At-a-Glance

Benefits:

- **Easily authenticate** authorized mobile users securely to access sensitive data.
- **Customize access** policy and intentionally increase or decrease sign on security level as appropriate and enforce additional authentication measures for higher-risk users.
- **Combine credentials** with device posture, location, behavior patterns, and other factors to establish assurance level in real-time during access attempt.

Cisco Identity Services Engine with Identity and Access Management and Single Sign-on Platforms

Easily Authenticate Mobile Users Securely to Sensitive Data

Employees now insist on using mobile devices to work anytime and anywhere to remain productive. More devices mean a continued expansion of the attack surface enterprises need to secure. A delicate balance must be maintained between security and productivity. In addition, enterprises have increased their use of software as a service (SaaS) and virtualization, making it increasingly difficult to securely authenticate and authorize users seeking access to corporate resources.

The integration of the Cisco® Identity Services Engine (ISE) with identity and access management solutions lets you supplement existing authentication and authorization policy attributes with contextual network information. This allows an appropriate level of challenge measures to be taken during the authentication process and enables authentication challenges to adapt to the level of risk so that users can access what they need, when they need it, with a high degree of security, regardless of device type, application environment, or other factors. This level of precision in authentication and application authorization decisions is critical to protect critical data and decrease the risk of a cyberattack.

How Cisco Identity Services Engine Integration with Identity and Access Management and Single Sign on Works

- Cisco ISE leverages pxGrid technology to provide user identity, device and network contextual information to identity and access management solutions.
- Cisco ISE contextual data is used to create policies for user populations or devices, such as policies specific to mobile devices or users regarding what web or cloud-based applications they can access.
- Users of identity and access management partner products can use the Cisco ISE contextual information to decrease authentication challenges and offer a single sign-on capability when appropriate.

Next Steps

To learn more about the Cisco Identity Services Engine, visit http://www.cisco.com/go/ISE.

For additional information regarding Cisco Identity and Access Management partners, visit http://www.cisco.com/c/en/us/products/security/partner-ecosystem.html.

Some of the main attributes available for use by identity and access management platforms for user- and device-related context are:

- **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 mobile device management (MDM) ecosystem partners

C45-732857-02 05/17