Cisco ISE – MDM 合作伙伴集成

概述

随着员工使用移动设备（例如，智能手机和平板电脑）的潮流兴起，形成了一个必须保护的新类型终端。对于那些非受管“自带设备”(BYOD) 移动设备（由最终用户个人拥有，但用于访问企业 WLAN 网络），尤其如此。移动设备安全方案包括对移动终端启用安全状态验证及访问策略实施。

移动终端的安全方案与传统计算终端的安全方案类似 – 评估终端的安全状态，然后根据结果指定特定网络访问权 – 尽管在移动终端中访问的状态属性有所不同。更重要的是，因为移动设备丢失的机率很高，所以为这些设备配置 PIN 锁或数据磁盘加密至关重要。

思科身份服务引擎 (ISE) 与移动设备管理 (MDM) 平台之间的集成使您能够对移动设备的状态有必要的了解，以便公司可根据 IT 部分需要实施相应网络访问策略。

解决方案的亮点和组件

Cisco ISE 和 MDM 解决方案包括一个带有高功能许可证的 Cisco ISE 平台和一个来自我们的某个集成合作伙伴（请参阅本文档结尾的列表）的 MDM 平台。集成允许对尝试访问网络的移动终端启用安全状态合规性评估和网络访问控制。此解决方案还会执行持续的安全状态检查检查以确保合规性，从而保持正确的网络访问级别。以下是集成步骤：

- Cisco ISE 在设备尝试访问网络时对其进行概要分析。此发现过程为 IT 专业人士提供初步的网络可视性。
- Cisco ISE 对移动设备进行由 IT 策略指定的安全状态评估。
- Cisco ISE 查询 MDM 合作伙伴平台收集的与移动设备关联的状态信息。
- Cisco ISE 根据 MDM 合作伙伴平台报告的状态来实施访问策略。可根据思科 ISE 内的特定属性或在相应 MDM 合作伙伴平台内的全局级别（“合规”或“不合规”）构造访问策略。
- 最终用户可以通过 Cisco ISE 的“我的设备”门户网站管理他们的设备状态。通过此门户网站，最终用户可在丢失或更改设备时锁定、暂停或注销设备。Cisco ISE 可在本机执行这些功能，也可通过与 MDM 合作伙伴平台集成进行。

MDM 合作伙伴平台针对 Cisco ISE 中的合规性和访问策略实施收集的特定终端安全评估属性包括：

- 该移动设备是否已向 MDM 注册？
- 该移动设备是否已启用磁盘加密？
- 该设备是否已启用 PIN 锁？
- 是否已解除该设备的限制或已获取该设备的 root 权限？
- 全局终状态合规性决策也可能由 MDM 平台而非思科 ISE 制定。在此情况下，系统可能会检查其他属性，例如，黑名单应用或是否预存了企业数据容器。MDM 平台会向思科 ISE 报告设备是否合规，然后 Cisco ISE 会实施相应的网络访问策略。

用例

- 只允许在网络上使用 MDM 注册设备 – 允许进行网络访问前，Cisco ISE 会向 MDM 查询设备是否已注册。系统会将未注册设备引导至注册门户网站。
- 阻止移动设备上的数据丢失 – Cisco ISE 会向 MDM 查询以确保已启用 PIN 锁和和磁盘加密，以便设备丢失时他人无法轻易访问数据。系统会将不合规设备引导至门户网站，此门户网站会向最终用户显示不合规说明。
- 确保访问网络的设备符合可接受使用策略 – Cisco ISE 会向 MDM 查询以确定是否已解除该设备的限制或已获取该设备的 root 权限。如果最终用户具有对移动设备的 root 访问权，那么该设备可能已违反制造商的可接受使用策略并增加了被恶意软件感染的机会。系统会将不合规设备引导至门户网站，此门户网站会向最终用户显示不合规说明。
- 确保已安装所需应用并且未安装黑名单应用 – MDM 合作伙伴平台可以执行这些应用合规性检查，然后将全局“合规”或“不合规”结果报告给 Cisco ISE，以便 ISE 可实施相应网络访问策略。系统会将不合规设备引导至门户网站，此门户网站会向最终用户显示不合规说明。

好处

- 提供详细策略控制，以确保移动设备的安全网络访问。
- 单点网络访问策略控制将 Cisco ISE 提供的具有更大网络访问范围的移动设备网络访问策略汇集到一起。
- 通过 Cisco ISE 将对 MDM 的深入移动设备洞察转换为网络访问策略。

功能部件和版本摘要

	AirWatch	Citrix	Fiberlink	Good Technology	MobileIron	SAP Afaria	Symantec
ISE 发布版本	1.2	1.2	1.2	1.2	1.2	1.2	1.2
MDM 供应商发布版本	6.2	8.0	2013 年 4 月在 MaaS360 上发布	2.3 （2.1 用于客户端）	5.5	7 SP3	Symantec 应用中心 4.1.10
指向 CDN 站点上的 MDM 供应商宣传资料的链接	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
状态/合规性实施							
已向 MDM 注册的设备	有	有	有	有	有	有	有
整体合规的设备	有	有	有	有	有	有	有
启用磁盘加密	有	有	有	有	有	有	有
启用 PIN 锁	有	有	有	有	有	有	有
突破设备限制/获取 root 访问权限	有	有	有	有	有	有	有
计划定期合规性复查	有	有	有	有	有	有	有
按需合规性复查	有	有	有	有	有	有	有
合规性故障处理							
最终用户合规性故障原因消息	有	有	有	有	有	有	有
设备操作							
远程锁定/暂停	有	有	有	有	有	有	有
远程擦除所有设备数据	有	有	有	有	有	有	有
仅远程擦除公司数据	有	有	有	有	有	有	有
收集到的设备信息							
制造商	有	有	有	有	有	有	有
型号	有	有	有	有	有	有	有
电话 IMEI	有	有	有	有	有	有	有
序列号	有	有	有	有	有	有	有
操作系统版本	有	有	有	有	有	有	有
电话号码	有	有	有	有	有	有	有
MAC 地址	有	有	有	有	有	有	有
报告/通知							
集成在 Cisco ISE 移动设备报告中	有	有	有	有	有	有	有

支持的 MDM 合作伙伴

自 Cisco ISE 版本 1.2 起：

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

更多详情

可在 Cisco Developer Network Marketplace 站点上的以下网址找到有关每个 MDM 合作伙伴的更多产品信息：http://marketplace.cisco.com/catalog。