



Cisco Identity Services Engine

Guest and Secure Wireless Access

Everyone needs wireless access. That doesn't mean carte blanche.

Carte blanche is a term that means, basically, the freedom to do whatever your want. From a cybersecurity perspective, it's certainly not a word you want associated with your organization's networks. Of course, you want to offer your visitors, contractors, and employees the wireless access they need. At the same time, you can't allow any unrestrained access to increase your risk of cyberattack.

You need to be able control who's allowed to connect with which types of devices, what they can do once they're on, and for how long. Guests might request basic internet access and nothing more. Contractors may need access to certain internal systems related to their work, and only for the duration of their contracts. Employees likely require more privileges based on their roles in the organization.

Providing the right level of access to the right people and devices sounds easy, but it's often hard to do. We have good news, though. We've made it fast and easy.

What does Secure Wireless 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 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

Guest and Secure Wireless 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 guest and secure wireless 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. Guest and secure wireless access is just one of several use cases that makes ISE a critical part of your cybersecurity program.

For guest and temporary contractor access, ISE lets you choose options that support your security policy:

- **Hotspot:** Immediate, basic internet access with no credentials required
- **Self-Registered:** A slick, customizable portal for guests to self-register and be approved by your sponsor
- **Sponsored:** Your sponsor creates the guest account, and shares credentials with your guest

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

