Cisco Cyber Threat Defense Solution 1.1

How-To Guide: Integrating the Identity Services Engine with StealthWatch 6.3

Guide

May 2013

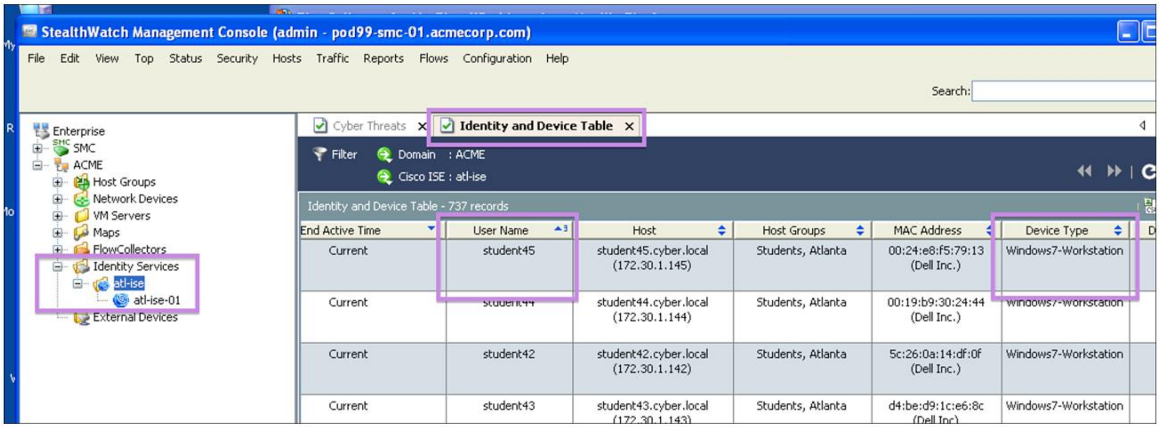
Integrating Flow and Identity Services

Overview

The Cisco Cyber Threat Solution is designed to operate cohesively with the Cisco TrustSec Solution, meaning that both solutions can be deployed simultaneously, and together offer administrators enhanced visibility and control over their network.

Note: It is assumed that the reader is familiar with and has deployed the Cisco TrustSec Solution 2.0 or later to at least a Monitor Mode or better deployment. For more information about TrustSec, refer to: http://www.cisco.com/go/trustsec.

Integration between the Lancope StealthWatch Management Console (SMC) and the Cisco Identity Services Engine (ISE) allows the administrator to quickly associate a user and device identity with a flow or set of flows from within the SMC console. The figure below illustrates this enhanced capability where the username, device type, and all other session information is available alongside all associated flows with an IP address. This section describes the process of integrating the Lancope SMC with a Cisco TrustSec Solution or Cisco ISE deployment to enhance the capabilities of the Cisco Cyber Threat Defense Solution.



Identity and Device Table - 737 records

End Active Time	User Name	Host	Host Groups	MAC Address	Device Type
Current	student45	student45.cyber.local (172.30.1.145)	Students, Atlanta	00:24:e8:f5:79:13 (Dell Inc.)	Windows7-Workstation
Current	student44	student44.cyber.local (172.30.1.144)	Students, Atlanta	00:19:b9:30:24:44 (Dell Inc.)	Windows7-Workstation
Current	student42	student42.cyber.local (172.30.1.142)	Students, Atlanta	5c:26:0a:14:df:0f (Dell Inc.)	Windows7-Workstation
Current	student43	student43.cyber.local (172.30.1.143)	Students, Atlanta	d4:be:d9:1c:e6:8c (Dell Inc)	Windows7-Workstation

Integrating the Lancope SMC with the Cisco ISE

StealthWatch 6.3 uses a Representational State Transfer (REST) API to collect identity information from a Cisco ISE Monitoring (MNT) node. The REST API calls are passed over a secure and authenticated HTTPS session.

Procedure 1: Validate ISE Monitoring Node deployment.

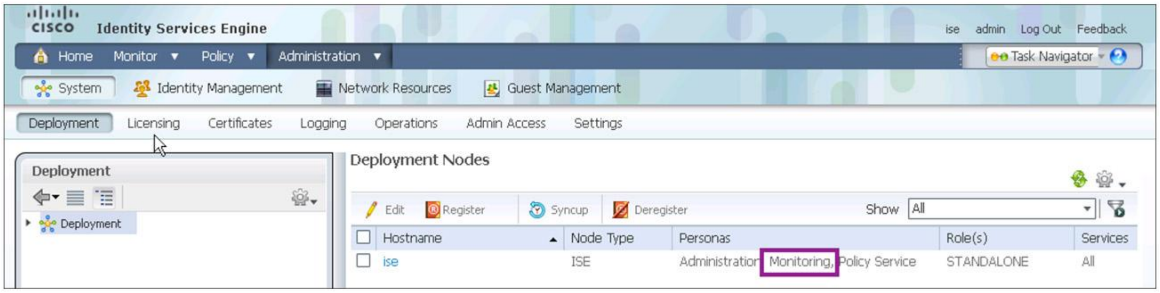
In order to successfully invoke the API call on a Cisco ISE node, the node must be deployed as a valid MNT node. This deployment can be verified by checking the ISE deployment configuration in the ISE dashboard.

Step 1. Log in to the Cisco ISE dashboard.

Step 2. Go to Administration → System → Deployment.

The Deployment Nodes page appears, which lists all configured nodes that are deployed.

Step 3. In the Role(s) column of the Deployment Nodes page, verify that the role for the target node that you want to monitor shows its type as a Cisco Monitoring ISE node. (Note: The Standalone role includes MNT functionality.)


Identity Services Engine
ise admin Log Out Feedback
Home Monitor Policy Administration
Task Navigator
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Operations Admin Access Settings
Deployment
Deployment
Deployment Nodes
Edit Register Syncup Deregister
Show All

Hostname	Node Type	Personas	Role(s)	Services
ise	ISE	Administration, Monitoring, Policy Service	STANDALONE	All

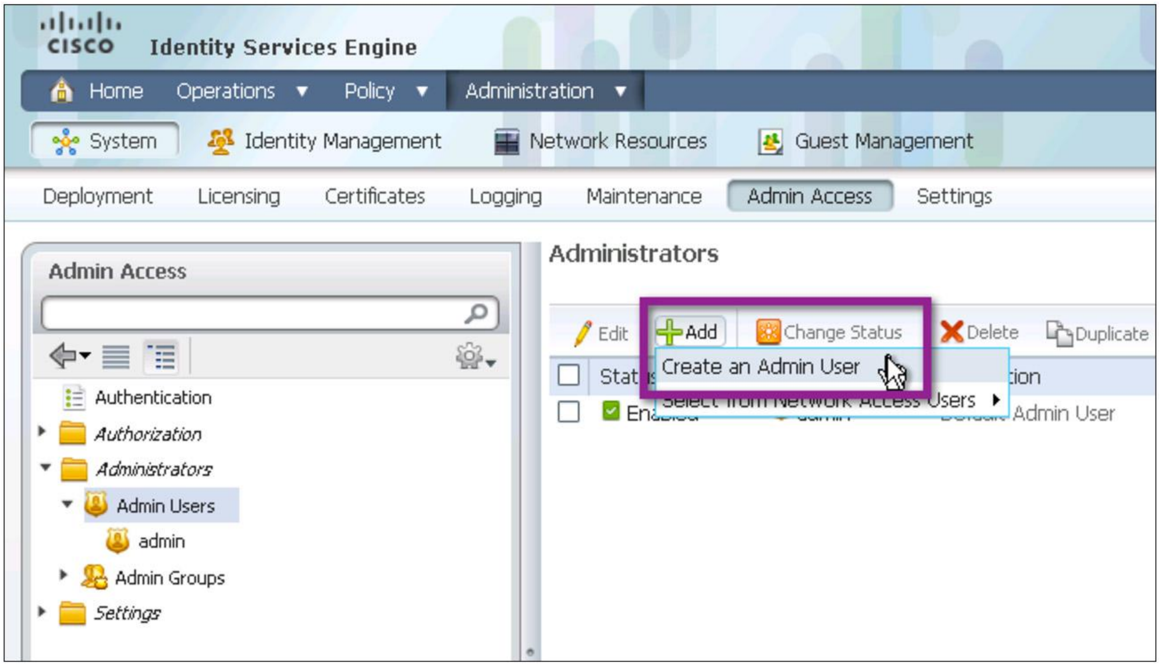
Procedure 2: Create an admin user on the ISE for monitoring access.

Best Practice: For the Cisco Cyber Threat Defense Solution and any deployment that makes use of the ISE REST APIs, the recommended practice is to create a separate user account on the ISE to authenticate API use.

Step 1. Log in to the ISE dashboard.

Step 2. Go to Administration → System → Admin Access → Administrators.

Step 3. Select **Admin Users**. Click **Add** and select **Create an Admin User**.


Identity Services Engine
Home Operations Policy Administration
System Identity Management Network Resources Guest Management
Deployment Licensing Certificates Logging Maintenance Admin Access Settings
Admin Access
Authentication
Authorization
Administrators
Admin Users
admin
Admin Groups
Settings
Administrators
Edit Add Change Status Delete Duplicate
Create an Admin User
Select from Network Access Users
Status
Enabled
admin
Default Admin User

Step 4. Fill out the Admin User, Password, User Information, Account Options, and Admin Groups sections.

Configuration Item	Settings
Admin User	Name the Admin user something easy to distinguish. Ensure that the account status is set to Enabled.
Password	Create a password for the user.
User Information	Optional: Add information to describe the user.
Account Options	Optional: Add a meaningful description; for example: **Account used by the SteathWatch Management Console to access ISE Session information for the Cisco Cyber Threat Defense Solution**
Admin Groups	Put the user in the pre-defined **Helpdesk Admin** group.

Step 5. Click **Submit**.

Procedure 3: Ensure that there are active sessions in ISE.

Step 1. Log in to the ISE dashboard.

Step 2. Click Operations → Authentications.

Step 3. Ensure that the Live Authentications table is not empty.

Procedure 4: Check the ISE APIs using a web browser.

The integration between the Cisco ISE and the Lancope SMC utilizes two API calls supported by the Cisco ISE:

- Authenticated Sessions List - Retrieve a list of all currently active authenticated sessions
- Endpoint by IP Address - Retrieve authenticated session information for host by IP Address

Before continuing the integration, it is recommended that the Admin credentials and API operation be validated using a web browser.

Step 1. Open a web browser (Mozilla Firefox is recommended).

Step 2. Call the **AuthList** API using the following URL: https://ise.demo.local/ise/mnt/api/Session/AuthList/null/null.

Note: In this example, ise.demo.local is the DNS name of the ISE node. Substitute the correct DNS name or IP address of the ISE MNT node in your environment.

Step 3. Log in using the monitoring credentials from Procedure 2.

Step 4. Verify that the Authentication List is displayed.

Note: The authentication list will be empty if there are no active authenticated sessions maintained within the ISE. If no sessions are returned from the API go to the ISE dashboard to validate that there are active sessions.

Step 5. Using an IP address from an active session in the ISE, call the **Endpoint by IP Address** API at the following URL: https://ise.demo.local/ise/mnt/api/Session/EndPointIPAddress/<*ip-address*>.

Step 6. Log in using the monitoring credentials from Procedure 2.

Step 7. Verify that the Authentication Session information is retrieved.

Procedure 5: Configure the Certificate Authority certificates.

The SMC must be configured to trust the certificate authority that issued the Cisco ISE's Identity Certificate. If best practices were followed in the deployment of the StealthWatch System this procedure is already complete, if not the Certificate Authority's Certificate needs to be obtained and installed on the SMC.

Step 1. Log into the SMC (administration) web interface.

Step 2. From the home page, click Configuration → Certificate Authority Certificates.

Step 3. Click **Choose File** and then browse the local disk to locate the CA certificate.

Step 4. Give the certificate a name to identify it in the SMC configuration.

Step 5. Click **Add Certificate**.

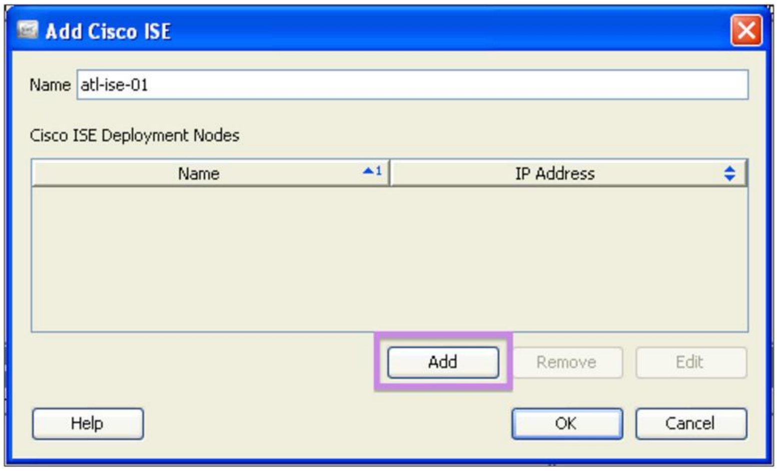
Procedure 6: Register the Cisco ISE with the Lancope SMC.

At this point in the deployment, it has been verified that there are active authentication session in the Cisco ISE, and that they can be retrieved by an external entity using a configured username and password.

Step 1. Log in to the SMC client software.

Step 2. Highlight the domain, then click Configuration → Add Cisco ISE…

Step 3. Enter a name for the ISE deployment.



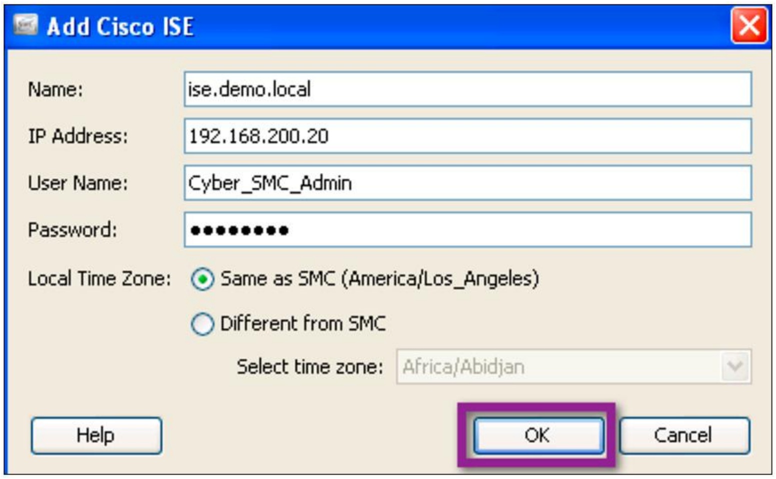
Add Cisco ISE

Name: atl-ise-01

Cisco ISE Deployment Nodes

Name	IP Address

Step 4. Click **Add**, enter Name, IP Address, User Name, and Password, then click **OK**.



Add Cisco ISE

Name: ise.demo.local

IP Address: 192.168.200.20

User Name: Cyber_SMC_Admin

Password: ●●●●●●●●

Local Time Zone: ● Same as SMC (America/Los_Angeles)

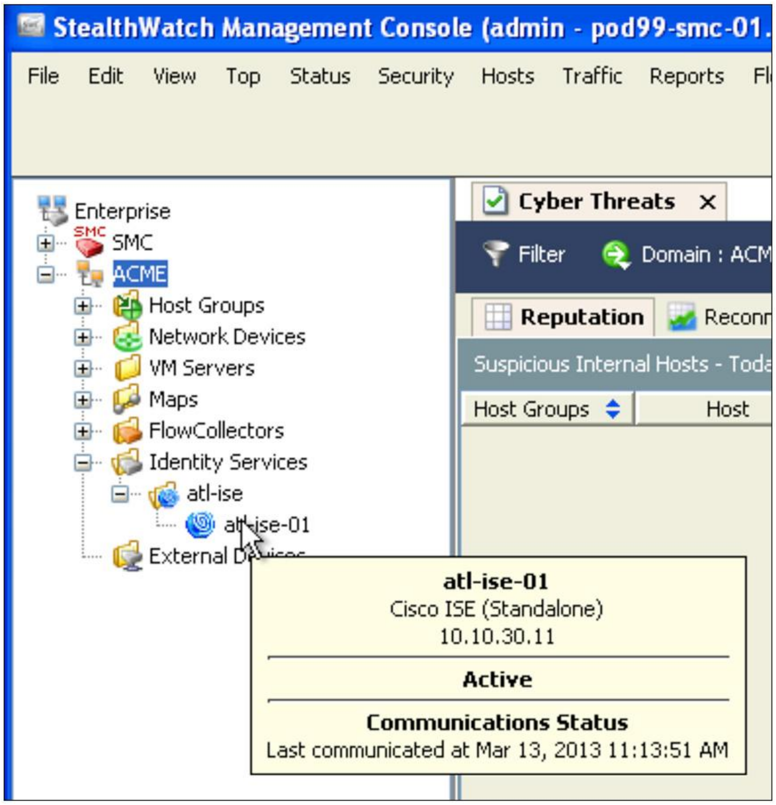
○ Different from SMC

Select time zone: Africa/Abidjan

Step 5. (optional) To enter a second ISE MNT node for redundancy, repeat Step 5 for the second node.

Step 6. Check the communication status with the Cisco ISE.

Expand the Identity Services menu and place the mouse pointer over the ISE icon to see communication status.



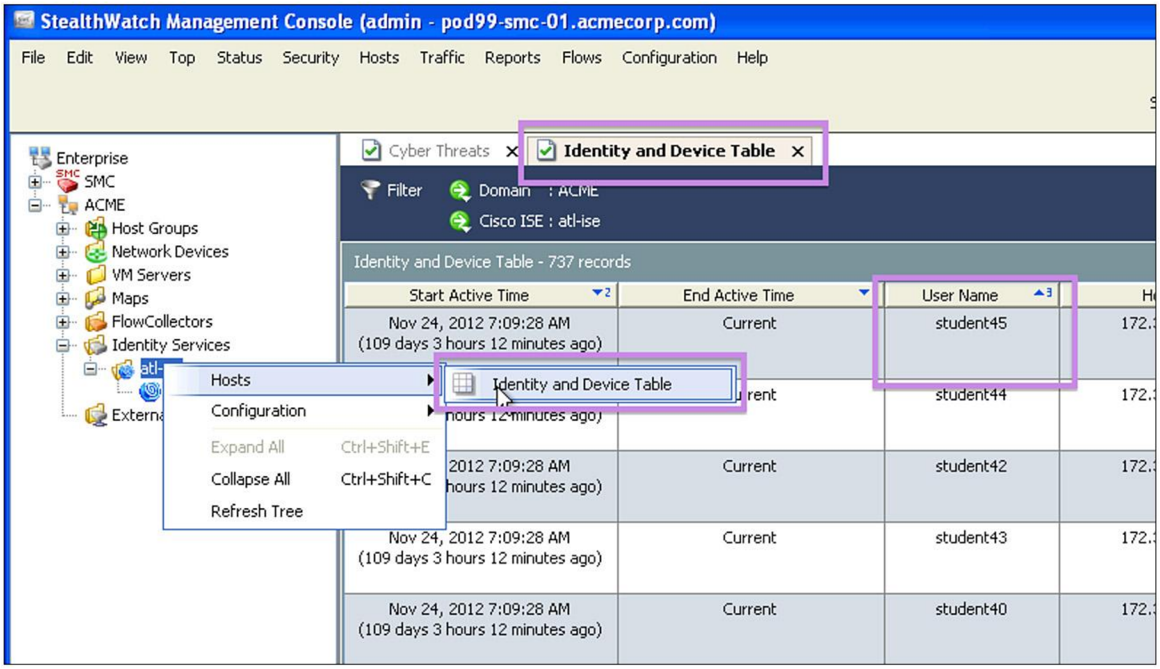
atl-ise-01
Cisco ISE (Standalone)
10.10.30.11

Active

Communications Status
Last communicated at Mar 13, 2013 11:13:51 AM

Step 7. Right-click the ISE icon and go Hosts → Identity and Device Table.

This will open the Identity and Device Table. Verify that authenticated usernames are present in the table.


StealthWatch Management Console (admin - pod99-smc-01.acmecorp.com)
File Edit View Top Status Security Hosts Traffic Reports Flows Configuration Help
Enterprise
SMC
ACME
Host Groups
Network Devices
VM Servers
Maps
FlowCollectors
Identity Services
atl-
Externa
Cyber Threats
Identity and Device Table
Filter
Domain : ACME
Cisco ISE : atl-ise
Hosts
Configuration
Expand All Ctrl+Shift+E
Collapse All Ctrl+Shift+C
Refresh Tree
Identity and Device Table

Identity and Device Table - 737 records

Start Active Time	End Active Time	User Name	H
Nov 24, 2012 7:09:28 AM (109 days 3 hours 12 minutes ago)	Current	student45	172.
hours 12 minutes ago)	rent	student44	172.
2012 7:09:28 AM hours 12 minutes ago)	Current	student42	172.
Nov 24, 2012 7:09:28 AM (109 days 3 hours 12 minutes ago)	Current	student43	172.
Nov 24, 2012 7:09:28 AM (109 days 3 hours 12 minutes ago)	Current	student40	172.

Procedure 7 (Optional): Check SMC logging.

At this point, it has been verified that authentication session information is available from the Cisco ISE. If the information is not being displayed appropriately in the Lancope SMC, verify that the SMC is calling the Cisco ISE using logging mechanisms on the SMC.

Step 1. Open a console connection to the SMC.

Step 2. Go to/etc/init.d.

Step 3. Open the file named lc-tomcat.

Step 4. Locate the following lines and uncomment the second line:

```
#Uncomment following line for debugging
JAVA_OPTS=$JAVA_OPTS" -Dcom.lancope.debug=2 -Xdebug -Xrunjdwp: transport=dt_socket,
server=y, address=8000, suspend=n"
```

Step 5. Log files will be placed under/lancope/var/smc/log. Check the logs to see if the SMC is appropriately calling the ISE APIs.

Working With Authenticated Session Information in the SMC

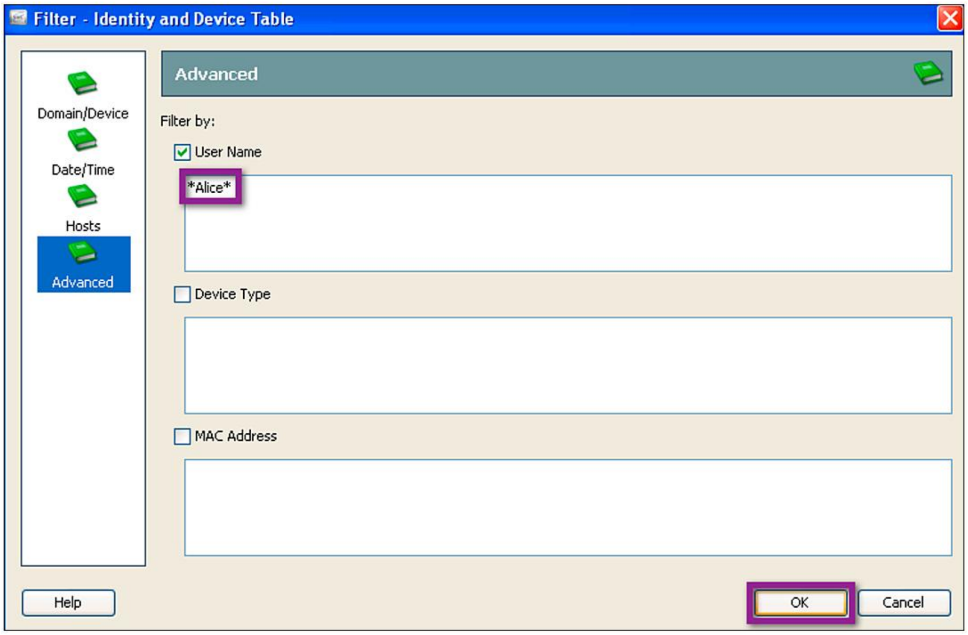
Authenticated session information from the Cisco ISE is available in the Lancope SMC in the Identity and Device Table. This information can be used to locate all of the flows based on authenticated session information. Authenticated session information can also be viewed in the **Identity, DHCP & Host Notes** section of the host snapshot.

The following procedures describe two workflows highlighting the capabilities of the integration.

Procedure 1: Find all flows for a given user.

Step 1. From the Enterprise Tree, right-click the ISE icon, then select Hosts → Identity and Device Table.

Step 2. In the Identity and Device Table, apply appropriate filters to locate the desired username.



Filter - Identity and Device Table

Advanced

Filter by:

☑ User Name

Alice

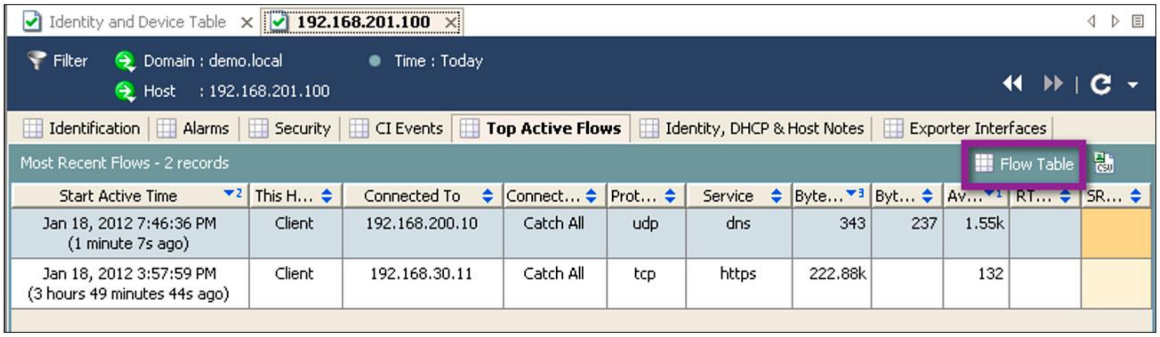
☐ Device Type

☐ MAC Address

Note: Username filters can contain the wildcard * character.

Step 3. Right click the username in the Identity and Device Table and click Host Snapshot.

Step 4. In the Top Active Flows tab, click the Flow Table icon.



Domain : demo.local

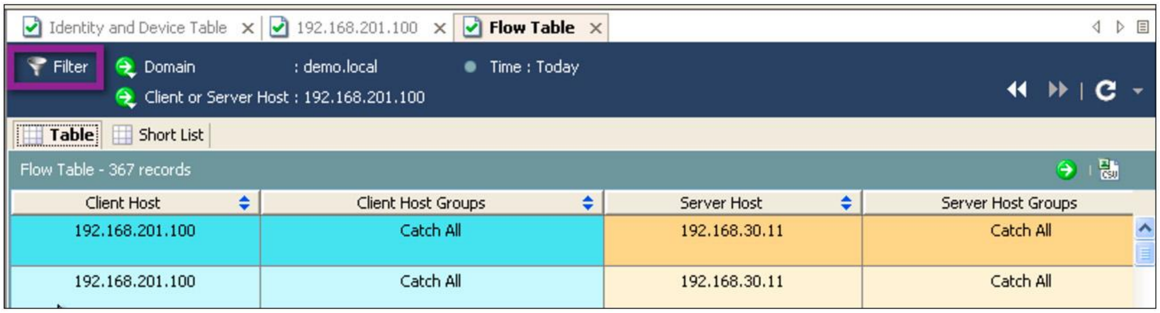
Host : 192.168.201.100

Time : Today

Most Recent Flows - 2 records

Start Active Time	This H...	Connected To	Connect...	Prot...	Service	Byte...	Byt...	Av...	RT...	SR...
Jan 18, 2012 7:46:36 PM (1 minute 7s ago)	Client	192.168.200.10	Catch All	udp	dns	343	237	1.55k		
Jan 18, 2012 3:57:59 PM (3 hours 49 minutes 44s ago)	Client	192.168.30.11	Catch All	tcp	https	222.88k		132		

Step 5. Apply the appropriate filters to drill down and locate the particular flow(s) of interest.



Domain : demo.local

Client or Server Host : 192.168.201.100

Time : Today

Flow Table - 367 records

Client Host	Client Host Groups	Server Host	Server Host Groups
192.168.201.100	Catch All	192.168.30.11	Catch All
192.168.201.100	Catch All	192.168.30.11	Catch All

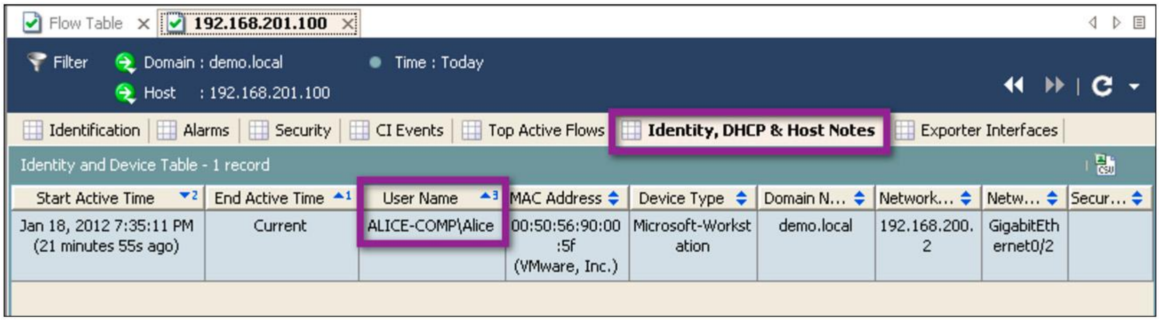
Procedure 2: Find the user responsible for a given flow.

Note: This procedure assumes that the reader has already identified a flow that needs further investigation, and is interesting in locating the user responsible for it. For more on how to identify suspicious flows, consult the Cisco Cyber Threat Defense Solution How-To Guides.

Step 1. From the Flow Table, right-click the IP address requiring investigation, then click Host Snapshot.

Step 2. In the Host Snapshot view for that IP address, select the Identity, DHCP & Host Notes tab.

Step 3. Locate the username and other authenticated session information in the Identity and Device Table.



Domain : demo.local

Host : 192.168.201.100

Time : Today

Identity and Device Table - 1 record

Start Active Time	End Active Time	User Name	MAC Address	Device Type	Domain N...	Network...	Netw...	Secur...
Jan 18, 2012 7:35:11 PM (21 minutes 55s ago)	Current	ALICE-COMP\Alice	00:50:56:90:00:5f (VMware, Inc.)	Microsoft-Workstation	demo.local	192.168.200.2	GigabitEthernet0/2	

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 C07-728137-00 05/13