Cisco ISE – MDM Partner Integration

Overview

The advent of mobile devices in the workforce, such as smartphones and tablets, has created a new class of endpoints that must be secured. This is especially true of non-managed "bring your own device" (BYOD) mobile devices that end users personally own but use to access the enterprise WLAN network. Part of the mobile device security equation is enabling security posture validation and access policy enforcement for mobile endpoints.

The scenario for mobile endpoints is similar to that of traditional computing endpoints – assess the security posture of the endpoint, then assign specific network access based on the results – although the posture attributes assessed in mobile endpoints are different. More importantly, given the high probability of losing a mobile device, it is critical to have PIN-lock or data disk encryption configured for these devices.

Integration between Cisco Identity Services Engine (ISE) and Mobile Device Management (MDM) platforms provides necessary insight into the posture of mobile devices so that companies can enforce appropriate network access policies as required by their IT organizations.

Solution Highlights & Components

The Cisco ISE and MDM solution comprises Cisco ISE with an Advanced Feature License and an MDM platform from one of our integration partners (see list at end of this document). Integration enables posture compliance assessment and network access control of mobile endpoints attempting to access the network. The solution also performs ongoing posture checks to ensure compliance and the correct network access level is maintained. The following are the integration steps:

- Cisco ISE profiles devices as they attempt to access the network. This discovery process provides IT professionals the first step of network visibility.
- Mobile devices are subjected by Cisco ISE to security posture assessment as specified by IT policy.
- Cisco ISE queries for posture information associated with mobile devices as collected by the MDM partner 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 partner platform.
- End users can manage the status of their devices via the Cisco ISE "My Device" portal. Through this portal, end users can lock, suspend, or un-enroll devices if they lose or replace them. Cisco ISE can perform these functions natively or by integration with the MDM partner platforms.

Specific posture attributes collected by the MDM partner platforms for compliance and access policy enforcement in Cisco ISE are:

- Is the mobile device registered with MDM?
- Does the mobile device have disk encryption enabled?
- Does the device have PIN-lock enabled?
- Has the device been jail-broken/rooted?
- Global posture compliance decisions may also be made by the MDM platform instead of Cisco ISE. In this scenario, additional attributes such as blacklisted applications or the presence of an enterprise data container may be checked. The MDM platform reports to Cisco ISE if a device is in compliance or not and then Cisco ISE enforces the appropriate network access policy.

Use Cases

- Only allow MDM-enrolled devices on the network – Cisco ISE queries MDM to check if a device has been enrolled before allowing network access. Un-enrolled devices can be diverted to an enrollment portal.
- Protect against data loss on mobile devices – Cisco ISE queries MDM to ensure PIN-lock and disk encryption are enabled so that if the device is lost, data is not easily accessed. Out of Compliance devices may be diverted to a portal delivering the non-compliance explanation to the end user.
- Ensure devices accessing the network conform to acceptable use policies – Cisco ISE queries MDM to identify if a device has been jail-broken or rooted. When end users have root access to a mobile device, the device is likely in violation of the manufacturer's acceptable use policies and increases the exposure to malware infections. Devices out of compliance may be diverted to a portal delivering the noncompliance explanation to the end user.
- Ensure required applications are installed and blacklisted applications are not installed – MDM partner platforms can perform these application compliance checks and then report a global "in compliance" or "not in compliance" result to Cisco ISE, upon which ISE can enforce the appropriate network access policy. Devices out of compliance may be diverted to a portal delivering the noncompliance explanation to the end user.

Benefits

- Delivers granular policy controls that enable secure network access for mobile devices.
- Single point of network access policy control converges mobile device network access policy with the broader network access footprint delivered by Cisco ISE.
- Translates the deep mobile device insight of MDM into network access policy via Cisco ISE.

Feature & Release Summary

	AirWatch	Citrix	Fiberlink	Good Technology	MobileIron	SAP Afaria	Symantec
ISE Release Version	1.2	1.2	1.2	1.2	1.2	1.2	1.2
MDM Vendor Release Version	6.2	8.0	April 2013 in MaaS360	2.3 (2.1 for clients)	5.5	7 SP3	Symantec App Center 4.1.10
Link to MDM Vendor Collateral on CDN Site	http://marketplace.cisco.com/catalog/companies/airwatch	http://marketplace.cisco.com/catalog/products/4062	http://marketplace.cisco.com/catalog/companies/fiberlink	http://marketplace.cisco.com/catalog/companies/good	http://marketplace.cisco.com/catalog/companies/mobileiron	https://marketplace.cisco.com/catalog/products/4058	http://marketplace.cisco.com/catalog/companies/symantec
Posture/Compliance Enforcement							
Device Registered with MDM	YES	YES	YES	YES	YES	YES	YES
Device in Overall Compliance	YES	YES	YES	YES	YES	YES	YES
Disk Encryption On	YES	YES	YES	YES	YES	YES	YES
PIN Lock On	YES	YES	YES	YES	YES	YES	YES
Jail-Broken/Root Access	YES	YES	YES	YES	YES	YES	YES
Scheduled Periodic Compliance Re-Check	YES	YES	YES	YES	YES	YES	YES
On-Demand Compliance Re-Check	YES	YES	YES	YES	YES	YES	YES
Compliance Failure Handling							
End-User Compliance Failure Reason Messages	YES	YES	YES	YES	YES	YES	YES
Device Actions							
Remote Lock/Suspend	YES	YES	YES	YES	YES	YES	YES
Remote Full Device Wipe	YES	YES	YES	YES	YES	YES	YES
Remote Corporate Data-Only Wipe	YES	YES	YES	YES	YES	YES	YES
Device Info Collected							
Manufacturer	YES	YES	YES	YES	YES	YES	YES
Model	YES	YES	YES	YES	YES	YES	YES
Phone IMEI	YES	YES	YES	YES	YES	YES	YES
Serial #	YES	YES	YES	YES	YES	YES	YES
OS Version	YES	YES	YES	YES	YES	YES	YES
Phone #	YES	YES	YES	YES	YES	YES	YES
MAC Address	YES	YES	YES	YES	YES	YES	YES
Reporting/Notification							
Integrated in Cisco ISE Mobile Device Report	YES	YES	YES	YES	YES	YES	YES

Supported MDM Partners

As of Cisco ISE Release 1.2:

- AirWatch
- Citrix
- Fiberlink
- Good Technology
- MobileIron
- SAP Afaria
- Symantec

For More Information

Additional product information regarding each of MDM partner may be found on the Cisco Developer Network Marketplace site at: http://marketplace.cisco.com/catalog.

C45-726284-04 09/13