Xerox and Cisco Security

Question and Answers

In 2011, Xerox joined forces with Cisco to enhance our MFP hardware and software security as a system to stay ahead of new threats and respond to them more rapidly. We have long placed security as a top priority in the development of our products, and partnering with Cisco to extend our security protection to the network augments our benchmark product security.

The Xerox/Cisco partnership addresses security challenges by leveraging the Cisco® Identity Services Engine (ISE) solution, which helps identify, monitor and manage devices centrally and protects the data paths to and from them. Security is further enhanced via real-time views and control over all users and devices on a network.

1. What is the Xerox and Cisco partnership?

Xerox has always been the leader in bringing security to printers and multifunction devices. Consistent with our continued emphasis on network security and mobility, Xerox has partnered with Cisco, one of the industry's premier IT network leaders.

The core effort of the Xerox and Cisco relationship has resulted in an unprecedented close alignment of Xerox® devices with the popular Cisco Identity Services Engine (ISE). To protect confidential information, companies need to secure network endpoints—such as printers, tablets and webcams—and deploy security policies faster than ever. By allowing IT managers to automatically identify, monitor and manage all devices from a central location, Cisco ISE helps ensure the network path to and from these devices is secure.

What this means to Xerox customers:

The solution enables unprecedented visibility of our printing endpoints, providing the infrastructure to centrally manage and deploy printer security policies and to monitor and enforce compliance. It also increases security and reduces administration overhead by automatically classifying MFPs and printers connecting to the network, granting appropriate network access and "firewalling" printers and preventing printer spoofing.

Cisco's ISE solution recognizes more than 200 Xerox® device models that are ready for security policy enablement. Customers will find that including Xerox® devices in their security policies is simpler and requires much less effort than adding non-Xerox® printing devices.

2. Why Cisco?

Cisco is the market leader in IT networking, as well as in the Network Admission Control (NAC), LAN switching, routing, and authentication, authorization and accounting (AAA) markets. Cisco pioneered the original NAC technology and developed numerous industry standards. Cisco provides the only comprehensive, single-vendor solution available today.

3. What is Cisco® ISE?

The Cisco Identity Services Engine (ISE) is the product for which Xerox has developed printer and MFP support.

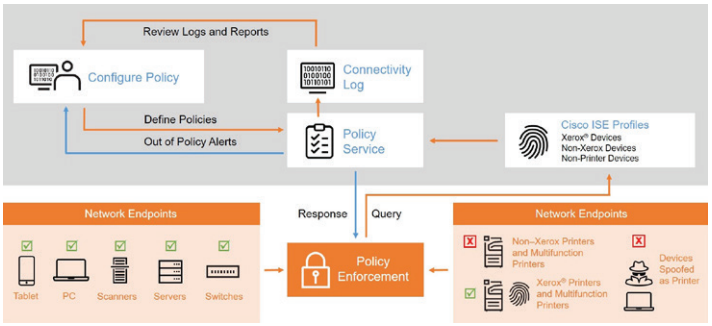
The Cisco Identity Services Engine provides comprehensive visibility via device sensors that are integrated into the infrastructure to automatically detect and classify all devices attaching to the network. Cisco ISE also provides real-time directed endpoint scans, based on policy. This includes dynamic detection and classification of Xerox® print devices to gain more relevant insight and accuracy. This provides the industry's most scalable, reliable and comprehensive view across an entire corporate infrastructure.

4. How does Cisco technology augment the Xerox security story?

Cisco ISE provides a higher level of security for MFPs and printers by automatically discovering them, which facilitates the creation of relevant security policies. These may include limiting network access to only approved print resources, monitoring and auditing print device behavior to prevent spoofing and blocking non-printers from connecting on ports assigned to printers. Cisco ISE guards the access points and paths to the device, and our security solutions protect the data.

In contrast, other print devices may show as a long list of IP and MAC addresses, which presents challenges to utilizing security policies.

Cisco Identity Services Engine



Cisco ISE provides dynamic detection and classification of network endpoints to gain relevant insight and accuracy. As an endpoint attempts to connect to the network, Cisco ISE queries the characteristics of the endpoint and attempts to match it to a known profile in the database. Unknown endpoints only show IP and MAC addresses, while known endpoints like Xerox® devices are identified and provide additional unique attributes. Policy Service performs various actions such as denying connection to out-of-policy endpoints, granting connections to known endpoints (e.g. Xerox) or controlling connectivity of endpoint ports.

To enable the Cisco ISE to function, the network administrator defines the network policies to comply with their organization's security guidelines. Whenever an out-of-policy attempt is made, an alert is generated and sent to the administrator to investigate. To address known or alleged security events, the administrator can utilize logs and reports to remediate if needed.

Xerox® ConnectKey® Technology's comprehensive security is based on four key principles:

Intrusion Prevention—Provides options for customers to ensure only authorized users have access to the device.

Device Detection—Ensures only digitally signed firmware is installed and any attempts to install malware is detected, stopped and reported. Cisco® ISE provides an additional layer of protection at the network level by automatically recognizing Xerox® devices and classifying them as printers/MFPs.

Document and Data Protection—Protects documents and data from unauthorized disclosure or modification.

External Partnerships—Recognizing that no single company can provide security alone, Xerox works with security partners like Cisco and McAfee to wrap their overarching standards around ours. We comply with industry standards such as FIPS 140-2 and measure our performance through stringent certifications like Common Criteria.

5. How do I enable Cisco technology on my MFPs?

With Cisco ISE, Xerox® MFPs and printers are automatically detected and customers can start managing devices immediately.

6. Which devices are supported by Cisco ISE technology?

Cisco's ISE solution ships with a list of more than 200 Xerox® device models that are ready for security policy enablement. Users can also manually create profiles for any new Xerox® products that are available in the future. Please see this site for the current list: www.xerox.com/en-us/connectkey/insights/cisco-ise-printers/devices.

7. So only experts/large enterprises will benefit from Xerox® printer integration with Cisco ISE?

Customers of any size that either have Cisco ISE or are planning to purchase it can benefit from this added endpoint printer integration.

8. Do I need to update the Xerox product installation procedure to support Cisco ISE?

No. Once Xerox® devices connect to the customer network, the Cisco ISE will detect and automatically recognize them as Xerox® devices.

9. What is Cisco TrustSec® and do Xerox® MFPs and printers work with Cisco TrustSec?

Cisco TrustSec technology is embedded in Cisco switches, routers, wireless and security devices such as Cisco ISE. Cisco ISE is used to establish and distribute TrustSec information to the network decision points. TrustSec provides a scalable mechanism for the enforcement of policies. It is a secure network architecture that extends from campus to branch to data center. Cisco TrustSec technology mitigates risk by reducing the attack surface through better segmentation while also increasing operational efficiency and making compliance goals easier to achieve.

For more information about the many security advantages offered by Xerox and about the Xerox partnership with Cisco, along with videos and images, visit **www.xerox.com/en-us/connectkey/printer-security**.

xerox®