Managing Modern Desktops

SECOND EDITION

Exam Ref MD-101

Andrew Bettany
Andrew Warren

Microsoft

Exam Ref MD-101 Managing Modern Desktops

Second Edition

Andrew Bettany
Andrew Warren

Authenticating remote users

Windows users authenticate using Kerberos when accessing the local network, but for remote authentication, this is not suitable; a separate protocol, which protects against network intrusion, must be used. During the initial negotiation sequence (using PPP), when a client connects to the remote computer, each party must agree on a shared authentication protocol to use. By default, Windows 10 will use the strongest protocol that both parties have in common.

In the Add A VPN Connection Wizard, Windows 10 offers three sign-in options when configuring a VPN, such as:

- Username and password
- Smart card
- One-time password

In addition to these options, you can also configure Windows 10 to use the common authentication protocols:

- **EAP-MS-CHAPv2** This is a protocol that uses Extensible Authentication Protocol (EAP), which offers the default and most flexible authentication option for Windows 10 clients. It offers the strongest password-based mechanism for the client side, with certificates being used on the server side. Authentication can be negotiated based on certificates or smart cards, and EAP-MS-CHAPv2 is likely to be further extended and developed as technology advances. Windows 10 aims to use this method for authentication connections where possible. IKEv2 connections must use EAP-MS-CHAPv2 or a certificate.
- **MS-CHAP v2** Stronger than the CHAP protocol, with significantly improved security when partnered with EAP to enable encryption of the password.
- **CHAP** Used for down-level client compatibility and has been surpassed by MS-CHAP v2. This protocol uses a pre-shared key between the client and server to enable encryption to take place.
- **PAP** This is the least secure protocol as it uses plaintext passwords. It is not considered secure and should only be used whenever other authentication methods cannot be negotiated.

Creating a VPN connection in Network and Sharing Center

To create a VPN in Windows 10, from the **Network and Sharing Center**, under **Change your network settings**, select **Set up a new connection or network** and then select **Connect to a workplace**.

To configure your VPN connection, in the **Connect to a Workplace** wizard, provide the following information:

- **How do you want to connect?** You can connect by using an existing internet connection or by dialing directly to your workplace.
- **Internet address** This is the name or IP address of the computer that you connect to at your workplace, as shown in Figure 1-22. Typically, this is an FQDN, such as remote.adatum.com.

- **Destination name** This is the name of this VPN connection.

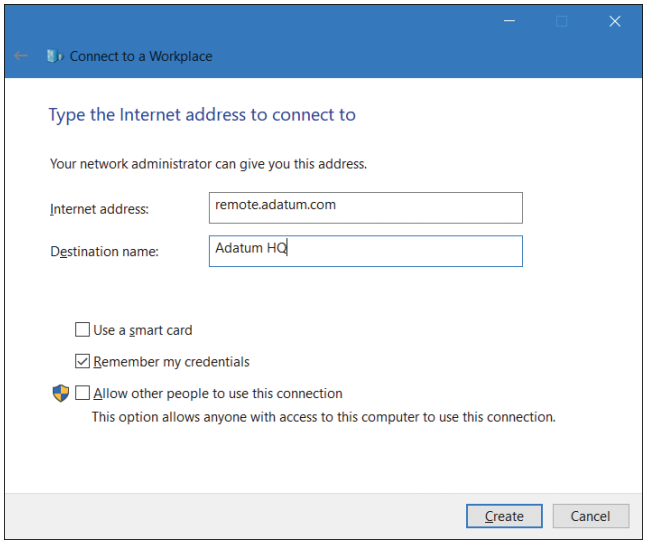

FIGURE 1-22 The Connect to a Workplace wizard

After you have created the VPN connection, from the Network And Sharing Center, select **Change adapter settings**, right-click your VPN connection, and select **Properties**. As shown in Figure 1-23, you can then configure additional options as required by your organization's network infrastructure.

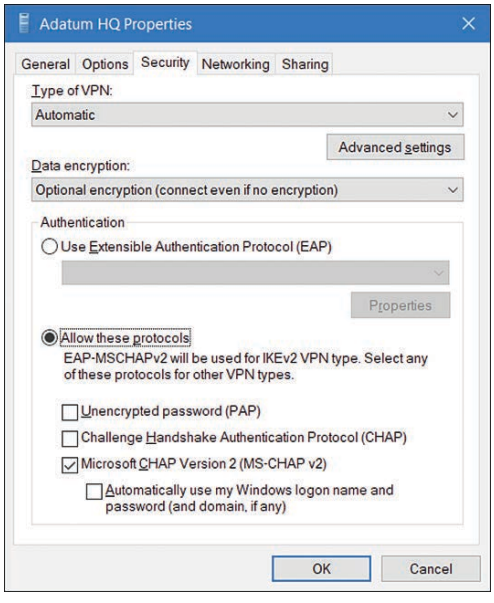

FIGURE 1-23 The Security tab of a VPN connection

These settings must match the remote access device that your device connects to, and includes the following options:

- **Type of VPN** Point-to-Point Tunneling Protocol (PPTP), Layer Two Tunneling Protocol with IPsec (L2TP/IPsec), Secure Socket Tunneling Protocol (SSTP), or Internet Key Exchange version 2 (IKEv2).
- **Data encryption** None, Optional, Required, or Maximum Strength.

In the Authentication section, you choose either Use Extensible Authentication Protocol (EAP) or Allow These Protocols. If you choose to use EAP, you then configure one of the following:

- Microsoft: EAP-AKA (Encryption Enabled)
- Microsoft: EAP-SIM (Encryption Enabled)
- Microsoft: EAP-TTLS (Encryption Enabled)
- Microsoft: Protected EAP (PEAP) (Encryption Enabled)
- Microsoft: Secured Password (EAP-MSCHAP v2) (Encryption Enabled)
- Microsoft: Smart Card Or Other Certificate (Encryption Enabled)

If you choose Allow These Protocols, you then configure the following options:

- Unencrypted Password (PAP)
- Challenge Handshake Authentication Protocol (CHAP)
- Microsoft CHAP Version 2 (MS-CHAP v2)
- Automatically Use My Windows Log-on Name And Password (And Domain, If Any)

Using the Settings app to create and configure a VPN

You can also use the Settings app to create and configure VPN connections. Use the following procedure:

1. Select **Start** and then select **Settings**.
2. In Settings, select **Network & Internet**.
3. Select the **VPN** tab, and then, in the details pane, select **Add a VPN connection**.
4. On the **Add a VPN connection** page, enter the following information:
   - **VPN provider:** Windows (Built-In).
   - **Connection name**
   - **Server name or address**
   - **VPN type:** Automatic (Default). You can also choose PPTP, L2TP/IPsec With Certificate, L2TP/IPsec With Pre-Shared Key, SSTP, or IKEv2.
   - **Type of sign-in info:** Username and password, Smart card, One-off password, or Certificate.

- **Username** and **Password**, although these options are only configurable if you selected Username And Password as the Type of sign-in info.

5. Select **Save**.

After you have created the VPN, you can manage it from Network Connections in Control Panel. Alternatively, on the VPN page in the Network & Internet node in Settings, you can select the VPN and then choose Advanced Options. From there, you can reconfigure the VPN's settings.

VPN profiles

Although manually configuring VPN connections is relatively simple, completing the process on many computers, with the same or similar settings, is very time-consuming. In these circumstances, it makes sense to create a VPN profile and then distribute the profile to your users' computers.

When you use VPN profiles in Windows 10, you can take advantage of a number of advanced features. These are:

- **Always On** This feature enables Windows to automatically connect to a VPN. The Always On feature can be triggered by sign-in when the desktop is unlocked, and on network changes. When the Always On profile is configured, VPN remains always connected unless the user disconnects manually or logs off the device. The profile is optimized for power and performance, and the profiles can be pushed and managed on devices using MDM tools.
- **App-Triggered VPN** You can configure the VPN profile to respond to a specific set of apps; if a defined app loads, then the VPN initiates.
- **Traffic Filters** To protect the server from a remote attack, an administrator can configure policies on a Windows 10 device to inspect and, if necessary, filter VPN traffic before it is enabled to travel over the VPN. There are two types of Traffic Filter rules available:
  - **App-based rules** An app-based rule will only enable VPN traffic originating from applications that have been marked as being allowed to traverse the VPN interface.
  - **Traffic-based rules** Enterprise-level traffic-based rules enable fine-tuning of what type of traffic is allowed. By using the industry-standard rules covered by five tuple policies (protocol, source/destination IP address, source/destination port), administrators can be very specific on the type of network traffic that is allowed to travel over the VPN interface.

  An administrator can combine both app-based rules and traffic-based rules.
- **LockDown VPN** The LockDown VPN profile is used to enforce the use of the VPN interface. In this scenario, the device is secured to only allow network traffic over the VPN, which is automatically always on and can never be disconnected. If the VPN is unable to connect, then there will be no network traffic allowed. The LockDown profile

overrides all other VPN profiles and must be deleted before other profiles can be added, removed, or connected.

You can create and distribute Windows 10 VPN profiles with these advanced settings by using Microsoft Intune and/or Endpoint Configuration Manager.

> ***NEED MORE REVIEW?*** **VPN CONNECTIONS IN MICROSOFT INTUNE**
>
> **To review further details about VPN connections in Microsoft Intune, refer to the Microsoft website at *https://docs.microsoft.com/intune/vpn-settings-configure*.**

> ***NEED MORE REVIEW?*** **HOW TO CREATE VPN PROFILES IN CONFIGURATION MANAGER**
>
> **To review further details about creating VPN profiles in Configuration Manager, refer to the Microsoft website at *https://docs.microsoft.com/en-us/sccm/mdm/deploy-use/create-vpn-profiles*.**

Enable VPN Reconnect

VPN Reconnect uses the IKEv2 protocol with the MOBIKE extension to automatically re-establish a lost VPN connection without user intervention. For mobile users, the prevalence of dropped WiFi or LTE connections can be frequent because of volatile signal strength. It is best to use and configure VPN Reconnect for your mobile users because this will reduce the frustration of having to reconnect manually, and it will also increase productivity.

The network outage time can be configured from five minutes up to an interruption of eight hours. To enable VPN Reconnect, follow these steps:

1. On the taskbar, in the search box, enter **VPN**.
2. Select **VPN settings** from the returned list.
3. In the **Settings** app, select **Change adapter options**.
4. Select the appropriate VPN adapter, and then select **Change settings of this connection**, as shown in Figure 1-24.
5. Select the **Security** tab in the **VPN Properties** dialog box, and select **Advanced Settings**.
6. In the **Advanced Properties** dialog box, check the **Mobility** option on the **IKEv2** tab.
7. Modify the **Network outage time** as necessary.
8. Select **OK** twice.

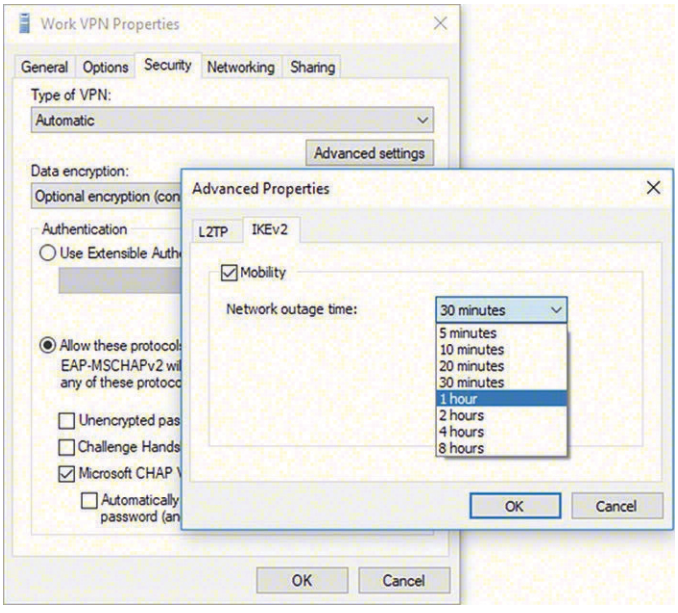

FIGURE 1-24 Configuring the Network Outage Time for VPN Reconnect

Configure and manage certificates on client devices

Certificates are commonly used to provide for device authentication. It's important that you know how to configure and manage certificates on your client devices.

Typically, in an on-premises environment, your organization will deploy the Active Directory Certificate Services (AD CS) role. This role provides the ability to deploy, manage, and provide revocation for digital certificates in your organization. You can also use Group Policy Objects (GPOs) to configure auto-enrollment of appropriate certificates to your users and their devices.

However, in a cloud-based scenario, your users won't automatically trust certificates issued by your internal certification authority (CA). In addition, because the users' devices are not AD DS domain-joined, you can't use GPOs to enable auto-enrollment.

Using Windows Configuration Designer to deploy certificates

Windows Configuration Designer is part of Windows ADK. To use Windows Configuration Designer to deploy certificates, use the following procedure:

1. Open **Windows Configuration Designer** and select the **Advanced provisioning** tile.
2. In the **New project** wizard, on the **Enter project details** page, enter a **Name** and **Description**, and then select **Next**.
3. On the **Choose which settings to view and configure** page, select **All Windows desktop editions**, and then select **Next**.