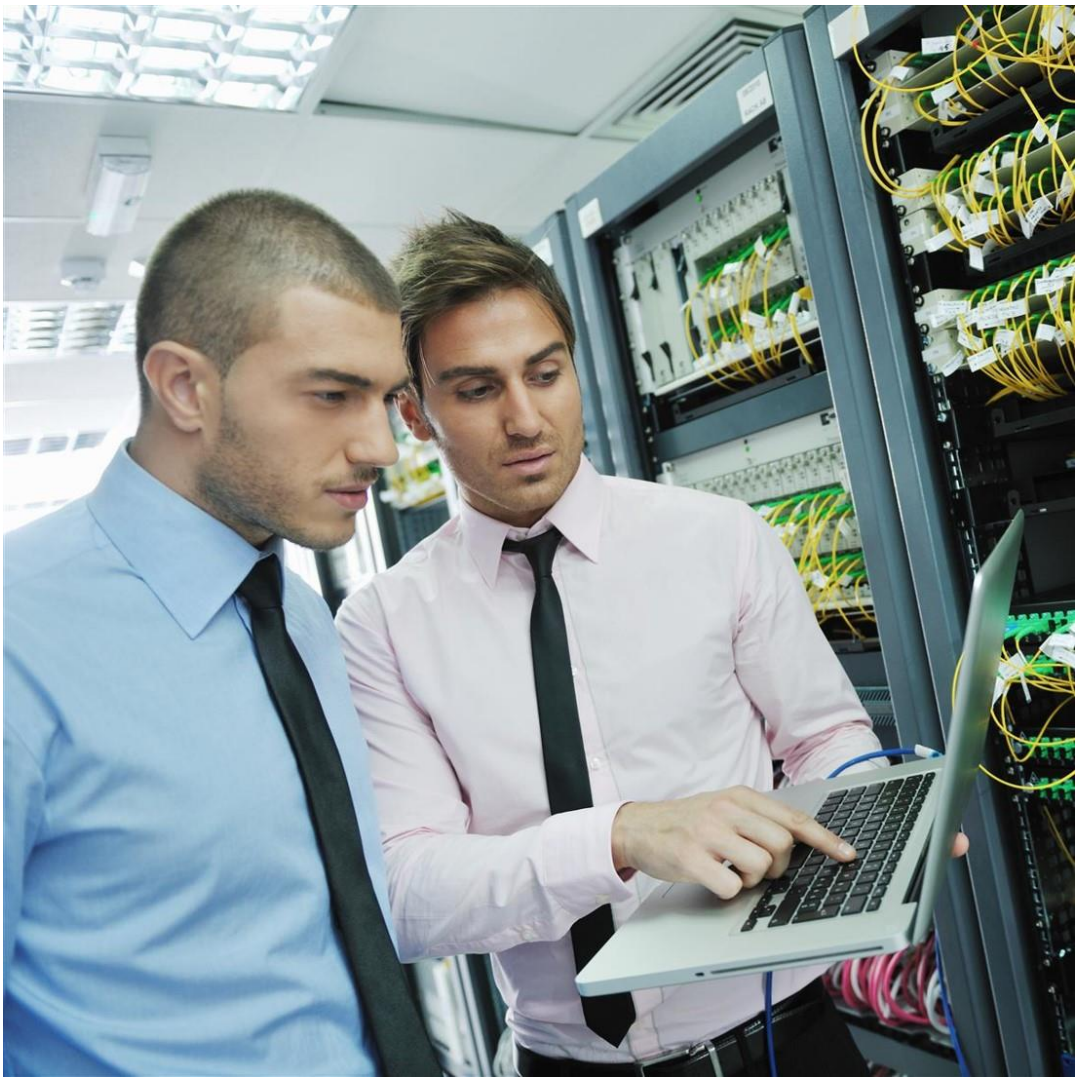


Xerox and Cisco® Identity Services Engine (ISE)

White Paper

Contents

Securing Your Networked Printing Devices

Information security is a vital part of your business. As a leader in the development of digital technology, Xerox has demonstrated a commitment of keeping digital information safe and secure by identifying potential vulnerabilities and proactively addressing them to limit risk. Still, securing information within your devices is not enough in today's data-intensive business world. This is why Xerox has joined forces with Cisco, the worldwide leader in networking technology, to create a comprehensive approach to enhancing your total network security environment.

This white paper is intended to give an overview of that initiative, highlighting the collaboration with the Cisco® Identity Services Engine (ISE) product.

Providing Security in an Internet of Things World

Today, customers recognize Xerox as a trusted provider of secure solutions with a wide array of security capabilities. Xerox® office devices are built with the most comprehensive security in the industry that prevents unauthorized access and protects the confidentiality of documents and data through a robust set of features. Xerox adheres to the highest security standards through industry certifications and our printers are full system Common Criteria certified. Our comprehensive security is based on four key principles:

- Intrusion Prevention
- Device Detection
- Document and Data Protection
- External Partnerships

While Xerox provides comprehensive printer security that protects data sent to and from the printer over the network, many businesses recognize a need to bolster information security outside their devices at a network level.

Our collaboration with Cisco, a worldwide leader in network security, addresses this challenge, taking information security beyond your device to enhance security across your total network environment. This comprehensive solution is based on the Cisco Identity Services Engine.

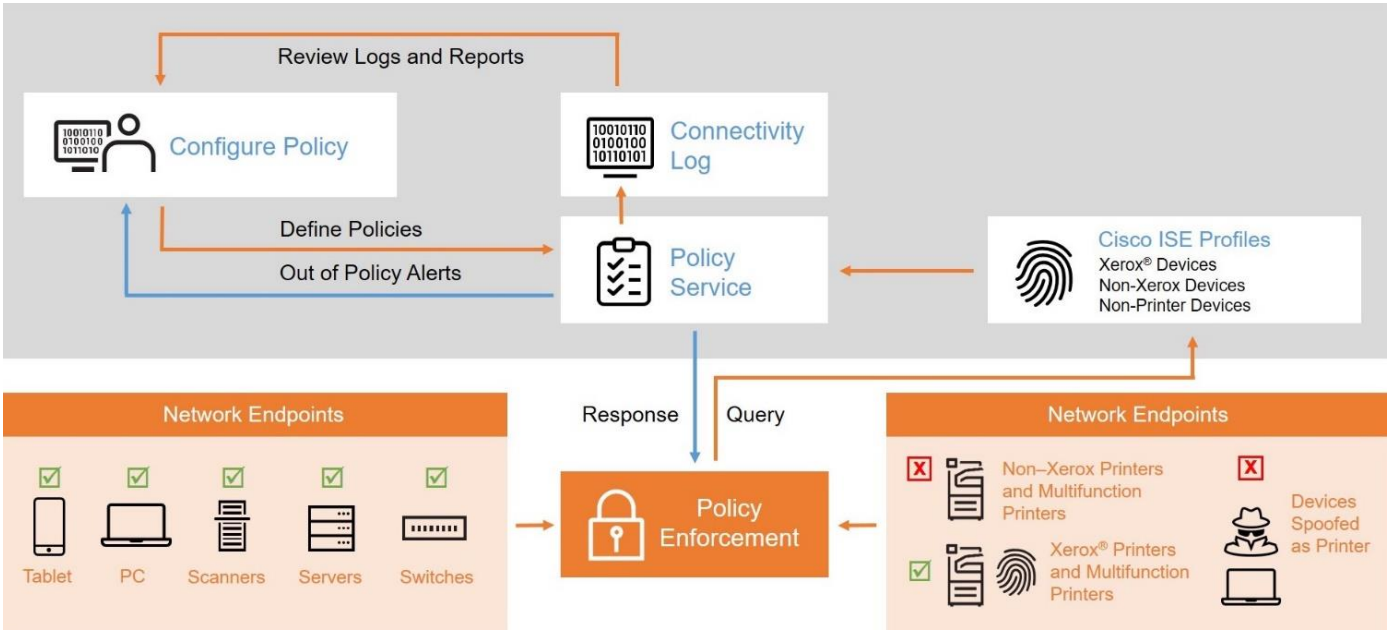
Cisco® ISE: A Powerful, Simple and Scalable Solution

Cisco ISE is the market-leading intelligent security policy enforcement platform that mitigates security risks by providing a complete view of which users and what devices are being connected across the entire network infrastructure. It also provides exceptional control over what users can access on your network and where they can go. The solution, including all of its components, has been thoroughly vetted and rigorously tested as an integrated system.

Cisco's ISE includes over 200 Xerox® device profiles that are ready for security policy enablement. This allows ISE to automatically detect Xerox® devices in your network. Xerox® devices are organized in Cisco ISE under product families, such as Xerox® AltaLink® and Xerox® VersaLink®, enabling Cisco ISE to automatically detect and profile new Xerox® devices from the day they are released. Customers who use Cisco ISE find that including Xerox® devices in their security policies is simpler and requires minimal effort.

With Cisco ISE, Xerox has elevated the multifunction device to have the same level of network manageability as the more traditional endpoints such as servers, routers and PCs. Xerox is making the multifunction printer (MFP) a "true network citizen" and allowing you to protect it as an integral part of today's security imperatives.

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.

SEAMLESS DEVICE PROFILING HELPS YOU CREATE ACCESS LEVELS.

Cisco ISE Profiling Services provides dynamic detection and classification of endpoints connected to the network. ISE collects various attributes for each network endpoint to build an endpoint database. The classification process matches the collected attributes to prebuilt or user-defined conditions, which are then correlated to an extensive library of device profiles. These profiles include a wide range of device types, including tablets, smartphones, cameras, desktop operating systems (for example, Windows®, Mac® OS X®, Linux® and others) and workgroup systems such as Xerox® printers and MFPs.

Once classified, endpoints can be authorized to the network and granted access based on their profile signature. For example, guests to your network will have a different level of access to printers and other endpoints in your network. As an example, you and your employees can get full printer access when accessing the network from a corporate workstation but be granted limited printer access when accessing the network from a personal Apple® iPhone®.

CISCO ISE ALLOWS YOU TO DEPLOY THE FOLLOWING CONTROLS AND MONITORING OF XEROX® DEVICES

- Automatically provision and grant network access rights to printers and MFPs to prevent inappropriate access (including automatically tracking new printing devices connecting to the network):
  - Block non-printers from connecting on ports assigned to printers
  - Prevent impersonation (aka spoofing) of a printer/MFP
  - Automatically prevent connection of non-approved print devices
  - Smart rules-based policies to govern user interaction with network printing devices
- Provide simplified implementation of security policies for printers and MFPs by:
  - Providing real-time policy violation alerts and logging
  - Enforcing network segmentation policy
  - Isolating printing devices to prevent general access to printers and MFPs in restricted areas
- Automated access to policy enforcement
- Provide extensive reporting of printing device network activity

A few real-life examples of these controls were demonstrated during an ISE pilot at Xerox:

- Automatically discovered and identified all network printing devices connected to the network on selected floors
- Configured network wall jacks to only allow a specific MFP and reject all other network-enabled devices
- Restricted access to network printing devices; configured ISE to only allow users connected in one floor to access that MFP but blocked users connecting from other floors
- Controlled network printing devices in a given area to only scan to a given file location in the network
- Customized the level of network printing devices' access assigned to visitors and BYOD users to have different access level than users on company-issued desktop

READY TO DEPLOY ACROSS YOUR ENTIRE FLEET OF XEROX® DEVICES

Xerox has made it extremely easy to achieve an outstanding level of control with Cisco® ISE. Xerox and Cisco engineers worked together to validate over 200 Xerox® devices to work with ISE. When you buy Cisco ISE, you are ready to start deploying access and control policies across your Xerox® MFP and printer fleet. You do not have to configure ISE to work with Xerox® products and validate that all the device settings were entered correctly; we have done all of that for you ahead of time. Figure 1 illustrates an ISE screen that displays some of the Xerox® devices available for policy creation. The ISE Feed Service from Cisco keeps you informed of new Xerox® products and automatically adds them to your ISE solution in the proper product family.

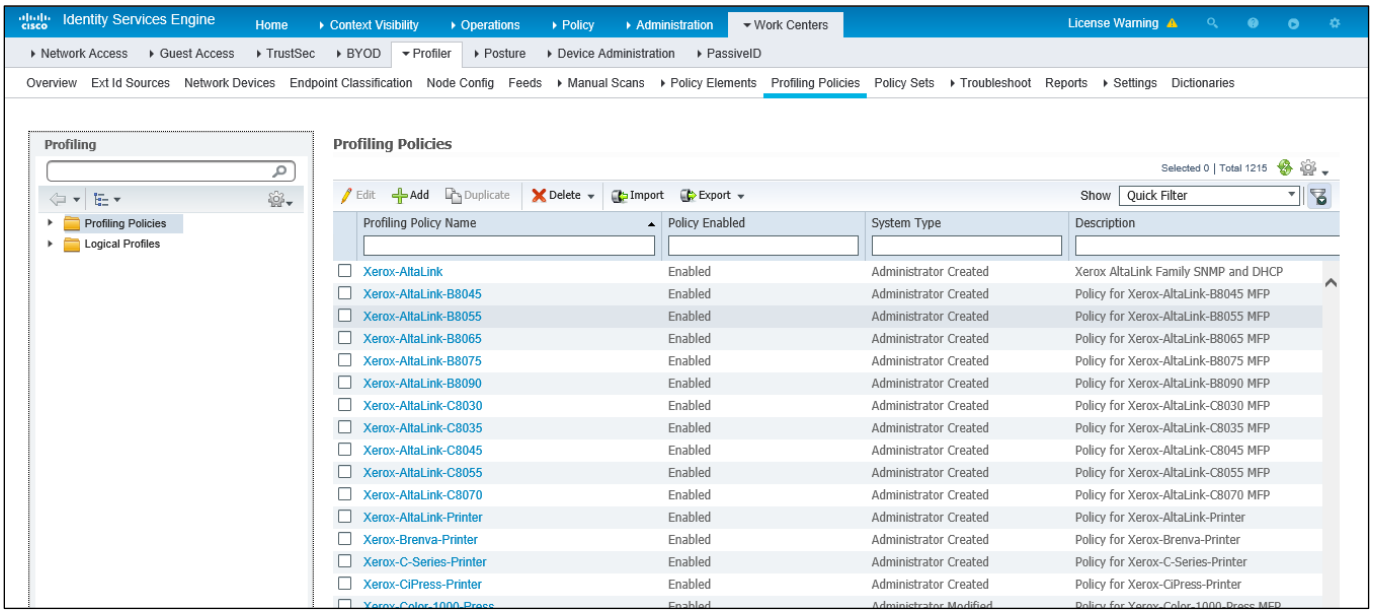


Figure 1: Over 200 Xerox® devices ready for policy implementation right out of the box.

Writing policies could not be easier. You can write policies for each individual device in the network or aggregate policies into logical groups (Figure 2 below). You can then apply access and security rules at the policy levels.

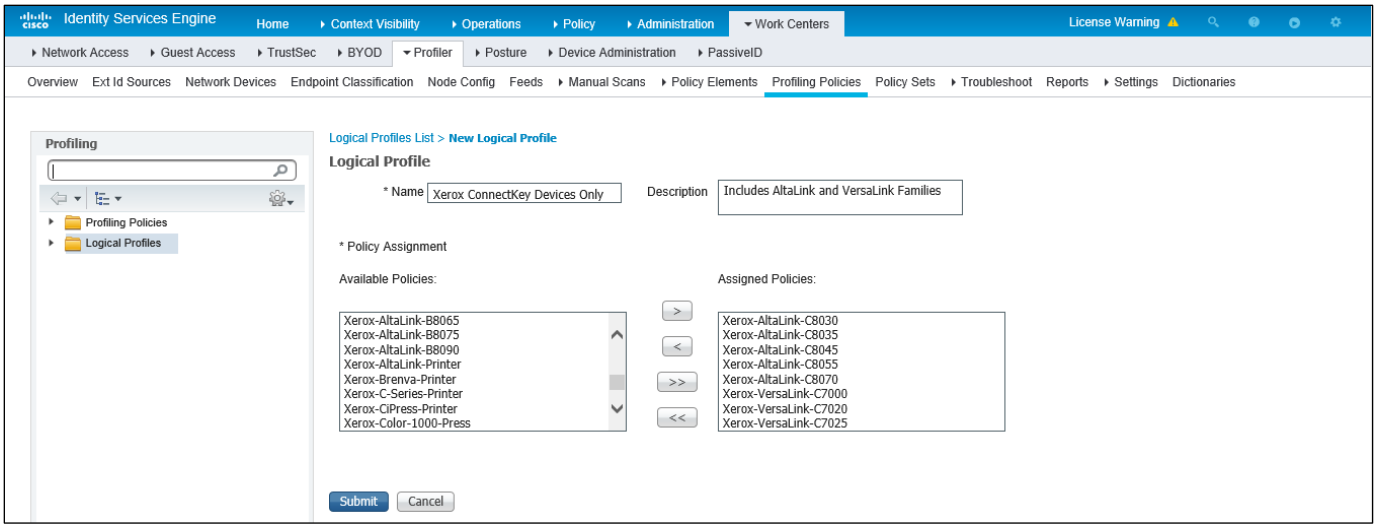


Figure 2: Logical Profile of "Xerox® ConnectKey® Devices Only", which groups all Xerox® AltaLink® and Xerox® VersaLink® devices and policies.

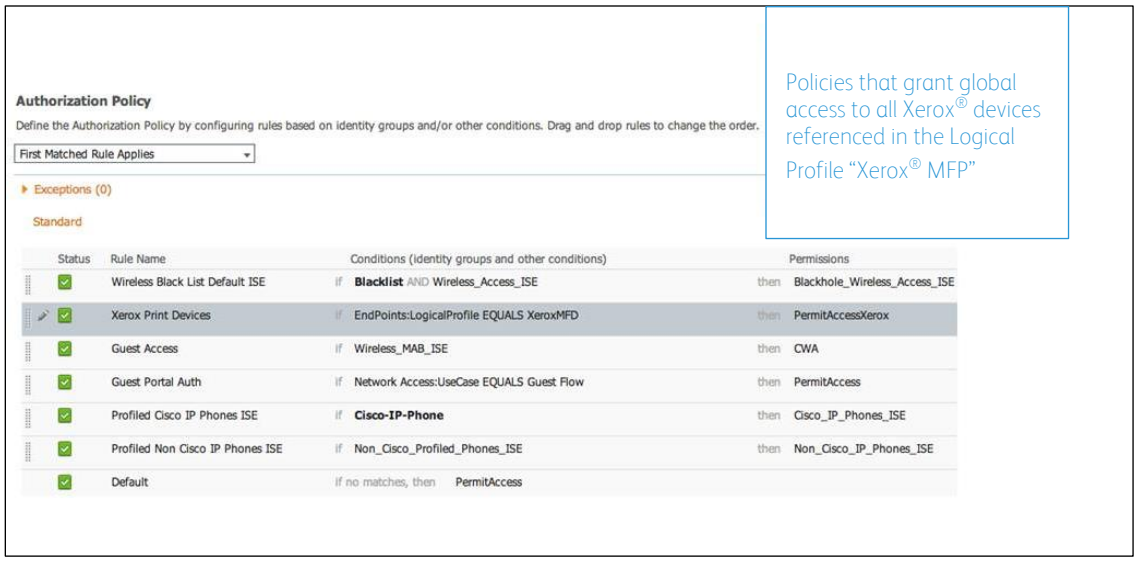


Figure 3: Permit Access Xerox is a customized policy to authorize all Xerox® devices in the "Xerox MFP" Logical Profile.

Collaborate with Confidence with Xerox and Cisco

OBTAIN REAL-TIME VISIBILITY INTO WHO AND WHAT IS ACCESSING THE NETWORK.

Ninety percent of surveyed organizations are not "fully aware" of the devices accessing their network. Moreover, 40 % of network/endpoint infrastructure can become unknown or unmanaged when an organization lacks visibility, which can drive operational costs and lead to security blind spots. But with Xerox® devices integrating with Cisco® ISE, you now have comprehensive, real-time visibility into which people and what devices are connecting across the entire network infrastructure.

ENSURE THAT YOUR ACCESS AND SECURITY POLICIES ARE ENFORCED.

As the number of connected devices that are accessing your network grows, creating access policies for different end users (i.e., guest, employee, BYOD) can be a cumbersome and time-consuming process. Additionally, if an infected device penetrates your network, it is critical to have the ability to quickly segment your network to prevent threats from spreading laterally across your network.

Our integration with Cisco ISE allows users to collaborate and print securely in your enterprise while confidently protecting against the security risks brought about by the explosion of network-connected devices. Cisco ISE empowers you to define customized access control over your diverse user populations.

ACHIEVE GREATER VALUE WHILE MANAGING PRINT.

Xerox® Managed Print Services (MPS) delivers customers great value by controlling your printing costs while delivering value-added document services. MPS leverages Cisco ISE to deliver access control, visibility and enhanced security to your network printing devices.

Cisco ISE is relevant to a wide range of our customers. Cisco ISE can help implement corporate governance through consistent access policy for all users and devices, addressing mandated monitoring, auditing and reporting requirements. And whether you're a mid-size organization needing to secure a hundred endpoints or a large enterprise with hundreds or thousands of endpoints, ISE is a scalable solution that can grow with your changing needs.

Together, they dramatically reduce cost of ownership while delivering world-class monitoring and troubleshooting features designed to streamline operations for your help desk and support teams. Automating labor-intensive tasks, such as provisioning access policy and network segmentation, has the added benefits of saving time, reducing costs and simplifying service delivery. This gives you greater flexibility to shift IT resources from office print monitoring to mission-critical business assignments. It's just another way that Xerox and Cisco help you get the most out of your networked printing devices and IT resources. The bottom line: your network, content and printing costs are protected.

Xerox® Devices Currently Profiled in Cisco® ISE

https://www.xerox.com/en-us/connectkey/insights/cisco-ise-printers/devices

References

- Xerox and Cisco Security Frequently Asked Questions (FAQ)
  http://www.office.xerox.com/latest/SECFS-06U.PDF
- Cisco® ISE Overview
  http://www.cisco.com/en/US/products/ps11640/index.html
- Cisco® ISE Profiling Design Guide
  https://communities.cisco.com/servlet/JiveServlet/previewBody/68156-102-1-125076/How-To_30_ISE_Profiling_Design_Guide.pdf

Authors

- Doug Tallinger, Platform Planning Manager, Xerox Corporation
- Zia Masoom, Product Marketing Manager, Xerox Corporation
- Kevin Gagnon, Product Manager, Cisco Systems
- Ed Cho, Marketing Manager, Cisco Systems