

ISE Training

Cisco TAC BN Team Liu Yang

Migration – From NAC/ACS to ISE

Why Migrate to ISE

- ✓ Existing ACS customer who require posture, profiling or guest services
- ✓ Existing NAC customers looking for 802.1X port level controls and adv authorization controls (e.g. SGA)
- ✓ Existing NAC Profiler customer who require additional capacity

Migration Offer

- ❑ NAC 3315/55/95 and ACS 1121 appliances can be reimaged to support ISE. Older appliances, NAC 33x0 platforms, NAC 3140 and ACS 1120, cannot. Customers with these older appliances qualify for discounted appliance migration skus (and yes they get to keep their older appliances)
- ❑ Existing ACS and NGS customers entitled to any number of Base Migration Licenses (50% discount over list price of Base Licenses)
- ❑ Existing NAC and NAC Profiler customers entitled to Advanced Migration License (3 YR) based on the total number of NAC and/or Profiler Licenses at \$0
- ❑ Existing support contracts transition to ISE support contract but prorated

Physical

Appliance SKUs

ISE-3315-M-K9

ISE-3395-M-K9

ISE-3355-M-K9

Virtual Appliance

(VM) SKUs

ISE-VM-M-K9=

ISE-5VM-M-K9=

ISE-10VM-K9=

Vmaware ISE-VM-K9

- CPU—Intel Dual-Core; 2.13 GHz or faster
- •Memory—4 GB RAM
- •Hard Disks (minimum allocated memory):
 - –Stand-alone—200 GB
 - –Administration—200 GB
 - –Policy Service and Monitoring—200 GB
 - –Monitoring—200 GB
 - –Policy Service—60 GB
- **Note** Cisco does not recommend allocating any more than 600 GB maximum space for any node.
- •NIC—1 GB NIC interface required (you can install up to 4 NICs)
- •Supported VMware versions include:
 - –ESX 4.x
 - –ESXi 4.x
 - –ESXi 5
- –For an evaluation or production version, the minimum disk space is 60 GB.
- •Memory—4 GB RAM

ISE Persona	Minimum Disk Space Requirements for Production ¹
Standalone ISE	600 GB
Administration	200 GB
Monitoring	500 GB
Administration and Monitoring	600 GB
Administration, Monitoring, and Policy Service	600 GB
Policy Service	100 GB

ISE Packaging and Licensing

ISE Base License

Base Feature Set

Perpetual Licensing

- Authentication / Authorization
- Guest Provisioning
- Link Encryption Policies

ISE Advanced License

Advanced Feature Set

3 / 5 Year Term Licensing

- Device Profiling
- Host Posture
- Security Group Access

Appliance Platforms

Small 3315/1121 | Medium 3355 | Large 3395 | Virtual Appliance

Note: Advanced License does not include Base

ISE Wireless Packaging and Licensing

ISE Wireless License

Wireless Package

Policy for Wireless Endpoints
5 Yr Term Licensing

Base

- Authentication / Authorization
- Guest Provisioning
- Link Encryption Policies



Advanced

- Device Profiling
- Host Posture
- Security Group Access

Platforms

Small 3315/1121 | Medium 3355 | Large 3395 | Virtual Appliance

Why Different Licenses

Advanced + Base License

- Default Customer Offer
- Common policy across Wired, Wireless, and VPN
- Advanced capabilities

Wireless License

- Customer wants base and advanced functionality only for wireless endpoints
- Looking for lower cost solution

Base License

- Customer wants basic authentication
- Customer wants only “Base” features

Internal licenses for labs

<http://wwwin-tools.cisco.com/SWIFT/SLT/viewIntPubKeyGen.do?subGroup=POSITRONFEAT&keytype=PUBLICINTERNAL>

CEC || CCO || SEARCH || INDEX || SUPPORT || FEEDBACK || DIRECTORY:

Internal License Generation Tool



Internal Key Generation

For internal use only by Cisco employees/contractors on Cisco owned equipment. All Actions on this page will be logged. Please use judiciously and with approval.

Product Family	Identity Services Engine		
Product Name *	ISE-ADV-365-DAY-100-ENDPTS : ▾		
Quantity:	<input type="text"/>		
Feature Name:	----- Select One ----- ▾	Quantity:	<input type="text"/>
	----- Select One ----- ▾	Quantity:	<input type="text"/>
	----- Select One ----- ▾	Quantity:	<input type="text"/>
	----- Select One ----- ▾	Quantity:	<input type="text"/>
	----- Select One ----- ▾	Quantity:	<input type="text"/>
	<input type="button" value="More Options"/>		
Email: *	<input type="text"/>		
Secondary Product Id:	<input type="text"/>		
Secondary Serial No:	<input type="text"/>		
Secondary Version Id:	<input type="text"/>		
Primary Product Id: *	<input type="text"/>		
Primary Serial No: *	<input type="text"/>		
Primary Version Id: *	<input type="text"/>		

Platform Scalability

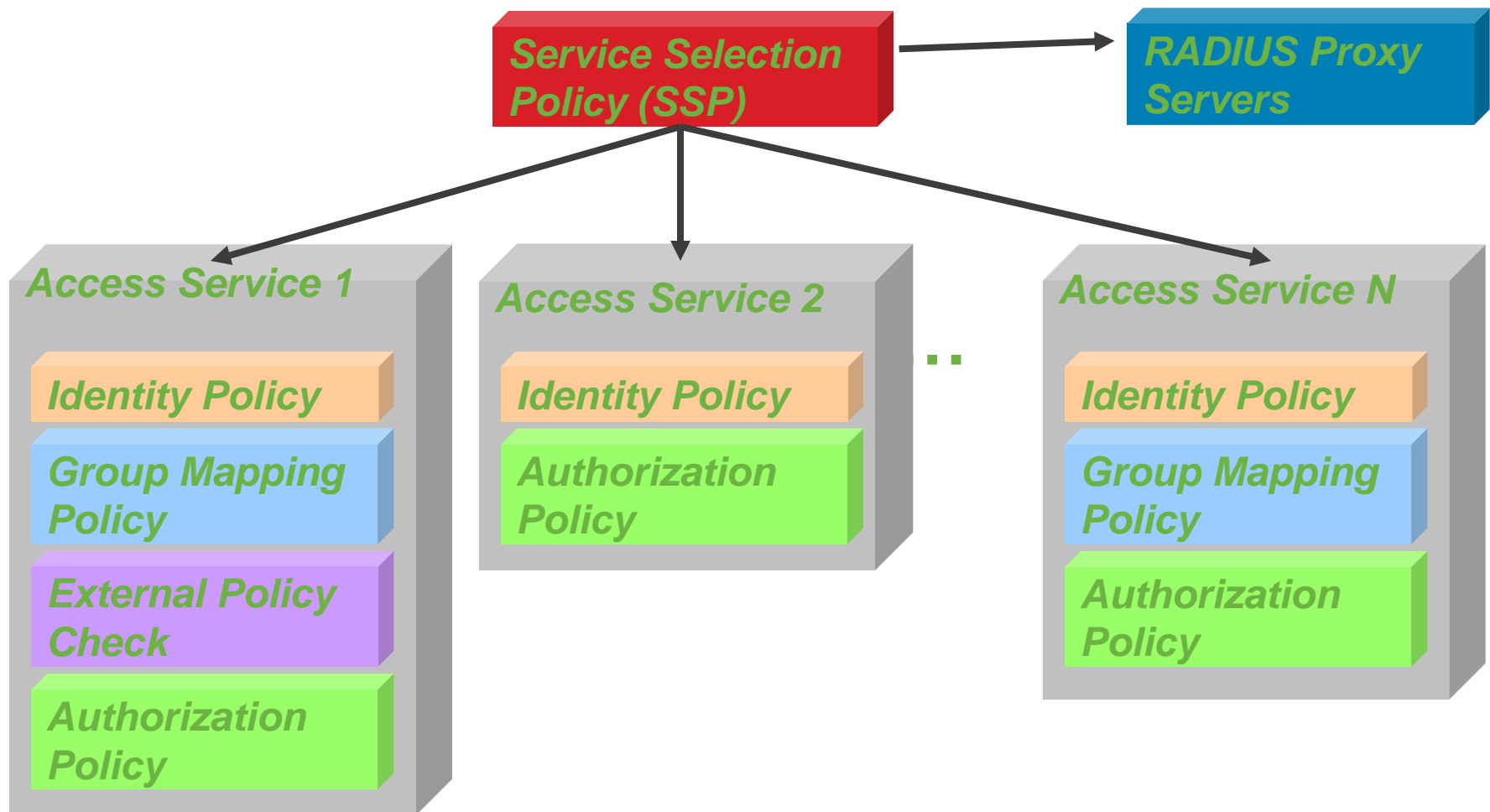
Description	Maximum
Max Concurrent Endpoints per ISE Instance	100,000
Max Policy Service Nodes per ISE Instance	40 (Currently Tested)
Max Inline Posture Service Nodes per ISE Instance	No Hard Limit
3315 Policy Service Node Running All Services*	3,000 Devices
3355 Policy Services Node Running All Services*	6,000 Devices
3395 Policy Services Node Running All Services*	10,000 Devices
VM Running All Services (Same Spec as 3395)	10,000 Devices
Single Server Running Admin/Policy Services/Monitoring Nodes	2,000 Devices

* Potentially higher without Posture/Profiling

ISE vs. ACS policy model – ACS Model

- First step in ACS policy flow was Access Service selection or RADIUS Proxy Service using “Service Selection Policy”
- Each service has a protocols configuration and set of policies (e.g. Identity and Authorization)
- A session processing is in the scope of the AccessService and according to the service configuration

ISE vs. ACS policy model – ACS (2)

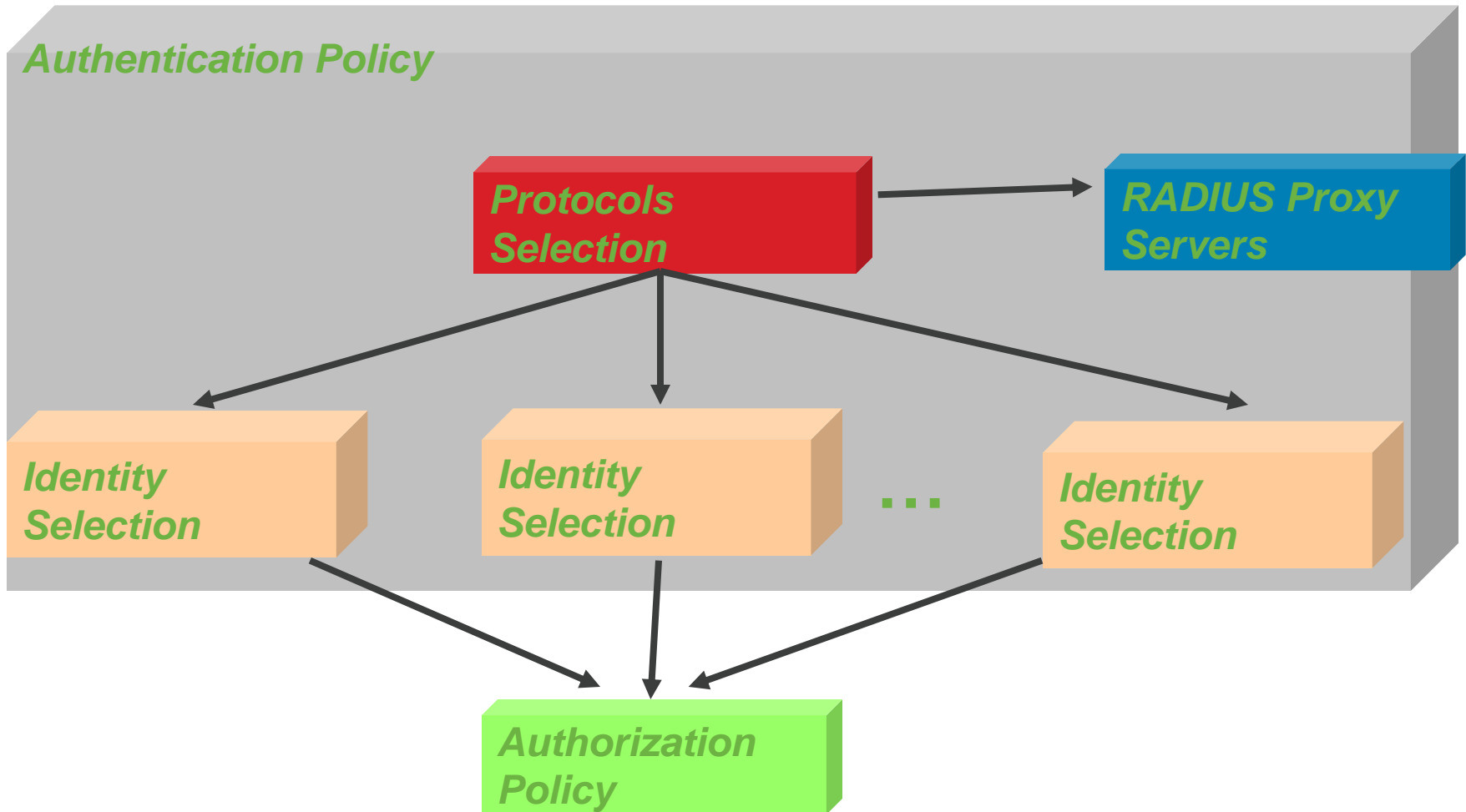


ISE vs. ACS policy model – ISE Model

- No more Access Services
- Global Authentication Policy (one set of rules)
- Authentication policy contains two phases:
 1. Protocols Selection - selection of the allow protocols for the session
 2. Identity Selection - selection of the Identity Source (along with the advanced processing options)

Outer set of rules to select allowed protocols, and under each rule there is additional set of inner rules for Identity Source selection
- Global Authorization Policy (one set of rules)

ISE vs. ACS policy model – ISE (2)



topology

DNS NTP
WINDOWS AD
10.75.61.220



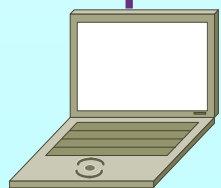
ISE
10.75.61.250



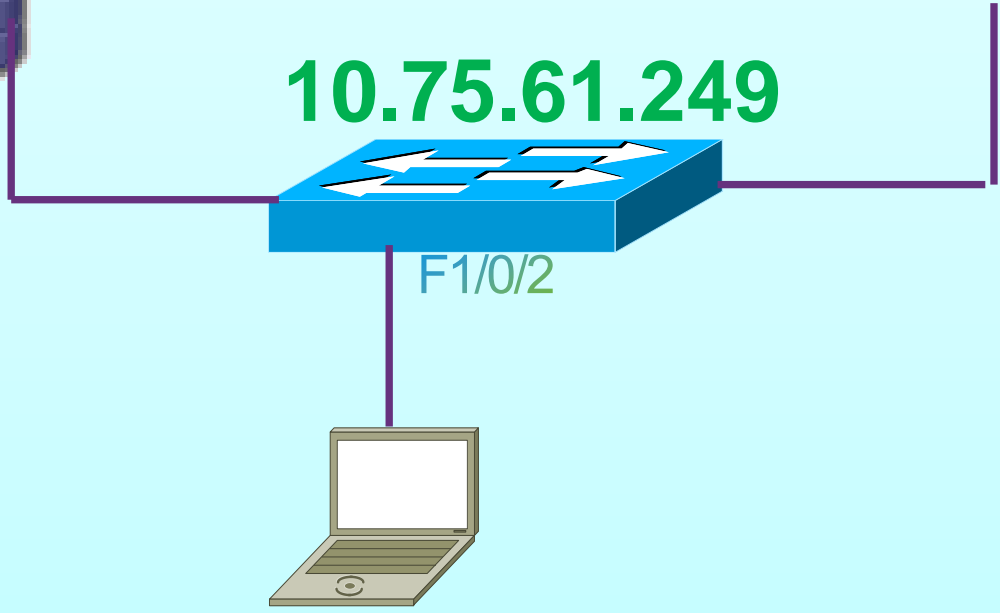
10.75.61.249



F1/0/2



DOT1X CLIENT PC(WIN 7)
ON 10.75.61.200



Lab password

1 ISE 10.75.61.250

SSH username : admin password : Payton123

GUI username : admin password : Cisco123

2 AD b.com 10.75.61.220

RDP Username : administrator password : Cisco123

3 DOT1X client Win7

On 10.75.61.200 username : administrator password : CisCo@123

Vmware→favorites→TestPC→WIN7→245-ISE-Training

4 C3750 console 10.75.60.10 : 2029

telnet 10.75.61.249 username : cisco password : cisco

Lab 1 Join to AD

Set NTP ,Timezone and DNS on ISE

```
hostname ISE
!
ip domain-name cisco.com
!
interface GigabitEthernet 0
 ip address 10.75.61.190 255.255.255.128
 ipv6 address autoconfig
!
interface GigabitEthernet 1
 shutdown
!
interface GigabitEthernet 2
!
interface GigabitEthernet 3
!
ip name-server 10.75.61.177
!
ip default-gateway 10.75.61.129
!
ip route 192.168.0.0 255.255.0.0 gateway 10.75.61.135
!
clock timezone Asia/Shanghai
!
ntp server 10.75.61.177
!
```



External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

Active Directory > AD1

- Connection
- Advanced Settings
- Groups
- Attributes

To configure Active Directory:

- First enter the required fields: the **Domain Name** to connect to and the **Identity Store Name** to refer to Active Directory in the ISE deployment.
- After the configuration has been submitted, then Join or Leave operations must be performed.

* Domain Name

* Identity Store Name

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before

Save Configuration Delete Configuration

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

Active Directory > security.lab

Connection Advanced Settings Groups Attributes

* Domain Name security.lab

* Identity Store Name security.lab

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select one node for Test Connection.

Join Leave Test Connection

<input type="checkbox"/>	ISE Node	ISE Node Role	Status
<input checked="" type="checkbox"/>	ISE	STANDALONE	Not Joined to Domain

Save Configuration Delete Configuration

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

Active Directory > security.lab

Connection Advanced Settings Groups Attributes

* Domain Name security.lab

* Identity Store Name security.lab

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before a rejoin. Select or

Join Leave Test Connection

<input type="checkbox"/>	ISE Node	ISE Node Role	Status
<input checked="" type="checkbox"/>	ISE	STANDALONE	⚠ Not Joined to Domain

Join Domain

* User Name: liuyang

* Password: ●●●●●●


OK Cancel

Join Operation Status



The list below shows the status of the requested operation for each node.

Status: Successful

ISE Node	Status
ISE	 Completed.



Close

Connection

Advanced Settings

Groups

Attributes

* Domain Name

* Identity Store Name

One or more nodes may be selected for Join or Leave operations. If a node is joined then a leave operation is required before

 Join  Leave  Test Connection ▼

<input type="checkbox"/>	ISE Node	ISE Node Role	Status
<input checked="" type="checkbox"/>	ISE	STANDALONE	 Connected to: win-grnegvct6l2.security.lab



External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

Active Directory > security.lab

Connection Advanced Settings **Groups** Attributes

+ Add - Delete Group

Name

No data available

Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory. Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.

Domain: security.lab

Filter: *

Retrieve Groups... Number of Groups Retrieved: 37 (Limit is 100)

<input type="checkbox"/> Name	Group Type
<input type="checkbox"/> security.lab/Builtin/Backup Operators	LOCAL
<input type="checkbox"/> security.lab/Builtin/Certificate Service DCOM Access	LOCAL
<input type="checkbox"/> security.lab/Builtin/Cryptographic Operators	LOCAL
<input type="checkbox"/> security.lab/Builtin/Distributed COM Users	LOCAL
<input type="checkbox"/> security.lab/Builtin/Event Log Readers	LOCAL
<input type="checkbox"/> security.lab/Builtin/Guests	LOCAL
<input type="checkbox"/> security.lab/Builtin/IIS_IUSRS	LOCAL
<input type="checkbox"/> security.lab/Builtin/Incoming Forest Trust Builders	LOCAL
<input type="checkbox"/> security.lab/Builtin/Network Configuration Operators	LOCAL
<input type="checkbox"/> security.lab/Builtin/Performance Log Users	LOCAL
<input type="checkbox"/> security.lab/Builtin/Performance Monitor Users	LOCAL
<input type="checkbox"/> security.lab/Builtin/Pre-Windows 2000 Compatible Access	LOCAL
<input type="checkbox"/> security.lab/Builtin/Print Operators	LOCAL
<input type="checkbox"/> security.lab/Builtin/Remote Desktop Users	LOCAL
<input type="checkbox"/> security.lab/Builtin/Replicator	LOCAL

Lab2 Add NAD to ISE

Network Devices

Search

Back Settings

- Network Devices
- Default Device

Network Devices

Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Location	Type	Description
------	---------	----------	------	-------------

No data available

Network Devices

Navigation icons: back, forward, settings

Network Devices

Default Device

Network Devices List > New Network Device

Network Devices

* Name

Description

* IP Address: /

Model Name

Software Version

* Network Device Group

Location

Set To Default

Device Type

Set To Default

Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

* Shared Secret

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

SNMP Settings

SGA Attributes

Lab3 Telnet testing

Compound Conditions

Navigation icons: back, list, table, settings

- Wired_MAB
- Wireless_MAB
- Wired_802.1X
- Wireless_802.1X
- Switch_Local_Web_Authentication
- WLC_Web_Authentication
- telnet

Authentication Compound Condition List > telnet

Authentication Compound Conditions

* Name telnet

Description

Condition Name	Expression
<input type="text"/>	Radius:NAS-Port-Type Equals Virtual

Save Reset



Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If	Wired_MAB	allow protocols	Allowed Protocol : Default Netw	and...	Actions
<input checked="" type="checkbox"/>	Dot1X	: If	Wired_802.1X	allow protocols	Allowed Protocol : Default Netw	and...	Actions
<input checked="" type="checkbox"/>	Default Rule (If no match)	: allow protocols	Allowed Protocol : Default Netw	and use identity source :	Internal Users		Actions Insert new row above

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type Simple Rule-Based

MAB : If Wired_MAB allow protocols Allowed Protocol : Default Network and...

Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Network and...

telnet : If Select Attribute allow protocols Select Network Access and...

Default

Add All Conditions Below to Library

Condition Name	Expression
Select Condition	

Dictionary

- Simple Condition
- Compound Condition**

Default Rule (If no match) : allow protocols Allowed Protocol : Internal Users source : Internal Users

Save Reset

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type Simple Rule-Based

MAB : If Wired_MAB allow protocols Allowed Protocol : Default Network and...

Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Network and...

telnet : If telnet allow protocols Select Network Access and...

Default : use Internal Users

Default Rule (If no match) : allow protocols Allowed Protocol : Default Network and use identity source :

Network Access Services

Allowed Protocols

RADIUS Server Sequence

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If	Wired_MAB	allow protocols	Allowed Protocol : Default Network	and...	Actions
<input checked="" type="checkbox"/>	Dot1X	: If	Wired_802.1X	allow protocols	Allowed Protocol : Default Network	and...	Actions
<input checked="" type="checkbox"/>	Standard Rule 1	: If	telnet	allow protocols	Allowed Protocol : Default Network	and...	Actions
<input checked="" type="checkbox"/>	Default	: use	security.lab				Actions
<input checked="" type="checkbox"/>	Default Rule (if no match)	: allow protocols	Allowed Protocol : Default Network	and use identity source :	Internal Users		Actions

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type Simple Rule-Based

- MAB : If Wired_MAB allow protocols Allowed Protocol : Default Network and...
- Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Network and...
- telnet : If telnet allow protocols Allowed Protocol : Default Network and...

- Default : use Internal Users
- Default Rule (if no match) : allow protocols

Identity Source: Internal Users

Options

If authentication failed: Reject

If user not found: Reject

If process failed: Drop

Note: For authentications using PEAP, LEAP, EAP-FAST or RADIUS it is not possible to continue processing when authentication fails. If continue option is selected in these cases, requests will be rejected.

Identity Source List

- Internal Endpoints
- Internal Users
- security_lab
- Guest_Portal_Sequence
- Sponsor_Portal_Sequence
- MyDevices_Portal_Sequence
- DenyAccess

Save Reset

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_802.1X	then Blackhole_Wireless_Access	Edit ▼
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones	Edit ▼
<input checked="" type="checkbox"/>	Default	if no matches, then PermitAccess		Edit ▼

User Access Verification

Username: liuyang

Password:

C3750>en

Home Operations Policy Administration Task Navigator

Authentications Endpoint Protection Service Alarms Reports Troubleshoot

Live Authentications

Add or Remove Columns Refresh Refresh: Every 1 minute Show: Latest 100 records within: Last 24 hours

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure Reason	Auth Method	Authentication Pro
Nov 22,12 11:36:42.688 AM	✖		cisco	10.75.43.40		switch	tty1				Authentication...	22056 Subject...	PAP_ASCII	PAP_ASCII
Nov 22,12 11:26:42.568 AM	✖		cisco	10.75.43.40		switch	tty2				Authentication...	22056 Subject...	PAP_ASCII	PAP_ASCII
Nov 22,12 11:16:42.517 AM	✖		cisco	10.75.43.40		switch	tty2				Authentication...	22056 Subject...	PAP_ASCII	PAP_ASCII
Nov 22,12 11:14:08.384 AM	✔		liuyang	72.163.226.66		switch	tty2	PermitAccess		NotApplicable	Authentication...		PAP_ASCII	PAP_ASCII

Lab 4 MAB

Authentication

Simple Conditions

Compound Conditions

Authentication Compound Condition List > Wired_MAB

Authentication Compound Conditions

* Name Wired_MAB

Description A Condition To Match MAC Authentication Bypass Service Requests From Cisco Catalyst Switches

Condition Name	Expression	AND
	Radius:Service-Type Equals Call Check	AND
	Radius:NAS-Port-Type Equals Ethernet	

Save Reset

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type Simple Rule-Based

<input checked="" type="checkbox"/>	MAB	: If	Wired_MAB	allow protocols	Allowed Protocol : Default Netw	and...	Actions
<input checked="" type="checkbox"/>	Default	: use	Internal Endpoints				Actions
<input checked="" type="checkbox"/>	Dot1X	: If	Wired_802.1X	allow protocols	Allowed Protocol : Default Netw	and...	Actions
<input checked="" type="checkbox"/>	Standard Rule 1	: If	telnet	allow protocols	Allowed Protocol : Default Netw	and...	Actions
<input checked="" type="checkbox"/>	Default Rule (If no match)	: allow protocols	Allowed Protocol : Default Netw	and use identity source :	Internal Users		Actions

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
☑	Wireless Black List Default	if Blacklist AND Wireless_802.1X	then Blackhole_Wireless_Access	Edit ▼
☑	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones	Edit ▼
☑	Default	if no matches, then PermitAccess		Edit ▼

Identities

▼

←

- Users
- Endpoints**
- Latest Network Scan Results

Endpoints

Edit **Add** Delete Import Export

Endpoint Profile	MAC Address	Static Assignment
No data available		

Identities

- Users
- Endpoints
- Latest Network Scan Results

Endpoint List > **New Endpoint**

Endpoint

* MAC Address (Example: 11:11:11:11:11:11)

Policy Assignment

Static Assignment

Identity Group Assignment

Static Group Assignment

```
C3750#show run int f1/0/2
Building configuration...
```

```
Current configuration : 621 bytes
```

```
!
interface FastEthernet1/0/2
 switchport access vlan 13
 switchport mode access
 switchport port-security maximum 3
 ip access-group 100 in
 authentication event server dead action authorize vlan 20
 authentication event server alive action reinitialize
 authentication host-mode multi-auth
 authentication order mab dot1x
 authentication priority dot1x mab
 authentication port-control auto
 authentication periodic
 authentication timer reauthenticate 30
 mab
 dot1x pae authenticator
 dot1x timeout quiet-period 30
 dot1x timeout tx-period 15
 dot1x timeout supp-timeout 3
 no mdix auto
 spanning-tree portfast
end
```

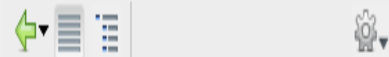
Live Authentications

Add or Remove Columns Refresh
Refresh Show within

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure Reason	Auth Method	Authentication Proto
Nov 22,12 11:55:22.201 AM	<input checked="" type="checkbox"/>		00:50:56:A8:67:06	00:50:56:A8:67:06		switch	FastEthernet1/0/2	PermitAccess	Unknown	NotApplicable	Authentication...		mab	Lookup

Lab 5 Dot1x

Authentication



- Simple Conditions
- Compound Conditions

Authentication Compound Condition List > Wired_802.1X

Authentication Compound Conditions

* Name Wired_802.1X

Description

A Condition To Match An 802.1X Based Authentication Requests From Cisco Catalyst Switches

Condition Name	Expression	AND
<input type="text"/>	Radius:Service-Type <input type="text" value="Equals"/> Framed	AND
<input type="text"/>	Radius:NAS-Port-Ty <input type="text" value="Equals"/> Ethernet	

Save Reset

Authentication Policy

Define the Authentication Policy by selecting the protocols that ISE should use to communicate with the network devices, and the identity sources that it should use for authentication.

Policy Type Simple Rule-Based

MAB : If Wired_MAB allow protocols Allowed Protocol : Default Network and...

Dot1X : If Wired_802.1X allow protocols Allowed Protocol : Default Network and...

Default : use security.lab

Standard Rule 1 : If telnet allow protocols Allowed Protocol : Default Network and...

Default Rule (If no match) : allow protocols Allowed Protocol : Default Network and use identity source : Internal Users

Results

Search bar with magnifying glass icon and navigation icons (back, list, table, settings).

- Authentication
- Authorization
 - Authorization Profiles
 - Downloadable ACLs
 - Inline Posture Node Profiles
- Profiling
- Posture
- Client Provisioning
- Security Group Access

Standard Authorization Profiles

Edit Add Duplicate Delete

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	Blackhole_Wireless_Access	Profile for Wireless Blackholing. Please make sure the BLACKHOLE ACL is
<input type="checkbox"/>	Cisco_IP_Phones	Profile For Cisco Phones.
<input type="checkbox"/>	DenyAccess	Default Network Authorization Profile with access type as Access-Reject
<input type="checkbox"/>	PermitAccess	Default Network Authorization Profile with access type as Access-Accept

Results

Navigation icons: back, list, settings

- Authentication
- Authorization
 - Authorization Profiles
 - Blackhole_Wireless_Access
 - Cisco_IP_Phones
 - DenyAccess
 - PermitAccess
 - Downloadable ACLs
 - Inline Posture Node Profiles
- Profiling
- Posture
- Client Provisioning
- Security Group Access

Authorization Profiles > New Authorization Profile

Authorization Profile

* Name

Description

* Access Type

Common Tasks

DACL Name

VLAN Tag ID 1

Voice Domain Permission

Web Authentication

Auto Smart Port

Filter-ID

Advanced Attributes Settings

Select an item = - +

Attributes Details

Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:91
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

Active Directory > security.lab

Connection Advanced Settings Groups Attributes

Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory. Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.

Domain: security.lab

Filter: * Retrieve Groups... Number of Groups Retrieved: 37 (Limit is 100)

<input type="checkbox"/>	Name	Group Type
<input type="checkbox"/>	security.lab/Users/Cert Publishers	LOCAL
<input type="checkbox"/>	security.lab/Users/Denied RODC Password Replication Group	LOCAL
<input type="checkbox"/>	security.lab/Users/DnsAdmins	LOCAL
<input type="checkbox"/>	security.lab/Users/DnsUpdateProxy	GLOBAL
<input type="checkbox"/>	security.lab/Users/Domain Admins	GLOBAL
<input type="checkbox"/>	security.lab/Users/Domain Computers	GLOBAL
<input type="checkbox"/>	security.lab/Users/Domain Controllers	GLOBAL
<input type="checkbox"/>	security.lab/Users/Domain Guests	GLOBAL
<input checked="" type="checkbox"/>	security.lab/Users/Domain Users	GLOBAL
<input type="checkbox"/>	security.lab/Users/Enterprise Admins	UNIVERSAL
<input type="checkbox"/>	security.lab/Users/Enterprise Read-only Domain Controllers	UNIVERSAL
<input type="checkbox"/>	security.lab/Users/Group Policy Creator Owners	GLOBAL
<input type="checkbox"/>	security.lab/Users/RAS and IAS Servers	LOCAL
<input type="checkbox"/>	security.lab/Users/Read-only Domain Controllers	GLOBAL
<input type="checkbox"/>	security.lab/Users/Schema Admins	UNIVERSAL

OK Cancel

Authorization Policy

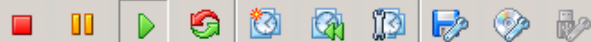
Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_802.1X	then Blackhole_Wireless_Access	Edit
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones	Edit
<input checked="" type="checkbox"/>	dot1x	if security.lab:ExternalGroups EQUALS security.lab/Users/Domain Users	then dot1x_v91	Edit
<input checked="" type="checkbox"/>	Default	if no matches, then PermitAccess		Edit

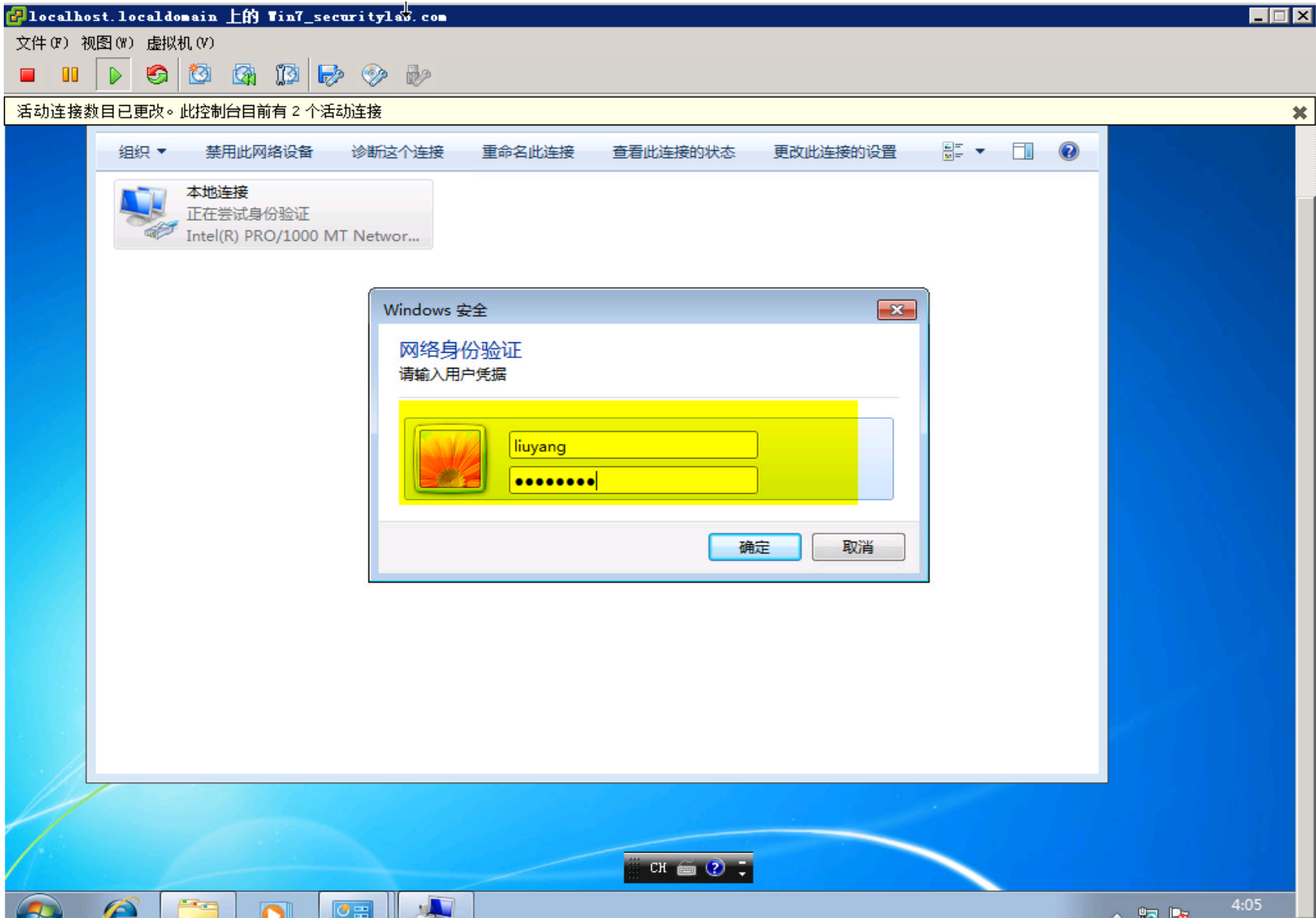


活动连接数目已更改。此控制台目前有 2 个活动连接

组织 禁用此网络设备 诊断这个连接 重命名此连接 查看此连接的状态 更改此连接的设置

本地连接
正在尝试身份验证
Intel(R) PRO/1000 MT Networ...

需要其他信息以连接到该网络
单击以提供其他信息。



```
C3750#show authentication sessions int f1/0/2
  Interface:      FastEthernet1/0/2
  MAC Address:    0000.0000.0003
  IP Address:     Unknown
  User-Name:      000000000003
  Status:         Running
  Domain:         DATA
  Security Policy: Should secure
  Security status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Idle timeout:   N/A
  Common Session ID: 0A4B3D870000000B03CC4CAEE
  Acct Session ID:  0x00000FA1
  Handle:          0x290000B0
```

```
Runnable methods list:
  Method      State
  mab         Failed over
  dot1x       Running
```

```
-----
  Interface:      FastEthernet1/0/2
  MAC Address:    0050.56a8.6706
  IP Address:     192.168.91.3
  User-Name:      liuyang
  Status:         Authz Success
  Domain:         DATA
  Security Policy: Should secure
  Security status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By:  Authentication Server
  Vlan Policy:    91
  Session timeout: 30s (local), Remaining: 9s
  Timeout action: Reauthenticate
  Idle timeout:   N/A
  Common Session ID: 0A4B3D870000000B33CC6382A
  Acct Session ID:  0x00000FA5
  Handle:          0x7F0000B3
```

```
Runnable methods list:
  Method      State
  mab         Failed over
  dot1x       Authc Success
```

Live Authentications

Add or Remove Columns Refresh Refresh Every 1 minute Show Latest 100 records within Last 24 hours

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure Reason	Auth Method	Authentication Protocol
Nov 22, 12 01:09:04.997 PM			liuyang	00:50:56:A8:67:06	192.168.91.3	switch	FastEthernet1/0/2	dot1x_y91		NotApplicable	Authentication...		dot1x	PEAP(EAP-MSCHAPv2)



Authentication Result

User-Name=liuyang
State=ReauthSession:0A4B3D87000000B33CC6382A
Class=CACS:0A4B3D87000000B33CC6382A:ISE/142887195/2895
Termination-Action=RADIUS-Request
Tunnel-Type=(tag=1) VLAN
Tunnel-Medium-Type=(tag=1) 802
Tunnel-Private-Group-ID=(tag=1) 91

Lab 6 DACL

Results

Search bar with magnifying glass icon and navigation icons (back, list, table, settings).

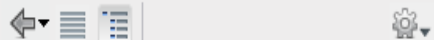
- Authentication
- Authorization
 - Authorization Profiles
 - Downloadable ACLs
 - Inline Posture Node Profiles
- Profiling
- Posture
- Client Provisioning
- Security Group Access

Downloadable ACLs

Edit Add Duplicate Delete

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	DENY_ALL_TRAFFIC	Deny all traffic
<input type="checkbox"/>	PERMIT_ALL_TRAFFIC	Allow all Traffic

Results



- Authentication
- Authorization
 - Authorization Profiles
 - Downloadable ACLs
 - Inline Posture Node Profiles
- Profiling
- Posture
- Client Provisioning
- Security Group Access

Downloadable ACL List > New Downloadable ACL

Downloadable ACL

* Name To_ISE

Description

* DACL Content

```
permit ip any host 10.75.61.190
deny ip any any
```

Submit Cancel

Results

Authentication

Authorization

- Authorization Profiles
 - Blackhole_Wireless_Access
 - Cisco_IP_Phones
 - DACL
 - DenyAccess
 - PermitAccess
 - dot1x_y91
- Downloadable ACLs
 - DENY_ALL_TRAFFIC
 - PERMIT_ALL_TRAFFIC
 - To_ISE
- Inline Posture Node Profiles

Profiling

Posture

Client Provisioning

Security Group Access

Authorization Profiles > dot1x_y91

Authorization Profile

* Name: dot1x_y91

Description: []

* Access Type: ACCESS_ACCEPT

Common Tasks

- DACL Name**: To_ISE
- VLAN**: Tag ID 1 [Edit Tag] ID/Name 91
- Voice Domain Permission
- Web Authentication
- Auto Smart Port
- Filter-ID

Advanced Attributes Settings

Select an item = [] - +

Attributes Details

```
Access Type = ACCESS_ACCEPT
Tunnel-Private-Group-ID = 1:91
Tunnel-Type=1:13
Tunnel-Medium-Type=1:6
DACL = To_ISE
```

Save Reset

```
C3750#show auth sess int f1/0/2
  Interface: FastEthernet1/0/2
  MAC Address: 0000.0000.0003
  IP Address: Unknown
  User-Name: 0000000000003
  Status: Authz Failed
  Domain: DATA
  Security Policy: should secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A4B3D870000000B93CDC60E5
  Acct Session ID: 0x00000FFD
  Handle: 0x340000B9
```

```
Runnable methods list:
  Method      State
  mab         Failed over
  dot1x       Failed over
```

```
-----
  Interface: FastEthernet1/0/2
  MAC Address: 0050.56a8.6706
  IP Address: 192.168.91.3
  User-Name: liuyang
  Status: Authz Success
  Domain: DATA
  security Policy: should secure
  Security Status: Unsecure
  Oper host mode: multi-auth
  Oper control dir: both
  Authorized By: Authentication Server
  Vlan Policy: 91
  ACS ACL: XACSACLX-IP-To_ISE-50adb6fc
  Session timeout: 30s (local), Remaining: 14s
  Timeout action: Reauthenticate
  Idle timeout: N/A
  Common Session ID: 0A4B3D870000000B83CDC4AB6
  Acct Session ID: 0x00001027
  Handle: 0x730000B8
```

```
Runnable methods list:
  Method      State
  mab         Failed over
  dot1x       Authc success
```

```
C3750#show ip access-lists interface f 1/0/2
  permit udp any any (9 matches)
  permit ip any host 10.75.61.190
C3750#
```

Lab 7

Machine Access restrictions (MAR)

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

Active Directory > security.lab

Connection Advanced Settings Groups Attributes

- Enable Password Change
 - Enable Machine Authentication
 - Enable Machine Access Restrictions
- Aging Time (hours) (Valid Range 1 to 8760)

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Wireless Black List Default	if Blacklist AND Wireless_802.1X	then Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
✓	dot1x	if Any and security.lab:ExternalGroups EQUALS...	then dot1x_v91
✓	Default	if no matches, then Perm	

Condition Name Expression

security.lab:ExternalGroups EQUALS security.lab/Users/G

AND

Add All Conditions Below to Library

- Add Attribute/Value
- Add Condition from Library
- Duplicate
- Add Condition to Library
- Delete

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	Wireless Black List Default	if Blacklist AND Wireless_802.1X	then Blackhole_Wireless_Access	Edit
✓	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones	Edit
✓	dot1x	if (security.lab:ExternalGroups EQUALS security.lab/Users/Domain Users AND Network Access:WasMachineAuthenticated EQUALS True)	then dot1x_y91	Edit
✓	Default	if no matches, then	DenyAccess	Edit

组织 ▾

禁用此网络设备

诊断这个连接

重命名此连接

查看此连接的状态

更改此连接设置的



本地连接

身份验证失败

Intel(R) PRO/1000 MT Network...

```
C3750#show authentication sess int f1/0/2
  Interface: FastEthernet1/0/2
  MAC Address: 0000.0000.0003
  IP Address: Unknown
  User-Name: 000000000003
  Status: Running
  Domain: DATA
  security Policy: should secure
  Security Status: Unsecure
  oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A4B3D87000000B93CDC60E5
  Acct Session ID: 0x00000FFD
  Handle: 0x340000B9
```

```
Runnable methods list:
  Method   State
  mab      Failed over
  dot1x    Running
```

```
-----
  Interface: FastEthernet1/0/2
  MAC Address: 0050.56a8.6706
  IP Address: Unknown
  User-Name: liuyang
  Status: Authz Failed
  Domain: DATA
  security Policy: should secure
  Security Status: Unsecure
  oper host mode: multi-auth
  Oper control dir: both
  Session timeout: N/A
  Idle timeout: N/A
  Common Session ID: 0A4B3D87000000BA3D091E08
  Acct Session ID: 0x000010A2
  Handle: 0x3E0000BA
```

```
Runnable methods list:
  Method   State
  mab      Failed over
  dot1x    Authc Failed
```

Live Authentications

Add or Remove Columns Refresh Refresh: Every 1 minute Show: Latest 100 records within: Last 24 hours

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure Reason	Auth Method	Authentication Protocol
Nov 22, 12 02:16:26.663 PM			00:00:00:00:00:03	00:00:00:00:00:03		switch	FastEthernet1/0/2					Authentication... 22056 Subject...	mab	Lookup
Nov 22, 12 02:16:22.092 PM			liuyang	00:50:56:A8:67:06		switch	FastEthernet1/0/2	DenyAccess				Authentication... 15039 Rejecte...	dot1x	PEAP(EAP-MSCHAPv2)

External Identity Sources

- Certificate Authentication Profile
- Active Directory
- LDAP
- RADIUS Token
- RSA SecurID

Active Directory > security.lab

Connection Advanced Settings Groups Attributes

+ Add - Delete Group

- Name
- security.lab/Users/Doma

Select Directory Groups

This dialog is used to select groups from the Directory. Click **Retrieve Groups..** to read directory. Use * for wildcard search (i.e. admin*). Search filter applies to group name and not the fully qualified path.

Domain: security.lab

Filter: *

Retrieve Groups...

Number of Groups Retrieved: 37 (Limit is 100)

<input type="checkbox"/> Name	Group Type
<input type="checkbox"/> security.lab/Builtin/Windows Authorization Access Group	LOCAL
<input type="checkbox"/> security.lab/Users/Allowed RODC Password Replication Group	LOCAL
<input type="checkbox"/> security.lab/Users/Cert Publishers	LOCAL
<input type="checkbox"/> security.lab/Users/Denied RODC Password Replication Group	LOCAL
<input type="checkbox"/> security.lab/Users/DnsAdmins	LOCAL
<input type="checkbox"/> security.lab/Users/DnsUpdateProxy	GLOBAL
<input type="checkbox"/> security.lab/Users/Domain Admins	GLOBAL
<input checked="" type="checkbox"/> security.lab/Users/Domain Computers	GLOBAL
<input type="checkbox"/> security.lab/Users/Domain Controllers	GLOBAL
<input type="checkbox"/> security.lab/Users/Domain Guests	GLOBAL
<input checked="" type="checkbox"/> security.lab/Users/Domain Users	GLOBAL
<input type="checkbox"/> security.lab/Users/Enterprise Admins	UNIVERSAL
<input type="checkbox"/> security.lab/Users/Enterprise Read-only Domain Controllers	UNIVERSAL
<input type="checkbox"/> security.lab/Users/Group Policy Creator Owners	GLOBAL
<input type="checkbox"/> security.lab/Users/RAS and IAS Servers	LOCAL

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_802.1X	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	machine authentication	if security.lab:ExternalGroups EQUALS security.lab/Users/Domain Computers	then PermitAccess
<input checked="" type="checkbox"/>	dot1x	if security.lab:ExternalGroups EQUALS security.lab/Users/Domain Users AND Network_Access:WasMachineAuthenticated EQUALS True	then dot1x_v91
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

Save

Reset

Reload dot1x client initail machine authen


CISCO Identity Services Engine ISE admin Logout Feeds

Home Operations Policy Administration Task Navigator

Authentications Endpoint Protection Service Alarms Reports Troubleshoot

Live Authentications

Add or Remove Columns Refresh Refresh: Every 1 minute Show: Latest 100 records within: Last 24 hours

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure Reason	Auth Method	Authentication Protocol
Nov 22, 12 02:38:33.196 PM	<input checked="" type="checkbox"/>	 host/WIN7PC.security		00:50:56:A8:67:06		switch	FastEthernet1/0/2	PermitAccess		NotApplicable	Authentication...		dot1x	PEAP(EAP-MGCHAPv2)

Live Authentications

Add or Remove Columns Refresh

Refresh Every 1 minute Show Latest 100 records within Last 24 hours

Time	Status	Details	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure Reason	Auth Method	Authentication Protocol
Nov 22, 12 02:42:12.552 PM	✓		#ACSAcl#-IP-To_ISE			switch						DAcl Downlo...		
Nov 22, 12 02:42:12.473 PM	✓		liuyang	00:50:56:A8:67:06		switch	FastEthernet1/0/2	dot1x_y91		NotApplicable	Authentication...		dot1x	PEAP(EAP-MSCHAPv2)
Nov 22, 12 02:41:21.968 PM	✗		00:00:00:00:03	00:00:00:00:03		switch	FastEthernet1/0/2				Authentication...	22056 Subject...	mab	Lookup
Nov 22, 12 02:41:09.433 PM	✗		00:50:56:A8:67:06	00:50:56:A8:67:06		switch	FastEthernet1/0/2				Authentication...	22056 Subject...	mab	Lookup
Nov 22, 12 02:39:37.029 PM	✗		00:50:56:A8:67:06	00:50:56:A8:67:06		switch	FastEthernet1/0/2				Authentication...	22056 Subject...	mab	Lookup
Nov 22, 12 02:39:34.969 PM	✗		00:00:00:00:03	00:00:00:00:03		switch	FastEthernet1/0/2				Authentication...	22056 Subject...	mab	Lookup
Nov 22, 12 02:39:05.227 PM	✓		host/WIN7PC.security	00:50:56:A8:67:06		switch	FastEthernet1/0/2	PermitAccess		NotApplicable	Authentication...		dot1x	PEAP(EAP-MSCHAPv2)

Troubleshooting – debug log

- For expert debug details, the following debug logs can help developers troubleshooting
- prrt.log replace the acs-runtime.log from acs – it has the same messages (without the rule-engine)
- ise-psc.log (component epm-pip) provides details on rule evaluation
- ise-prrt.log provides details on runtime-JNI
- catalina.out can provide details about errors in the initial policy configuration (less relevant for runtime)

Change log level to debug

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The navigation menu includes Home, Operations, Policy, Administration, System, Identity Management, Network Resources, and Web Portal Management. The 'Logging' menu is expanded, showing options like Local Log Settings, Remote Logging Targets, Logging Categories, Message Catalog, and Debug Log Configuration. The 'Debug Log Configuration' page is active, displaying a table of components and their current log levels. The table has columns for Component Name, Log Level, and Description. Several rows are highlighted with red boxes, indicating the target components for log level changes.

Component Name	Log Level	Description
<input type="radio"/> epm-pap	WARN	All entites query related messages
<input type="radio"/> epm-pap-api.services	WARN	all entities like user,role,group, resources implementation messages
<input type="radio"/> epm-pdp	WARN	Policy decision point messages
<input type="radio"/> epm-pip	WARN	Policy information point messages
<input type="radio"/> eps	WARN	Endpoint Protection Service (EPS) debug messages
<input type="radio"/> guest	WARN	Core Guest debug messages
<input type="radio"/> guestadmin	WARN	Administration guest and sponsor management messages
<input type="radio"/> guestauth	WARN	Web portal authentication debug messages
<input type="radio"/> guestportal	WARN	Guest portal debug messages
<input type="radio"/> identity-store-AD	WARN	Active Directory interaction messages
<input type="radio"/> infrastructure	INFO	infrastructure business logic messages
<input type="radio"/> mnt-alarm	WARN	Debug alert manager on M&T nodes
<input type="radio"/> mnt-collector	WARN	Debug collector on M&T nodes
<input type="radio"/> mydevices	WARN	My Devices Portal debug messages
<input type="radio"/> nsf	WARN	NSF related messages
<input type="radio"/> nsf-session	WARN	Session cache messages
<input type="radio"/> org-apache	WARN	Apache internal messages
<input type="radio"/> org-apache-cxf	WARN	CXF messages
<input type="radio"/> org-apache-digester	WARN	XML processing apache internal messages
<input type="radio"/> posture	WARN	Posture debug messages
<input type="radio"/> profiler	WARN	profiler debug messages
<input type="radio"/> provisioning	WARN	Client Provisioning client debug messages
<input type="radio"/> prrt-JNI	WARN	prrt policy decision request processing layer related messages
<input type="radio"/> runtime-AAA	WARN	AAA runtime messages (prrt)
<input type="radio"/> runtime-config	WARN	AAA runtime configuration messages (prrt)
<input type="radio"/> runtime-logging	WARN	customer logs center messages (prrt)
<input type="radio"/> sponsorportal	WARN	Sponsor portal debug messages
<input type="radio"/> swiss	WARN	Swiss protocol internal messages

Download debug log-1

The screenshot shows the Cisco ISE Troubleshoot interface. The navigation bar includes Home, Operations, Policy, and Administration. The main menu has Authentication, Endpoint Protection Service, Alarms, Reports, and Troubleshoot. The Troubleshoot section is active, showing Diagnostic Tools and Download Logs. The Appliance node list on the left shows a single node named ISE. The main content area is titled 'Support Bundle' and 'Debug Logs', displaying a table of debug log types and their corresponding log files.

Debug Log Type	Log File
ise-psc	ise-psc.log
ise-prrt	ise-prrt.log
ise-edf	ise-edf.log
prrt	prrt.log
profiler	profiler.log
ise-tracking	ise-tracking.log
mnt-alarm	mnt-alarm.out
mnt-collector	mnt-collector.out

Download debug log-2

The screenshot shows the Cisco ISE management console interface. At the top, there is a navigation bar with tabs for Home, Operations, Policy, and Administration. Below this, there are several functional buttons: Authentications, Endpoint Protection Service, Alarms, Reports, and Troubleshoot. A 'Diagnostic Tools' section is visible, with a 'Download Logs' button highlighted. On the left side, there is a sidebar titled 'Appliance node list' containing a single entry for 'ISE'. The main content area is titled 'Support Bundle' and has a 'Debug Logs' button. Below this, a table lists various debug log types and their corresponding log files. The 'catalina' node is highlighted with a red box, and its associated log files are listed below it.

Debug Log Type	Log File
isebootstrap	isebootstrap-20121121-232927.log
monit	monit.log
pki	pki.log
iseLocalStore	iseLocalStore.log iseLocalStore.log.2012-11-21-23-44-58-807 iseLocalStore.log.2012-11-22-00-00-40-537
ad_agent	ad_agent.log
catalina	catalina.2012-11-21.log catalina.2012-11-22.log catalina.out