

# Norton Antivirus卸载后，Windows Defender签名数据库为空，导致ISE状态故障

## 目录

---

## 问题

通过VPN连接的Windows 11 25H2终端未通过ISE状态检查并标记为不兼容，从而阻止身份验证和网络资源的访问。终端符合ISE规则要求，但在VPN连接后仍报告“用户不符合要求”。

Windows Defender防病毒定义版本验证的状况检查特别失败，出现以下错误：

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

状态代理报告Windows Defender的定义版本和定义日期为空0，导致AUC\_WIN11\_IT要求失败。

## 环境

- 身份服务引擎(ISE)3.3
- Windows 11 25H2终端
- 带ISE终端安全评估模块的思科安全客户端
- ISECcompliance module version 4.3.5626.8192
- Windows Defender版本4.18.25080.5
- 之前已安装和卸载Norton 360防病毒软件
- 已启用ISE终端安全评估实施的VPN连接

## 分辨率

解决方案包括卸载Norton，然后手动更新Windows Defender签名并了解第三方防病毒软件与Windows Defender之间的共存行为。

### 步骤 1：更新Windows Defender签名

1. — 导航到Windows安全设置并手动更新签名数据库：
2. — 转到Settings → Privacy & security → Windows Security → Virus & threat protection → Virus & threat protection updates → Check for updates。
3. — 请等待Security intelligence version显示非空值和当前时间戳，然后再继续状态验证。

### 步骤 3：验证状态合规性

更新签名后，重新连接到VPN并验证状态检查通过。安全情报版本现在必须显示有效值而不是为空。

### 第三方防病毒的重要注意事项

安装任何第三方防病毒软件并正确注册到Windows安全中心后，Microsoft Windows会故意将Windows Defender置于被动模式以避免冲突。在被动模式下，Defender不会通过OPSWAT读取的Windows安全中心/WMI API发布其签名更新数据，导致状态检查失败。

要防止此问题，请卸载windows设置为活动模式的第三方应用程序。如果需要重新安装Norton或其他第三方防病毒软件，请注意这会导致终端再次变得不合规。

## 原因

根本原因在于，当第三方防病毒软件(Norton)是主要防病毒解决方案时，Windows Defender签名数据库会过时。安装Norton时，Windows故意使Defender定义存储保持陈旧，因为被动模式防病毒软件不会接收计划的更新。在卸载Norton后，Windows Defender成为主要防病毒软件，但其签名数据库仍然为空，因为第一个签名提取在Windows Update后排队，并且仅在下一个计划触发时自动运行，或者当用户手动强制时。

当Defender本地定义存储为空时，OPSWAT v4 SDK方法1001(GetDefinitionState)返回空负载，导致ISE终端安全评估代理向ISE传输空定义版本。然后，ISE将此空值与策略阈值进行比较，并将终端标记为不合规。

## 相关内容

- [Cisco Secure Client管理员指南 — 第三方软件注意事项](#)
- [思科技术支持和下载](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。