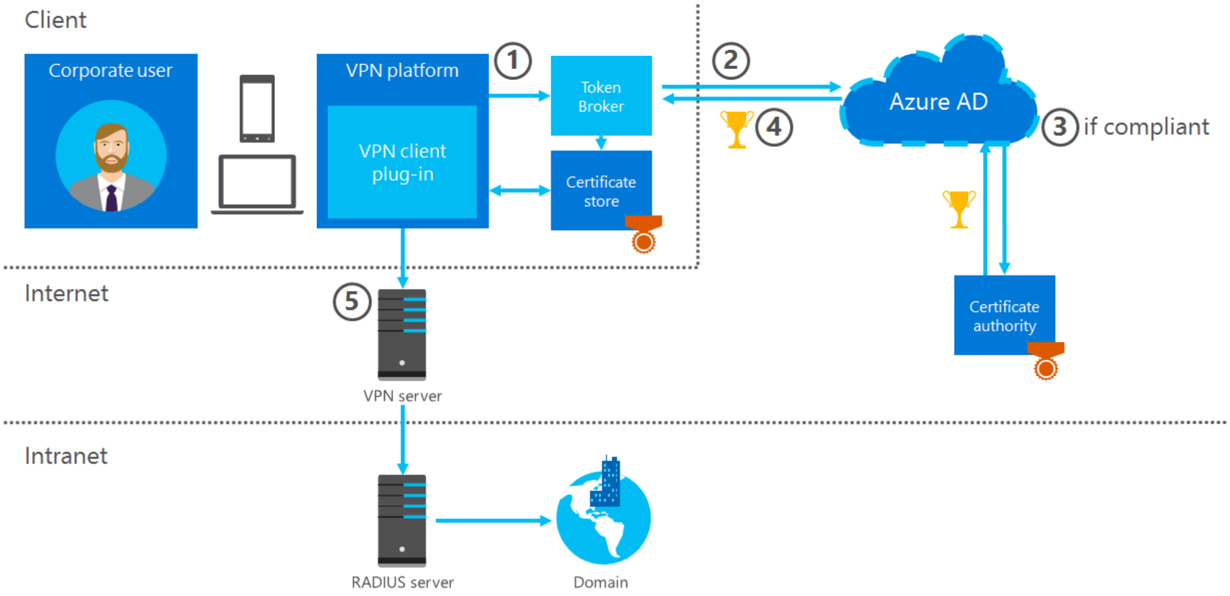


Figure 2. The client side VPN connection flow

When a device compliance–enabled VPN connection profile is triggered (either manually or automatically):

1. The VPN client calls into the Windows 10 Azure AD Token Broker on the local device, and identifies itself as a VPN client.
2. The Azure AD Token Broker authenticates to Azure AD and provides it with information about the device trying to connect. A device check is performed by Azure AD to determine whether the device complies with our VPN policies.
3. If the device is compliant, Azure AD requests a short-lived certificate. If the device isn't compliant, we perform remediation steps.
4. Azure AD pushes down a short-lived certificate to the Certificate Store via the Token Broker. The Token Broker then returns control back over to the VPN client for further connection processing.
5. The VPN client uses the Azure AD–issued certificate to authenticate with the VPN server.

Supported authentication methods

Our preferred credential is backed by certificate-based authentication (public key infrastructure, or PKI) and multi-factor authentication solutions.

Windows 10 Anniversary Update with Always-On VPN

When employees first use of the Always-On VPN connection profile, they will be prompted to authenticate strongly. Our VPN infrastructure supports Windows Hello for Business and Multi-Factor Authentication.

The VPN connection profile uses the same certificate-based and multi-factor authentication as the legacy VPN with client connection manager solution that it has mostly replaced, but it also stores a cryptographically protected certificate upon successful authentication that allows for either a persistent or automatic connection.

Windows Mobile

On Windows Phone 8/8.1 and Windows Mobile 10, VPN profiles are deployed via Microsoft Intune. The VPN profiles are set to connect automatically using the Always-On functionality and are configured to route only corporate data through the tunnel (using split tunneling). In Windows 10 Mobile, there's greater flexibility for secure authentication with new features like Windows Hello for Business, and additional security features like Conditional Access and Windows Information Protection.

Remote access infrastructure

The infrastructure for providing remote access to all the supported operating systems at Microsoft is shared by both connection methods, except for a few key pieces that we included to issue certificates and to manage non–domain-joined systems.

Figure 3 shows our remote access infrastructure.

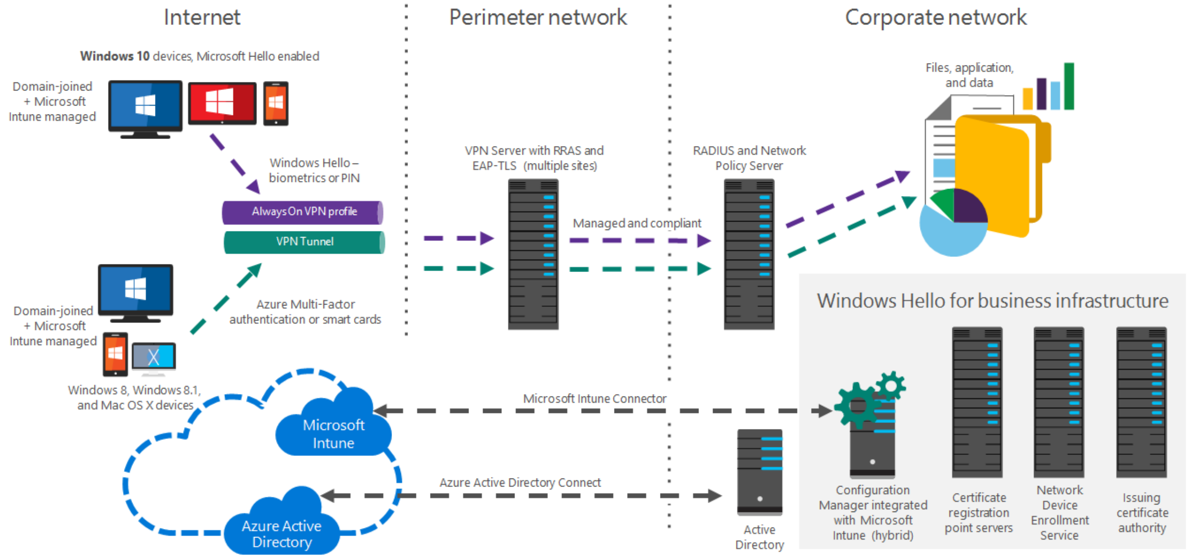

Internet
Perimeter network
Corporate network
Windows 10 devices, Microsoft Hello enabled
Domain-joined + Microsoft Intune managed
Windows Hello – biometrics or PIN
Always On VPN profile
VPN Tunnel
Azure Multi-Factor authentication or smart cards
Domain-joined + Microsoft Intune managed
Windows 8, Windows 8.1, and Mac OS X devices
VPN Server with RRAS and EAP-TLS (multiple sites)
Managed and compliant
RADIUS and Network Policy Server
Files, application, and data
Windows Hello for business infrastructure
Microsoft Intune
Microsoft Intune Connector
Azure Active Directory
Azure Active Directory Connect
Active Directory
Configuration Manager integrated with Microsoft Intune (hybrid)
Certificate registration point servers
Network Device Enrollment Service
Issuing certificate authority

Figure 3. Microsoft remote access

Certificate and device enrollment

We use an Azure AD certificate for single sign-on to the Always-On VPN connection profile. And we currently use Simple Certificate Enrollment Protocol (SCEP) and Network Device Enrollment Service (NDES) to deploy certificates to our mobile devices via Microsoft Intune and Configuration Manager. The SCEP certificate we use is for wireless and for VPN. NDES allows software on routers and other network devices running without domain credentials to obtain certificates based on the SCEP.

NDES performs the following functions:

1. It generates and provides one-time enrollment passwords to administrators.
2. It submits enrollment requests to the certificate authority (CA).
3. It retrieves enrolled certificates from the CA and forwards them to the network device.

For more information about deploying NDES, including best practices, see Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS). Also, see Securing and Hardening Network Device Enrollment Service for Microsoft Intune and System Center Configuration Manager.

RADIUS server

Remote Authentication Dial-In User Service (RADIUS) servers, or Network Policy Server, perform authentication, authorization, and accounting for RADIUS clients. A RADIUS client can be an access server, such as a dial-up server or wireless access point, or a RADIUS proxy. When NPS is used as a RADIUS server, it provides authentication, authorization, and accounting services for network access servers.

For more information, see Network Policy and Access Services Overview.

RRAS

We use Routing and Remote Access Service (RRAS) to deploy VPN, dial-up remote access services, multiprotocol LAN-to-LAN, LAN-to-WAN, and network address translation (NAT) routing services.

For more information about deploying VPN using RRAS, see Routing and Remote Access Service (RRAS).

VPN tunnel types

Our VPN solution supports the following tunnel types:

- **IKEv2.** This tunnel type is preferred and is set as the default. IKEv2 is more resilient to changing network connectivity, so it's a good choice for mobile users who move between access points and even switch between wired and wireless connections.
- **SSTP.** The default tunnel fail-over strategy for the Always-On VPN connection. Secure Socket Tunneling Protocol (SSTP) provides firewall traversal capability. This means mobile users who are trying to access corporate network resources from behind customer firewalls, airport hotspots, hotels, and other public Wi-Fi hotspots can successfully use VPN.

Split tunneling

Split tunneling allows only the traffic destined for the Microsoft corporate network to be routed through the VPN tunnel, and all Internet traffic goes directly through the Internet without traversing the VPN tunnel. In the VPN connection profile, split tunneling is enabled by default.

Applying policies

Configuration Manager and Intune handle policy enforcement, as well as certificate enrollment and deployment, on behalf of the client. Remote computers and devices that use VPN to connect to the corporate network must be checked for compliance. For Windows 8.1 and earlier, we still use a separate compliance check that will quarantine a system; it has limited access to corporate resources while it performs a system health check and installs required updates.

We require certificates from Configuration Manager on Windows 10 domain-joined computers, or from Microsoft Intune for computers that are enrolled to be managed. That certificate implies that because the computer is managed, it should be able to pass a system health check. If a computer doesn't have all the system and security requirements installed, Configuration Manager or Intune will install them—if they're not installed, the certificate that's needed to connect won't be issued.

With every new Windows 10 update, we rolled out a pre-release version to a group of about 15,000 early adopters a few months before its release. Early adopters validated the new credential functionality and used remote access connection scenarios to provide valuable feedback that we could take back to the product development team. Using early adopters helped validate and improve features and functionality, influenced how we prepared for the broader deployment across Microsoft, and helped us prepare support channels for the types of issues that employees might experience.

Enforcement of the VPN compliance policy

The Microsoft IT Conditional Access administrator is responsible for defining the VPN Compliance Policy for domain-joined Windows 10 desktops, including enterprise laptops and tablets, within the Microsoft Azure Portal administrative experience. This policy will then be published so that the enforcement of the applied policy can be managed through Microsoft Intune and the System Center Configuration Manager. For more information, see Conditional access in Azure Active Directory.

Encouraging adoption

When we released Windows 10 Anniversary Update, we first encouraged employees to upgrade, then we began enforcing installation of the update through System Center Configuration Manager and Windows Intune. After the upgrade, policies were applied, and the script that included the VPN connection profile was installed. Employees simply needed to sign in with their corporate credentials and either their Windows Hello or physical smart card for multi-factor authentication. We sent email communications to employees to inform them about the new profile, and explained how it would act as a persistent connection, automatically connecting whenever they access corporate resources. We also provided more information about the VPN connection profile on our mobility portal.

Most employees on corporate-provisioned devices are now running Windows 10 Anniversary Update and are using the new connection profile as their connection to the remote access infrastructure.

> *Note: We still support multi-factor authentication methods used by earlier operating system versions and non–domain-joined devices running Windows 10.*

Measuring service health

We measure connection rates and response times to monitor the service and report on the number of unique users that connect every month, the number of daily users, and the duration of connections. By measuring connection events, we know who has connected and who has failed to connect. Our connection metrics have been trending higher because with the Always-On VPN connection profile, after employees sign on, they are always connected. The infrastructure in our worldwide VPN deployment hasn’t seen any significant spikes in connectivity or resource consumption. Use of the connection profile doesn’t increase the total number of connections that the infrastructure capacity was designed to accommodate.

Our scalability considerations include planning for bandwidth requirements and traffic patterns. In bandwidth requirements, we considered:

- How many employees will typically connect to that VPN server in any given region?
- What other bandwidth-consuming services are running on the same network segment as the VPN servers?

Where necessary, we moved the VPN servers to their separate network segment to improve bandwidth availability.

In terms of traffic patterns, we considered the location of resources employees access when they’re auto-connected to the corporate network. If most of the connections at a remote site are for resources situated at headquarters and/or central datacenters, consideration is given to bandwidth availability and connection health between that remote site and the destination. In some cases, additional network bandwidth infrastructure has been deployed as needed.

Benefits

After the deployment of Windows 10 Anniversary Update and the rollout of the Always-On VPN connection profile, we saw benefits when our employees started using the new connection profile to connect to remote access. Specific benefits include:

- **Auto-connection improves the user experience.** The VPN connection profile we enabled through System Center Configuration Manager and through Microsoft Intune has replaced the VPN with client connection manager solution for most of our employees that have remote access. The profiles are automatically configured for connection and authentication types and have improved mobile productivity. They also improve the user experience by providing employees the option to stay connected to VPN without additional interaction after they sign in.
- **Minimize user touch points.** For employees running Windows 10 Anniversary Update with the VPN connection profile, connections are seamless. Employees who are still using client connection manager with Window Hello for Business can enter their PIN to gain a secure connection, with a consistent and simple connection experience.

- **Making IT future ready.** Our corporate polices require that devices must be compliant and enrolled in a device management service. With Windows 10, we can enforce ongoing compliance without additional scripts to connect remotely.

For more information

Microsoft IT Showcase

microsoft.com/itshowcase

Windows 10 VPN technical guide

VPN profile options

How to Create VPN Profiles in Configuration Manager

How to Deploy VPN Profiles in Configuration Manager

VPN and Conditional Access

Conditional access in Azure Active Directory