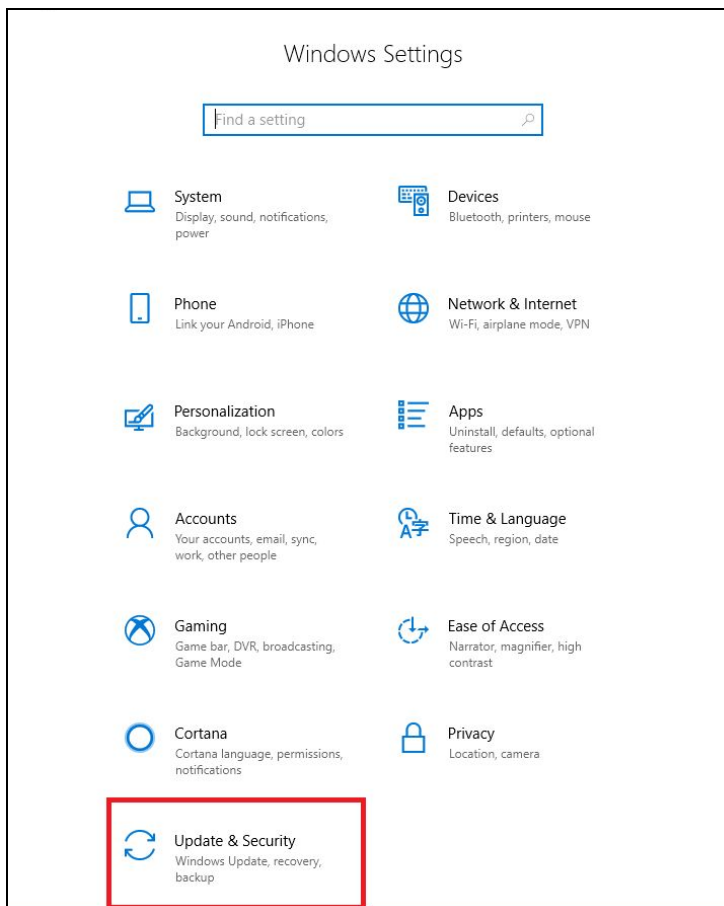


MSSND #3: Host-based Firewall Software

Log Firewall Activity

Windows

1. Settings > Update and Security



2. Windows Security > Firewall and Network Protection

The image shows a screenshot of the Windows Settings application. On the left is a navigation pane with a search bar and a list of categories. The 'Update & Security' category is expanded, and 'Windows Security' is highlighted with a red box. On the right, the 'Windows Security' page is displayed. It features a title, a brief description, and a button to 'Open Windows Security'. Below this is a section titled 'Protection areas' which lists several security features. 'Firewall & network protection' is highlighted with a red box. Each feature includes a status icon (a shield with a checkmark) and the text 'No actions needed.'

Home

Find a setting

Update & Security

- Windows Update
- Delivery Optimization
- Windows Security**
- Backup
- Troubleshoot
- Recovery
- Activation
- Find my device
- For developers
- Windows Insider Program

Windows Security

Windows Security is your home to view and manage the security and health of your device.

Open Windows Security

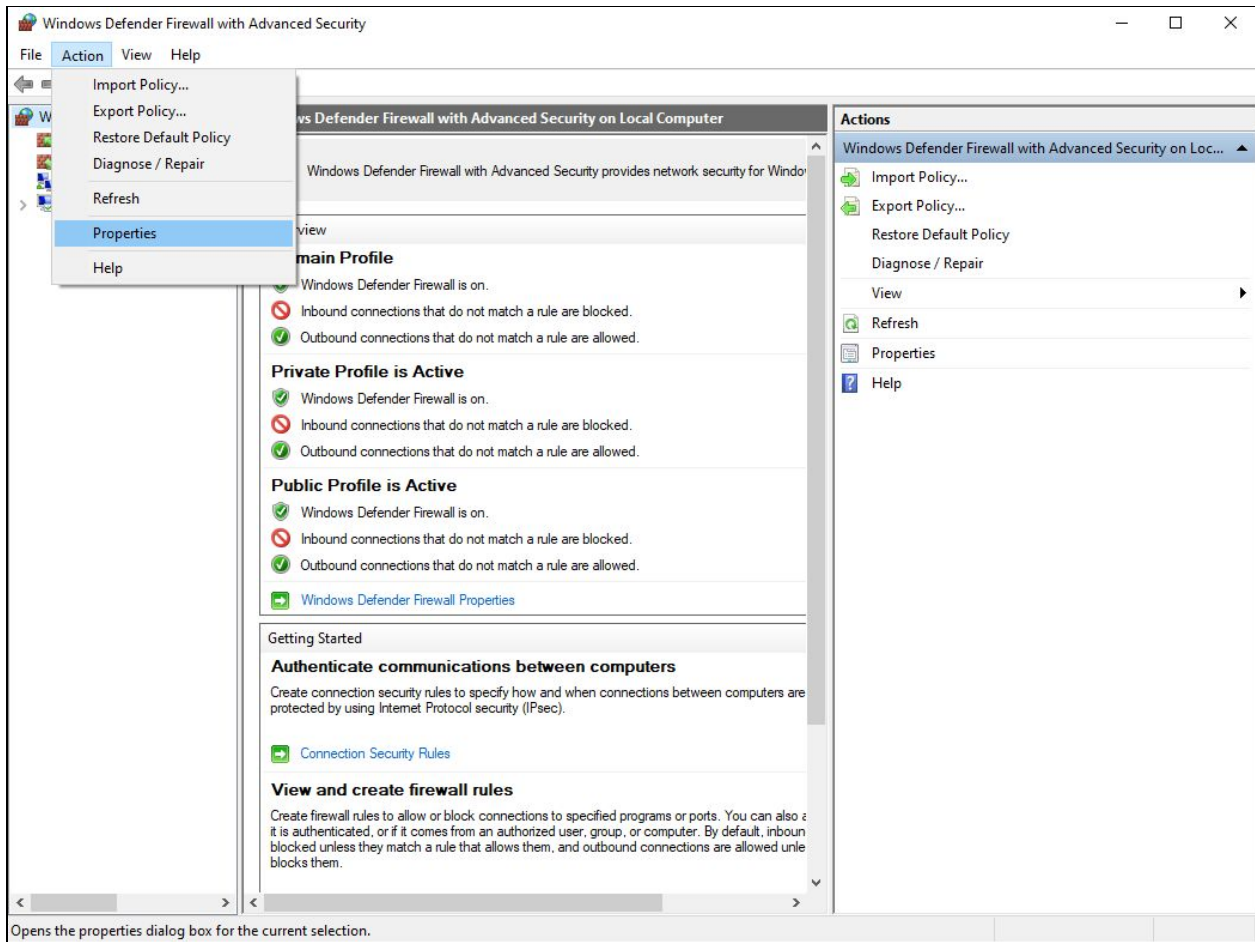
Protection areas

- Virus & threat protection
No actions needed.
- Account protection
No actions needed.
- Firewall & network protection**
No actions needed.
- App & browser control
No actions needed.
- Device security
No actions needed.
- Device performance & health
Reports on the health of your device.
- Family options
Manage how your family uses their devices.

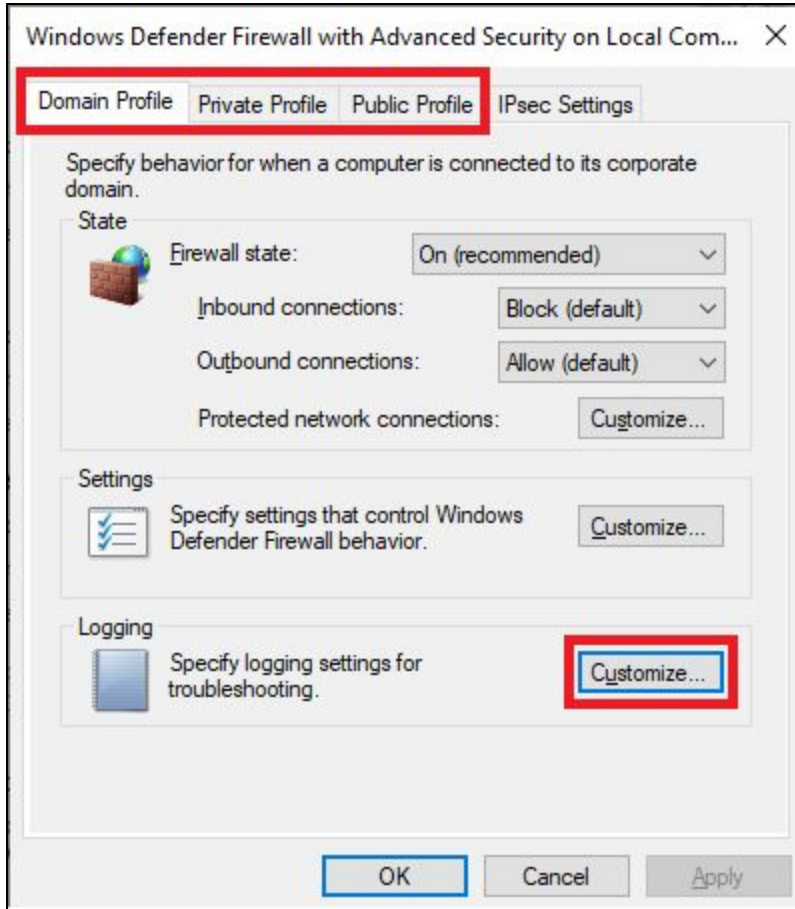
3. Advanced Settings

The screenshot shows the Windows Settings application with the 'Firewall & network protection' page open. The left sidebar contains navigation options: Home, Virus & threat protection, Account protection, Firewall & network protection (selected), App & browser control, Device security, Device performance & health, and Family options. The main content area is titled 'Firewall & network protection' and includes a description: 'Who and what can access your networks.' Below this, three network profiles are listed: 'Domain network', 'Private network (active)', and 'Public network', each with the status 'Firewall is on.' A list of links is provided at the bottom of the main area: 'Allow an app through firewall', 'Network and Internet troubleshooter', 'Firewall notification settings', 'Advanced settings' (highlighted with a red box), and 'Restore firewalls to default'. On the right side, there are additional links: 'Windows Community videos', 'Learn more about Firewall & network protection', 'Have a question? Get help', 'Who's protecting me? Manage providers', 'Help improve Windows Security Give us feedback', 'Change your privacy settings', 'View and change privacy settings for your Windows 10 device.', 'Privacy settings', 'Privacy dashboard', and 'Privacy Statement'.

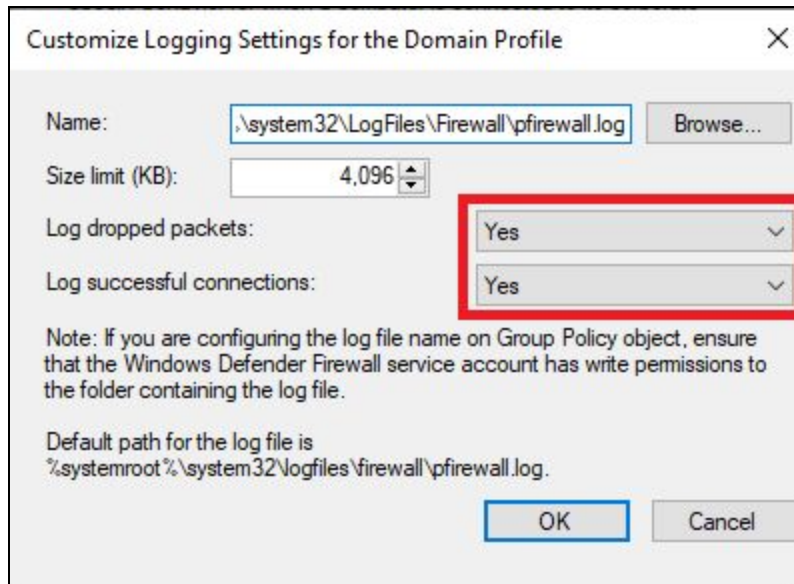
4. Windows Defender Firewall with Advanced Security > Action > Properties



5. For each Domain, Private, and Public profiles, click **Logging > Customize**



6. Log dropped packets: Yes, Log successful connections: Yes



Customize Logging Settings for the Domain Profile

Name:

Size limit (KB):

Log dropped packets:

Log successful connections:

Note: If you are configuring the log file name on Group Policy object, ensure that the Windows Defender Firewall service account has write permissions to the folder containing the log file.

Default path for the log file is
%systemroot%\system32\logfiles\firewall\pfirewall.log.