

Remote Windows Security

Last Modified on 01.08.26

The **Remote Windows Security** tool lets you view critical security information associated with your environment and devices. You can run some actions directly from within Remote Windows Security.

To run this tool, right-click on a device and select **Right Click Tools > Security Tools > Remote Windows Security**.

Interested in Remote Windows Security training?
Enroll in our [Recast Academy course](#)!

Remote Windows Security Permissions

Plugin	Permissions
ActiveDirectory	GetADComputersBitLockerStatus
BitLocker	GetBitLockerStatus AddTPMAndSKKeyProtector AddPassphraseKeyProtector DecryptVolume EncryptVolume AddProtectorsAndEncrypt ResumeBitLockerVolume ForceBitLockerRecovery AddTPMAndPINKeyProtector BackupProtectorToAD AddTPMKeyProtector BackupProtectorToAzureAD RegenerateBitLockerRecoveryKey SetVolumeIDField AddNumericalPasswordKeyProtector SuspendBitLockerVolume GetRecoveryPasswordFromDevice
ConfigMgrServer	GetSystemsBitLockerEncryptionStatus
SCEP	GetDefenderStatus StartDefenderScan UpdateSCEPDefinitions GetDefenderExclusions FullSCEPScan GatherSCEPLogs AddDefenderExclusion
SystemInformation	ResetBitLockerRecoveryPassword

Recast

Plugin	Permissions
WindowsSecurity	GetWindowsFirewallProfiles EnableSystemGuardSecureLaunch EnableCredentialGuardSettings GetAllVirtualizationBasedSecuritySettings GetUefiSecureBootStatus EnableTpmAutoProvisioning ProvisionTpm ClearTpm GetTpmStatus GetWindowsFirewallRules GetSecureBootStatus EnableVirtualizationBasedSecurity GetCredentialGuardSettings GetSystemGuardSecureLaunchSettings GetVirtualizationBasedSecuritySettings

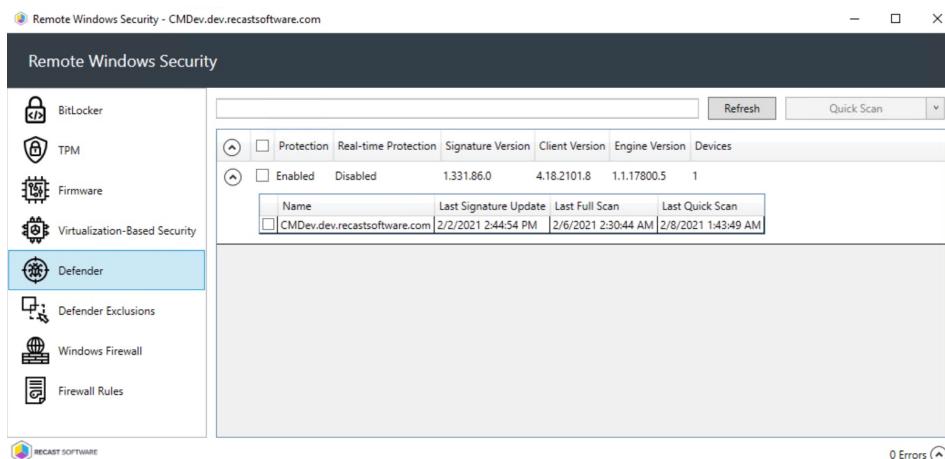
Defender

The **Defender** tab shows information about the status of Windows Defender Antivirus on selected computers.

- Defender Protection (Enabled/Disabled)
- Real-time Protection (Enabled/Disabled)
- Installed antivirus Signature Version
- Installed Defender Client Version
- Installed Defender Engine Version
- Number of Devices in this selection

Expand a section to display the following information for each device selected when running Remote Windows Security.

- Date and time of Last Signature Update
- Date and time of Last Full Scan completion
- Date and time of Last Quick Scan completion



Name	Last Signature Update	Last Full Scan	Last Quick Scan
CMDev.dev.recastsoftware.com	3/2/2021 2:44:54 PM	3/6/2021 2:30:44 AM	3/8/2021 1:43:49 AM

Defender Actions

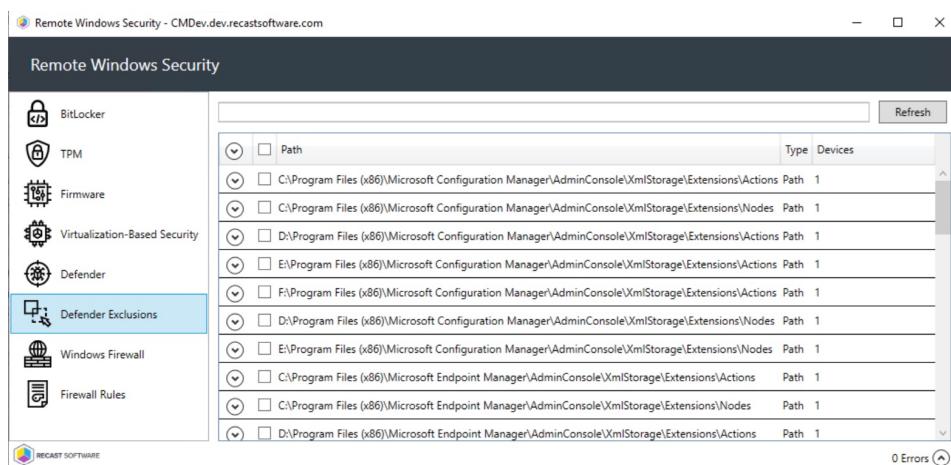
- **Quick Scan** (recommended): Scans the locations where malware might be registered to start with the system, such as registry keys and knows Windows startup folders.

Recast

- **Full Scan:** Starts with a Quick Scan, then extends the search with a sequential file scan of mounted fixed disks and network drives. A full scan can take hours or days to complete, depending on the amount and type of data included in the scan. If new security intelligence update become available during a full scan, the scan should be repeated to include new threat detections contained in the update.
- **Update Definitions:** Downloads updates to the definition files used to identify malware and other potentially unwanted software.

Defender Exclusions

The **Defender Exclusions** tab lists the exclusions applied to selected computers, including the exclusion **Path** and **Type**.



Path	Type	Devices
C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1
C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Nodes	Path	1
D:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1
E:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1
F:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1
D:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Nodes	Path	1
E:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Nodes	Path	1
C:\Program Files (x86)\Microsoft Endpoint Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1
C:\Program Files (x86)\Microsoft Endpoint Manager\AdminConsole\XmlStorage\Extensions\Nodes	Path	1
D:\Program Files (x86)\Microsoft Endpoint Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1

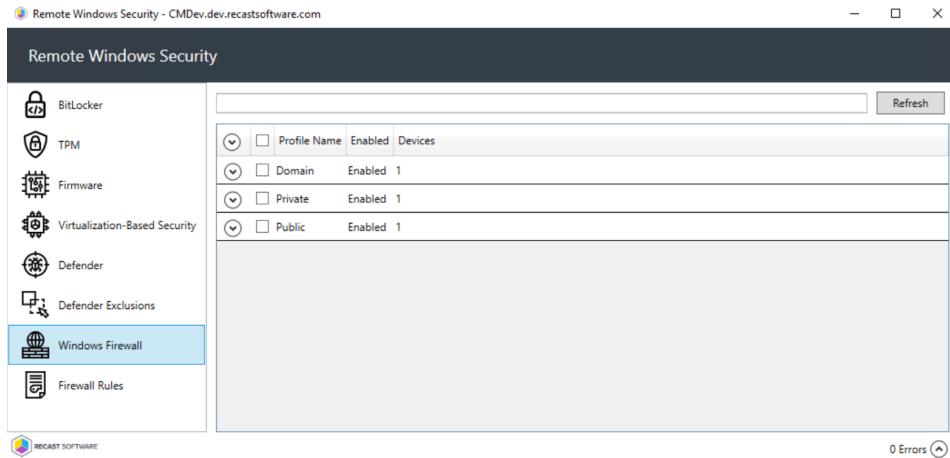
Windows Firewall

The **Windows Firewall** tab display firewall details for selected computers, including whether profiles have been enabled for:

- Domain
- Private
- Public

Expand a section to display more information about an individual firewall profile. The data shown can help determine the inbound and outbound communications allowed on each device and which ports are used. This is also where you can see if logging is enabled and where logs are located.

Recast



The screenshot shows the 'Remote Windows Security' interface. On the left, a sidebar lists security components: BitLocker, TPM, Firmware, Virtualization-Based Security, Defender, Defender Exclusions, Windows Firewall (which is selected and highlighted in blue), and Firewall Rules. The main pane displays a table with columns: Profile Name, Enabled, and Devices. The table shows four rows: Domain (Enabled, 1 device), Private (Enabled, 1 device), and Public (Enabled, 1 device). A 'Refresh' button is in the top right of the main pane, and a '0 Errors' status is at the bottom right.

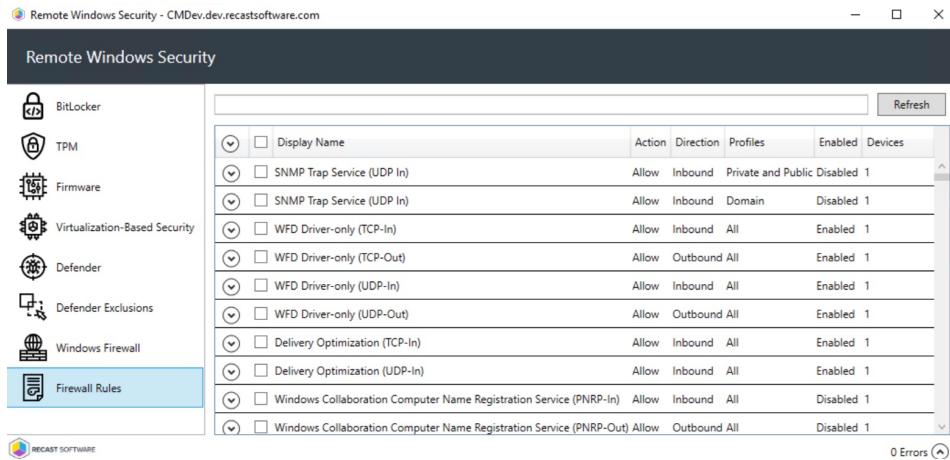
Firewall Rules

This tab displays Windows firewall rules applied to selected computers.

Details include:

- Action: Allow / Block
- Direction: Inbound / Outbound
- Profiles: All, Domain, Private, Public
- Firewall rule Enabled or Disabled
- Number of Devices in this selection

Expand the section for each rule to see the devices on which the rule is applied.



The screenshot shows the 'Remote Windows Security' interface with the 'Firewall Rules' tab selected. The main pane displays a table with columns: Display Name, Action, Direction, Profiles, Enabled, and Devices. The table lists 14 firewall rules, each with a collapse icon (a triangle with a circle). The rules include: SNMP Trap Service (UDP In), WFD Driver-only (TCP-In), WFD Driver-only (TCP-Out), WFD Driver-only (UDP-In), WFD Driver-only (UDP-Out), Delivery Optimization (TCP-In), Delivery Optimization (UDP-In), Windows Collaboration Computer Name Registration Service (PNRP-In), and Windows Collaboration Computer Name Registration Service (PNRP-Out). The 'Refresh' button is in the top right of the main pane, and a '0 Errors' status is at the bottom right.

BitLocker

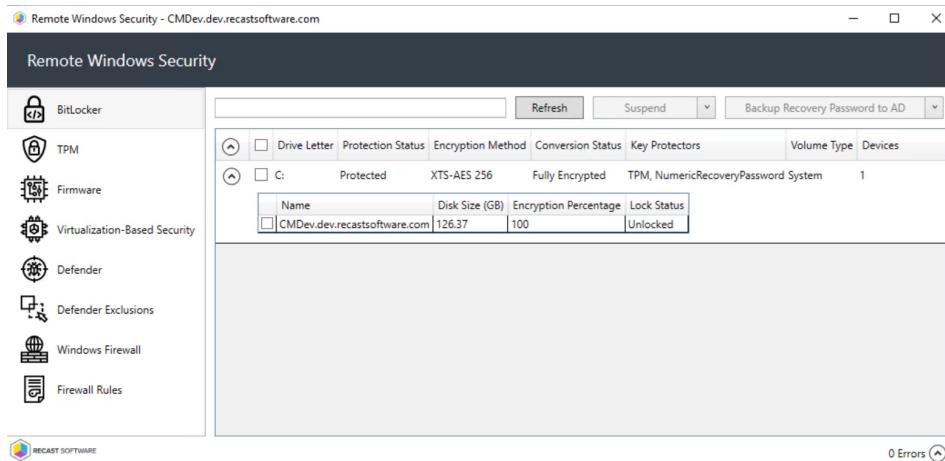
View the current protection status for the drives on selected computers.

Details include:

Recast

- Associated Drive Letter
- Protection Status for the drive
- Encryption Method for the drive
- Conversion Status for the drive, if encrypted
- Key Protectors used for this drive
- Volume Type for this drive
- Number of devices in this selection

Expand the section for each drive to view Disk Size in GB, Encryption Percentage, and Lock status.



The screenshot shows the 'Remote Windows Security' interface with the 'BitLocker' tab selected. On the left, a sidebar lists various security components: BitLocker, TPM, Firmware, Virtualization-Based Security, Defender, Defender Exclusions, Windows Firewall, and Firewall Rules. The main pane displays a table for drive C, which is protected, XTS-AES 256, Fully Encrypted, using TPM, Numeric Recovery Password, and System as the Volume Type. The table includes columns for Name, Disk Size (GB), Encryption Percentage, and Lock Status, with one entry for 'CMDev.dev.recastsoftware.com' showing 126.37 GB, 100% encryption, and an unlocked status. A 'Backup Recovery Password to AD' button is also visible in the top right of the main pane.

BitLocker Actions

- **Suspend or Resume** BitLocker encryption
- **Decrypt or Encrypt** the content of the volume.
 - A confirmation prompt appears before decryption begins.
 - When you click **Encrypt**, the Right Click Tools Encryption Wizard will open and you'll be asked to choose options such as encryption method and its scope.
- **Backup Recovery Password to AD**: Saves the password to Active Directory Domain Services.
- **Backup Recovery Password to Azure**: Saves the password to Entra ID (formerly Azure Active Directory) Domain Services.
- **Force Recovery on Next Restart**: Forces the user to enter the recovery key upon device restart.
- **Regenerate Recovery Password**: Generates a new recovery password.

TPM

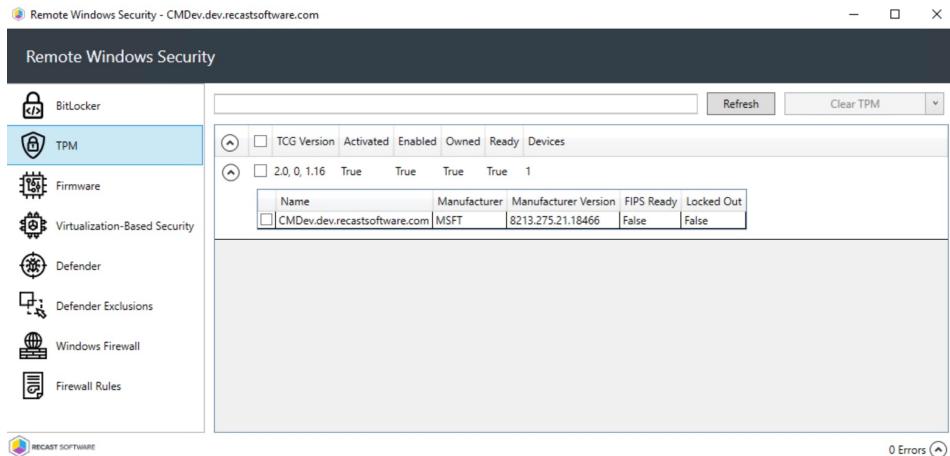
The TPM tab shows information about the status of the Trusted Platform Module on selected computers.

Included details:

- Trusted Computing Group (TCG) Version
- TPM Activated (T/F)
- TPM Enabled (T/F)
- TPM Owned by the OS (T/F)
- TPM Ready (T/F)
- Number of Devices in this selection

Expand a section to display Manufacturer and Manufacturer Version details, as well as whether the device is FIPS Ready or Locked Out.

Recast



The screenshot shows the 'Remote Windows Security' application window. The left sidebar has a 'TPM' tab selected, showing icons for BitLocker, TPM, Firmware, Virtualization-Based Security, Defender, Defender Exclusions, Windows Firewall, and Firewall Rules. The main pane displays a table for TPM devices. The table has columns: TCG Version, Activated, Enabled, Owned, Ready, and Devices. One device is listed: Name (CMDev.dev.recastsoftware.com), Manufacturer (MSFT), Manufacturer Version (8213.275.21.18466), FIPS Ready (False), and Locked Out (False). A 'Refresh' and 'Clear TPM' button are at the top of the table area. A '0 Errors' message is at the bottom right.

TPM Actions

Clear TPM: Resets the TPM to its default state. This function removes the owner authorization value and any keys stored in the TPM.

Provision TPM: Executes part of the provisioning process which prepares a TPM for use.

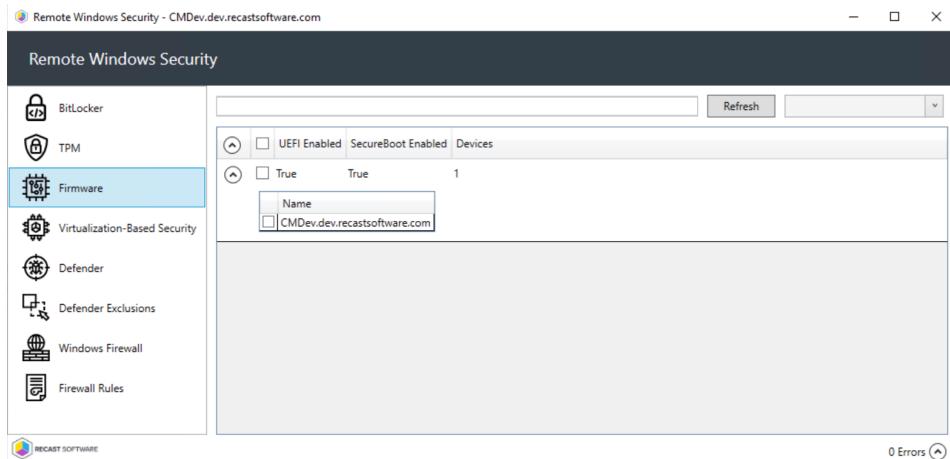
Enable Auto-Provisioning: Allows TPM provisioning to happen during auto-provisioning.

Firmware

The **Firmware** tab shows information about specific security settings related to selected computers.

Included details:

- Unified Extensible Firmware Interface (UEFI) Enabled (T/F)
- SecureBoot Enabled (T/F)
- Number of Devices in this selection



The screenshot shows the 'Remote Windows Security' application window. The left sidebar has a 'Firmware' tab selected, showing icons for BitLocker, TPM, Firmware, Virtualization-Based Security, Defender, Defender Exclusions, Windows Firewall, and Firewall Rules. The main pane displays a table for firmware settings. The table has columns: UEFI Enabled, SecureBoot Enabled, and Devices. One device is listed: Name (CMDev.dev.recastsoftware.com). A 'Refresh' button is at the top of the table area. A '0 Errors' message is at the bottom right.

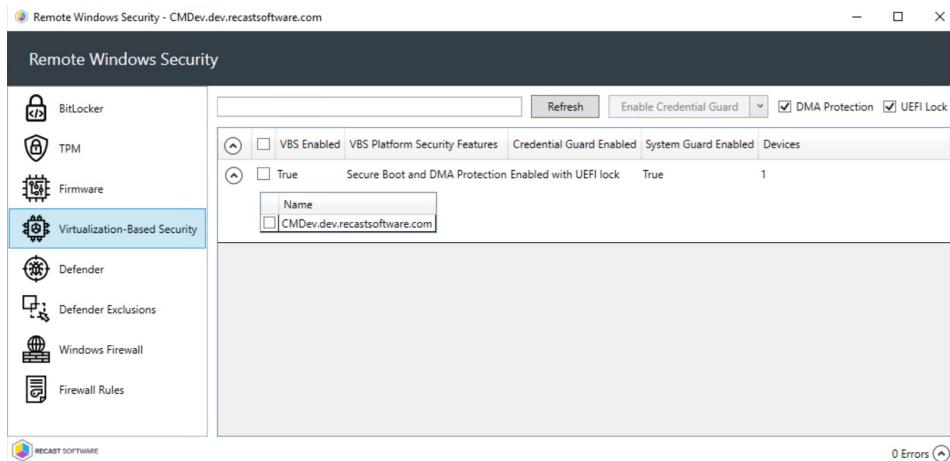
Recast

Virtualization-Based Security

This tab shows information about virtualization-based security options for selected computers.

Included details:

- Virtualization-Based Security (VBS) Enabled (T/F)
- VBS Platform Security Features
- Credential Guard Enabled
- System Guard Enabled (T/F)
- Number of Devices in this selection



VBS Enabled	VBS Platform Security Features	Credential Guard Enabled	System Guard Enabled	Devices		
<input type="checkbox"/> True	Secure Boot and DMA Protection Enabled with UEFI lock	<input type="checkbox"/> True	<input type="checkbox"/> 1			
<table border="1"><thead><tr><th>Name</th></tr></thead><tbody><tr><td><input type="checkbox"/> CMDDev.dev.recastsoftware.com</td></tr></tbody></table>					Name	<input type="checkbox"/> CMDDev.dev.recastsoftware.com
Name						
<input type="checkbox"/> CMDDev.dev.recastsoftware.com						

Virtualization-Based Security Actions

- Enable Credential Guard
- Enable System Guard
- Enable or disable DMA Protection: Enabled by default
- Enable or disable UEFI Lock: Enabled by default