# Table of Contents

**Deploying F5 Access for Windows 10** .................................................................5
- Windows 10 auto-trigger VPN options..............................................................5
- Configuring Azure active directory..................................................................5
- About configuring VPN profile in Azure Intune...............................................5
  - Creating device configuration profile...............................................................5
  - Configuring base VPN profile for F5 Access................................................6
  - Configuring app trigger for F5 Access............................................................6
  - Configuring Name-based trigger for F5 Access..............................................8
  - Configuring Always On for F5 Access............................................................8
  - Configuring trusted network detection for F5 Access....................................8
  - Assigning a device profile to group.................................................................9

**Setting up client side directory** .......................................................................11
- Connecting Windows 10 to Azure active directory..........................................11
- Accessing F5 Access logs..................................................................................11
- Viewing configuration for F5 Access.................................................................11

**Configuring Azure Conditional Access** ..........................................................13
- Configuring BIG-IP client certificate inspection.............................................13
- Configuring Azure AD conditional access policy..............................................15
- Marking the device as compliant in Azure AD...............................................16
- Adding conditional access to VPN profile.......................................................17
- Configuring custom XML in profile using Intune............................................17
- Accessing certificates.......................................................................................18
Deploying F5 Access for Windows 10

Windows 10 auto-trigger VPN options

You can configure F5 Access for Windows 10 using Intune. In Windows 10, a number of features were added to auto-trigger VPN so you won’t have to manually connect when VPN is needed to access necessary resources. There are four different types of auto-trigger rules:

- App trigger
- Name-based trigger
- Always On
- Trusted network detection

Refer to [VPN auto-triggered profile options](#) for more information.

**Note:** In this release, the Name-based trigger and the Trusted network detection features do not work for F5 Access VPN.

Configuring Azure active directory

**Add/Delete a user**

Refer to [How to: Add or delete users using Azure Active Directory](#) for information on adding new users or deleting existing users from the Azure active directory.

**Create a new group**

Refer to [How to: Create a basic group and add members using Azure Active Directory](#) for information on creating a basic group using the Azure active directory portal.

About configuring VPN profile in Azure Intune

Virtual private networks (VPNs) give users secure remote access to the company network. Devices use a VPN connection profile to initiate a connection with the VPN server.

Creating device configuration profile

Refer to [Create a device profile in Microsoft Intune](#) for information on creating device profile in Microsoft Intune.
Configuring base VPN profile for F5 Access

To create a base VPN profile:

1. Sign in to the Azure portal.
2. Select All services, filter on Intune, and select Microsoft Intune.
3. Click Device configuration > Profiles > Create profile.
4. Type the Name and Description for the VPN profile.
5. From the Platform list, select Windows 10 and later.
6. From the Profile type list, select VPN.
7. Depending on the platform you chose, the settings you can configure are different. Open configured settings.
8. Click Base VPN to open the Base VPN settings.
9. Enter the name for this connection. End users see this name when they browse their device for the list of available VPN connections.
10. Add/Import one or more VPN servers that devices connect to. When you add a server, you enter the following information:
   - Description: Enter a descriptive name for the server, such as F5 VPN server.
   - IP address or FQDN: Enter the IP address or fully qualified domain name of the VPN server that devices connect to.
   - Default server: Enables this server as the default server that devices use to establish the connection.
     Set only one server as the default.
11. From the Connection type list, select F5 Access.
12. From the Authentication method list, select how you want the users to authenticate to the VPN server. Using certificates provides enhanced capabilities, such as zero-touch experience, on-demand VPN, and per-app VPN.
13. Select Remember credentials at each logon to cache the authentication credentials.
14. Enter Custom XML commands that configure the VPN connection.
15. Click OK.
   The profile is created and appears on the profiles list.

Configuring app trigger for F5 Access

VPN profiles in Windows 10 can be configured to connect automatically on the launch of F5 Access. To configure App trigger:

1. Sign in to the Azure portal.
2. Select All services, filter on Intune, and select Microsoft Intune.
3. Click Device configuration > Profiles > Apps and Traffic Rules.
4. From the Associate WIP or apps with this VPN list, select Associated apps with this connection.
5. The Restrict VPN connection to these apps option lets you to restrict VPN connection to apps you enter in Associated Apps table. The apps you enter automatically use the VPN connection. The type of app determines the app identifier. For a universal app, enter the package family name. To get the package family name of an app, use the Get-AppxPackage package_name powershell command on the client machine. For a desktop app, enter the file path of the app. For example, to start the VPN every time
Microsoft Remote Desktop app is launched, use **App identifier** as `C:\Program Files\WindowsApps\Microsoft.RemoteDesktop.exe`

**Note:** Add associated apps in before enabling **Restrict VPN connection to these apps**, as the list will become read-only after enabling. Traffic rules for apps will automatically be added to the network traffic rules when you click **Enable**.

![Figure 1: Example of a PowerShell command to get package family name](image)

6. The **Network traffic rules for this VPN connection** option is not required to be setup for F5 Access.

![Figure 2: Apps and Traffic Rules Screen](image)
**Configuring Name-based trigger for F5 Access**

You can configure a domain name-based rule so that a specific domain name triggers the VPN connection. Refer to *Name-based trigger* for information on configuring name-based trigger rule.

*Note: Always specify the DnsIPAddress parameter with an actual DNS Server IP address. This parameter cannot be overwritten by APM server configuration.*

**Configuring Always On for F5 Access**

The Always On feature in Windows 10 enables the active VPN profile to connect automatically on the following triggers:

- User sign-in
- Network change
- Device screen on

Refer to *Name-based trigger* for information on configuring Always On trigger rule.

**Configuring trusted network detection for F5 Access**

The Trusted Network Detection feature checks the DNS suffix on the physical interface to decide if a user is on a trusted corporate network. If the user is not on a trusted corporate network, the VPN gets triggered. Trusted network detection can be configured using the `VPNv2/ProfileName/TrustedNetworkDetection` setting in the *VPNv2 CSP*. This rule should be applied to an existing F5 Access connection.

To configure Trusted network detection:

1. Sign in to the Azure portal.
2. Select All services, filter on Intune, and select Microsoft Intune.
3. Open an existing device configuration profile.
4. From the Platform list, select Windows 10 and later.
5. From the Profile type list, select Custom.
6. Depending on the platform you chose, the settings you can configure are different. Open configured settings.
7. In Custom OMA-URI Settings, select Add to create a new setting with the following information:
   - **Name**: Enter the same name as configured for the Base VPN profile for F5 Access. Let us assume that in our example the name configured is *vpnt1*.
   - **Description**: Optionally, enter a description for the setting.
   - **OMA-URI (case sensitive)**: Enter OMA-URI with the profile name as `./user/Vendor/MSFT/VPNv2/vpnt1/TrustedNetworkDetection`.
   - **Data type**: From the list, select String.
   - **Value**: Enter the value or file to associate with the OMA-URI. For example *f5net.com*. 

---

**Deploying F5 Access for Windows 10**

---
8. Click OK.

Assigning a device profile to group

After you create a profile, you can assign the profile to Azure active directory groups.

Refer to *Assign user and device profiles* for information on assigning a device profile in Microsoft Intune.
Connecting Windows 10 to Azure active directory

In Windows 10, an Azure AD user account is called a **Work or school account**. To join to or register on Azure AD requires Windows 10 PRO, Education or Enterprise edition. To connect to Azure active directory:

1. Open Windows Settings, click **Accounts > Access work or school**.
   a) For applied Condition Access settings, click **Connect to Azure Active Directory**. Enter the email address and password of Azure AD account.
   b) For connect to MDM Intune, click **Connect**. Enter the email address and password of Azure AD account.

2. Login to the Azure Active Directory account on the client machine.
3. Install F5 Access from the Microsoft store. Ensure that the F5 VPN server address is trusted for the client.

Accessing F5 Access logs

To view the admin log:

1. Open Event Viewer.
2. Expand **Applications and Services Log**.
3. Click **Microsoft > Windows > Vpn Plugin Platform > OperationalVerbose**.

Viewing configuration for F5 Access

To verify existing configuration applied to F5 Access, run the following command in PowerShell:

```
Get-WmiObject -Namespace root\cimv2\mdm\dmmmap -Class MDM_VPNv2_01
```
Figure 4: Get-WmiObject command
Configuring Azure Conditional Access

Configuring BIG-IP client certificate inspection

To configure BIG-IP client certificate inspection:

1. Sign in to the Azure portal.
2. In Azure active directory, click **Conditional access > VPN connectivity**.
3. Create a new certificate with:
   - **Validity**: One year
   - **Primary**: Yes
4. Import the certificate onto the BIG-IP system.
5. Navigate to **System > Certificate Management > Traffic Certificate Management > SSL Certificate List**. Click **Import** to import certificate.
6. Navigate to **BIG-IP System manager > Local traffic > Profiles > SSL > Client**.
7. Choose the certificate for **Trusted Certificate Authorities**, and enable **request** for **Client Certificate**.
8. Add Client Certificate Inspection to your current VPN APM Access Policy.
Configuring Azure AD conditional access policy

To configure your conditional access policy:

1. Sign in to the Azure portal.
2. In Azure active directory, in the Manage section, click Conditional access > Add.
3. In the example here, we want make sure that all VPN connections from "VPN Users" group are controlled. Create a new policy with the following selections:
   - **Name:** Type VPN CA Policy
   - **Users and Groups:** VPN Users
   - **Cloud Apps:** VPN Server
   - **Conditions:** No conditions
   - **Grant:** Select Grant access and then select Require device to be marked as compliant. You can also use Require multi-factor authentication or Require domain joined (Hybrid Azure AD) options.
   - **Session:** No session
Figure 7: Conditional access policy settings

4. Enable the new policy in Azure active directory > Conditional access.

Figure 8: Policy enabled in conditional access

Marking the device as compliant in Azure AD

You can deploy compliance policy to users in user groups or devices in device groups. When a compliance policy is deployed to a user, all of the user's devices are checked for compliance. If a device doesn't have a compliance policy assigned, then this device is considered not compliant. To become a managed device, a device must be a device that has been marked as compliant. To mark the device as compliant in Azure AD:

1. Sign in to the Azure portal.
2. Click **Device compliance > Policies > Create Policy**.
3. Create a new compliance policy without configuring any settings.
4. Assign this policy to VPN users group.

![Image of device compliance policy]

**Figure 9: Example of a device compliance policy**

### Adding conditional access to VPN profile

To add a conditional access to VPN profile using Intune:

1. Sign in to the Azure portal.
2. Create a new VPN profile for Windows 10. Follow the steps similar to creating a base VPN profile. Enable the **Enable conditional access for this VPN connection** to ensure that devices that connect to the VPN are tested for conditional access compliance before connecting.

![Image of conditional access settings]

**Figure 10: Conditional access enabled for VPN connection**

### Configuring custom XML in profile using Intune

F5 Access for Windows Desktop supports the following three authentication flows:
- Username
- Certificate only (no prompt for credentials)
- Username & certificate

These authentication flows can be configured through custom XML commands. You can enter Custom XML commands that configure the VPN connection in F5 Access profile using Intune.
The following example shows how a certificate is configured using custom XML.

```
<f5-vpn-conf>
<prompt-for-credentials>false</prompt-for-credentials>
<client-certificate>
<issuer>Microsoft VPN root CA gen 1</issuer>
</client-certificate>
</f5-vpn-conf>
```

Figure 11: Example of a custom XML command

Refer to *Configuration Notes: F5 Access for Microsoft Windows 10 and Windows 10 Mobile* for more information.

**Accessing certificates**

To access pre-defined certificates:

1. Follow the below steps to connect to VPN:
a) On the Windows 10 device, navigate to **Settings > Sync**.
b) Wait for the new VPN to be installed. Connect to VPN.

![VPN connected screen](image1.png)

**Figure 12: VPN connected screen**

2. On successful VPN connection, run the **Certmgr.msc** command in cmd prompt or PowerShell window. This will launch the Current User certificate MSC.

3. Navigate to **Certificates - Current User > Personal > Certificates**. You should see a newly provisioned certificate issued by "Microsoft VPN root CA gen 1".

![Current User certificate MSC](image2.png)

**Figure 13: Current User certificate MSC**

Certificate's expiry date will be 60 minutes from when it was last requested.
Figure 14: Certificate’s expiry date
Index

A
always on 8
app trigger 6
assign device profile 9
authentication flows
certificate 17
username 17
username & certificate 17
auto-trigger rules 5
Azure AD 11

B
base VPN 6

C
client certificate inspection 13, 18
conditional access policy 15–17
create device configuration 5

D
deployment 5

F
F5 Access Logs 11
F5 Access Windows
  Adding cloud-based users 5
  Create new group 5

G
Get-WmiObject 11

N
name-based trigger 8

T
trusted network detection 8