At a glance
Cisco Public

Cisco Identity Services Engine
Device Compliance

Your security policy is there for a good reason. So who’s ignoring it?

At Cisco, our internal device compliance policy is known as the Trusted Device Standard. Among the requirements are Cisco-approved operating system images and versions, endpoint security technology, automatic updates, and time limits for critical security patches. All workstations and mobile devices must comply before they’re trusted on our corporate network. No doubt your organization has a security policy like ours too.

Device posture is critical because outdated software often have vulnerabilities that hackers routinely exploit. Unauthorized applications can be big threat. Weak security settings practically invite attacks. And without current endpoint security protections, people can unwittingly turn their devices into a real menace on your network.

Do you know if non-compliant devices are running on your network? Can you limit their access or remove them from the network? You can, with Cisco Identity Services Engine.

© 2019 Cisco and/or its affiliates. All rights reserved.

Why is the security posture of devices so important?

- Vulnerabilities are everywhere in outdated software
- Unauthorized apps and software can cause data leaks
- Weak security settings make devices easy to exploit
- Endpoints lacking the latest security technology are risky
Cisco ISE assures device compliance with your security policy

Cisco Identity Services Engine (ISE) together with Cisco AnyConnect Secure Mobility Client checks the security posture of devices that connect to your network. Device compliance is just one of several use cases that make ISE and AnyConnect a critical part of your network operations and cybersecurity programs.

Posture assessment begins with user authentication and, once validated, ISE grants very limited network access so that it can assess the device. During the assessment, it checks the device operating system version, system settings, endpoint protection software, and other indicators against your policy. If the device lacks critical patches, for example, ISE triggers software update systems to apply them.

That way, only compliant devices gain trusted access to your network. Cisco ISE and AnyConnect won’t let anyone or anything ignore your security policy anymore.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1    | Authentication  
Validate user credentials first |
| 2    | Limited Access  
Permit just enough for the posture assessment |
| 3    | Posture Assessment  
Check device compliance with security policy |
| 4    | Remediation  
Apply updates or take other necessary action |
| 5    | Authorization  
Grant appropriate access with compliant device |

**Posture Assessment Flow**

![Diagram](https://www.cisco.com/c/en/us/td/docs/ios-nxos/ire/ire_2110/ire_2110酒业_2110v0_0013.pdf)