Administrative privileges are powerful. Administrators are human.

Privileged users hold the keys to your kingdom. Network and security administrators need elevated permissions to install and maintain network devices like routers, switches, and firewalls. These administrative privileges enable them to perform software updates, make configuration changes, and issue commands like shutdown that can affect the overall security and operations of your network.

Usually the goal is operational improvement, but rogue administrators and human error present very real and significant risks. With too much access for their role, for example, they can cause big problems either intentionally or unintentionally. Stolen or abused administrative credentials can also accelerate cyberattacks. Without proper control of your administrative privileges, you could find yourself locked out of your own network.

That’s why most cybersecurity best practices recommend tight controls on your administrative privileges. But how can you do it efficiently and effectively?

Why is administrative privilege control so critical?

- Abused admin credentials can worsen and spread cyberattacks
- Rogue admins can misuse their rights to intentionally inflict major damage
- Admins with too many access rights place your organization at risk
- Admins are humans who can simply make bigger mistakes
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 Administration requires the Device Admin license for each of your Policy Service Nodes configured to control network device access. 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 controls network device administration**

Cisco Identity Services Engine (ISE) helps you control administrative rights and implements role-based access control. Network device administration is just one of several use cases that make ISE a critical part of your network operations and cybersecurity programs.

ISE performs Authentication, Authorization, and Accounting (AAA) to ensure that administrators are who they say they are, that they have only the appropriate level of access, and to keep track of their activity. It even verifies their access down to the individual command level. Its built-in Terminal Access Controller Access-Control System (TACACS+) server makes it fast and easy.

With Cisco ISE, you’ll get the administrative privilege control you need to mitigate the major risks associated with too much access.

---

### Roles

- **Network Admin**
- **Support Analyst**
- **Security Admin**

### Criteria

- Net Admin
- Switch
- Asia Pacific
- Help Desk
- Router
- Europe
- Cyber Admin
- Firewall
- North America
- Active Directory Group
- Device Type
- Location

### Permissions

- Full Privileges (CLI)
- Full Access
- Read-Only Privileges
- Show Cmds Only
- Full Privileges (UI/CLI)
- Full Access

---

© 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