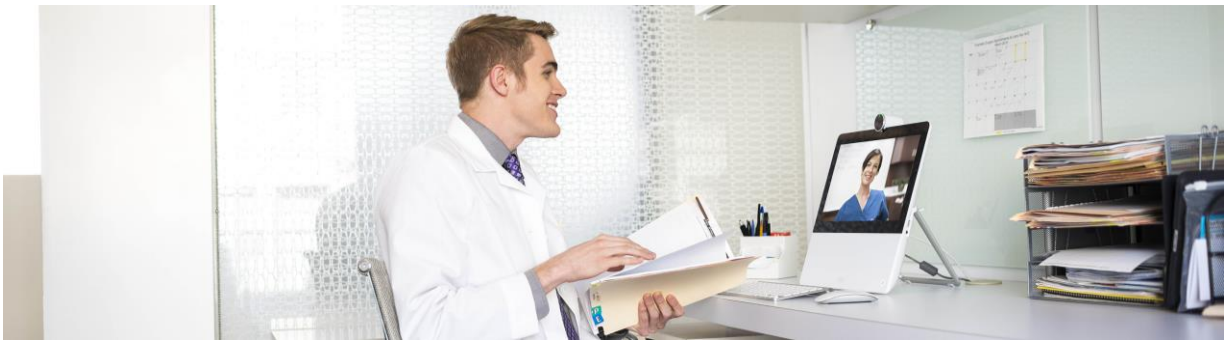
Gain Location-Based Services with Cisco ISE and Cisco MSE



Now you can give network access to users only when they're in a specific location. Protect confidential data by denying access when an individual leaves a board room, lab, or other designated area.

BENEFITS

- Apply granular control of network access with location-based authorization for individual users
- Enhance policy enforcement with automated location checks and reauthorizations
- Simplify management by configuring authorization with ISE tools

The days of employees tethered to desks are long gone. They move across the enterprise, room to room, floor to floor, building to building. At the same time, they use their laptops and other wireless devices to get stay connected and get their jobs done. Organizations need a single source of dynamic access control that adapts automatically and simply for this mobile workforce.

The Cisco® Identity Services Engine (ISE) 2.0 now features integration with the Cisco Mobility Services Engine (MSE). Administrators can grant access to users based on their specific physical location. This ability adds another level of context by which access is authorized.

As We Move Around, Our Network Access Should Change Accordingly

Currently, the definition of "location" on the network is static. It is based on the network access devicethat a user came through to access the network. Even within a specific building, "location" hasn't been based on the geographic whereabouts of a user who may be moving around that building. You may want to control network access more precisely, however. For example, you might want to grant doctors in a hospital access to patient records or to certain applications during an emergency. But when those doctors work in the medical lab, you might want to limit their access to those same records or applications.

Securing Confidential Information

Network access by mobile devices is often critical for productivity as individuals move within a facility. Yet protecting confidential assets is equally important. Take for example the need to grant executives access to confidential information only in the boardroom, or or denying access to healthcare professionals trying to access patient records while in the hospital cafeteria. Location-based network access allows you to give users access to certain files and data only while they're in the board room, the lab, or whatever the classified area may be. When an individual leaves the designated area, access to specific information is automatically denied, protecting corporate secrets and other confidential data.

Components

The location-based authorization enabled by the integration of the Cisco Mobility Services Engine with Cisco ISE 2.0 increases the granular control administrators have and their ability to be more sensitive in their access authorization. MSE will also help administrators enforce location-based policies by periodically checking for location change and automatically reauthorizing the user if a location change is detected. Finally, ISE 2.0 with MSE streamlines the configuration of location-based policies. You can define user access policies using the same management tools already available through ISE.

Main Features

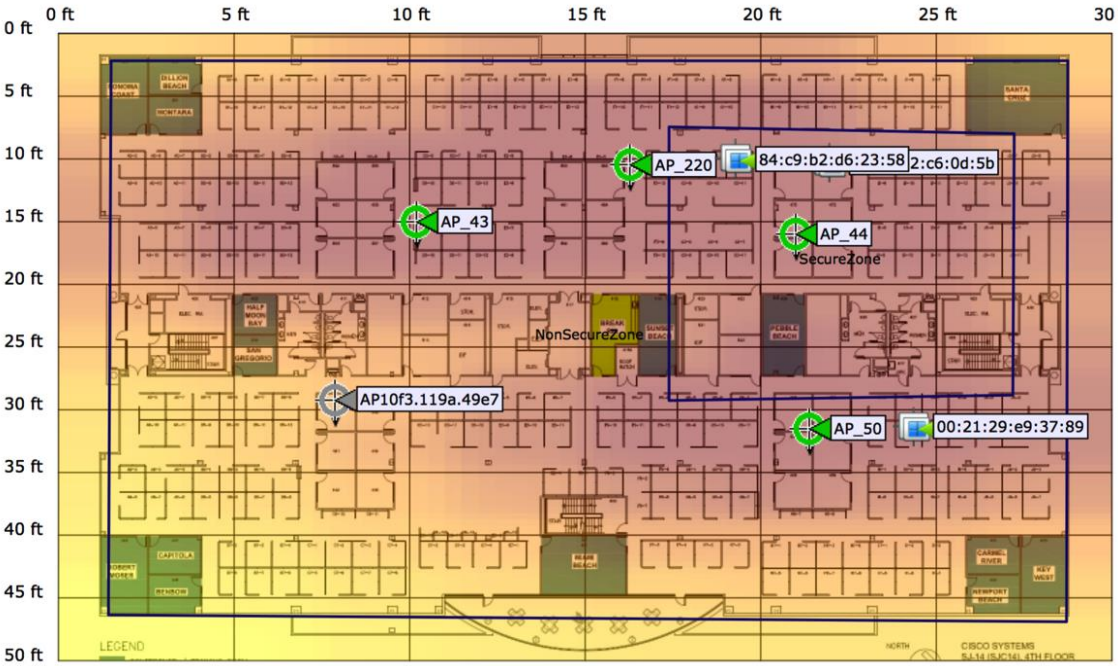
The integration of Cisco MSE with Cisco ISE 2.0:

- Enables you to configure location hierarchy across all location entities
- Applies MSE location attributes to access requests to be used in your authorization policy
- Checks the MSE periodically (every 5 minutes) for location changes
- Reauthorizes access or updates the policy based on the new location

How It Works

A network administrator defines the location hierarchy and grants users specific access rights to specific data based on their location (Figure 1). These rights can vary by room, floor, or building as needed.

Figure 1. Map of Network Access Policy Based on Building Location



Note: Good system design of the wireless systems and the building infrastructure is required. It should be evaluated when you integrate policies involved with granting access to critical systems and to roaming users between areas of a given environment. Location accuracy depends on the number of access points and the density and type of access point modules being used. Maps are configured and managed by Cisco Prime.

If the location accuracy is questionable for critical data, then we recommend that you do not permit access to such data at all on the floor using the wireless system.

Use Cases

Healthcare	Use cases are plentiful. For example, allowing access to medical records only inside the treatment room and not elsewhere can prevent data leakage and protect patients' sensitive information from unauthorized parties. A healthcare organization can also limit the medical devices themselves, disabling them when they're taken outside a specific room, floor, or building.
Retail	Savvy retailers that offer customers in-store Wi-Fi connectivity gain an opportunity to enhance the shopping experience and boost sales. But access needs to be controlled so that certain resources are available only in specific areas of the store. As an example, a retailer may have a showroom where shoppers can stream demonstration videos to their mobile devices.
Finance	Access to trading systems and other financial service systems is heavily regulated. With location-based network access, financial institutions can allow traders access to trading systems only when the trader is on the trading floor and give limited access (or no access at all) when the trader leaves the floor. Similarly, banks can give employees access to banking systems only when they are in the bank and only from sanctioned devices.
Manufacturing	For manufacturing facilities, maintaining schedules, processes, and quality control requires that only authorized personnel have access to machines. With location-based network access manufacturers can allow access to machinery and changes to machines only when employees are on the production floor. This level of control mitigates the risk of unauthorized parties hijacking mobile devices to disrupt operations.
Education	Academic institutions strive to maintain an unrestricted learning environment, providing students with access to content relevant to their course of study. Increasingly that content is video based. Location-based network access allows schools to incorporate video within the curriculum, so students can stream content only when physically inside the classroom as part of a specific learning objective.
Internet of Things	The Internet of Things is creating unprecedented opportunities for organizations as more devices come online. But it also can create risks, depending on who, what, when, where, and what is connecting. The ability to limit device connectivity

	based on location is an important security and confidentiality measure. For example, if someone enters a conference facility to attend a meeting and brings a wireless IP camera, location-based network access can control the camera's ability to widely broadcast any confidential information that may be discussed by restricting the camera to a limited-access VLAN.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

Next Steps

To learn more about the Cisco Identity Services Engine, visit http://www.cisco.com/go/ise. For information about Cisco Mobility Services Engine, visit http://www.cisco.com/go/mse.

Or contact your Cisco Services sales representative or Cisco authorized channel partner for additional information or demonstration.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C22-736885-00 4/16