At-a-Glance

Mobile Device Management and Enterprise Mobility Management Integrations with Cisco Identity Services Engine

Benefits

- **Accelerate bring-your-own-device (BYOD) and enterprise mobility initiatives** with easy out-of-the-box setup, self-service device onboarding and management, internal device certificate management, and integrated mobile device management/enterprise mobility management (MDM/EMM) partner software.
- **Prevent unenrolled and noncompliant devices from accessing the network** by protecting access with detailed policy controls based on ongoing security posture checks that use Cisco ISE device profiling and MDM/EMM posture information.
- **Protect your network against data loss** on mobile devices by using queries for enrollment, PIN lock and jailbreak, and disk encryption using Cisco ISE queries and MDM/EMM partner software.

Overview

Employees now insist on using mobile devices to work anytime and anywhere to remain productive in today's competitive marketplace. However, more devices mean a continued expansion of the surface an enterprise needs to protect from an attack. It also means your IT staff has to struggle to create a delicate balance between security and productivity.

This balance becomes more difficult to obtain as employees bring their own devices into the workplace and attempt to access network resources. How can enterprises accommodate these new productivity devices while still protecting the network from threats? While network access policy is paramount in preventing unauthorized access to networks, enterprises must also find ways to safeguard the actual devices themselves in order to enforce endpoint compliance. The Cisco Identity Services Engine (ISE), with its integrations with leading mobile device management (MDM) and enterprise mobility management (EMM) software, serves as a crucial bridge between securing devices and securing network access.

Delivering Device Visibility and Dynamic Access Control

Unlike traditional corporate-provisioned endpoints, personal mobile devices are not supplied to employees by the enterprise. Therefore the challenge lies in making sure they comply with security policies before granting them network access. The key to protecting these devices to reduce overall risk lies in greater visibility and more dynamic control: greater visibility into the mobile devices accessing your network and more dynamic control to properly classify and protect the devices to help ensure that only compliant devices get the right access to the enterprise network.

Enterprises that use integrations between Cisco ISE and MDM/EMM platforms gain greater insight into the posture of mobile devices to enforce appropriate network access policies.

Next Steps

To learn more about the Cisco ISE, visit http://cisco.com/go/ise.

For additional information regarding Cisco ISE EMM/MDM partners, visit http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html.

How It Works

- Cisco ISE profiles devices as they attempt to access the network. This discovery process provides IT professionals with the first step of network visibility. Mobile devices are subjected by Cisco ISE to a security posture assessment as specified by the company's IT policy. Cisco ISE queries for posture information associated with mobile devices as collected by the MDM/EMM platforms.
- Cisco ISE enforces access policy based on the posture status reported by the MDM partner platforms. Access policy may be constructed on specific attributes within Cisco ISE or at a global level of "in compliance" or "not in compliance" within the respective MDM/EMM platform. End users can manage the status of their devices through the Cisco ISE MyDevices portal. End users can lock, suspend, or unenroll devices if they lose or replace them. Cisco ISE can perform these functions natively or through MDM/EMM integrations.

Cisco ISE collects and delivers contextual data that includes the following:

- **User:** User name, IP address, authentication status, location
- **User class:** Authorization group, guest, quarantined
- **Device:** Manufacturer, model, OS, OS version, MAC address, IP address, network connection method (wired or wireless), location
- **Posture:** Posture compliance status, antivirus installed, antivirus version, OS patch level, mobile device posture compliance status (through MDM or MDM ecosystem partners)

C45-726284-06 05/17