



You make **possible**



# Configuring Cisco ISE-PIC (Passive Identity Connector)

Aditya Ganjoo  
Puneesh Chhabra

TME  
CX High Touch Delivery

LTRSEC-1655

**CISCO** *Live!*

Barcelona | January 27-31, 2020



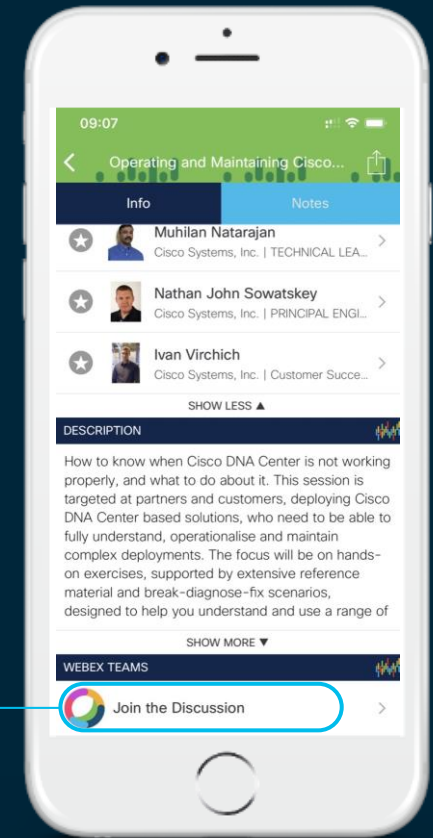
# Cisco Webex Teams

## Questions?

Use Cisco Webex Teams to chat with the speaker after the session

## How

- 1 Find this session in the Cisco Events Mobile App
- 2 Click “Join the Discussion”
- 3 Install Webex Teams or go directly to the team space
- 4 Enter messages/questions in the team space



# AGENDA

## **PRESENTATION (45 min-1 hr.)**

## **LABS (2.30 hrs.)**

- PASSIVE ID LAB
- PROVIDERS AND SUBSCRIBER TASK
- EASY CONNECT TASK



Aditya & Puneesh  
Security TME & Technical  
Consulting CSE

CISCO *Live!*

Barcelona | January 27-31, 2020



# WHAT IS PIC ?



Offers a centralized installation and implementation to gather passive authentication data from a variety of sources.



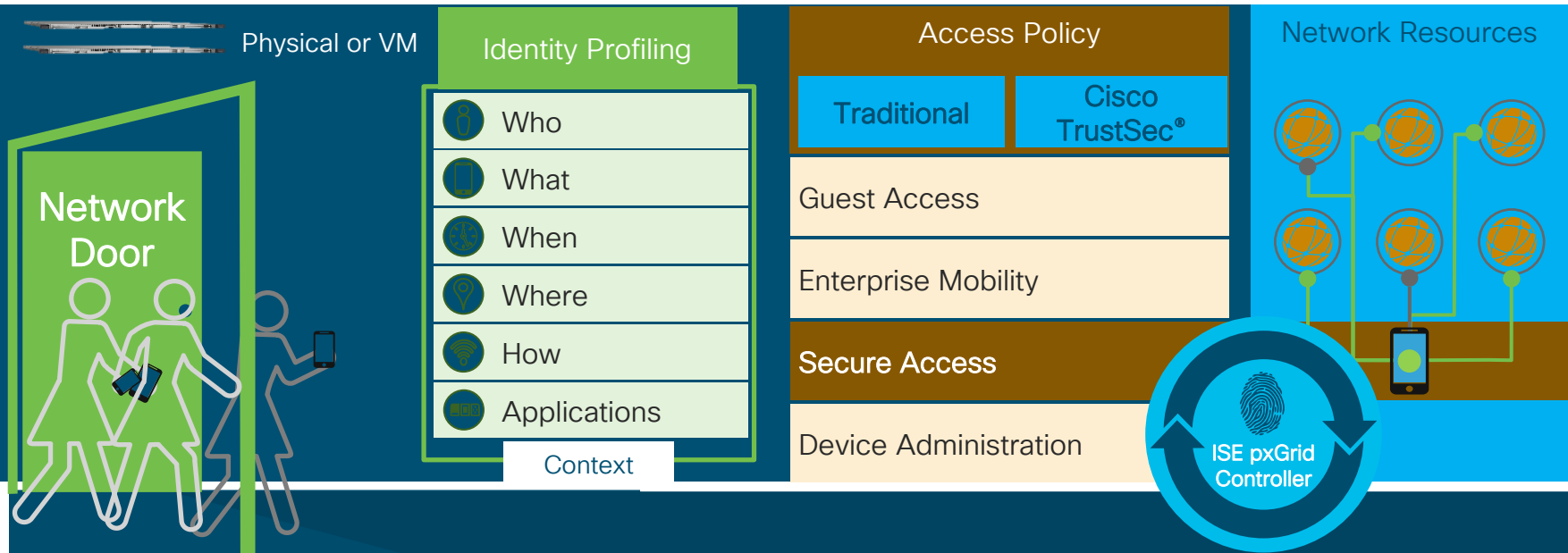
Gathers concise information from a variety of different security product providers



Interoperability

# Introducing Cisco Identity Services Engine (ISE)

A centralized security solution that automates context-aware access to network resources and shares contextual data



# With Cisco Identity Services Engine You Can



See and share rich user  
and device details



Control all access  
throughout the network  
from one place



Stop and contain threats





# Personas



- Policy Service Node (PSN)

- Makes policy decisions



- Policy Administration Node (PAN)

- Interface to configure policies and manage ISE deployment
- Replication hub for all database config changes



- Monitoring & Troubleshooting Node (MnT)

- Interface to reporting and logging
- Destination for syslog from other ISE nodes and optionally NADs



- pxGrid Controller

- Facilitates sharing of information between network elements

All can run in a single host

# ISE PIC PERSONA



ISE-PIC supports only virtual machines.



Licensed for up to 3,000 sessions (will support 3,000 sessions in either standalone or high availability modes).



Can go up to 300,000 sessions.



There are no special operating system or software requirements. The ISO images for ISE-PIC include all necessary software items.

# ISE-PIC Terminology



Probes



Providers



Subscribers



Parser

# Probes

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.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation menu at the top includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The 'Administration' menu is expanded to show Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, and PassiveID. The 'Providers' sub-menu is selected, showing Overview, Providers, Subscribers, Certificates, Troubleshoot, and Reports. The left sidebar lists various configuration categories: Active Directory, Agents, API Providers, SPAN, Syslog Providers, Mapping Filters, and Endpoint Probes. The main content area is titled 'Active Directory' and features a table of providers. The table has columns for 'Join Point Name' and 'Active Directory Domain'. The providers listed are SCRI\_AD (scri.edu.sg) and TEST\_CL (ravsing2.local). Above the table are action buttons for Edit, Add, and Delete, along with Node View, Advanced Tools, and Scope Mode options.

Join Point Name	Active Directory Domain
<input type="checkbox"/> SCRI_AD	scri.edu.sg
<input type="checkbox"/> TEST_CL	ravsing2.local

# Providers on ISE



WMI



Syslog



SPAN



Agent

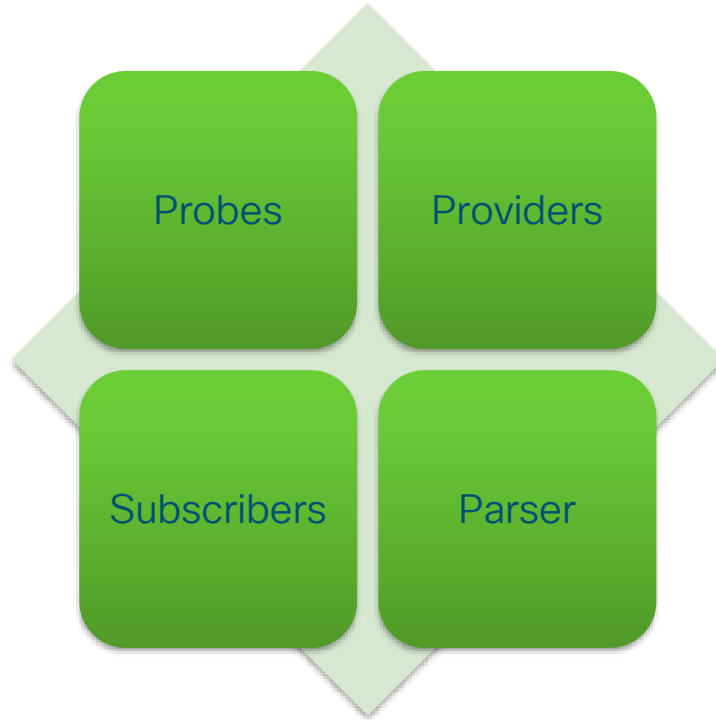


REST API



Endpoint Probes

# PIC TERMINOLOGY



# ISE WMI Integration



WMI is a publish/subscribe (pub/sub) messaging system within AD.



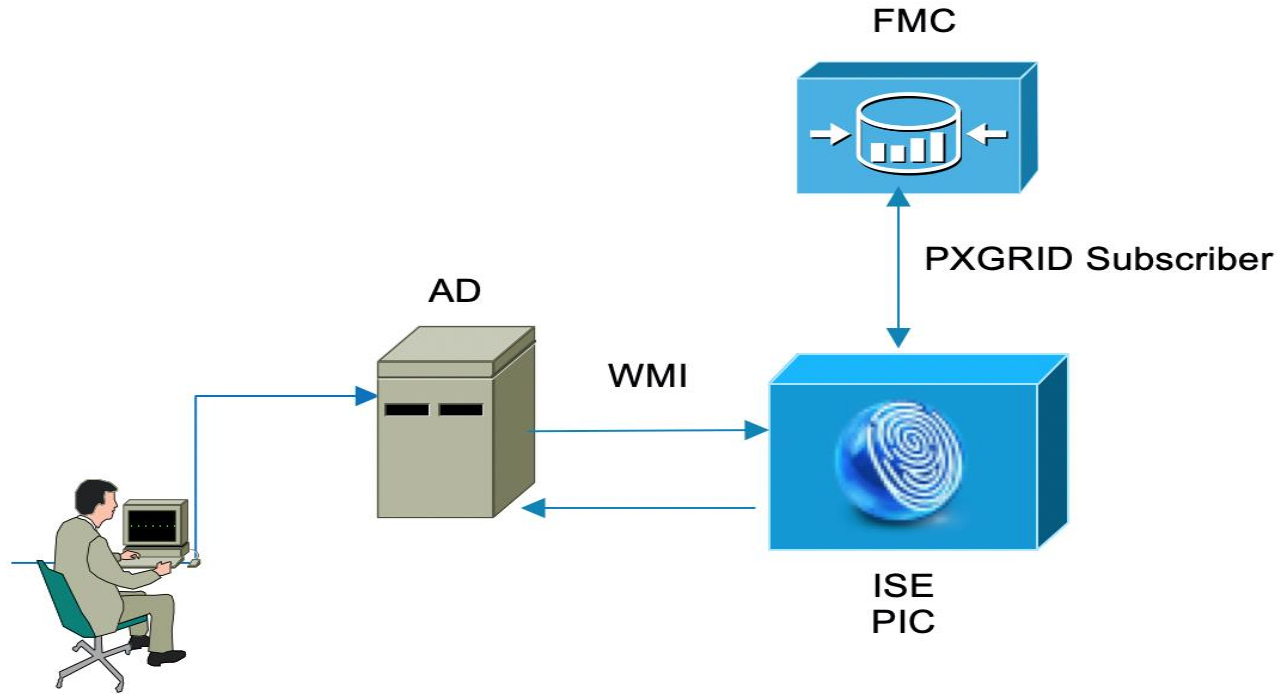
ISE may remotely communicate with AD using WMI and subscribe to certain security events, like logins. When those events occur, ISE is notified by AD.



WMI is the only passive identity source that can be used with EasyConnect.



# Basic ISE WMI integration





Active Directory

Agents

API Providers

SPAN

Syslog Providers

Mapping Filters

Endpoint Probes

Connection

Whitelisted Domains

**PassiveID**

Groups

Attributes

Advanced Settings

### PassiveID Domain Controllers

Rows/Page 1

1 / 1

Go 1 Total Rows

Refresh Edit Trash Add DCs Use Existing Agent Config WMI Add Agent

<input type="checkbox"/>	Domain	DC Host	Site	IP Address	Monitor Using
<input type="checkbox"/>	cltr.com	WIN-QK8F2PP1T46.cltr.com	Default-First-Site-Name	192.168.168.2	WMI

# ISE PIC AD Agent



With ISE you can remotely push the agent to gather the Passive ID information.



You get an option to deploy or register an Agent.



The agent can be installed manually or from the ISE on the AD server to fetch username/IP mappings and AD related events.

# ISE PIC AD Agent

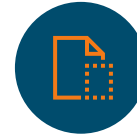
The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Agents > New. The left sidebar contains a tree view with categories like Active Directory, Agents, API Providers, SPAN, Syslog Providers, Mapping Filters, and Endpoint Probes. The main content area is titled 'Agents > New' and contains two radio button options: 'Deploy New Agent' (selected and highlighted with a red box) and 'Register Existing Agent'. Below these are five required input fields: Name, Description, Host FQDN, User Name, and Password. A 'Show Password' button is located next to the Password field. At the bottom right, there are 'Cancel' and 'Deploy' buttons.

# ISE PIC Syslog



ISE PIC can be used to integrate with different Syslog providers.

Supports providers such as InfoBlox, Blue Coat, BlueCat, and Lucent) as well as DHCP syslog messages, and sends back user identity information, including MAC addresses. This mapped user identity data is then delivered to subscribers.



You can use System defined or create a Custom Syslog Template.



Supports both TCP and UDP logging.

# ISE PIC Syslog Configuration

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID > Providers > Syslog Providers > New. The left sidebar contains a navigation menu with items: Active Directory, Agents, API Providers, SPAN, Syslog Providers (selected), Mapping Filters, and Endpoint Probes. The main content area is titled 'Syslog Providers > New' and contains the following configuration fields:

- Name: TEST
- Description: (empty)
- Status: Enabled
- Host FQDN: asa.cisco.com
- Connection Type: UDP - Port 40514
- Template: ASA VPN (highlighted with a red box, with 'View' and 'New' buttons next to it)
- Default Domain: cisco.com

At the bottom right, there are 'Cancel' and 'Submit' buttons.

# ISE PIC REST API



ISE PIC can also be integrated using REST API.



ISE uses REST API to update username/IP address mappings.



For instance, Guest user information can be updated using REST API.



Cisco Terminal Services (TS) Agent can be installed onto MS and Citrix Terminal Servers to fetch Passive ID information.



Cisco TS is a kernel-level agent.

# ISE PIC using SPAN



Cisco SPAN aka Port Mirroring/Monitoring can be used to gather Passive ID information.



Simply configure the SPAN on the switch to copy the AD traffic going to the DC (SOURCE) and send it over to the configured SPAN PORT on the ISE PIC (DESTINATION).



Tip to filter only Kerberos traffic:



Use VACL (VLAN ACL) to filter only Kerberos related traffic.



# ISE PIC using Endpoint-Probes



Enabled by default when ISE-PIC is installed.



Must have network connectivity to port 445.



In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point, which enables the Endpoint probe to run even when the Active Directory probe is not fully configured.



In order to ensure Endpoint runs in the background, you must first configure an initial Active Directory join point and ensure you choose to Store Credentials.

# ISE PIC Endpoint-Probes

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". Below this, a series of tabs are visible: Home, Context Visibility, Operations, Policy, Administration, and Work Centers. Under the Administration tab, there are sub-tabs for Network Access, Guest Access, TrustSec, BYOD, Profiler, Posture, Device Administration, and PassivID. The PassivID sub-tab is active, and within it, the "Providers" sub-tab is selected. The left-hand navigation pane lists various configuration categories: Active Directory, Agents, API Providers, SPAN, Syslog Providers, Mapping Filters, and Endpoint Probes. The main content area is titled "Endpoint Probes > New" and "Endpoint Probes". The form contains the following fields:

- Name \***: EP-TEST
- Description**: (empty)
- Status \***: Enabled
- Host Name \***: swarajise2
- Subnets \***: 10.1.1.0/24

The "Host Name" and "Subnets" fields are enclosed in a red rectangular box. At the bottom of the form, there are two buttons: "Cancel" and "Submit".

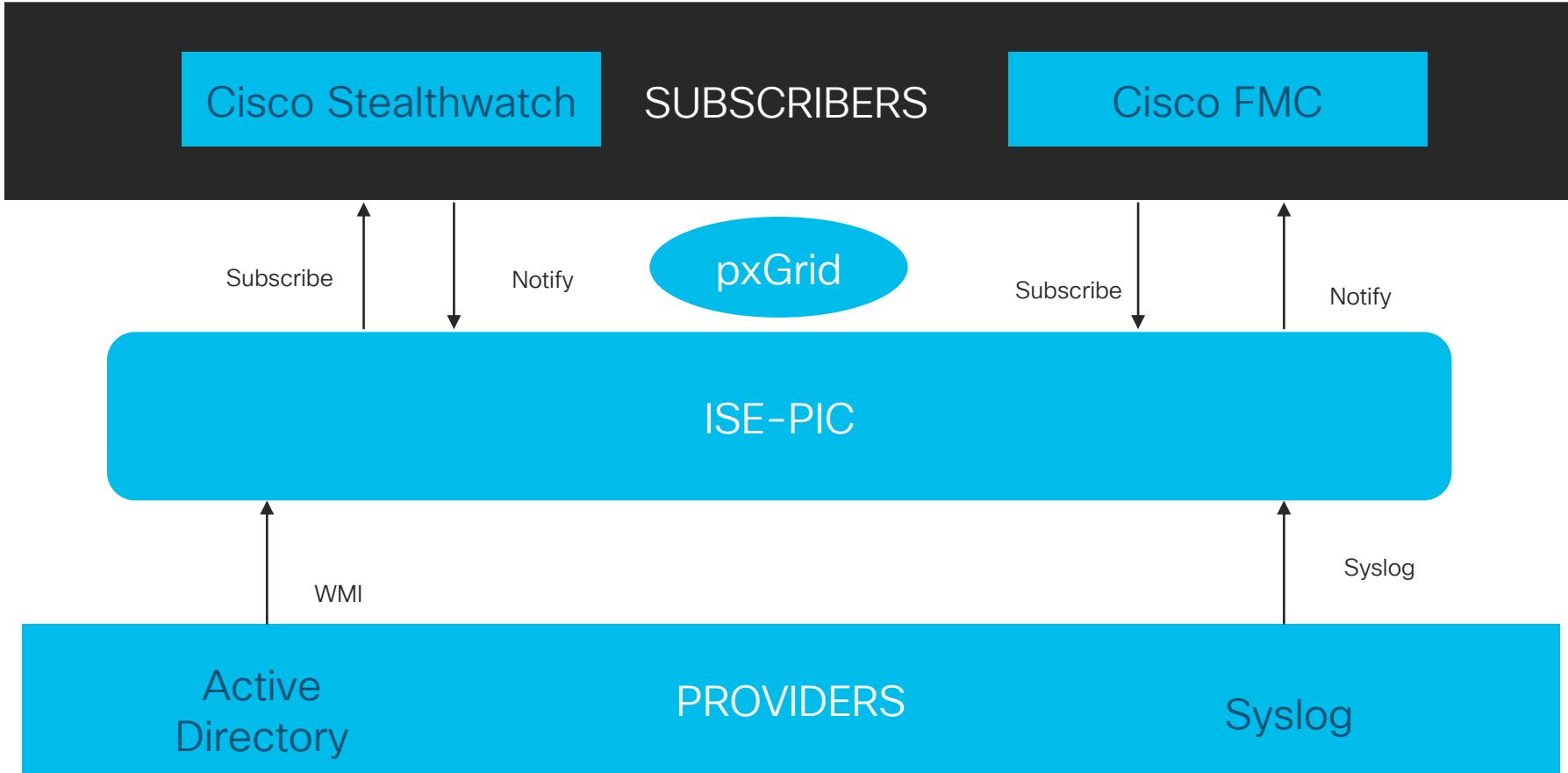
# Subscribers

Systems that subscribe to the ISE-PIC services in order to receive user identity information.

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Identity Services Engine', 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The 'Administration' menu is expanded to show 'Subscribers'. The 'Subscribers' page has a toolbar with actions like 'Enable', 'Disable', 'Approve', 'Group', 'Decline', 'Delete', and 'Refresh'. A table lists the subscribers with the following data:

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
ise-bridge-ise		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate	<a href="#">View</a>
ise-admin-ise		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate	<a href="#">View</a>
ise-mnt-ise		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	<a href="#">View</a>
ise-pubsub-ise		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	<a href="#">View</a>

At the bottom of the page, a green status bar indicates 'Connected to pxGrid ISE.ravising2.local'.



# LIVE SESSION INFO

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassivID

Overview Providers Subscribers Certificates Troubleshoot Reports

Introduction Dashboard Live Sessions

Refresh Every 1 minute Show Latest 20 records Within Last 24 hours

Refresh Export To Filter

Initiated	Updated	Session Status	Provider	Action	Endpoint ID	Identity	IP Address	Server	En
Jan 06, 2019 02:45:...	Jan 06, 2019 0...	Authenticated	WMI	Show Actions	10.106.61.67	CiscoLive	10.106.61.67	swarajise2	Er
Jan 06, 2019 11:14:...	Jan 06, 2019 1...	Authenticated	WMI	Show Actions	10.106.47.204	Administrator	10.106.47.204	swarajise2	Er
Jan 06, 2019 10:35:...	Jan 06, 2019 1...	Authenticated	WMI	Show Actions	10.106.63.67	CiscoLive	10.106.63.67	swarajise2	Er

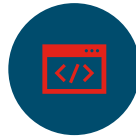
Last Updated: Sun Jan 06 2019 19:38:01 GMT+0530 (India Standard Time) Records Shown: 3



# Parser



The ISE-PIC backend component that receive syslog messages



For example, if a parser is configured to look for “mac=”, the parser then parses each line while looking for that phrase.



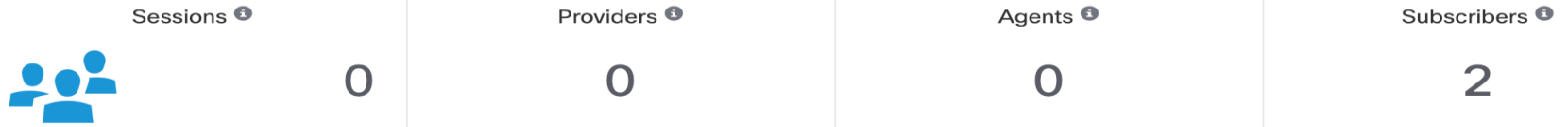
The parser goes through each line of information of a syslog message as it arrives, looking for key information.

# ISE-PIC VS ISE-PassiveID DASHBOARD

**ISE Passive Identity Connector** | Home | Live Sessions | Providers | Subscribers | Certificates | Troubleshoot | Reports | Administration | Settings

Main | Additional

## PASSIVE IDENTITY METRICS



**Identity Services Engine** | Home | Context Visibility | Operations | Policy | Administration | Work Centers

Network Access | Guest Access | TrustSec | BYOD | Profiler | Posture | Device Administration | PassiveID

Overview | Providers | Subscribers | Certificates | Troubleshoot | Reports

- Introduction
- Dashboard
- Live Sessions

## Passive Identity Introduction

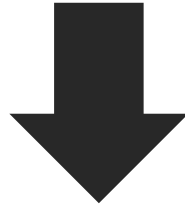
Passive Identity gathers user identity data from a variety of sources, such as Active Directory, Infoblox or Terminal Server Agent, known as providers. Then using Cisco pxGrid services, it securely delivers this user identity data to its subscribers such as Cisco Stealthwatch or Cisco Firepower Management Center (FMC).



IS SETTING UP DOT1X A  
CHALLENGE ???



WE HAVE A SOLUTION



CISCO EASY CONNECT

# What is Easy Connect ?



Provides port-based authentication similar to 802.1X, but easier to implement.



Learns about the authentication from Active Directory and provides session-tracking for active network sessions.

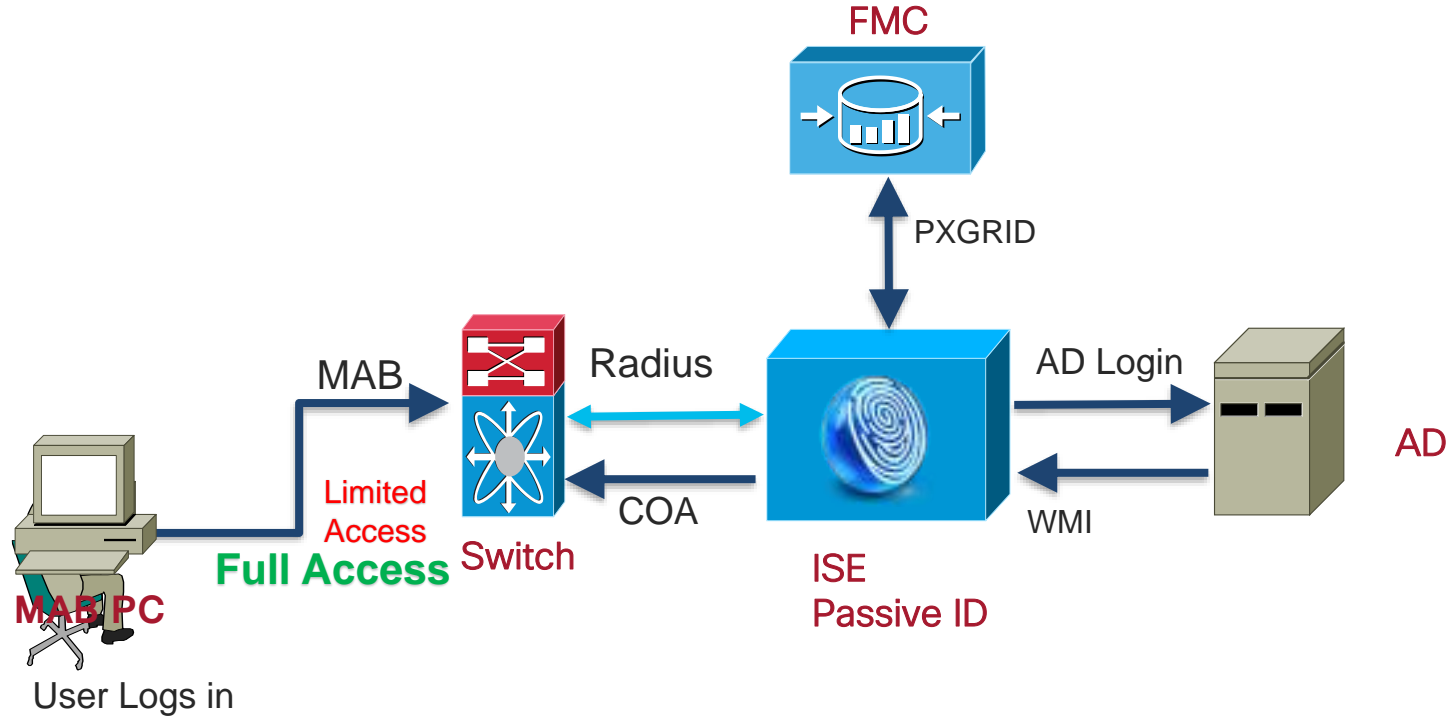


Session Directory notifications can be published with PxGrid.



EasyConnect can be used as a backup authentication method or way to add a second level of identity.

# EASYCONNECT-FLOW



# Benefits of Easy Connect



No 802.1X supplicant required for user authentication



No Public Key Infrastructure (PKI) required for trusted credential transport



Can be used as primary user identity or supplement another active identity such as MAB or 802.1X with Radius

# Easy Connect Limitations



EasyConnect cannot be used with BYOD use case.



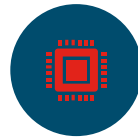
Supports only Cisco Devices.



Endpoint logoff Event is not supported.



Windows Endpoints only



Wired MAB only

# Identity Policy

The screenshot displays the Cisco ISE interface for editing an identity rule. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The 'Policies' section is active, showing 'Access Control > Identity' and 'Network Discovery', 'Application Detectors', 'Correlation', and 'Actions'. The rule being edited is 'IDRULE' under 'Active Authentication'. The dialog box 'Editing Rule - IDRULE' contains the following fields and options:

- Name: IDRULE
- Enabled:
- Action: Passive Authentication (dropdown menu)
- Realms: AD (dropdown menu)
- Authentication Protocol: HTTP Basic
- Exclude HTTP User-Agents: None
- Zones: No Authentication
- Realm: AD (dropdown menu)
- Use active authentication if passive or VPN identity cannot be established:

A 'Realm & Settings' button is highlighted in the dialog. The background shows a table of rules with one row selected.

# Mapping Identity to Access Policy

The screenshot displays the Cisco ISE GUI for editing an Access Control Policy (ACP) rule. The main interface shows the 'Policies' tab with 'Access Control' selected. The 'Editing Rule - Allow-icmp' dialog box is open, showing the rule configuration. The 'Users' tab is selected, and the 'Available Users' list is highlighted with a red box. The 'Selected Users' list shows 'AD/david'.

**Editing Rule - Allow-icmp**

Name: Allow-icmp  Enabled Move

Action:  Allow

Zones Networks VLAN Tags **Users** Applications Ports URLs SGT/ISE Attributes Inspection **Logging** Comments

**Available Realms**

- Special Identities
- AD

**Available Users**

- Search by name or value
- AD/david
- AD/jason
- AD/jeffrey
- AD/jerry
- AD/jon
- AD/joseph
- AD/joshua
- AD/kerik
- AD/krbtgt
- AD/logan

**Selected Users (1)**

- AD/david

Buttons: Add to Rule, Save, Cancel

# Verification of Identity

Overview **Analysis** Policies Devices Objects AMP Intelligence Deploy 4 System Help **admin**

Context Explorer Connections Intrusions Files Hosts **Users > Users** Vulnerabilities Correlation Custom Lookup Search

Bookmark This Page Report Designer Dashboard View Bookmarks Search

## Users

[Table View of Users](#) > Users

▶ Search Constraints ([Edit Search](#) [Save Search](#))

Jump to... ▼

<input type="checkbox"/>	User ×	Last Seen ×	Realm ×	Username ×	First Name ×	Last Name ×	E-Mail ×	Department ×	Phone ×	Discovery Application ×	Active Session Count ×	Available For Policy ×
▼	david (AD\david, LDAP)	2019-05-31 02:33:13	AD	david	david		david@clltr.com	users (clltr)		<input type="checkbox"/> LDAP	0	No

<< Page 1 of 1 >> Displaying row 1 of 1 rows

View Delete

View All Delete All



# ISE PIC REPORTS

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers License Warning

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Providers Subscribers Certificates Troubleshoot Reports

### Export Summary

My Reports

Reports

Passive ID Reports

- AD Connector Operations
- Administrator Logins
- Change Configuration Audit
- Current Active Sessions
- Health Summary
- Operations Audit
- PassiveID
- pxGrid Administrator Audit
- System Diagnostic
- User Change Password Audit

Scheduled Reports

### PassiveID Details

From 2019-01-06 00:00:00.0 to 2019-01-06 14:38:37.0  
Reports exported in last 7 days 0

+ My Reports Export To Schedule


Filter Refresh

	Provider Type	Domain	Host	Event	Admin Identity
	Provider Type	Domain	Host	Event	Admin Identity
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Successfully establish connection to Domain Controller	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Lost connection with Domain Controller	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Cannot connect to Domain Controller	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Successfully establish connection to Domain Controller	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Cannot connect to Domain Controller	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Lost connection with Domain Controller	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	The number of events handled in the last 24 hours	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Successfully establish connection to Domain Controller	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Cannot connect to Domain Controller	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Lost connection with Domain Controller	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Successfully establish connection to Domain Controller	
	WMI	ravsing2.local	WIN2K8.ravsing2.local/1...	Cannot connect to Domain Controller	



# ISE PIC Troubleshooting

 Live Sessions

 Available Reports

 Cisco ISE-PIC Alarms

 TCP Dump Utility to Validate the Incoming Traffic

 Logging Mechanism to capture Debugs

 Active Directory Troubleshooting

# ISE PIC Debugs/Troubleshoot

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC. The current page is 'Debug Level Configuration' for node 'ISE.raving2.local'. The table below lists the debug components and their log levels. The 'pxgrid' component is highlighted with a red box.

Component Name	Log Level	Description
<input type="radio"/> Active Directory	DEBUG	Active Directory client internal messages
<input type="radio"/> identity-store-AD	DEBUG	Active Directory interaction messages
<input type="radio"/> PassiveID	DEBUG	PassiveID events and messages
<input checked="" type="radio"/> pxgrid	DEBUG	pxGrid messages
<input type="radio"/> spog	DEBUG	Spog messages

# Helpful Links

- <https://community.cisco.com/t5/security-documents/ise-pic-faq/ta-p/3639377>
- [https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/control\\_users\\_with\\_ise\\_ise\\_pic.pdf](https://www.cisco.com/c/en/us/td/docs/security/firepower/623/configuration/guide/fpmc-config-guide-v623/control_users_with_ise_ise_pic.pdf)
- [https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/pic\\_admin\\_guide/PIC\\_admin/PIC\\_admin\\_chapter\\_00.pdf](https://www.cisco.com/c/en/us/td/docs/security/ise/2-2/pic_admin_guide/PIC_admin/PIC_admin_chapter_00.pdf)

# Complete your online session survey



- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (starting on Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Content Catalog on [ciscolive.com/emea](https://ciscolive.com/emea).

Cisco Live sessions will be available for viewing on demand after the event at [ciscolive.com](https://ciscolive.com).

# Continue your education



Demos in the  
Cisco campus



Walk-in labs



Meet the engineer  
1:1 meetings



Related sessions



Thank you





You make **possible**