Cisco ISE Passive Identity Connector

The Cisco® ISE Passive Identity Connector consolidates multiple sources of authentication data into a single source of truth. It simplifies the installation of Cisco security products, and it offloads work from key infrastructure.

Product Overview

Username is a key element in determining access to a network. Username can also help you alert you users to potentially suspicious activity with their devices. It answers the all-important question of who is connected to your network.

The Cisco Identity Services Engine (ISE) Passive Identity Connector centralizes, consolidates, and distributes identity information, including IP addresses, MAC addresses, and usernames. At the same time it offloads work from key infrastructure such as Microsoft Active Directory.

Many servers on the network are active participants in user authentication. They take user credentials and either verify them or look them up in a dedicated repository such as Active Directory. Rather than being actively involved in user authentication, the Passive Identity Connector listens to the various authentication servers on the network. It centralizes the authentication information, becoming the single source of truth for its subscribers.

The Passive Identity Connector distributes the session identity information to other devices on the network that are natural consumers of such information. These devices include firewalls, web security appliances, and traffic analyzers. Using the Cisco Platform Exchange Grid (pxGrid), the Cisco ISE Passive Identity Connector can support up to 20 subscribers.

Features and Benefits

Feature	Benefit
Centralized information	Consolidates data from multiple authentication sources, eliminating the need for every system that requires authentication data to interact with every authentication source
Improved performance	Eliminates the burden on an often-overtaxed infrastructure with a single system that caches data for other authentication data consumers
Syslog server support	Gathers authentication data from systems that support syslog
Active Directory support	Gathers authentication data from Active Directory through the Microsoft Windows Management Interface (WMI)
Kerberos SPAN support	Gathers Active Directory authentication data from switches supporting Kerberos SPAN
Endpoint probes	Understands when endpoints log off
Active Directory agent	Gathers authentication data from up to 10 Microsoft Active Directory domain controllers
Support for custom APIs	Gathers authentication data from systems that support a custom interface
Citrix Terminal Server support	Gathers authentication data from Citrix Terminal Server
High availability	Supports active/passive redundancy

Feature	Benefit
Migration support	Customers may upgrade from the Cisco ISE Passive Identity Connector to Cisco ISE, adding the Passive Identity Connector node to an existing Cisco ISE cluster.
Virtual machine support	Supports KVM, VMware, and Hyper-V
Scalability	Tailored to fit your organization with support for 3,000 and 300,000 sessions

Microsoft Active Directory Integration

The Cisco ISE Passive Identity Connector can gather session data from many authentication servers on the network but arguably none is more important than the Microsoft Active Directory. The Passive Identity Connector can gather information from up to 100 domain controllers either using the Microsoft Windows Management Interface (WMI), through a Cisco Active Directory agent installed on each domain controller, through the use of a switched port analyzer (SPAN) port, or through syslog. The Microsoft WMI interface has the advantage of not requiring any additional software to be installed on the domain controllers. The Active Directory agent can gather information from up to 10 domain controllers. It requires no configuration changes on the domain controller and can be installed on either a domain controller or a member server.

For those who want to limit the load on their Active Directory infrastructure or who simply want a quick and easy way to retrieve data without having to configure the Active Directory, the Cisco ISE Passive Identity Connector offers the ability to gather session data through the use of a SPAN port. SPAN sniffs network traffic, specifically examining Kerberos messages. It extracts user identity information also stored by the Active Directory and sends that information to the Passive Identity Connector.

Predefined and User-Definable Syslog Parsers

There are numerous sources of identity on the network and countless ways to interface with them, creating an impossible combination. The Cisco ISE Passive Identity Connector overcomes this challenge by providing a generic syslog parser. Customers can point syslog agents on the authentication servers to the Passive Identity Connector for it to parse out the identity information.

The syslog parser can support both a countless variety of syslog message formats by using regular expressions to tease out the syslog messages containing authentication information. Different header types are also no problem for the Passive Identity Connector, which uses the same regular expression capability for the headers as well. In addition to a generic syslog parser, the Passive Identity Connector provides predefined parsers, including those from Cisco ISE, the Cisco Secure Access Control System (ACS), the Cisco Adaptive Security Appliance (ASA) VPN, Aerohive, BlueCat, Blue Coat, F5 VPN, InfoBlox, Lucent QIP, Nortel VPN, and Safe Connect.

Application Programming Interface

The Cisco ISE Passive Identity Connector provides a custom API for applications that publish session data but not using syslog.

Terminal Server Support

The Cisco ISE Passive Identity Connector provides the ability to gather session information from a Citrix terminal server environment by using an agent installed on the terminal server.

Standalone and High-Availability Configurations

The Cisco ISE Passive Identity Connector can operate standalone or may be paired with a second virtual machine for high availability. The primary updates the secondary in the high-availability configuration operating in an active/passive environment.

Hardware Solutions

Customers looking for a hardware solution from Cisco may purchase the Secure Network Server (SNS) 3515 or 3595 Appliances with Cisco ISE version 2.2 or later. The SNS 3515 can support up to 100,000 sessions, and the SNS 3595 can support up to 300,000 sessions.

Upgrades to ISE

Customers may upgrade from the Cisco ISE Passive Identity Connector to Cisco ISE by adding the Passive Identity Connector node to an existing Cisco ISE cluster. Customers may also upgrade the Passive Identity Connector to a standalone Cisco ISE instance with the appropriate licenses. This is all accomplished through the installation of licenses and does not require any additional software to be installed. You can thus protect your investment as your business needs expand and do so without a substantial investment from the IT staff.

Product Specifications

Maximum number of Microsoft Active Directory domain controllers supported using WMI or an Active Directory agent	100
Maximum recommended number of Microsoft Active Directory domain controllers supported per Active Directory agent when installed on a Microsoft Active Directory domain controller	1
Maximum recommended number of Microsoft Active Directory domain controllers supported per Active Directory agent when installed on a member server	10
Maximum number of pxGrid subscribers	20
Maximum number of nodes per Cisco ISE Passive Identity Connector cluster	2
Maximum number of REST API providers	50
Maximum number of syslog clients	50
Maximum number of SPAN ports	1 with a single standalone machine, 2 in a high-availability cluster

System Requirements

Hypervisor	VMware version 8 for ESXi 5.x, VMware version 11 (default) for ESXi 6.x, KVM on Red Hat Enterprise Linux 7.0, or Microsoft Hyper-V
CPU	6 cores; 2.0 GHz or faster – up to 100,000 sessions 8 cores; 2.0 GHz or faster – up to 300,000 sessions
Memory	16 GB – up to 100,000 sessions 64 GB – up to 300,000 sessions
Disk	Minimum 200 GB

Ordering Information

The Passive Identity Connector Q&A will help you understand ISE passive identity and the licensing types that will best serve the needs of your organization. To place an order, visit the Cisco ordering homepage. To download the ISE Passive Identity Connector software, visit the Cisco Software Center.

Part #	Product Description
R-ISE-PIC-VM-K9=	ISE Passive Identity Connector 3,000 session Virtual Machine
L-ISE-PIC-UPG=	ISE Passive Identity Connector – upgrade to maximum 300,000 sessions

Warranty Information

The Cisco ISE Passive Identity Connector has a 90-day limited liability warranty. Warranty information can be found at: http://www.cisco.com/go/warranty.

Cisco and Partner Services

Cisco offers a wide range of service programs. These innovative programs are delivered through a combination of people, processes, tools, and partners that results in high levels of customer satisfaction. Cisco Services help you protect your network investment, optimize network operations, and prepare your network for new applications to extend network intelligence and the power of your business. For more information about Cisco Services, see Cisco Technical Support Services or Cisco Security Services. For more information, please visit http://www.cisco.com/go/services.

Cisco Capital

Financing to Help You Achieve Your Objectives

Cisco Capital® financing can help you acquire the technology you need to achieve your objectives and stay competitive. We can help you reduce CapEx. Accelerate your growth. Optimize your investment dollars and ROI. Cisco Capital financing gives you flexibility in acquiring hardware, software, services, and complementary third-party equipment. And there's just one predictable payment. Cisco Capital is available in more than 100 countries. Learn more.

For More Information

For more information about the Cisco ISE solution, visit http://www.cisco.com/go/ise or contact your local account representative.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C78-738846-00 04/17