CCIE Professional Development

Integrated Security Technologies and Solutions

Volume II

Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity and Virtualization

Aaron Woland, CCIE® No. 20113
Vivek Santuka, CCIE® No. 17621
Jamie Sanbower, CCIE® No. 13637
Chad Mitchell, CCIE® No. 44090

ciscopress.com

Integrated Security Technologies and Solutions - Volume II

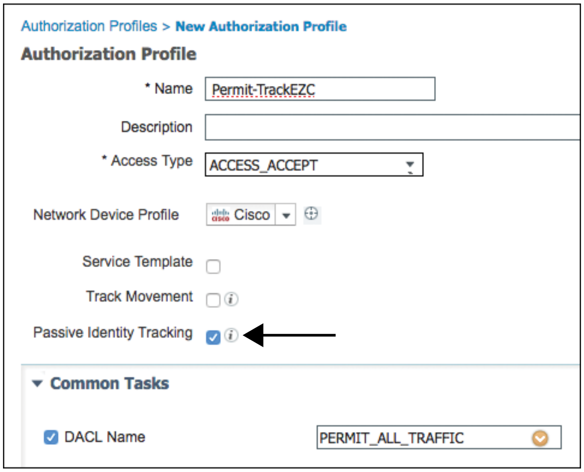
Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity, and Virtualization

Aaron Woland, CCIE® No. 20113
Vivek Santuka, CCIE® No. 17621
Jamie Sanbower, CCIE® No. 13637
Chad Mitchell, CCIE® No. 44090

Cisco Press

- EZC requires an AD login event to be processed from the endpoint to AD. If access to the domain controllers is not permitted at time of user login, EZC will fail.
- The NADs are not configured any differently:
  - They must still process network authentications (MAB and 802.1X).
  - ISE must still be configured as the RADIUS server.

When a machine joins the network, a MAB is processed. The authorization result must include the Passive Identity Tracking option checked, such as shown in Figure 3-32.



Authorization Profiles > **New Authorization Profile**

Authorization Profile

* Name	Permit-TrackEZC
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	Cisco
Service Template	□
Track Movement	□
Passive Identity Tracking	☑

Common Tasks

☑ DACL Name	PERMIT_ALL_TRAFFIC

Figure 3-32 *Authorization Profile with Passive Identity Tracking Enabled*

When a network session is authorized with this flag, ISE will monitor the session and look for WMI events that leverage the same endpoint ID (MAC address), to stitch the passive identity together with the network session.

After the WMI event for that endpoint is stitched together, a CoA-Reauth is sent to the NAD and a new authorization result may be applied to that based on the combined authentication (MAB + EZC).

Figures 3-33 and 3-34 show the EasyConnect flow leveraging MAB for the network session.

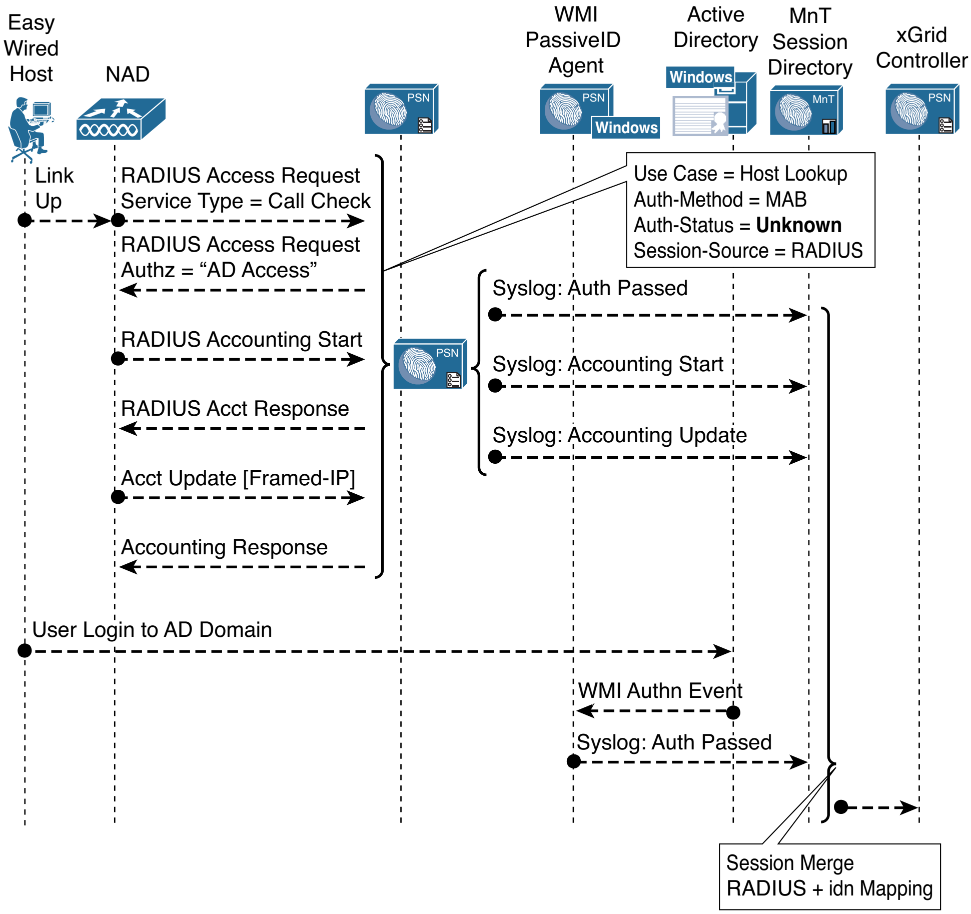


Figure 3-33 *EasyConnect Flow with MAB*

Windows Management Instrumentation

Windows Management Instrumentation (WMI) is a core Windows management technology that enables you to manage Windows servers or workstations locally or remotely. WMI acts as a publish/subscribe (pub/sub) messaging system within Microsoft Active Directory.

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

The main benefits to using this WMI method to learn about the passive authentication is that it does not require installation of an agent on a domain controller or a member server. Before WMI can be used, connectivity requirements for successful WMI connections must be met. The good news is that the *Config WMI* function from ISE's UI will perform that configuration for you.

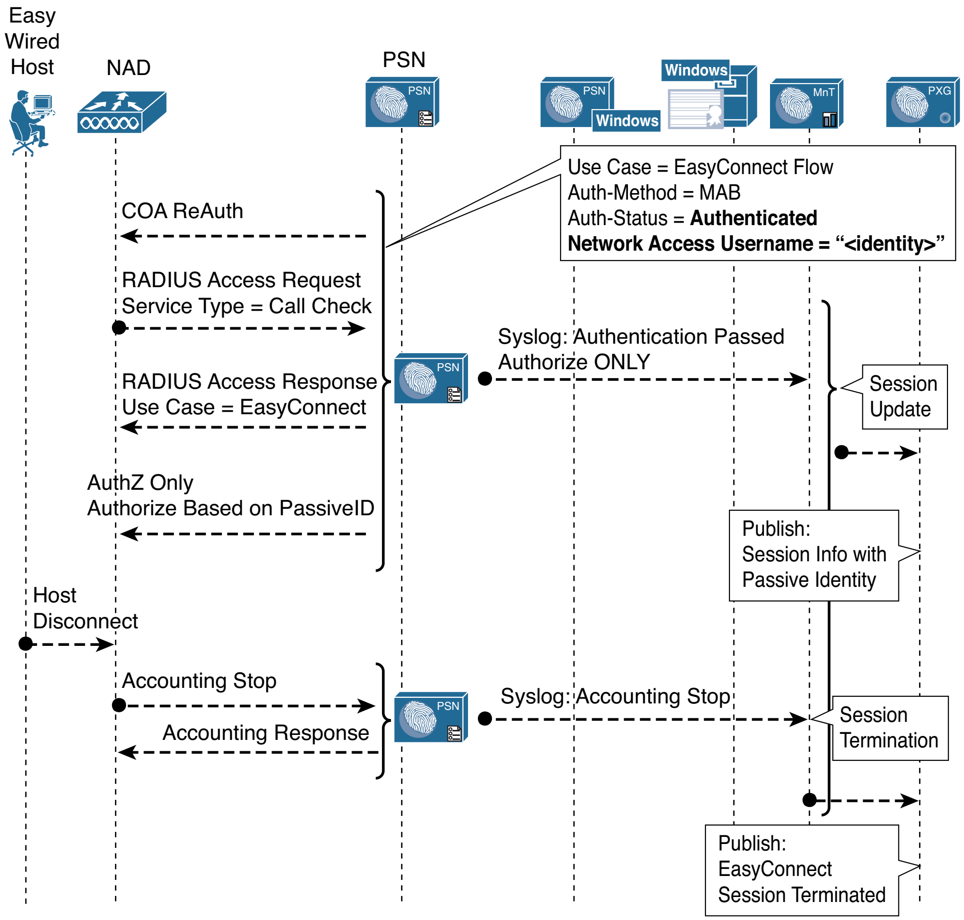


Figure 3-34 *EasyConnect Flow with MAB (continued)*

This type of connection to AD has been around for a very long time. The Cisco Context Directory Agent (CDA) used it, and it's been a part of ISE since version 1.3. In ISE, it was previously referred to as "pxGrid Identity Mapping" and was designed to bring the passive identity functionality of CDA into ISE for sharing with pxGrid subscribers.

This functionality was extended to create the EasyConnect deployment method in ISE version 2.1 and then given a tremendous boost in capability and ease of use in ISE version 2.2.

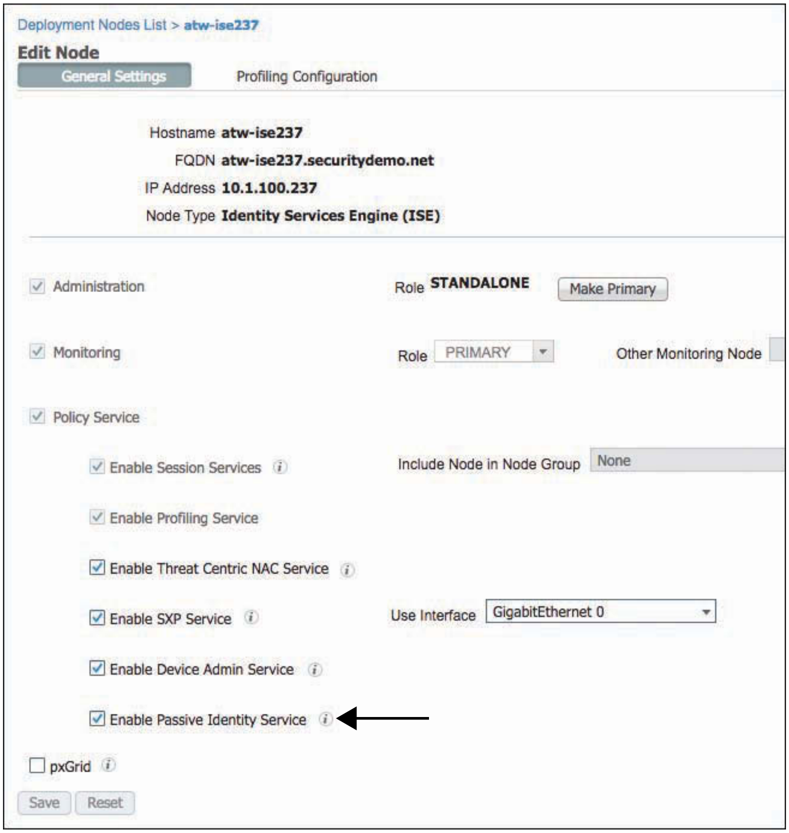
The WMI connection allows ISE to remotely communicate to an AD domain controller as a subscriber of WMI security events. Specifically, ISE looks for new Kerberos tickets that are granted and when those tickets are renewed. The granting of a ticket shows that a new Windows authentication session has occurred; it could be a user authentication or a machine authentication, but that is for ISE to sort through after it is notified. The renewing of Kerberos tickets shows that the session is still active and should not be timed out or purged.

Note At the time of writing, with ISE version 2.4, WMI is the only passive identity source that can be used with EasyConnect.

Configuring WMI

To integrate ISE with Active Directory via WMI:

Step 1. Navigate to **Administration > System > Deployment**. Ensure that at least one PSN has the Passive Identity service enabled, as shown in Figure 3-35.



Deployment Nodes List > atw-ise237

Edit Node

General Settings | Profiling Configuration

Hostname **atw-ise237**

FQDN **atw-ise237.securitydemo.net**

IP Address **10.1.100.237**

Node Type **Identity Services Engine (ISE)**

☑ Administration — Role **STANDALONE** [Make Primary]

☑ Monitoring — Role PRIMARY — Other Monitoring Node

☑ Policy Service

☑ Enable Session Services — Include Node in Node Group None

☑ Enable Profiling Service

☑ Enable Threat Centric NAC Service

☑ Enable SXP Service — Use Interface GigabitEthernet 0

☑ Enable Device Admin Service

☑ Enable Passive Identity Service

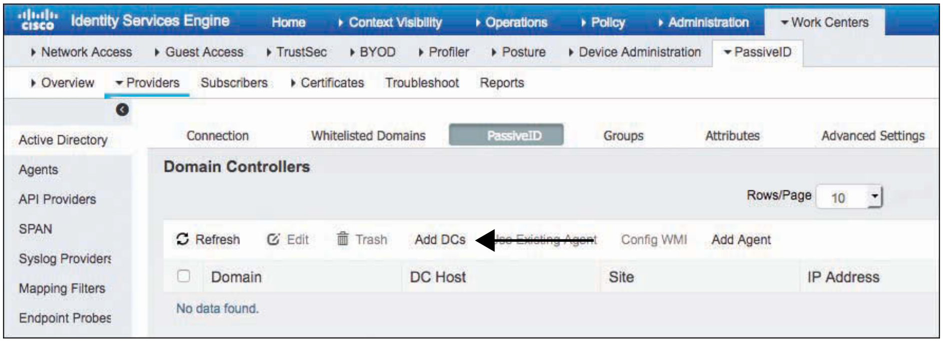
□ pxGrid

Figure 3-35 *Passive Identity Service Enabled for PSN*

Step 2. Navigate to **Work Centers > PassiveID > Providers > Active Directory**.

Step 3. Select your Active Directory join point that you previously created. In the example used in this book, it is named AD-SecurityDemo.

Step 4. Click the **PassiveID** tab, shown in Figure 3-36.



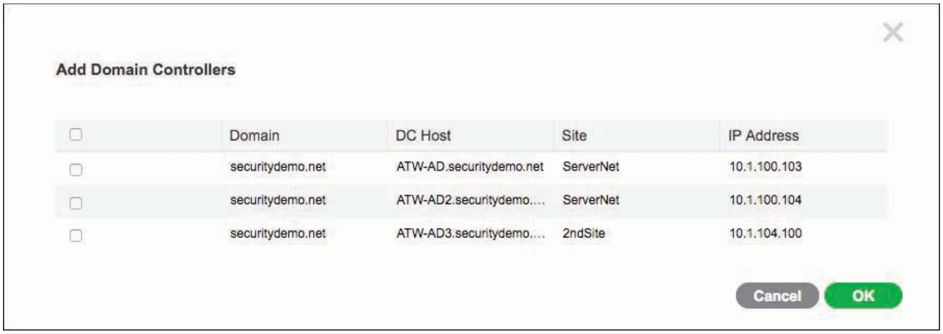
Domain Controllers

□	Domain	DC Host	Site	IP Address

No data found.

Figure 3-36 *PassiveID Tab*

Step 5. Click **Add DCs**. The list of domain controllers is displayed, as shown in Figure 3-37.



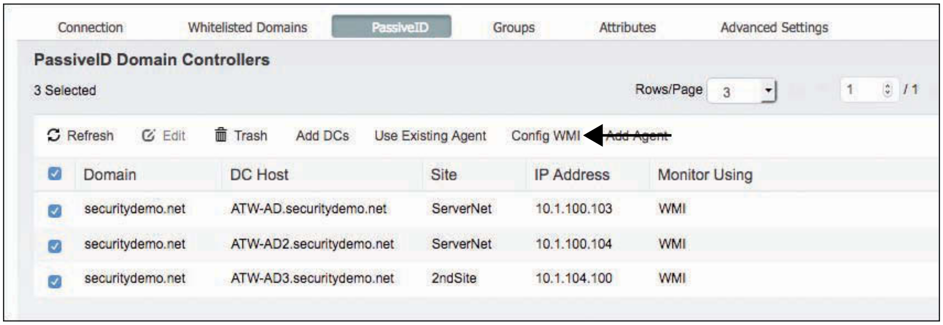
Add Domain Controllers

□	Domain	DC Host	Site	IP Address
□	securitydemo.net	ATW-AD.securitydemo.net	ServerNet	10.1.100.103
□	securitydemo.net	ATW-AD2.securitydemo....	ServerNet	10.1.100.104
□	securitydemo.net	ATW-AD3.securitydemo....	2ndSite	10.1.104.100

Figure 3-37 *Adding Domain Controllers*

Step 6. Check the check boxes for the domain controller(s) that you wish to monitor and click **OK**.

Step 7. The domain controllers are added to the list of PassiveID Domain Controllers. Check the check boxes for the DCs and click **Config WMI**, as highlighted in Figure 3-38.



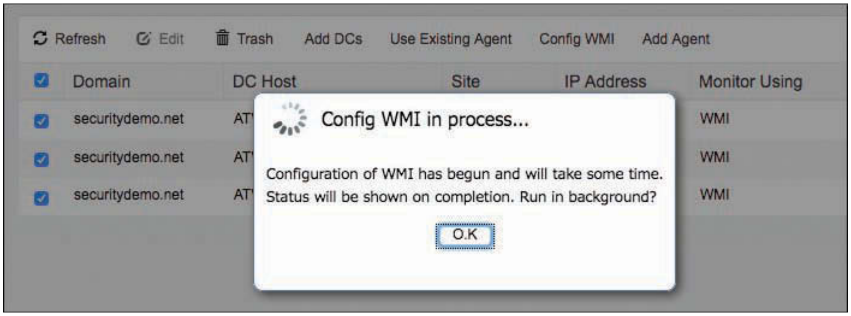
PassiveID Domain Controllers

3 Selected

☑	Domain	DC Host	Site	IP Address	Monitor Using
☑	securitydemo.net	ATW-AD.securitydemo.net	ServerNet	10.1.100.103	WMI
☑	securitydemo.net	ATW-AD2.securitydemo.net	ServerNet	10.1.100.104	WMI
☑	securitydemo.net	ATW-AD3.securitydemo.net	2ndSite	10.1.104.100	WMI

Figure 3-38 *Configuring WMI on Selected DCs*

The “Config WMI in process” message is displayed, as shown in Figure 3-39.



☑	Domain	DC Host	Site	IP Address	Monitor Using
☑	securitydemo.net	AT			WMI
☑	securitydemo.net	AT			WMI
☑	securitydemo.net	AT			WMI

Config WMI in process...

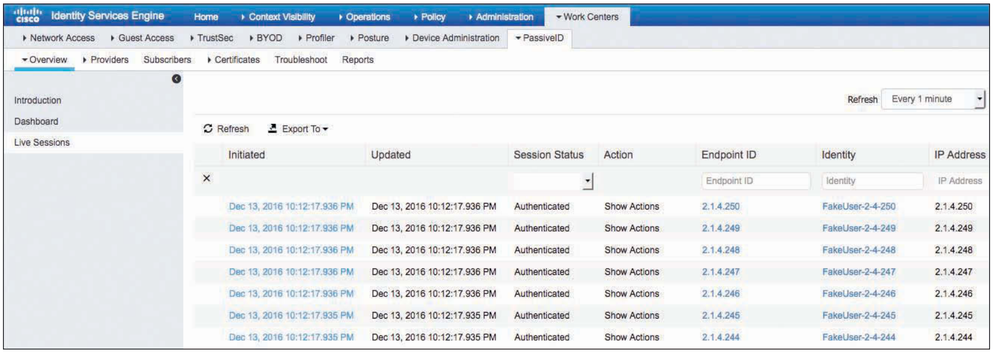
Configuration of WMI has begun and will take some time. Status will be shown on completion. Run in background?

O.K

Figure 3-39 *Configuration of WMI in Process*

When the configuration process is complete, a success message is displayed. The process performed by the Config WMI function is quite extensive and detailed after these configuration steps.

ISE is now configured to subscribe to the WMI security events, and the AD controllers are configured to send those events to ISE. When AD authentications occur, those sessions will be displayed in the Live Sessions screen, as shown in Figure 3-40.



Refresh Every 1 minute

Initiated	Updated	Session Status	Action	Endpoint ID	Identity	IP Address
Dec 13, 2016 10:12:17.936 PM	Dec 13, 2016 10:12:17.936 PM	Authenticated	Show Actions	2.1.4.250	FakeUser-2-4-250	2.1.4.250
Dec 13, 2016 10:12:17.936 PM	Dec 13, 2016 10:12:17.936 PM	Authenticated	Show Actions	2.1.4.249	FakeUser-2-4-249	2.1.4.249
Dec 13, 2016 10:12:17.936 PM	Dec 13, 2016 10:12:17.936 PM	Authenticated	Show Actions	2.1.4.248	FakeUser-2-4-248	2.1.4.248
Dec 13, 2016 10:12:17.936 PM	Dec 13, 2016 10:12:17.936 PM	Authenticated	Show Actions	2.1.4.247	FakeUser-2-4-247	2.1.4.247
Dec 13, 2016 10:12:17.936 PM	Dec 13, 2016 10:12:17.936 PM	Authenticated	Show Actions	2.1.4.246	FakeUser-2-4-246	2.1.4.246
Dec 13, 2016 10:12:17.935 PM	Dec 13, 2016 10:12:17.935 PM	Authenticated	Show Actions	2.1.4.245	FakeUser-2-4-245	2.1.4.245
Dec 13, 2016 10:12:17.935 PM	Dec 13, 2016 10:12:17.935 PM	Authenticated	Show Actions	2.1.4.244	FakeUser-2-4-244	2.1.4.244

Figure 3-40 *Live Sessions*

What Does That Config WMI Button Do?

The Config WMI process performs an awful lot in the background. Prior to ISE version 2.2, everything detailed in this section needed to be performed manually. To see more of the painful process of the past, check out the *Cisco Identity Services Engine Administrator Guide* for ISE version 1.3 or 1.4 and the process for setting up the pxGrid Identity Mapping function.

There are five main things that Config WMI must complete for you: