MobileIron

MobileIron and Cisco Identity Services Engine

Unprecedented Visibility and Control for Mobile Devices

Mobile computing has brought about phenomenal improvements in workforce productivity, flexibility, and job satisfaction but - whether it is device operating system, form factor, ownership, or app selection and utilization - the diversity of the mobile landscape creates an entirely new dynamic for managing access to enterprise resources.

In order to effectively address the challenges posed by this diverse landscape, IT organizations need a comprehensive solution with the ability to extend corporate policies from the endpoint to the data center.

Historically, Network Access Control (NAC) systems have relied on information from specialized agent software running on laptops and desktops to determine their security posture. Lacking similar visibility for mobile devices, access control decision criteria were limited to user credentials and directory attributes: detailed information about the mobile endpoint was not available. This absence of information created inconsistent policy application between traditional network endpoints and mobile devices, exposing organizations to a variety of risks.

Conversely, while the MobileIron Enterprise Mobility management (EMM) platform has very detailed visibility into the state of mobile devices and a rich set of device level management capabilities, access control capabilities were confined to specific enterprise services like email.

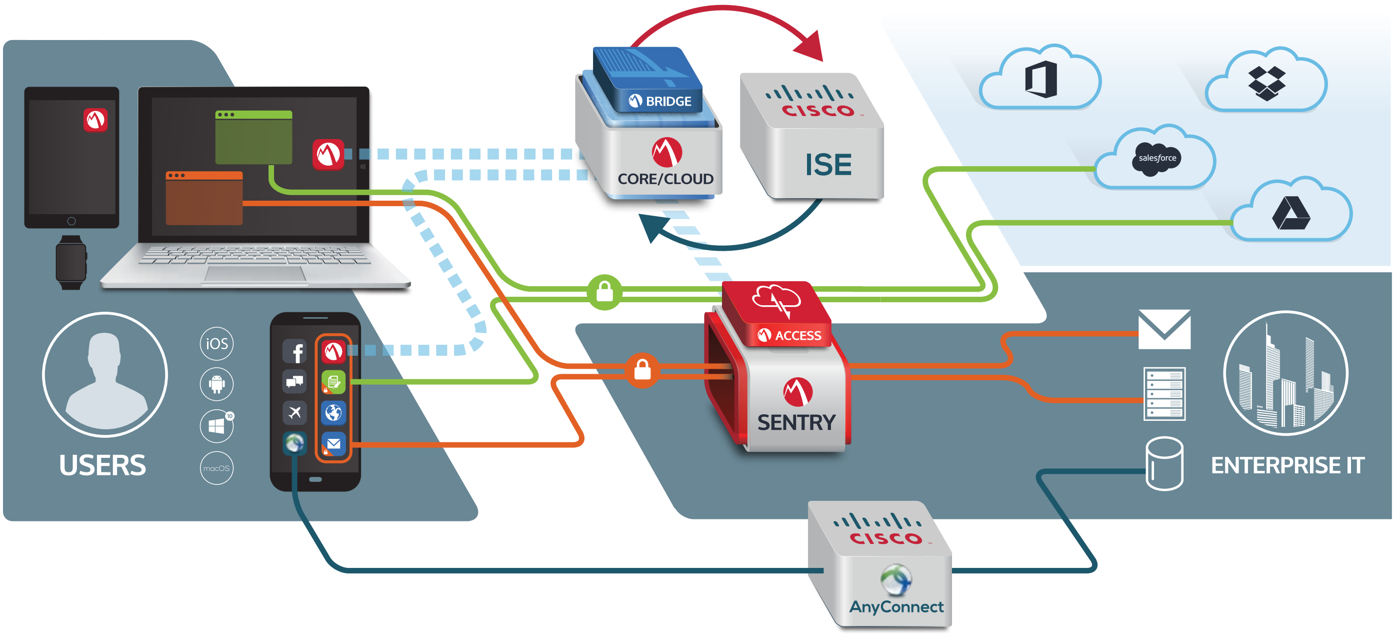
Cisco Identity Services Engine (ISE) integrates with the industry-leading MobileIron platform to bring unprecedented visibility and control to mobile devices. The resulting best-of-breed solution allows mobile device policies to be extended into the network, and network policies to be seamlessly extended to mobile endpoints.

By combining the robust endpoint profiling capabilities of ISE with the comprehensive management capabilities of MobileIron, network and security administrators can identify mobile devices attempting to access the network and take appropriate actions to ensure that the posture of the device is acceptable for the level of access being requested. MobileIron enables ISE to make more intelligent network admission control decisions by providing information about the configuration and security state of mobile devices. This information can be evaluated in ISE authorization policies to provide customized on-boarding processes and granular access controls for mobile users and devices.

Once the mobile devices are granted access to the network, MobileIron continues to monitor and update device posture information so that ISE can dynamically apply the appropriate access controls.

Benefits

- Accelerate enterprise mobility initiatives - whether BYOD (Bring Your Own Device), COPE (Corporate Owned, Personally Enabled), or even CYOD (Choose Your Own Device). Key workflows such as device configuration and policy application and enforcement are automated, enabling organizations to embrace the power of mobile computing while simplifying the end user experience and minimizing IT overhead.
- Prevent unmanaged or non-compliant devices from having access to corporate data by protecting access with detailed policy controls based on ongoing security posture checks.
- Protect your network against data loss on mobile devices by using queries for various device attributes like device registration status, device compliance status, disk encryption status, pin lock status, and jailbreak status.


BRIDGE
CORE/CLOUD
CISCO
ISE
salesforce
iOS
macOS
USERS
ACCESS
SENTRY
ENTERPRISE IT
CISCO
AnyConnect