

# **Remote Windows Security**

Last Modified on 05.06.25

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!

#### 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

Rem	note Windows Security - CMDev.	.dev.recas	tsoftv	vare.com						-		×
Rer	note Windows Securit	ty										
¢	BitLocker								Refresh	Quick Scar	n	*
0	ТРМ	$\odot$		Protection	Real-time Protection	Signature Version	Client Version	Engine Version	Devices			
鬱	Firmware	$\odot$		Enabled	Disabled	1.331.86.0 Last Signature Upda	4.18.2101.8 ate Last Full Sc	1.1.17800.5	1 Quick Scan			
\$	Virtualization-Based Security			CMDev.dev	v.recastsoftware.com	2/2/2021 2:44:54 PM	1 2/6/2021 2:	30:44 AM 2/8/20	021 1:43:49 AM			
۲	Defender											
먚;	Defender Exclusions											
	Windows Firewall											
J	Firewall Rules											
_												
RECA	ST SOFTWARE										0 Error	rs 🔿

#### **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.

Rem	note Windows Security - CMDev.d	ev.recastsoftware.com		-		×	í.
Ren	note Windows Security						
ß	BitLocker				Re	efresh	
0	ТРМ		Туре	Devices			
虈	Firmware	⊙ C\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1			6 -
		C:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Nodes	Path	1		_	
<b>1</b>	Virtualization-Based Security	⊙ □ D:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1		_	1
*	Defender	💿 🗌 E:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1			
<b>~</b>		🕞 🗌 F:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Actions	Path	1			
43	Defender Exclusions	💿 🗌 D:\Program Files (x86)\Microsoft Configuration Manager\AdminConsole\XmlStorage\Extensions\Nodes	Path	1			
<b>A</b>	Windows Firewall	💿 🗌 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,	Firewall Rules	⊙ □ 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		~	1
RECA	ST SOFTWARE				0 E	rrors (A	.)

### 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.

Remote Windows Security - CMDe	ev.dev.recastsoftware.com	-		×				
Remote Windows Security								
BitLocker			Refre	ih				
Ф трм	Profile Name Enabled Devices							
Firmware	Domain Enabled 1			_				
Virtualization-Based Security	Image: Second							
Defender								
Defender Exclusions								
Windows Firewall								
Firewall Rules								
RECAST SOFTWARE			0 Erro	rs 🔿				

# 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.

Remote Windows Security - CMDev.	iev.recastsoftware.com	-		×
Remote Windows Securit				
BitLocker			Refresh	
П ТРМ	🕞 🗆 Display Name Action Direction Profiles E	Enabled	Devices	
- विक्री	SNMP Trap Service (UDP In) Allow Inbound Private and Public D	Disabled	1	^
Firmware	SNMP Trap Service (UDP In) Allow Inbound Domain D	Disabled	1	
Virtualization-Based Security	⊙         □         WFD Driver-only (TCP-In)         Allow         Inbound         All         En	nabled	1	-
Defender	⊙         □         WFD Driver-only (TCP-Out)         Allow         Outbound All         En	nabled	1	
•	⊙         □         WFD Driver-only (UDP-In)         Allow         Inbound         All         En	nabled	1	
Defender Exclusions		nabled	1	-
Windows Firewall	Delivery Optimization (TCP-In)       Allow     Inbound     All     End	nabled	1	-
	Delivery Optimization (UDP-In)       Allow     Inbound     All     En	nabled	1	
Firewall Rules	🕑 🗌 Windows Collaboration Computer Name Registration Service (PNRP-In) Allow Inbound All D	Disabled	1	-
	(♥)         □         Windows Collaboration Computer Name Registration Service (PNRP-Out) Allow         Outbound All         D	Disabled	1	~
RECAST SOFTWARE			0 Errors	$\bigcirc$

### 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 view Disk Size in GB, Encryption Percentage, and Lock status.

Ren	Remote Windows Security - CMDev.dev.recastsoftware.com     -      X													
Rer	mote Windows Security	ý												
<del>C</del>	BitLocker							Refresh	Suspend	* Backup	Recovery Passv	vord to	AD	*
0	TPM	$\odot$		Drive Letter	Protection Status	Encryption Met	hod	Conversion Status	Key Protecto	ors	Volume Type	Devic	es	
虈	Firmware	$\odot$		C:	Protected	XTS-AES 256	Env	Fully Encrypted	TPM, Numer	icRecoveryPasswore	d System	1		
ŝ	Virtualization-Based Security		CMDev.dev	recastsoftware.com	n 126.37	100		Unlocked	]					
۲	Defender													
덏	Defender Exclusions													
<b>₽</b>	Windows Firewall													
<b>III</b>	Firewall Rules													
RECA	IST SOFTWARE												0 Errors	

#### **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.

Remote Windows Security - CMDev.	Jev.recastsoftware.com	>	×
Remote Windows Securit	у		
BitLocker	Refresh	Clear TPM	•
🙆 трм	Contraction CCG Version Activated Enabled Owned Ready Devices		
Firmware	2.0,0,1.16 True True True 1      Name Manufacturer Manufacturer Version FIPS Ready Locked Out		
Virtualization-Based Security	CMDev.dev.recastsoftware.com MSFT 8213.275.21.18466 False False		
Defender			
Defender Exclusions			
Windows Firewall			
Firewall Rules			
RECAST SOFTWARE		0 Errors (	2

#### **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

Remote Windows Security - CMDev.dev.recastsoftware.com							
Remote Win	idows Securit	ity					
BitLocker		Refresh			*		
Ф ТРМ		O UEFI Enabled SecureBoot Enabled Devices					
Firmware		True True 1					
Virtualizatio	n-Based Security	CMDev.dev.recastsoftware.com					
Defender							
Defender Ex	clusions						
Windows Fir	rewall						
Firewall Rule	es						
~							
RECAST SOFTWARE				0 Erron	s 🔿		

#### 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

Remote Windows Security - CMDev.dev.recastsoftware.com     -							
Remote	e Windows Security	y I					
BitLo	ocker	Refresh         Enable Credential Guard         V         Image: DMA F	rotection	UEFI	Lock		
🙆 трм		⊘ □ VBS Enabled VBS Platform Security Features Credential Guard Enabled System Guard Enabled Devices					
Firmv	ware	True Secure Boot and DMA Protection Enabled with UEFI lock True 1  Name					
Virtua	ualization-Based Security	CMDev.dev.recastsoftware.com					
Defer	ender						
Defer	ender Exclusions						
Wind	dows Firewall						
Firew	vall Rules						
<u>^</u>							
RECAST SOFTW	WARE			0 Error	5		

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

Copyright © 2025 Recast Software Inc. All rights reserved.