Cisco Identity Services Engine

Secure Wired Access

We often think of wireless first, but don't overlook your wired network.

Almost everything is mobile these days, so it makes sense to secure your wireless networks first. However, too much focus on wireless could blind you to the risks of uncontrolled access through your wired networks. If unauthorized people or devices connect to your physical switch ports, the wired network could become the main pathway to a data breach. Don't let it happen.

Secure wired access means full knowledge and control over who's and what's allowed to connect, what they can do once they're on, and for how long. It means continually monitoring active user and device sessions for anomalies and threats, and enforcing appropriate changes of authorization when necessary.

Providing the right level of access to the right people and devices sounds easy, but it's often difficult to do. The challenge is even greater when making access policies consistent across wired, wireless, and VPN connections.

We have good news, though. We've made it fast and easy.

What does Secure Wired Access mean?

Identity: Know the people behind your user accounts – including visitors and temporary workers.

Authentication: Make sure that people are actually who they claim to be.

Authorization: Control the right level of wired access based on who the person or device is.

Accounting: Track who's on your network, what they're doing, and for how long.

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

Secure Wired Access requires the **Base** incense 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.

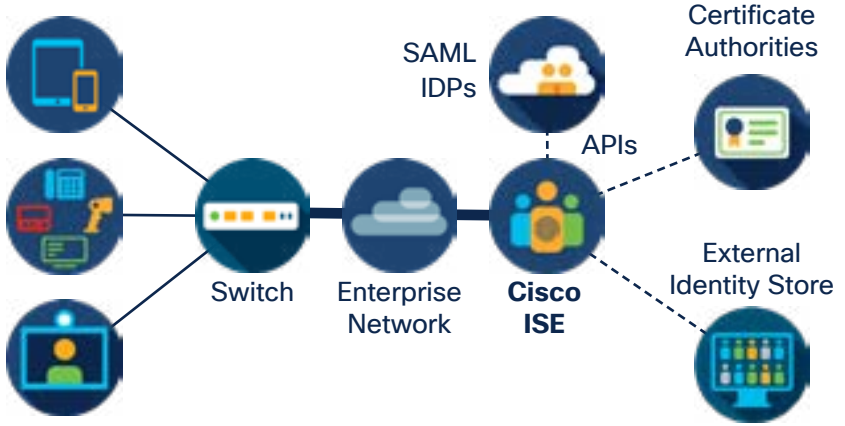
Cisco ISE simplifies secure wired access control

Cisco Identity Services Engine (ISE) makes it easy to gain visibility and control over who and what's on your network consistently across wireless, wired, and VPN connections. Secure wired access is just one of several use cases that makes ISE a critical part of your cybersecurity program.

ISE offers active authentication through IEEE 802.1X port-based access control, and passive authentication by learning about identity through external integrations like Microsoft Active Directory and others. Other methods include web authentication or simple MAC Authentication Bypass. Then ISE enforces authorization policy by linking the device's session with a group-based policy that's enforced by the network itself.

With Cisco ISE, you'll benefit from simplified, secure wired access control needed to grant appropriate access while protecting your organization from the risks of unauthorized people and devices.

How Secure Wired Access Works



As users and devices plug into the network, ISE confirms identities and device types against its own repository or through APIs to external sources. Then it grants and controls access based on who and what requested network access.