Enhancing VPN performance at Microsoft

Modern workers are increasingly mobile and require the flexibility to get work done outside of the office. Every weekday, an average of 45,000 to 55,000 Microsoft employees use a virtual private network (VPN) connection to remotely connect to the corporate network. On weekends and during non-peak hours, that number only dips slightly to 25,000 to 35,000. Microsoft Core Services Engineering and Operations (CSEO), as part of our overall Zero Trust Strategy, has redesigned the VPN infrastructure at Microsoft—simplifying the design and consolidating access points. We have increased capacity and reliability, while also reducing reliance on VPN by moving services and applications to the cloud.

Providing a seamless remote access experience

Remote access at Microsoft is reliant on the VPN client, our VPN infrastructure, and public cloud services. We have had several iterative designs of the VPN service inside Microsoft. Regional weather events in the past required large increases in employees working from home, heavily taxing the VPN infrastructure and requiring a completely new design. Three years ago, we built an entirely new VPN infrastructure, a hybrid design, using Microsoft Azure Active Directory (Azure AD) load balancing and identity services with gateway appliances across our global sites.

Key to our success in the remote access experience was our decision to deploy a split-tunneled configuration for the majority of employees. We have migrated nearly 100% of previously on-premises resources into Azure and Office 365. Our continued efforts in application modernization are reducing the traffic on our private corporate networks as cloud-native architectures allow direct internet connections. The shift to internet-accessible applications and a split-tunneled VPN design has dramatically reduced the load on VPN servers in most areas of the world.

Using VPN profiles to improve the user experience

We use Microsoft Endpoint Manager to manage our domain-joined and Azure AD–joined computers and mobile devices that have enrolled in the service. In our configuration, VPN profiles are replicated through Microsoft Intune and applied to enrolled devices; these include certificate issuance that we create in Configuration Manager for Windows 10 devices. We support Mac and Linux device VPN connectivity with a third-party client using SAML-based authentication.

We use certificate-based authentication (public key infrastructure, or PKI) and multi-factor authentication solutions. When employees first use the Auto-On VPN connection profile, they are prompted to authenticate strongly. Our VPN infrastructure supports Windows Hello for Business and Multi-Factor Authentication. It stores a cryptographically protected certificate upon successful authentication that allows for either persistent or automatic connection.

For more information about how we use Microsoft Intune and Endpoint Manager as part of our device management strategy, see Managing Windows 10 devices with Microsoft Intune.

Configuring and installing VPN connection profiles

We created VPN profiles that contain all the information a device requires to connect to the corporate network, including the supported authentication methods and the VPN gateways that the device should connect to. We created the connection profiles for domain-joined and Microsoft Intune–managed devices using Microsoft Endpoint Manager.

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

The Microsoft Intune custom profile for Intune-managed devices uses Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings with XML data type, as illustrated in Figure 1.
Figure 1. Creating a Profile XML and editing the OMA-URI settings to create a connection profile in System Center Configuration Manager

Installing the VPN connection profile
The VPN connection profile is installed using a script on domain-joined computers running Windows 10, through a policy in Endpoint Manager.

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

Conditional Access
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 this 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.

Certificate and device enrollment
We use an Azure AD certificate for single sign-on to the 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 Endpoint Manager. The SCEP certificate we use is for wireless and 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 Securing and Hardening Network Device Enrollment Service for Microsoft Intune and System Center Configuration Manager.
VPN client connection flow
The diagram in Figure 2 illustrates the VPN client-side connection flow.

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 gateway.

Remote access infrastructure
At Microsoft, we have designed and deployed a hybrid infrastructure to provide remote access for all the supported operating systems—using Azure for load balancing and identity services and specialized VPN appliances. We had several considerations when designing the platform:

- **Redundancy.** The service needed to be highly resilient so that it could continue to operate if a single appliance, site, or even large region failed.
- **Capacity.** As a worldwide service meant to be used by the entire company and to handle the expected growth of VPN, the solution had to be sized with enough capacity to handle 200,000 concurrent VPN sessions.
- **Homogenized site configuration.** A standard hardware and configuration stamp was a necessity both for initial deployment and operational simplicity.
- **Central management and monitoring.** We ensured end-to-end visibility through centralized data stores and reporting.
- **Azure AD–based authentication.** We moved away from on-premises Active Directory and used Azure AD to authenticate and authorize users.
- **Multi-device support.** We had to build a service that could be used by as much of the ecosystem as possible, including Windows, OSX, Linux, and appliances.
- **Automation.** Being able to programmatically administer the service was critical. It needed to work with existing automation and monitoring tools.
When we were designing the VPN topology, we considered the location of the resources that employees were accessing when they were connected to the corporate network. If most of the connections from employees at a remote site were to resources located in central datacenters, more consideration was 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. Figure 3 provides an overview of our remote access infrastructure.

![Figure 3. Microsoft remote access infrastructure](https://example.com/figure3.png)

**VPN tunnel types**

Our VPN solution provides network transport over Secure Sockets Layer (SSL). The VPN appliances force Transport Layer Security (TLS) 1.2 for SSL session initiation, and the strongest possible cipher suite negotiated is used for the VPN tunnel encryption. We use several tunnel configurations depending on the locations of users and level of security needed.

**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 or infrastructure. Our migration to Office 365 and Azure has dramatically reduced the need for connections to the corporate network. We rely on the security controls of applications hosted in Azure and services of Office 365 to help secure this traffic. For end point protection, we use Microsoft Defender Advanced Threat Protection on all clients. In our VPN connection profile, split tunneling is enabled by default and used by the majority of Microsoft employees. [Learn more about Office 365 split tunnel configuration](https://example.com/link).

**Full tunneling**

Full tunneling routes and encrypts all traffic through the VPN. There are some countries and business requirements that make full tunneling necessary. This is accomplished by running a distinct VPN configuration on the same infrastructure as the rest of the VPN service. A separate VPN profile is pushed to the clients who require it, and this profile points to the full-tunnel gateways.

**Full tunnel with high security**

Our IT employees and some developers access company infrastructure or extremely sensitive data. These users are given Privileged Access Workstations, which are secured, limited, and connect to a separate highly controlled infrastructure.
Applying and enforcing policies

In CSEO, the 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 is then published so that the enforcement of the applied policy can be managed through Microsoft Endpoint Manager. Microsoft Endpoint Manager provides policy enforcement, as well as certificate enrollment and deployment, on behalf of the client device.

For more information about policies, see VPN and Conditional Access.

Early adopters help validate new policies

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.

Measuring service health

We measure many aspects of the VPN service and report on the number of unique users that connect every month, the number of daily users, and the duration of connections. We have invested heavily in telemetry and automation throughout the Microsoft network environment. Telemetry allows for data-driven decisions in making infrastructure investments and identifying potential bandwidth issues ahead of saturation.

Using Power BI to customize operational insight dashboards

Our service health reporting is centralized using Power BI dashboards to display consolidated data views of VPN performance. Data is aggregated into an SQL Azure data warehouse from VPN appliance logging, network device telemetry, and anonymized device performance data. These dashboards, shown in Figures 4 and 5, are tailored for the teams using them.
Figure 4, global VPN status dashboard. Figure 5. Power BI reporting dashboards

Benefits

With our optimizations in VPN connection profiles and improvements in the infrastructure, we have seen significant benefits:

- **Reduced VPN requirements.** By moving to cloud-based services and applications and implementing split tunneling configurations, we have dramatically reduced our reliance on VPN connections for many users at Microsoft.
- **Auto-connection for improved user experience.** The VPN connection profile automatically configured for connection and authentication types have improved mobile productivity. They also improve the user experience by providing employees the option to stay connected to VPN—without additional interaction after signing in.
- **Increased capacity and reliability.** Reducing the quantity of VPN sites and investing in dedicated VPN hardware has increased our capacity and reliability, now supporting over 500,000 simultaneous connections.
- **Service health visibility.** By aggregating data sources and building a single pane of glass in Power BI, we have visibility into every aspect of the VPN experience.

For more information

Microsoft IT Showcase
microsoft.com/itshowcase

Running on VPN: How Microsoft is keeping its remote workforce connected

For more information on these and other Azure and Office network optimizing practices, please see:

- Office 365 Network Connectivity Principles
- Prepare your network for upgrading to Teams
- What is VPN Gateway?
- About Azure Point-to-Site VPN
- VPN Network Virtual Appliances in the Azure Marketplace
- Working remotely using Azure networking services