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Device posture is critical because outdated software often have vulnerabilities that hackers routinely exploit.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.
With Cisco ISE, you can:

- Grant and control the right level of network access
- Improve your security posture and quickly contain breaches
- Gain complete endpoint visibility with context
- Streamline your access control policy management

**Licensing**
Device Compliance requires both the ISE Apex and AnyConnect Apex licenses for each active endpoint session. Check out the Ordering Guide to learn more.

**Learn More**
To learn more, please visit https://www.cisco.com/go/ise or contact your account representative.

---

**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.

---

**Posture Assessment Flow**

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

---

Cisco ISE, SCCM, and Jamf are connected through the posture assessment flow diagram.

---

© 2019 Cisco and/or its affiliates. All rights reserved. Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R) 06/19