

## Practical No – 06 IP Security (IPsec) Configuration:

**Aim :** To Configure IPsec on network devices to provide secure communication and protect against unauthorized access and attacks.

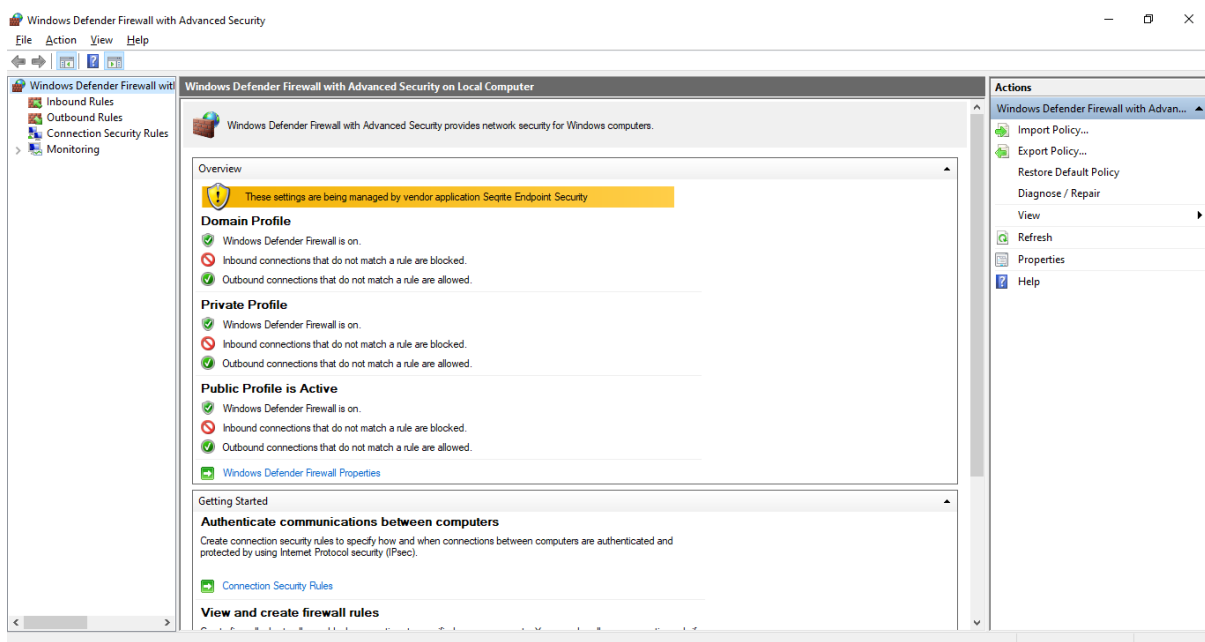
### About this task

Historian supports encryption based on Internet Protocol Security to secure traffic between various Historian components and collectors without the need to use VPN or other security protocols.

### Procedure

1. Run `wf.msc`.

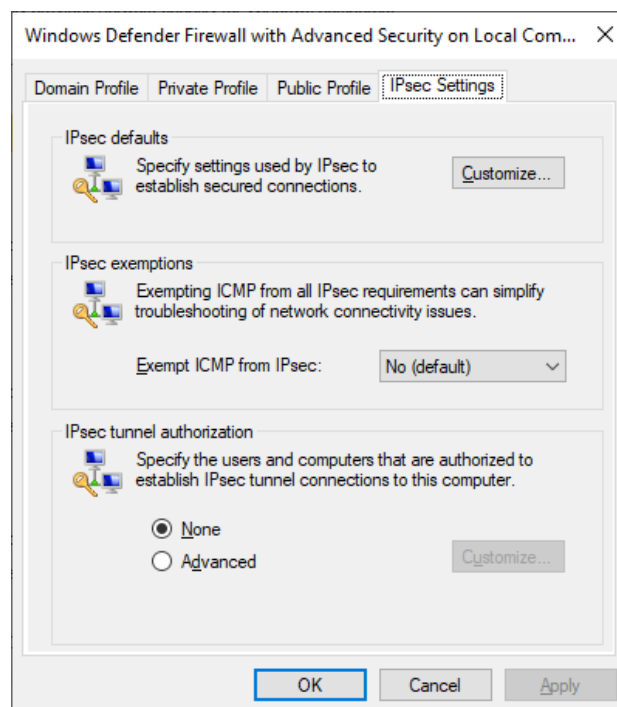
The **Windows Defender Firewall with Advanced Security** window appears.



2. Create a security method:
  - a. Select **Actions > Properties**.

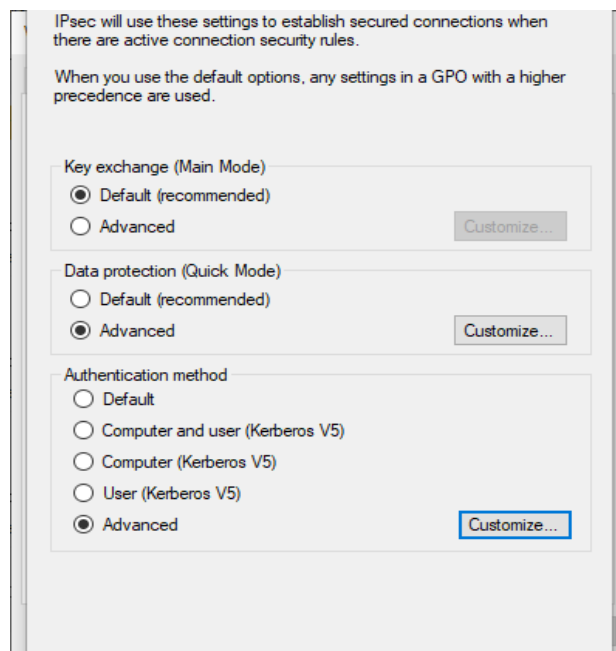
The **Windows Defender Firewall with Advanced Security on Local Computer** window appears

## Information and Network Security



- b. Select **IPsec Settings > Customize**.

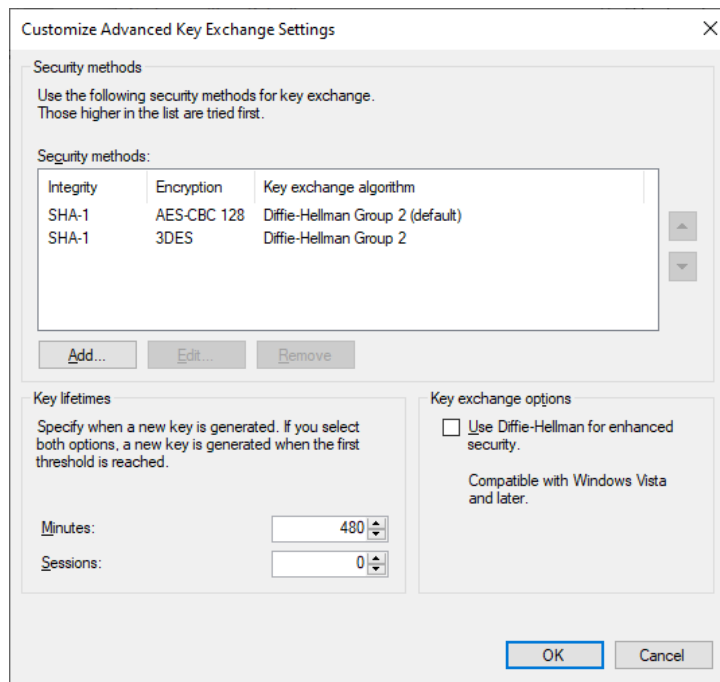
The **IPsec Defaults** window appears.



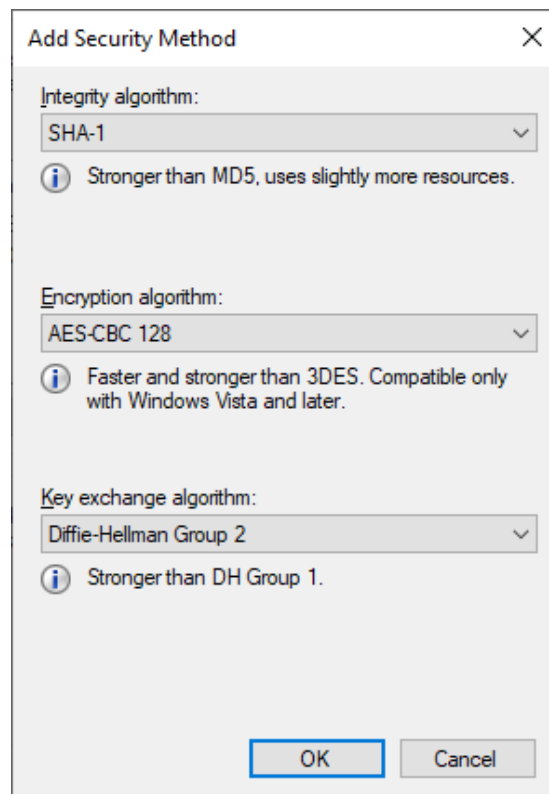
- c. Under **Key exchange (Main Mode)**, select **Advanced > Customize**.

The **Customize Advanced Key Exchange Settings** window appears.

## Information and Network Security



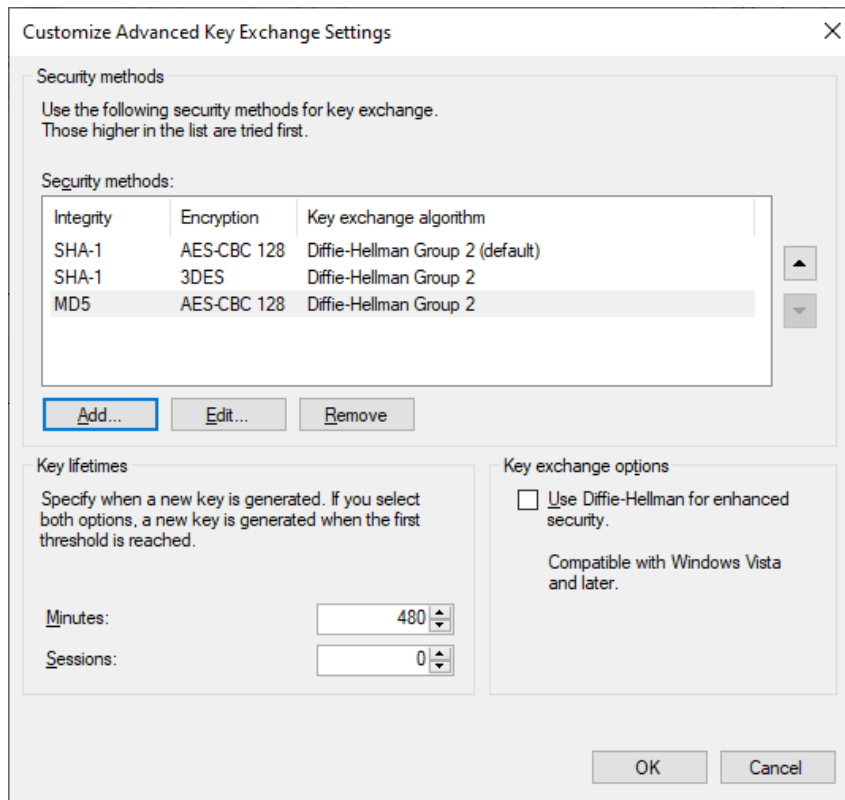
- d. Select **Add**. The **Add Security Method** window appears.



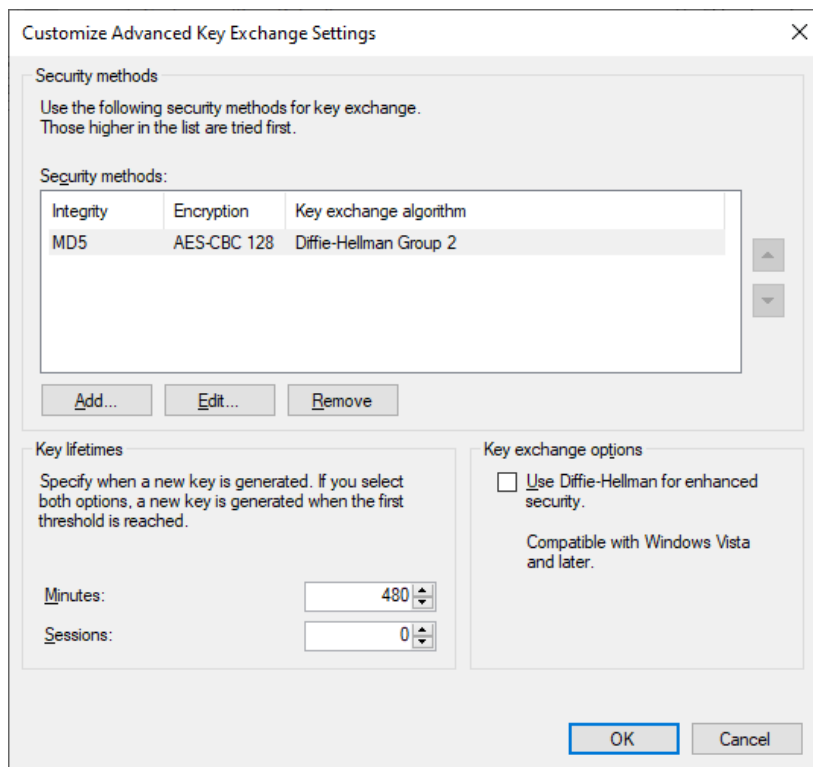
- e. Select the algorithms that you want to use for each purpose.

## Information and Network Security

The security method that you have added appears in the list



- f. Move the security method that you have added to the top of the list. We recommend that you remove the other methods.



- g. Select **OK**.

### 3. Add integrity and encryption algorithms:

- a. In the **Customize IPsec Defaults** window, under **Data protection (Quick Mode)**, select **Advanced > Customize**.

The **Customize Data Protection Settings** window appears.

Customize Data Protection Settings

Data protection settings are used by connection security rules to protect network traffic.

☐ Require encryption for all connection security rules that use these settings

**Data integrity**  
Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first.

Data integrity algorithms:

Protocol	Integrity	Key Lifetime (minutes/KB)
ESP	SHA-1	60/100,000
AH	SHA-1	60/100,000

**Data integrity and encryption**  
Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first.

Data integrity and encryption algorithms:

Protocol	Integrity	Encryption	Key Lifetime (min...)
ESP	SHA-1	AES-CBC ...	60/100,000
ESP	SHA-1	3DES	60/100,000

OK Cancel

- b. Select the **Require encryption for all connection and security rules that use these settings** check box.

Customize Data Protection Settings

Data protection settings are used by connection security rules to protect network traffic.

☒ Require encryption for all connection security rules that use these settings

**Data integrity**  
Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first.

Data integrity algorithms:

Protocol	Integrity	Key Lifetime (minutes/KB)
ESP	SHA-1	60/100,000
AH	SHA-1	60/100,000

**Data integrity and encryption**  
Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first.

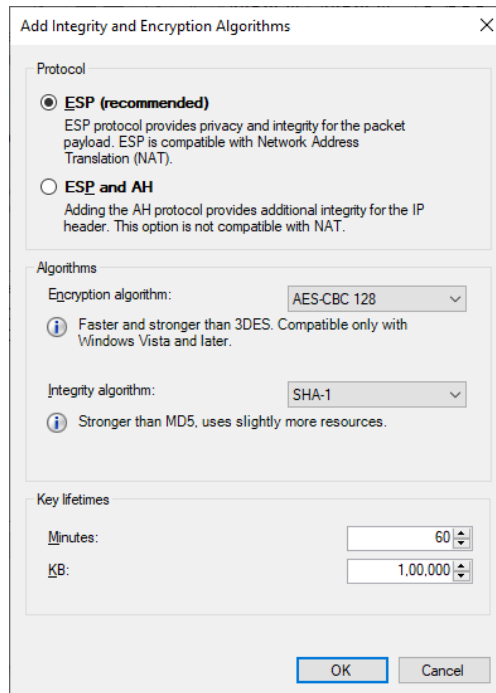
Data integrity and encryption algorithms:

Protocol	Integrity	Encryption	Key Lifetime (min...)
ESP	SHA-1	AES-CBC ...	60/100,000
ESP	SHA-1	3DES	60/100,000

OK Cancel

- c. Under **Data integrity and encryption**, select **Add**.

The **Add Integrity and Encryption Algorithms** window appears.



The dialog box titled "Add Integrity and Encryption Algorithms" contains three sections: "Protocol", "Algorithms", and "Key lifetimes".

**Protocol:** Two radio buttons are present. The first is "ESP (recommended)" with a description: "ESP protocol provides privacy and integrity for the packet payload. ESP is compatible with Network Address Translation (NAT)." The second is "ESP and AH" with a description: "Adding the AH protocol provides additional integrity for the IP header. This option is not compatible with NAT."

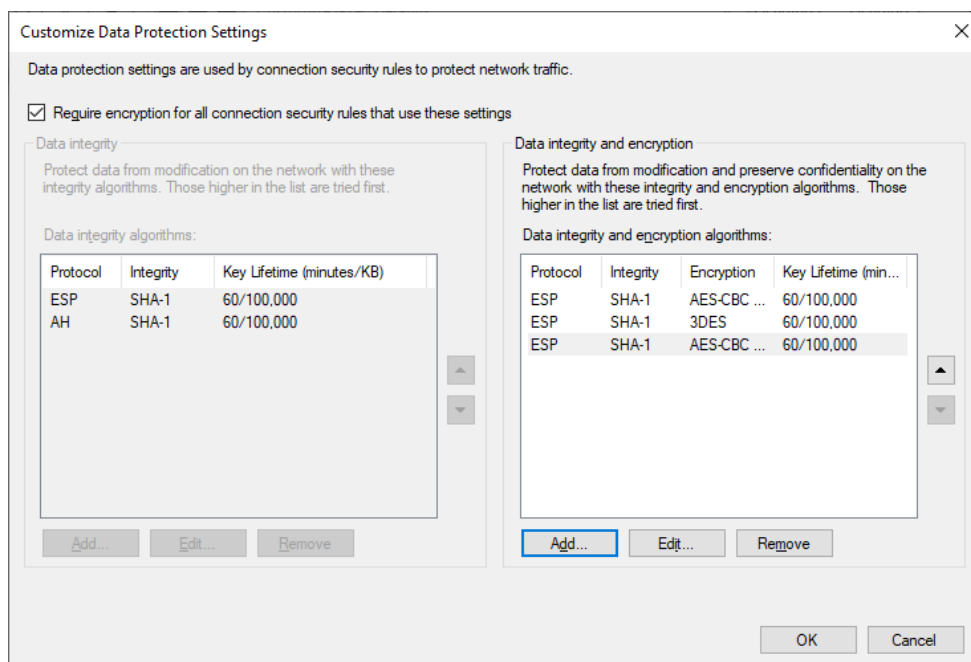
**Algorithms:** Two dropdown menus are shown. The "Encryption algorithm:" dropdown is set to "AES-CBC 128" with a note: "Faster and stronger than 3DES. Compatible only with Windows Vista and later." The "Integrity algorithm:" dropdown is set to "SHA-1" with a note: "Stronger than MD5, uses slightly more resources."

**Key lifetimes:** Two spinners are shown. "Minutes:" is set to 60 and "KB:" is set to 1,00,000.

Buttons at the bottom: "OK" and "Cancel".

- d. Under **Protocol**, ensure that **ESP** is selected.
- e. Select the algorithms that you want to use for each purpose, and then select **OK**.

The algorithms that you have selected appear in the list.



The dialog box titled "Customize Data Protection Settings" has a checkbox "Require encryption for all connection security rules that use these settings" which is checked.

**Data integrity:** A section with a description: "Protect data from modification on the network with these integrity algorithms. Those higher in the list are tried first." It contains a table of "Data integrity algorithms:".

Protocol	Integrity	Key Lifetime (minutes/KB)
ESP	SHA-1	60/100,000
AH	SHA-1	60/100,000

Buttons: "Add...", "Edit...", "Remove".

**Data integrity and encryption:** A section with a description: "Protect data from modification and preserve confidentiality on the network with these integrity and encryption algorithms. Those higher in the list are tried first." It contains a table of "Data integrity and encryption algorithms:".

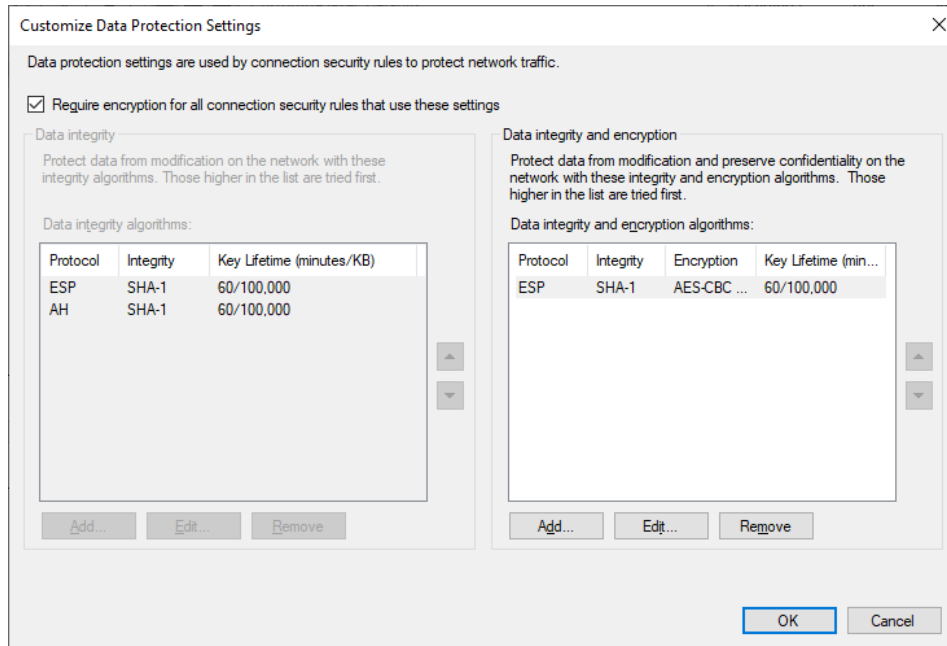
Protocol	Integrity	Encryption	Key Lifetime (min...)
ESP	SHA-1	AES-CBC ...	60/100,000
ESP	SHA-1	3DES	60/100,000
ESP	SHA-1	AES-CBC ...	60/100,000

Buttons: "Add..." (highlighted), "Edit...", "Remove".

Buttons at the bottom: "OK" and "Cancel".

## Information and Network Security

- f. Move the algorithms to the top of the list. We recommend that you remove the remaining items in the list.



- g. Select **OK**.