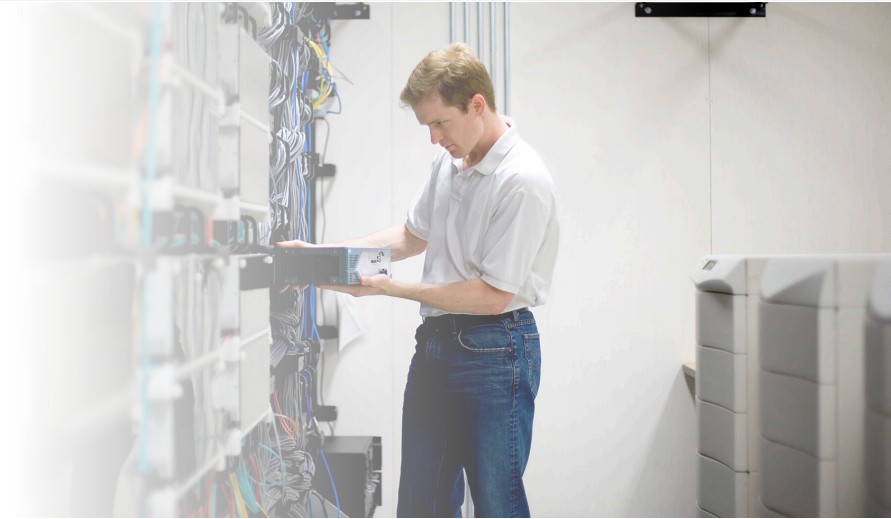


Cisco ISE Passive Identity Connector



General

Q What is the Cisco® ISE Passive Identity Connector?

A The Cisco ISE Passive Identity Connector is designed to gather authentication data from numerous sources of information in the data center, consolidate the authentication data into a single source of truth, and disseminate it to its subscribers.

Q Why not have the subscribers gather the authentication data from the sources in the data center?

A That would make perfect sense if one or two systems were gathering authentication data from the data center, but it does not scale. The Cisco ISE Passive Identity Connector reduces the burden on the authentication servers in the data center and on the subscriber systems. It also reduces the burden on the IT staff, which doesn't have to configure the details of multiple authentication servers on the subscriber systems, not to mention dealing with the different user interfaces and functionalities that are bound to creep into the mix.

Q How does the Cisco ISE Passive Identity Connector compare with the Cisco Identity Service Engine?

A The Passive Identity Connector offers a subset of the functionality of the Cisco Identity Services Engine. It supports only the passive ID functionality contained in the Identity Services Engine.

Q How does the Cisco ISE Passive Identity Connector compare with the Cisco Context Directory Agent?

A The Passive Identity Connector is designed to support a variety of authentication sources and to provide investment protection by offering additional services with an upgrade to the Cisco Identity Services Engine.

Q I have the Cisco Identity Services Engine in production today. Does it support the passive identity capabilities of the Cisco ISE Passive Identity Connector?

A Yes, the Passive Identity Connector functionality is contained in the Cisco Identity Services Engine starting with version 2.2.

Q Does the Cisco ISE Passive Identity Connector support RADIUS, guest, profiling, and posture functionality?

A No, the Passive Identity Connector does not offer any additional functionality beyond passive ID.

Q How does the Cisco ISE Passive Identity Connector gather data from other servers in the data center?

A The Passive Identity Connector gathers information from the Microsoft Active Directory environment using the Microsoft Windows Management Interface or the Active Directory agent, or through a switched port analyzer (SPAN) port on a switch. It can also gather authentication information through syslogs, a Citrix terminal server agent, and a custom API.

Q What is the maximum number of sessions supported by the Cisco ISE Passive Identity Connector?

A The Passive Identity Connector can be licensed to support up to 300,000 sessions.

Q Can the Cisco ISE Passive Identity Connector be clustered to scale beyond 300,000 sessions?

A No, it is not capable of scaling by linking multiple machines together.

Q How does the Cisco ISE Passive Identity Connector know when a user logs off?

A The Passive Identity Connector supports a Microsoft Windows endpoint probe that checks each endpoint every 4 hours. It also has a configurable session timeout.

Microsoft Active Directory

Q What is the maximum number of Microsoft Active Directory domain controllers that the Cisco ISE Passive Identity Connector can support?

A The Passive Identity Connector is limited to a maximum of 100 domain controllers.

Q What technologies can the Cisco ISE Passive Identity Connector leverage to gather authentication data from Microsoft Active Directory domain controllers?

A The Passive Identity Connector can leverage the Microsoft Windows Management Interface (WMI), an Active Directory agent installed on a domain controller, or an Active Directory agent installed on a member server. It can also gather Kerberos data from a SPAN port on a switch.

Q What are the advantages of installing an Active Directory agent on a server that is a member of a given domain?

A The Cisco ISE Passive Identity Connector can monitor up to 10 domain controllers when the Active Directory agent is installed on a domain member server.

Q What are the advantages of using the Microsoft WMI interface with the Cisco ISE Passive Identity Connector?

A No software is installed on the domain controller when using the Microsoft WMI interface.

Q What are the advantages of installing an Active Directory agent directly on a domain controller?

A The Active Directory agent is a native Windows application and thus the most efficient way to monitor a domain controller.

Q When would it be beneficial to use a SPAN port in lieu of either the Microsoft WMI or an Active Directory agent?

A A SPAN port is recommended when the Microsoft Active Directory domain infrastructure is heavily burdened and is unable to support any additional load.

Q How many SPAN ports are supported by the Cisco ISE Passive Identity Connector?

A The Passive Identity Connector supports one SPAN port when configured in standalone mode and two SPAN ports when configured in high-availability mode.

Syslog Parser

Q Does the Cisco ISE Passive Identity Connector support both User Datagram Protocol (UDP) and Transport Control Protocol (TCP) syslogs?

A Yes, it can consume both UDP and TCP syslogs.

Q Does the Cisco ISE Passive Identity Connector support the creation of custom syslog templates?

A Yes.

Q Does the Cisco ISE Passive Identity Connector come with any syslog templates out of the box?

A Yes, the Passive Identity Connector supports the following templates out of the box: Cisco Access Control Server (ACS), Cisco Adaptive Security Appliance (ASA), Cisco Identity Services Engine (ISE), Aerohive, BlueCat, DHCPD, F5 VPN, InfoBlox, Lucent QIP, Microsoft Active Directory DHCP, Nortel VPN, and SafeConnect NAC.

Q Can the Cisco ISE Passive Identity Connector support different syslog headers?

A Yes, both the header and the body of the syslog message can be customized as part of an individual syslog template.

High Availability

Q Does the Cisco ISE Passive Identity Connector offer a high-availability configuration?

A Yes, the Passive Identity Connector can be used in either a standalone configuration or as part of a high-availability pair.

Q Is the Cisco ISE Passive Identity Connector active/active or active/passive when operating in high-availability mode?

A The Passive Identity Connector operates in high-availability mode using an active/passive concept. The primary node is active with the secondary node as a hot standby.

Q What is the maximum number of sessions that a Cisco ISE Passive Identity Connector can support when it is configured for high availability?

A A Passive Identity Connector that is licensed for up to 3000 sessions will support 3000 sessions in either standalone or high-availability mode. A Passive Identity Connector licensed for up to 300,000 sessions will support 300,000 sessions in either standalone or high-availability modes.

Orders and Upgrades

Q How is the Cisco ISE Passive Identity Connector offered?

A It is offered in a virtual machine form factor.

Q How is the Cisco ISE Passive Identity Connector licensed?

A The Passive Identity Connector license is for up to 3000 sessions. There is an upgrade license for up to 300,000 sessions.

Q Does Cisco offer the Cisco ISE Passive Identity Connector as a hardware solution?

A No, the Passive Identity Connector is offered only as a virtual machine. If you would like a hardware solution from Cisco, you need to purchase the Cisco Identity Services Engine. The Cisco Identity Services Engine is offered as either a virtual or a physical appliance.

Q Can the Cisco ISE Passive Identity Connector be converted to the Cisco Identity Services Engine at a later point in time?

A Yes, a Passive Identity Connector licensed for 300,000 sessions may be joined to an existing Identity Services Engine cluster. A 300,000-session Passive Identity Connector may be used as the basis for a new Identity Services Engine cluster by adding Identity Services Engine Base licenses.

Q What are the Cisco ISE Passive Identity Connector part numbers and configurations?

A Below please find a table with the different part numbers, and configurations:

	Standalone	High Availability
Up to 3,000 sessions	Qty 1 – R-ISE-PIC-VM-K9=	Qty 2 – R-ISE-PIC-VM-K9=
Up to 300,000 sessions	Qty 1 – R-ISE-PIC-VM-K9= Qty 1 – L-ISE-PIC-UPG=	Qty 2 – R-ISE-PIC-VM-K9= Qty 2 – L-ISE-PIC-UPG=

Q Does the Cisco ISE Passive Identity Connector come with a trial license?

A Yes, it comes with a 90-day trial license.