

Windows Defender Signature Database Empty After Norton Antivirus Uninstallation Causes ISE Posture Failure

Contents

Issue

Windows 11 25H2 endpoints connecting through VPN fail ISE posture checks and are marked as non-compliant, preventing authentication and access to network resources. The endpoint meets the ISE rule requirements but still reports "user not meeting the requirement" after VPN connection.

The posture check specifically fails for Windows Defender antivirus definition version validation with this error:

```
[csc_iseposture]Function: CheckOpswat::CheckOpswatProd Thread Id: 0x277C File: CheckOpswat.cpp Line: 27
```

The posture agent reports that Windows Defender has an empty definition version and definition date of 0, causing the AUC_WIN11_IT requirement to fail.

Environment

- Identity Services Engine (ISE) 3.3
- Windows 11 25H2 endpoints
- Cisco Secure Client with ISE Posture module
- ISECompliance module version 4.3.5626.8192
- Windows Defender version 4.18.25080.5
- Previously had Norton 360 antivirus installed and uninstalled
- VPN connection with ISE posture enforcement enabled

Resolution

The resolution involves uninstalling Norton, then manually updating Windows Defender signatures and understanding the coexistence behavior between third-party antivirus and Windows Defender.

Step 1: Update Windows Defender Signatures

- 1.- Navigate to the Windows Security settings and manually update the signature database:
- 2.- Go to **Settings** → **Privacy & security** → **Windows Security** → **Virus & threat protection** → **Virus & threat protection updates** → **Check for updates**.
- 3.- Wait until the **Security intelligence version** shows a non-empty value and a current timestamp before proceeding with posture validation.

Step 3: Verify Posture Compliance

After updating the signatures, reconnect to the VPN and verify that the posture check passes. The security intelligence version must now display a valid value instead of being empty.

Important Considerations for Third-Party Antivirus

When any third-party antivirus is installed and properly registered with Windows Security Center, Microsoft Windows intentionally puts Windows Defender into passive mode to avoid conflicts. In passive mode, Defender does not publish its signature-freshness data through the Windows Security Center/WMI API that OPSWAT reads, causing posture checks to fail.

To prevent this issue uninstall the 3rd party application which windows puts into Active mode. If reinstalling Norton or other third-party antivirus software is required, be aware that this causes the endpoint to become non-compliant again.

Cause

The root cause is that the Windows Defender signature database becomes stale when a third-party antivirus (Norton) is the primary antivirus solution. While Norton was installed, Windows intentionally kept the Defender definitions store stale because passive-mode antivirus software does not receive scheduled updates. After Norton was uninstalled, Windows Defender became the primary antivirus but its signature database remained empty because the first signature pull is queued behind Windows Update and only runs automatically on its next scheduled trigger or when manually forced by the user.

The OPSWAT v4 SDK method 1001 (**GetDefinitionState**) returns an empty payload when the Defender local definitions store is empty, causing the ISE posture agent to transmit an empty definition version to ISE. ISE then compares this empty value to the policy threshold and marks the endpoint as non-compliant.

Related Content

- [Cisco Secure Client Administrator Guide - Third-Party Software Considerations](#)
- [Cisco Technical Support & Downloads](#)