Introduction to ISE-PIC

User identities must be authenticated in order to protect the network from unauthorized threats. To do so, security products are implemented on the networks. Each security product has its own method of retrieving the necessary authentication, often identifying authorized IP addresses, rather than authorized users. As a result, these products refer to different external servers and methods that provide authentications based on user login information, resulting in a de-centralized network. Cisco Identity Services Engine (ISE) Passive Identity Connector (ISE-PIC) offers a centralized installation and implementation enabling you to simply gather passive authentication data from a variety of sources and share those identities with security product subscribers.

Cisco ISE-PIC Terminology

This guide uses the following terms when discussing Cisco ISE-PIC:

Term	Definition
GUI	Graphic user interface. GUI refers to any of the screens and tabs in the software installation of ISE-PIC.
NIC	Network interface card.
Node	An individual physical or virtual Cisco ISE-PIC appliance.
PAN	The main node in your ISE-PIC deployment is the primary administration node (PAN) and this is the node from which you can perform all available actions. In ISE-PIC, you can install up to two nodes. If you install the second node, it is referred to as the secondary administration node (secondary PAN).

Term	Definition
Parser	The ISE-PIC backend component that receives syslog messages and breaks that input up into parts that can then be managed, mapped and published to ISE-PIC. The parser goes through each line of information of a syslog message as it arrives, looking for key information. For example, if a parser is configured to look for “mac=”, the parser then parses each line while looking for that phrase. The parser is set up to then communicate the defined information to ISE once it has found the key phrase that was configured.
Primary node	The main node in your ISE-PIC deployment is the primary administration node (PAN) and this is the node from which you can perform all available actions. In ISE-PIC, you can install up to two nodes. If you install the second node, it is referred to as the secondary administration node (secondary PAN).
Probe	Probes are mechanisms that collect data from a given source. Probe is a generic term that describes any mechanism, but does not specifically describe how the data is collected or what is collected. For example, an Active Directory (AD) probe helps ISE-PIC collect data from AD while a syslog probe collects data from a parser that reads syslog messages.
Provider	Clients or sources from which ISE-PIC receives, maps and publishes user identity information.
Secondary node	The main node in your ISE-PIC deployment is the primary administration node (PAN) and this is the node from which you can perform all available actions. In ISE-PIC, you can install up to two nodes. If you install the second node, it is referred to as the secondary administration node (secondary PAN).
Subscriber	Systems that subscribe to the ISE-PIC services in order to receive user identity information.

ISE-PIC Overview

Passive Identity Connector (ISE-PIC) offers a centralized, one-stop installation and implementation enabling you to easily and simply configure your network in order to receive and share user identity information with a variety of different security product subscribers such as Cisco Firepower Management Center (FMC) and Stealthwatch. As the full broker for passive identification, ISE-PIC collects user identities from different provider sources, such as Active Directory Domain Controllers (AD DC), maps the user login information to the relevant IP addresses in use and then shares that mapping information with any of the subscriber security products that you have configured.

Note For information about the FMC and Stealthwatch releases that are validated with ISE, see *Cisco Identity Services Engine Network Component Compatibility*.

What is Passive Identity?

Products such as the Cisco Identity Services Engine (ISE), which provide an authentication, authorization and accounting (AAA) server, and utilize technologies such as 802.1X or Web Authentication, communicate directly with the user or endpoint, requesting access to the network, and then using their login credentials in order to verify and actively authenticate their identity.

Passive identity services do not authenticate users directly, but rather gather user identities and IP addresses from external authentication servers such as Active Directory, known as providers, and then share that information with subscribers. ISE-PIC first receives the user identity information from the provider, usually based on the user login and password, and then performs the necessary checks and services in order to match the user identity with the relevant IP address, thereby delivering the authenticated IP address to the subscriber.

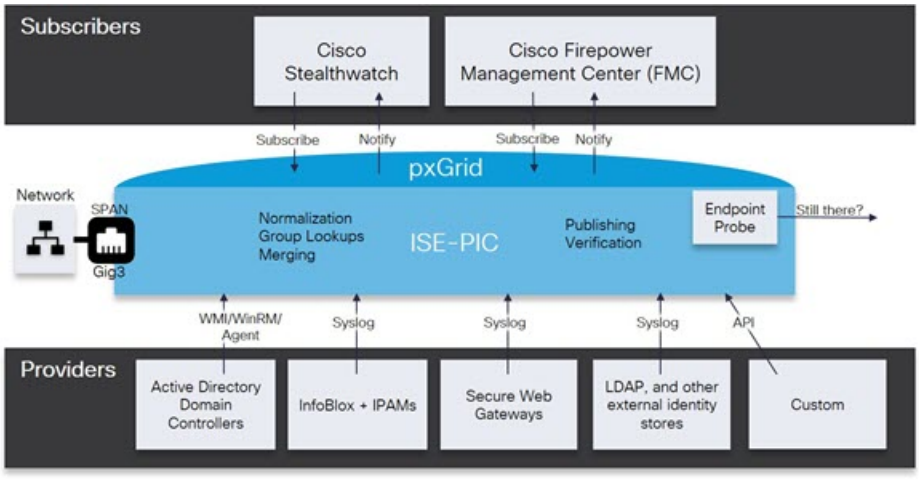
Passive Identity Connector (ISE-PIC) Flow

The flow for ISE-PIC is as follows:

1. Provider performs the authentication of the user or endpoint.
2. Provider sends authenticated user information to ISE-PIC.
3. ISE-PIC normalizes, performs lookups, merges, parses and maps user information to IP addresses and publishes mapped details to pxGrid.
4. pxGrid subscribers receive the mapped user details.

The following diagram illustrates the high-level flow offered by ISE-PIC.

Figure 1: High Level Flow



Cisco ISE-PIC Architecture, Deployments, and Nodes

Cisco ISE-PIC architecture includes the following components:

- Nodes—in a Cisco ISE-PIC deployment, up to two nodes can be configured as described below
- Network resources
- Endpoints

A deployment that has a single Cisco ISE-PIC node is called a *standalone deployment*.

A deployment that has two Cisco ISE-PIC nodes is called a *high availability deployment*, where one node functions as the primary appliance (the primary administration node, or the PAN). A high availability deployment improves service availability.

The PAN provides all the configuration capabilities that are required for this network model, and the secondary Cisco ISE node (the secondary PAN) functions in a backup role. The secondary node supports the primary node and resumes functionality whenever connectivity is lost with the primary node.

Cisco ISE-PIC synchronizes or replicates all of the content that resides on the primary Cisco ISE-PIC node with the secondary Cisco ISE-PIC node in order to ensure that your secondary node is current with the state of your primary node (and therefore can be used as a backup).

ISE Community Resource

For information about deployment and scaling, see ISE Deployment Journey.

Benefits of ISE-PIC

ISE-PIC offers you:

- A single identity solution that interacts with a variety of different providers.
- Friendly GUI enabling simple configuration, monitoring and troubleshooting
- Simple installation and configuration
- Easily upgraded to ISE for active authentication. When upgrading from ISE-PIC to a full ISE deployment and using the ISE-PIC node to create a standalone ISE deployment, or when adding this node as your primary node to an existing deployment, ISE will continue to offer all features that were available to you in ISE-PIC prior to upgrade and your existing configuration is preserved.

Note In order to upgrade to ISE, download a trial version or, contact your Cisco representative in order to discuss licensing options.

When you add your upgraded ISE-PIC to an existing ISE deployment, but not as the primary node, the previous ISE-PIC configurations will be overwritten.

For a full description of the upgrade flow, see Upgrading ISE-PIC to a Full ISE Installation.

Comparing ISE-PIC with Cisco ISE and Cisco Context Directory Agent

ISE-PIC brings with it many benefits, including the ability to smoothly and easily upgrade to Cisco ISE. In addition to ISE-PIC and Cisco ISE, Cisco also offers Cisco Context Directory Agent (CDA), an additional security mechanism. This section compares the three offers in the following tables:

A Detailed Comparison of ISE-PIC with Cisco ISE

ISE-PIC is designed to share passive identities only and provides no authorization or authentication services, both of which are provided by ISE, which offers authentication, authorization and accounting (AAA) servers. The differences between the two products are fully illustrated in the following table.

Table 1: Comparing ISE-PIC with Cisco ISE

Category	Feature	ISE-PIC	Cisco ISE
Smart Licensing		—	√
Authentication and Authorization types	Authorization policies	—	√
	TrustSec	—	√
	Active Directory passive authentication including WMI	√	√
Passive Identity sources		√	√
	Easy Connect	—	√
	SysLog sources	√	√
	REST API sources	√	√
	SPAN	√	√
	Security Group eXchange Protocol (SXP)	—	√
	RADIUS including RADIUS proxy	—	√
	BYOD	—	√
	Guest	—	√
	Posture	—	√
	Device Administration (TACACS+)	—	√

Category	Feature	ISE-PIC	Cisco ISE
pxGrid	pxGrid controller	√ For Cisco subscribers only	√
	pxGrid controller redundancy	√	√
	Topic extensibility	—	√
Certificate Authority (CA)	pxGrid certificate templates	√	√
	Endpoint CA	—	√
	Enrollment over secure transport (EST)	—	√
	Other certificate templates	—	√
Visibility and Context	Context Directory	—	√
	Profiling	—	√
Reports		! **Note** ISE-PIC offers reports that you can use to monitor the health of the system and troubleshoot issues in the network. However, ISE-PIC offers a subset of functionality in comparison with ISE, and hence some of the ISE reports are not available in ISE-PIC.	√

An Overview Comparison of ISE-PIC with Cisco ISE and CDA

Cisco Context Directory Agent (CDA) is a mechanism that maps IP Addresses to usernames in order to allow security gateways to understand which user is using which IP Address in the network, so those security gateways can now make decisions based on those users (or the groups to which the users belong to). ISE-PIC, however, collects user identities much more precisely by accessing additional data such as user name, MAC addresses and ports. The following table offers a high-level comparison of ISE-PIC, Cisco ISE and CDA.

Table 2: Comparing ISE-PIC with Cisco ISE and CDA

Passive Auth Details	Full ISE	ISE-PIC	CDA
Number of domain controllers	100	100	80
Number of subscribers	20	20	—
WMI (Agentless)	Yes	Yes	Yes
Windows server agent available	Yes	Yes	—
DCOM required	No (SPAN)	No (SPAN)	Yes
Easy Connect	Yes	—	—
Kerberos sniffing with SPAN	Yes	Yes	—
Bindings (IP address, MAC address and user name)	300,000	300,000	64,000