Remote Windows Security

Last Modified on 07.04.24

The **Remote Windows Security** tool lets you view critical security information in your Configuration Manager console. You can also run some actions directly from within Remote Windows Security.

To view security information in your Configuration Manager console, navigate to **Assets and Compliance** > **Devices** > **Right Click Tools** > **Security Tools** > **Remote Windows Security**.

Interested in Remote Windows Security training?
Enroll in our Recast Academy course!

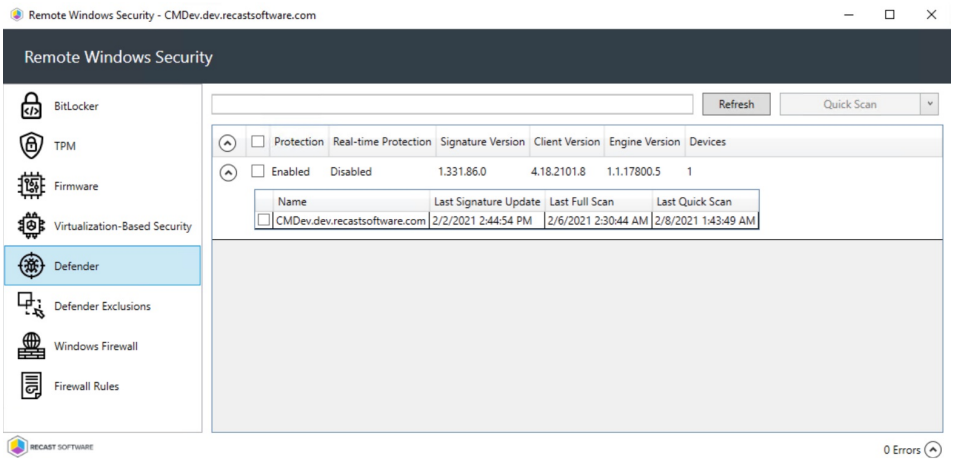
Defender

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

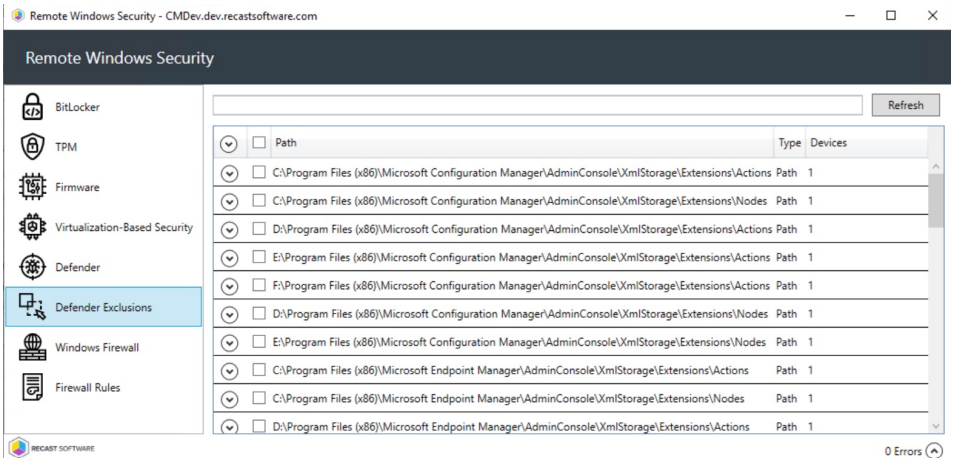


Defender Actions

- **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.
- **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.**

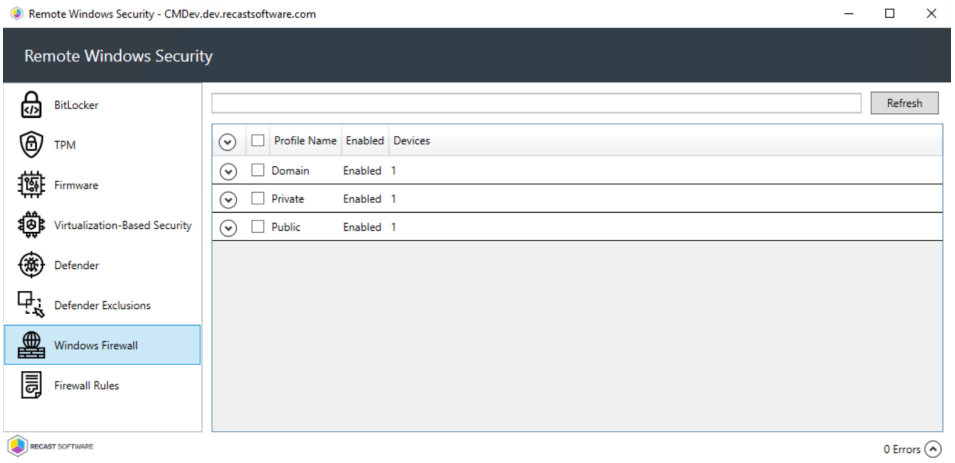


Windows Firewall

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.



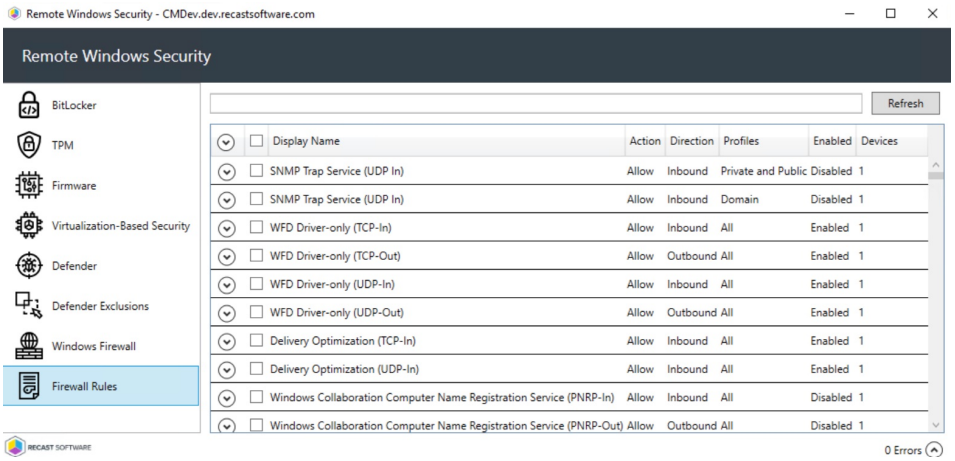
Firewall Rules

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.



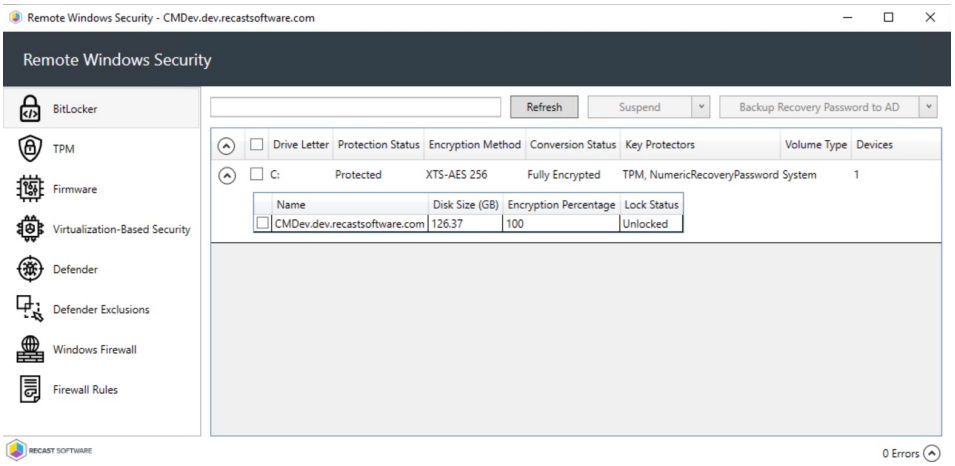
BitLocker

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

Details include:

- 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 see details about the Disk Size in GB, Encryption Percentage, and Lock status.



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.

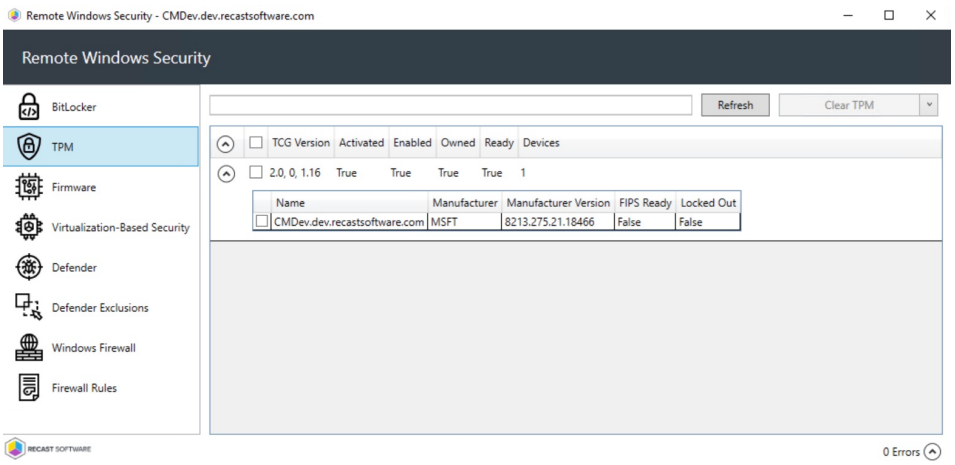
TPM

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.



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.

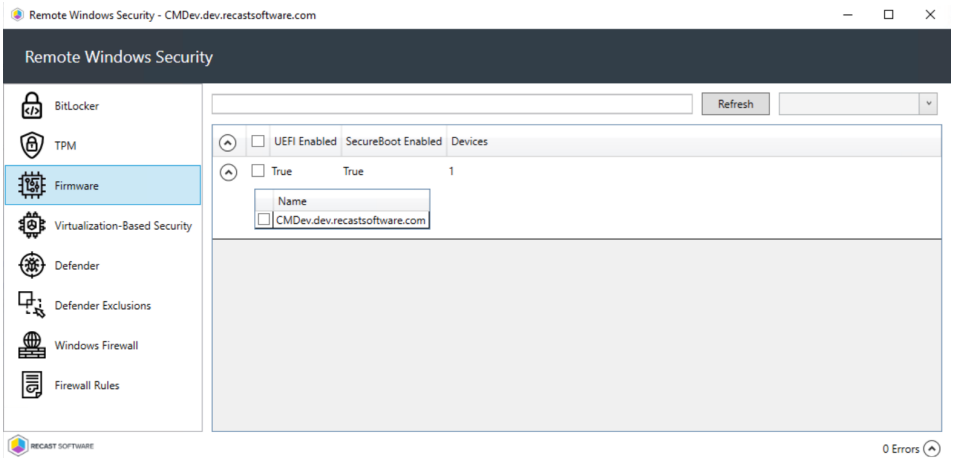
Enable Auto-Provisioning: Allows TPM provisioning to happen during auto-provisioning.

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

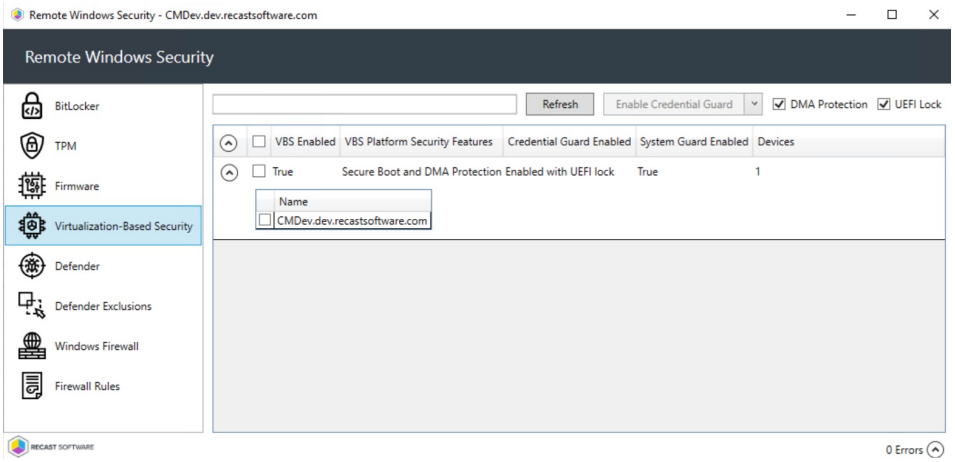


Virtualization-Based Security

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



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