

17. Cisco Firepower 与ISE PIC整合实战

教主VIP, 聊点高级的!



乾颐堂

教主技术进化论 2022

主讲人: 现任明教教主

北京乾颐堂网络实验室出品

- 
1. ISE PIC技术介绍
 2. 环境介绍
 3. AD, FMC, ISE整合
 4. FMC策略





乾硕堂

1. ISE PIC技术介绍

ISE-PIC Overview

Passive Identity Connector (ISE-PIC) offers a centralized, one-stop installation and implementation enabling you to easily and simply configure your network in order to **receive and share user identity information**[接收并分享用户身份信息给不同的安全产品] with a variety of different security product subscribers such as Cisco Firepower Management Center (FMC) and Stealthwatch. As the full broker for passive identification, **ISE-PIC collects user identities from different provider sources, such as Active Directory Domain Controllers (AD DC), maps the user login information to the relevant IP addresses in use and then shares that mapping information with any of the subscriber security products that you have configured.**[ISE-PIC从不同的提供源, 例如:AD域控制器, 收集用户登录信息, 并且映射到IP地址, 然后分享给配置的订阅者]

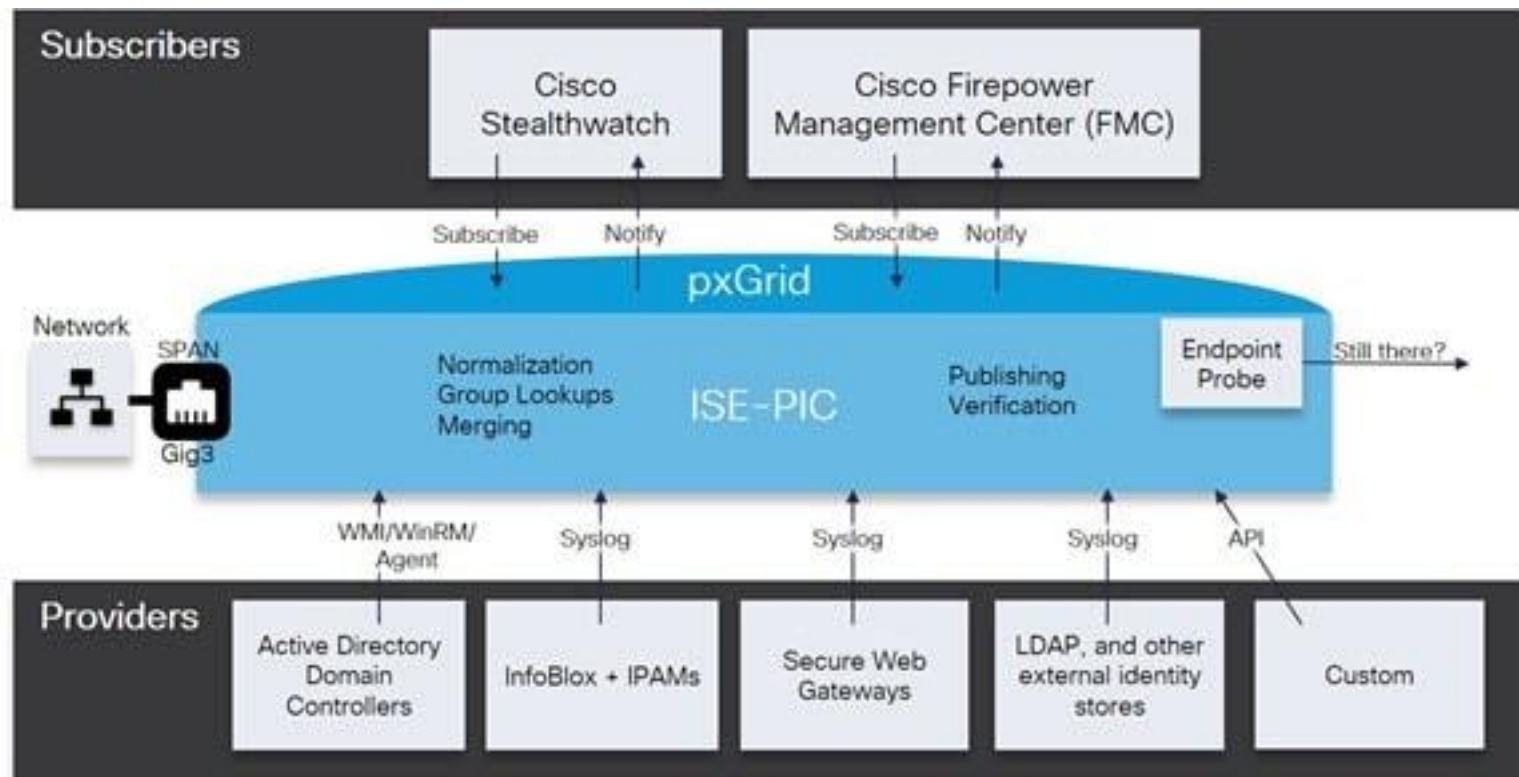
What is Passive Identity?

Products such as the Cisco Identity Services Engine (ISE), which provide an authentication, authorization and accounting (AAA) server, and utilize technologies such as 802.1X or Web Authentication, **communicate directly with the user or endpoint**[主动认证直接和用户或者终端通信], requesting access to the network, and then using their login credentials in order to verify and actively authenticate their identity.

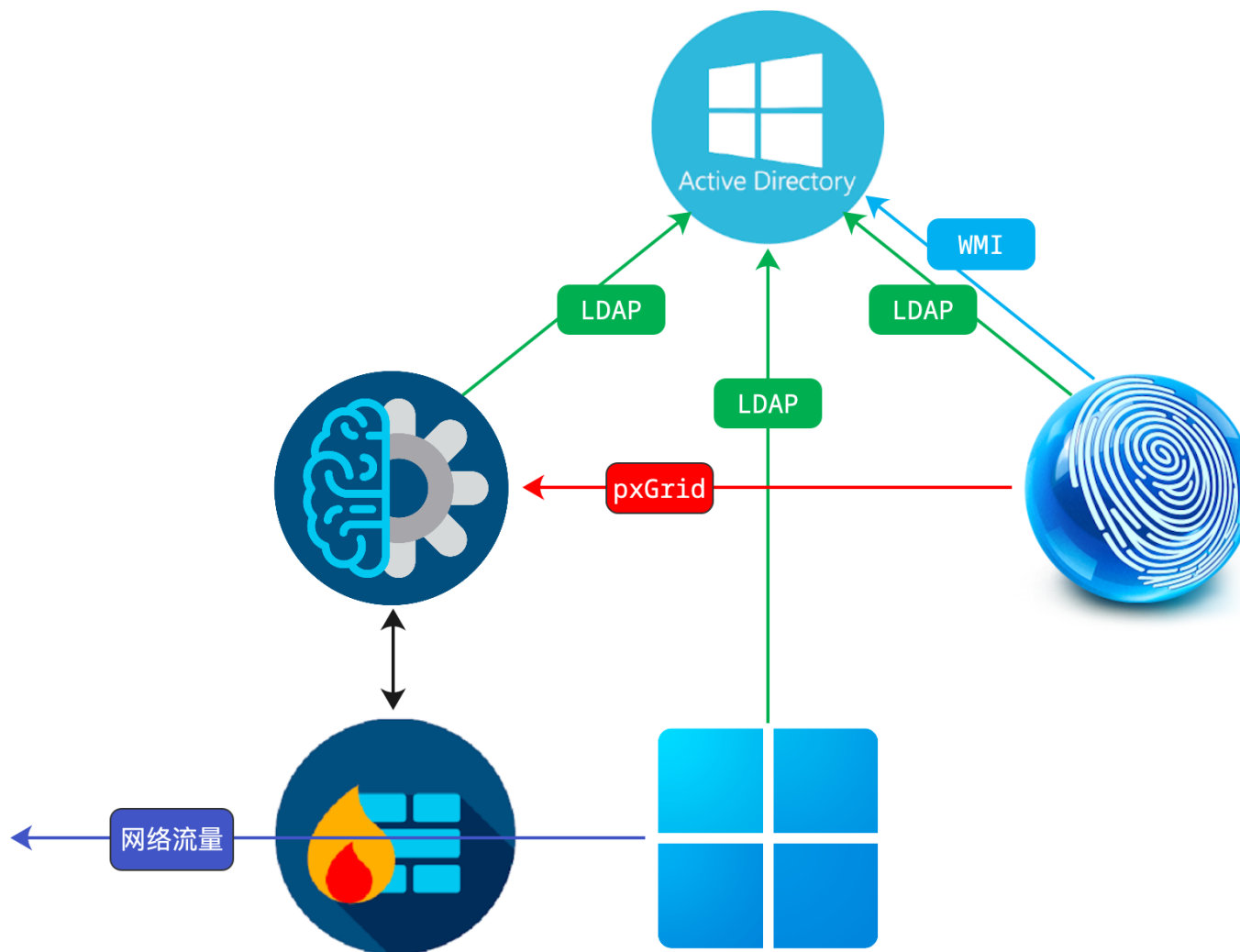
Passive identity services do not authenticate users directly[被动身份服务不直接认证用户], but rather **gather user identities and IP addresses from external authentication servers such as Active Directory, known as providers, and then share that information with subscribers**[从外部认证服务器, 例如AD, 收集用户和IP信息, 并分享这些信息给订阅者]. ISE-PIC first receives the user identity information from the provider, usually based on the user login and password, and then performs the necessary checks and services in order to match the user identity with the relevant IP address, thereby delivering the authenticated IP address to the subscriber.

Passive Identity Connector (ISE-PIC) Flow

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



流程示意图

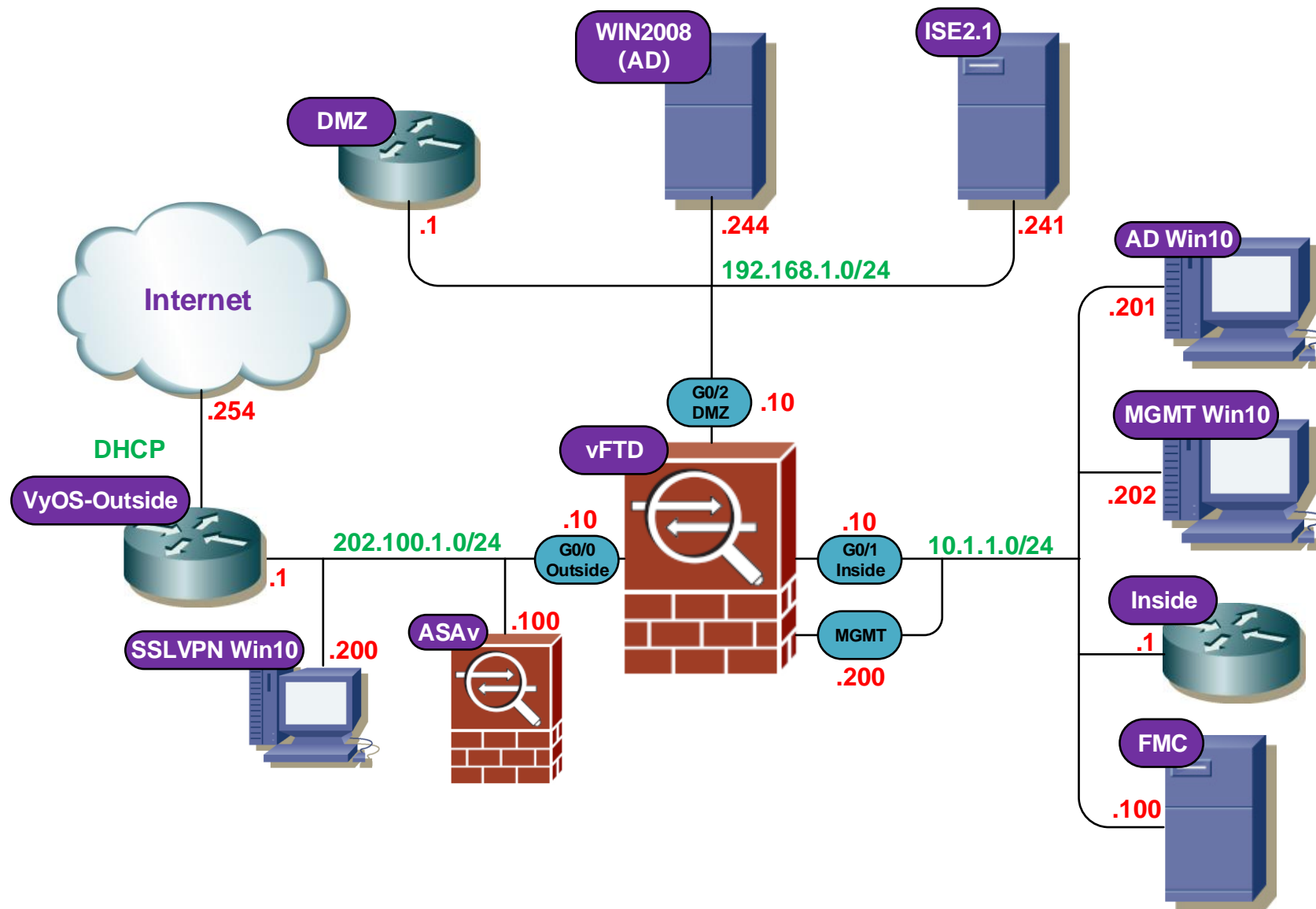




乾颐堂

2. 环境介绍

实验拓扑





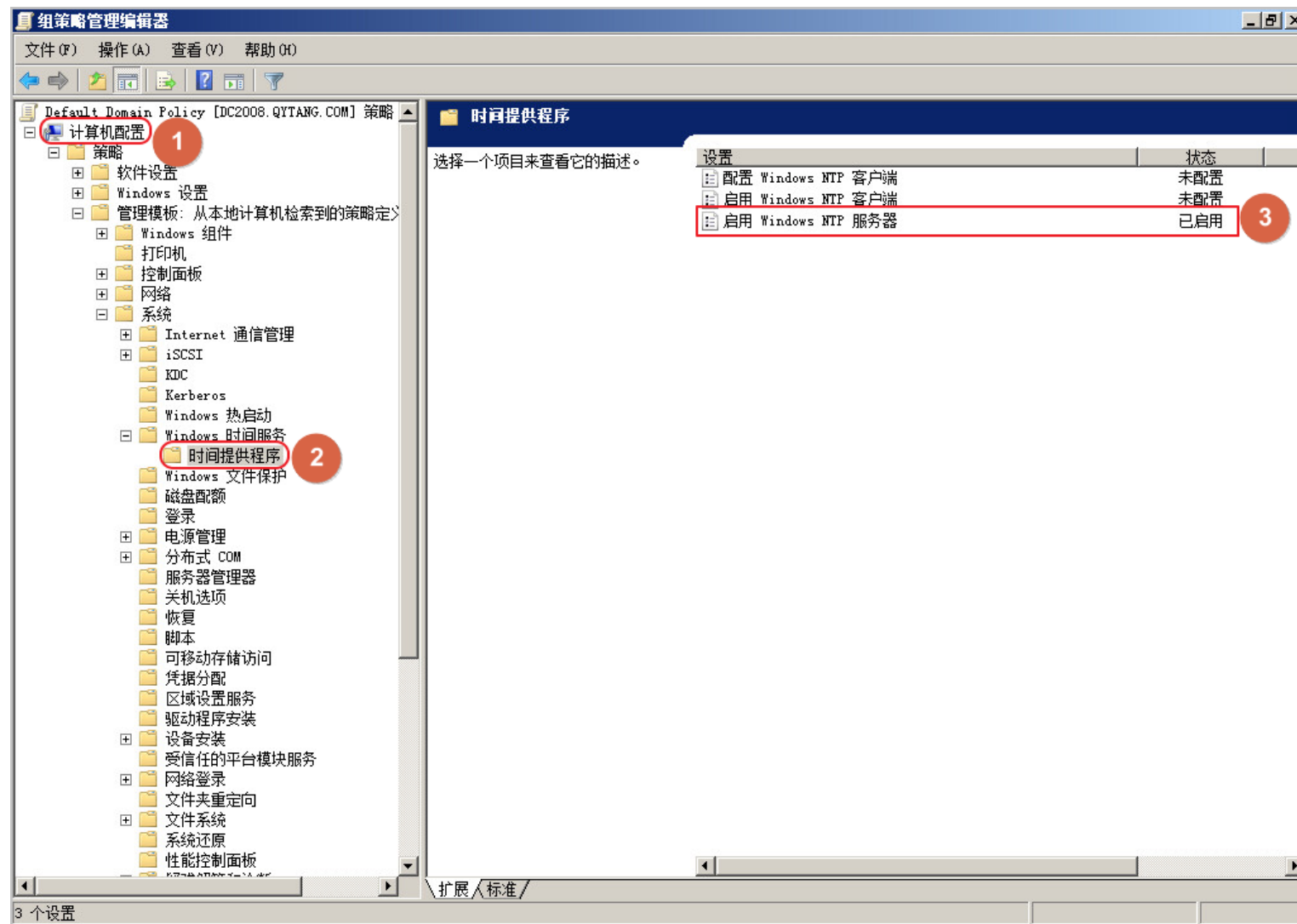
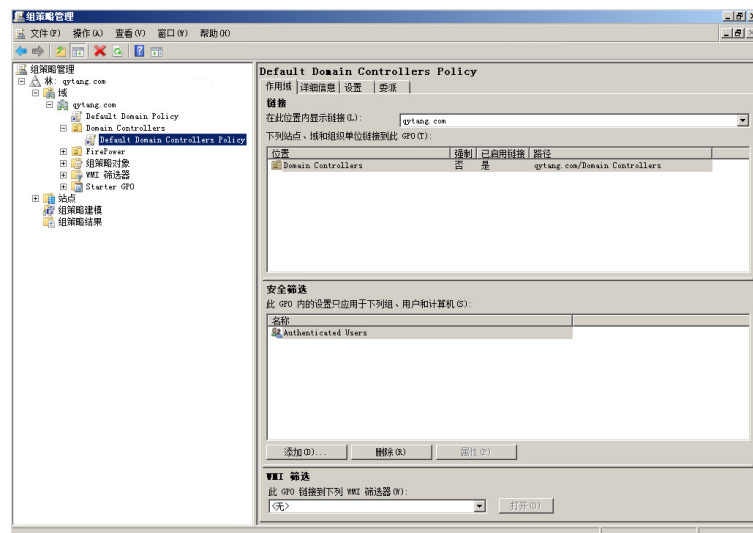
乾颐堂

3. AD, FMC, ISE整合

激活pxGrid和Passive ID服务

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation path is: Administration > Deployment Nodes List > ISE24. The main content area shows the configuration for the ISE24 node, including Hostname (ISE24), FQDN (ISE24.qytang.com), IP Address (192.168.1.241), and Node Type (Identity Services Engine (ISE)). The Role is set to STANDALONE, and the 'Make Primary' button is visible. The 'Administration' checkbox is checked. Under 'Monitoring', the Role is set to PRIMARY. Under 'Policy Service', the 'Enable Session Services' checkbox is checked, and the 'Include Node in Node Group' is set to None. The 'Enable Passive Identity Service' checkbox is checked and highlighted with a red circle and the number 7. The 'pxGrid' checkbox is also checked and highlighted with a red circle and the number 8. The 'Save' button is highlighted with a red circle and the number 9.

激活WIN2008 NTP



FMC配置NTP

Firepower Management Center
System / Configuration

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy admin

1

2

3

4 Save

Serve Time via NTP Enabled

Set My Clock

Manually in Local Configuration

Via NTP

Use the authenticated NTP server only + Add

NTP Server	Authentication	Action
192.168.1.244	N/A	<input type="checkbox"/> <input type="checkbox"/>

登录地址: 10.1.1.100

用户/密码: admin/Cisc0@123

How To

FMC配置DNS

The screenshot shows the Cisco Firepower Management Center (FMC) configuration interface. The left sidebar contains a navigation menu with 'Management Interfaces' highlighted and circled in pink with a '2'. The main content area is titled 'System / Configuration' and shows the configuration for the 'eth0' interface. The 'Shared Settings' section is expanded, showing the following fields:

- Hostname: firepower
- Domains: qytang.com (circled in pink with a '3')
- Primary DNS Server: 192.168.1.244 (circled in pink with a '4')
- Secondary DNS Server: (empty)
- Tertiary DNS Server: (empty)
- Remote Management Port: 8305

The 'ICMPv6' section is also expanded, showing two checked options:

- Allow Sending Echo Reply Packets
- Allow Sending Destination Unreachable Packets

The 'Proxy' section is expanded, showing the 'Enabled' checkbox is unchecked.

At the bottom right, there are 'Cancel' and 'Save' buttons. The 'Save' button is circled in pink with a '5'. A 'How To' button is located at the bottom center.

The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The user 'admin' is logged in, and the 'Deploy' button is visible.

WIN2008 DNS配置

The screenshot shows the Windows DNS Manager interface. The left pane displays the DNS hierarchy for DC2008, including Forward Lookup Zones, Reverse Lookup Zones, and Conditional Forwarders. The right pane shows a list of DNS records for the qytang.com zone. The records are as follows:

名称	类型	数据	时间戳
_msdcs			
_sites			
_tcp			
_udp			
DomainDnsZones			
ForestDnsZones			
(与父文件夹相同)	起始授权机构 (SOA)	[35], dc2008.qytang.c...	静态
(与父文件夹相同)	名称服务器 (NS)	dc2008.qytang.com.	静态
(与父文件夹相同)	主机 (A)	192.168.1.244	2017/10/30 15:00:00
cloud	主机 (A)	10.1.1.222	静态
console	主机 (A)	10.1.1.222	静态
dc2008	主机 (A)	192.168.1.244	静态
firepower	主机 (A)	10.1.1.100	静态
ise24	主机 (A)	192.168.1.241	静态
management	主机 (A)	10.1.1.222	静态
update	主机 (A)	10.1.1.222	静态

FMC整合AD(创建Realm)

Firepower Management Center
System / Integration / Realms

Overview Analysis Policies Devices Objects AMP Intelligence

Cloud Services **Realms** Realm Sequences Identity Sources High Availability eStreamer Host Input Client Smart Software Satellite

Name	Description	Domain	Type	Base DN	Group DN	Group A
There are no realms created. Add a new realm						

Configuration
Users
Domains
Integration
Updates
Licenses
Smart Licenses
Classic Licenses
Logging
Security Analytics & Logging
Health
Monitor
Policy
Events
Blacklist
Monitor Alerts
Monitoring
Audit
Syslog
Statistics
Tools
Backup/Restore
Scheduling
Import/Export
Data Purge

How To

FMC整合AD(创建Realm)

The screenshot shows the Cisco Firepower Management Center (FMC) interface with the 'Add New Realm' dialog box open. The dialog is used to configure an AD realm for integration. The fields are numbered 1 through 11, indicating the sequence of steps to complete the configuration.

Fields and values shown in the dialog:

- 1 Name: qytangad
- 2 Type: AD
- 3 AD Primary Domain: qytang.com (ex: domain.com)
- 4 AD Join Username: administrator@qytang.com (ex: user@domain)
- 5 AD Join Password: [Redacted]
- 6 Directory Username: administrator@qytang.com (ex: user@domain)
- 7 Directory Password: [Redacted]
- 8 Base DN: dc=qytang,dc=com (ex: ou=user,dc=cisco,dc=com)
- 9 Group DN: dc=qytang,dc=com (ex: ou=group,dc=cisco,dc=com)
- 10 Test AD Join button
- 11 OK button

Buttons: Cancel, OK, Test AD Join

Background interface elements: Firepower Management Center System / Integration / Realms, Overview, Analysis, Policies, Devices, Objects, AMP, Intelligence, Deploy, admin, Compare realms, Add Realm, Group DN, Group Attribute, State.

FMC整合AD(创建Realm)

The screenshot shows the Firepower Management Center interface for creating a new realm. The 'Add New Realm' dialog is open, displaying the following configuration details:

- Name: qytangad
- Description: (empty)
- Type: AD
- AD Primary Domain: qytang.com (example: domain.com)
- AD Join Username: administrator@qytang.com
- AD Join Password: (empty)
- Directory Username: (empty)
- Directory Password: (empty)
- Base DN: dc=qytang,dc=com (example: ou=user,dc=cisco,dc=com)
- Group DN: dc=qytang,dc=com (example: ou=group,dc=cisco,dc=com)
- Group Attribute: Member

A 'Test AD Join' button is located to the right of the AD Join Password field. A 'Status' dialog box is overlaid on the form, showing the message: 'Test AD join succeeded'. The dialog has an 'OK' button. At the bottom of the 'Add New Realm' dialog, there are 'Cancel' and 'OK' buttons. A 'How To' link is visible at the bottom center of the page.

FMC整合AD(创建目录)

Firepower Management Center
System / Integration / Realm Edit

Overview Analysis Policies Devices Objects AMP Intelligence

qytangad
Enter Description

Save Cancel

Directory Realm Configuration User Download

1

2 Add directory

URL (Hostname/IP Address and Port)	Encryption
------------------------------------	------------

How To

FMC整合AD(创建目录)

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The main page is titled "qytangad" and is in the "Directory" tab. A dialog box titled "Add directory" is open in the center. The dialog box has the following fields and options:

- Hostname / IP Address:** A text input field containing "qytang.com".
- Port:** A text input field containing "389".
- Encryption:** Radio buttons for "STARTTLS", "LDAPS", and "None". The "None" option is selected.
- SSL Certificate:** A dropdown menu with a plus sign next to it.

At the bottom of the dialog box, there are three buttons: "Cancel", "Test", and "OK".

Four red circles with numbers 1, 2, 3, and 4 are overlaid on the dialog box to highlight specific elements:

- 1: Points to the "Hostname / IP Address" field.
- 2: Points to the "None" radio button.
- 3: Points to the "Test" button.
- 4: Points to the "OK" button.

FMC整合AD(创建目录)

The screenshot displays the Cisco Firepower Management Center (FMC) interface for configuring a directory in a realm named 'qytangad'. The breadcrumb trail is 'System / Integration / Realm Edit'. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The user is logged in as 'admin'. The 'Add directory' configuration page is active, showing the following fields:

- URL (Hostname/IP Address and Port):** A large text input field.
- Hostname / IP Address:** A text input field containing 'qytang.com'.
- Port:** A text input field containing '389'.
- Encryption:** Radio button options for 'STARTTLS', 'LDAPS', and 'None' (selected).
- SSL Certificate:** A dropdown menu with a plus sign to add a certificate.

A 'Status' dialog box is overlaid on the configuration page, indicating that the 'Test connection succeeded'. The dialog has an 'OK' button. At the bottom of the configuration area, there are 'Cancel', 'Test', and 'OK' buttons. A 'How To' link is visible at the bottom center of the page.

FMC整合AD(选择组)

Firepower Management Center
System / Integration / Realm Edit

Overview Analysis Policies Devices Objects AMP Intelligence

qytangad
Enter Description

Directory Realm Configuration **User Download**

You have unsaved changes: **Save** Cancel

Download users and groups (2)
(Warning: You must enable the realm in order to perform an on-demand user/group download. [Enable Realm](#))

Begin automatic download at 8 PM America/New York Repeat Every 24 Hours

Download Now

Available Groups

- Group Policy Creator Owners
- Replicator
- Incoming Forest Trust Builders
- Network Configuration Operators
- Domain Guests
- Read-only Domain Controllers
- fpgroup** (3)
- Administrators
- Denied RODC Password Replication Group
- DnsUpdateProxy
- Certificate Service DCOM Access
- Enterprise Admins
- DnsAdmins
- RAS and IAS Servers
- IIS_IUSRS
- Enterprise Read-only Domain Controllers

Groups to Include (1) (4)

- fpgroup

Groups to Exclude(0)

Enter User Inclusion Add Enter User Exclusion Add

How To



FMC整合AD(下载用户和组)

Firepower Management Center
System / Integration / Realms

Overview Analysis Policies Devices Objects AMP Intelligence

Cloud Services **Realms** Realm Sequences Identity Sources High Availability eStreamer Host Input Client Smart Software Satellite

Compare realms Add Realm

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
qytangad		Global	AD	dc=qytang,dc=com	dc=qytang,dc=com	member	 

How To

FMC整合AD(下载用户和组)

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The main navigation bar includes 'Cloud Services', 'Realms', 'Realm Sequences', 'Identity Sources', 'High Availability', 'eStreamer', 'Host Input Client', and 'Smart Software Satellite'. The 'Realms' section is active, showing a table with one realm: 'qytangad'. A modal dialog box titled 'Refresh Realm' is displayed, asking 'Are you sure you want to download users/groups for this realm?' with 'No' and 'Yes' buttons.

Name	Description	Domain	Type	Base DN	Group DN	Group Attribute	State
qytangad		Global	AD	dc=qytang,dc=com	dc=qytang,dc=com	member	<input checked="" type="checkbox"/>

Refresh Realm

Are you sure you want to download users/groups for this realm?

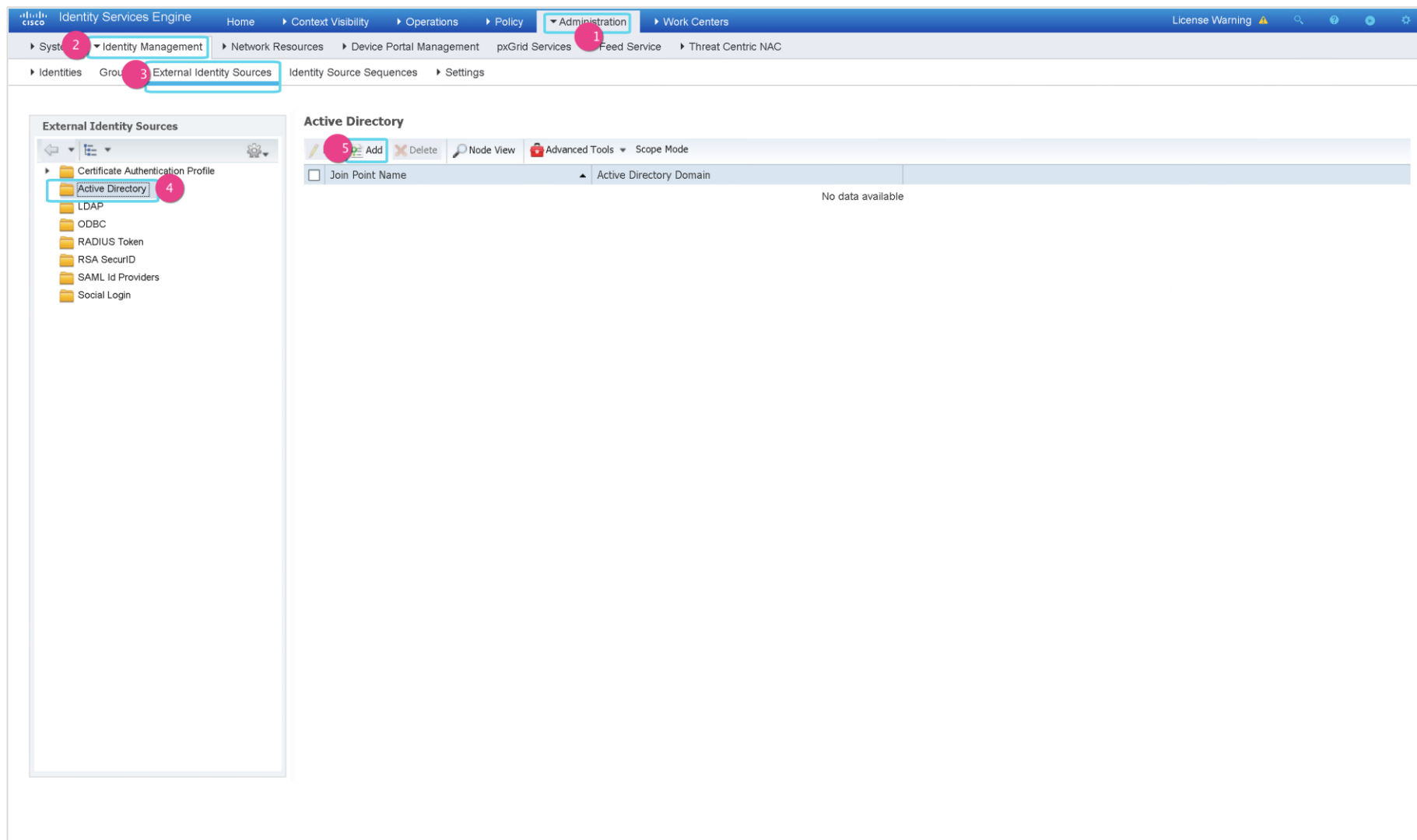
[How To](#)

FMC整合AD(下载用户和组)

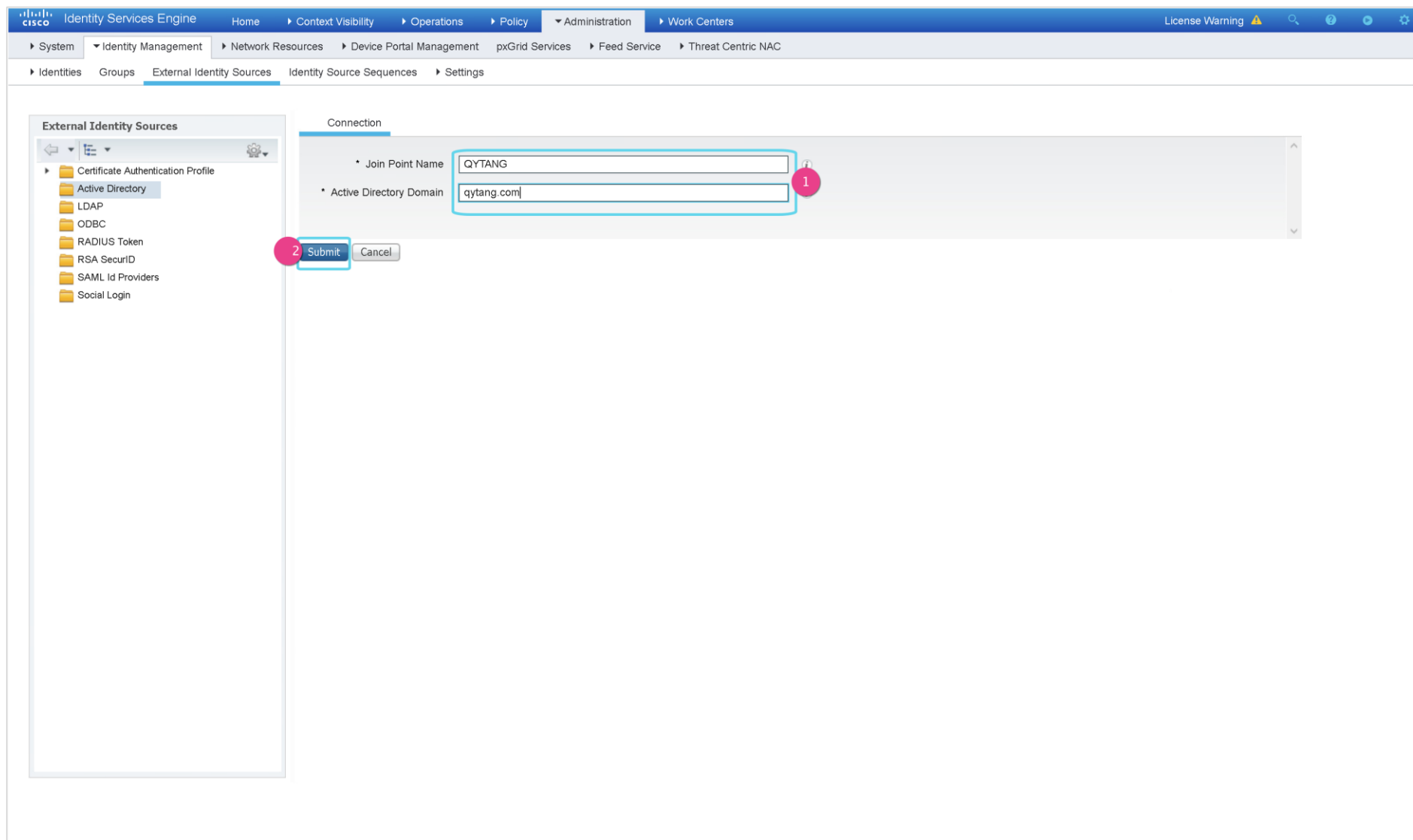
The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. Below this, a secondary navigation bar shows 'Cloud Services', 'Realms', 'Realm Sequences', 'Identity Sources', 'High Availability', 'eStreamer', 'Host Input Client', and 'Smart Software Satellite'. The 'Realms' tab is active, showing a table of LDAP realms. A notification box on the right indicates a successful 'LDAP Download' for the 'qytangad' realm, stating 'LDAP download successful: 1 groups, 1 users downloaded.' A 'How To' button is visible at the bottom center.

Name	Description	Domain	Type	Base DN	Group DN	
qytangad		Global	AD	dc=qytang,dc=com	dc=qytang,dc=com	member

ISE整合AD(添加域)



ISE整合AD(添加域)



ISE整合AD(添加域)

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation pane on the left shows the 'External Identity Sources' section, with 'Active Directory' expanded to show the 'QYTANG' domain. The main content area shows the 'Join Domain' configuration page for the 'QYTANG' domain. The 'Join Point Name' is 'QYTANG' and the 'Active Directory Domain' is 'qytang.com'. A table below shows the status of ISE nodes, with one node 'ISE24.qytang.com' listed as 'STANDALONE' and 'Not Joined'. A 'Join Domain' dialog box is open, prompting for credentials. The dialog box contains the following fields and options:

- * AD User Name: administrator
- * Password: [Redacted]
- Specify Organizational Unit
- Store Credentials
- Buttons: OK, Cancel

Red circles with numbers 1 and 2 highlight the 'AD User Name' field and the 'OK' button, respectively.

ISE整合AD(添加域)

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The main interface is in the 'External Identity Sources' section, specifically the 'Connection' tab for an Active Directory source named 'QYTANG'. The 'Join Point Name' is set to 'QYTANG' and the 'Active Directory Domain' is 'qytang.com'. A modal dialog box titled 'Join Operation Status' is open in the foreground, showing a 'Status Summary: Successful' and a table of node statuses.

ISE Node	Node Status
ISE24.qytang.com	✔ Completed.

The dialog box also includes a 'Close' button at the bottom right. In the background, the 'Join' button is visible, and the 'Save' and 'Reset' buttons are at the bottom of the main configuration area.

ISE整合AD(添加域)

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation path is: Administration > Work Centers > Identity Management > External Identity Sources. The left sidebar shows a tree view of External Identity Sources, with 'Active Directory' expanded to show a configuration for 'QYTANG'. The main content area shows the configuration details for this Active Directory source.

External Identity Sources

- Certificate Authentication Profile
- Active Directory
 - QYTANG
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
 - SAML Id Providers
 - Social Login

Active Directory Configuration (QYTANG)

- Join Point Name: QYTANG
- Active Directory Domain: qytang.com

ISE Node Table

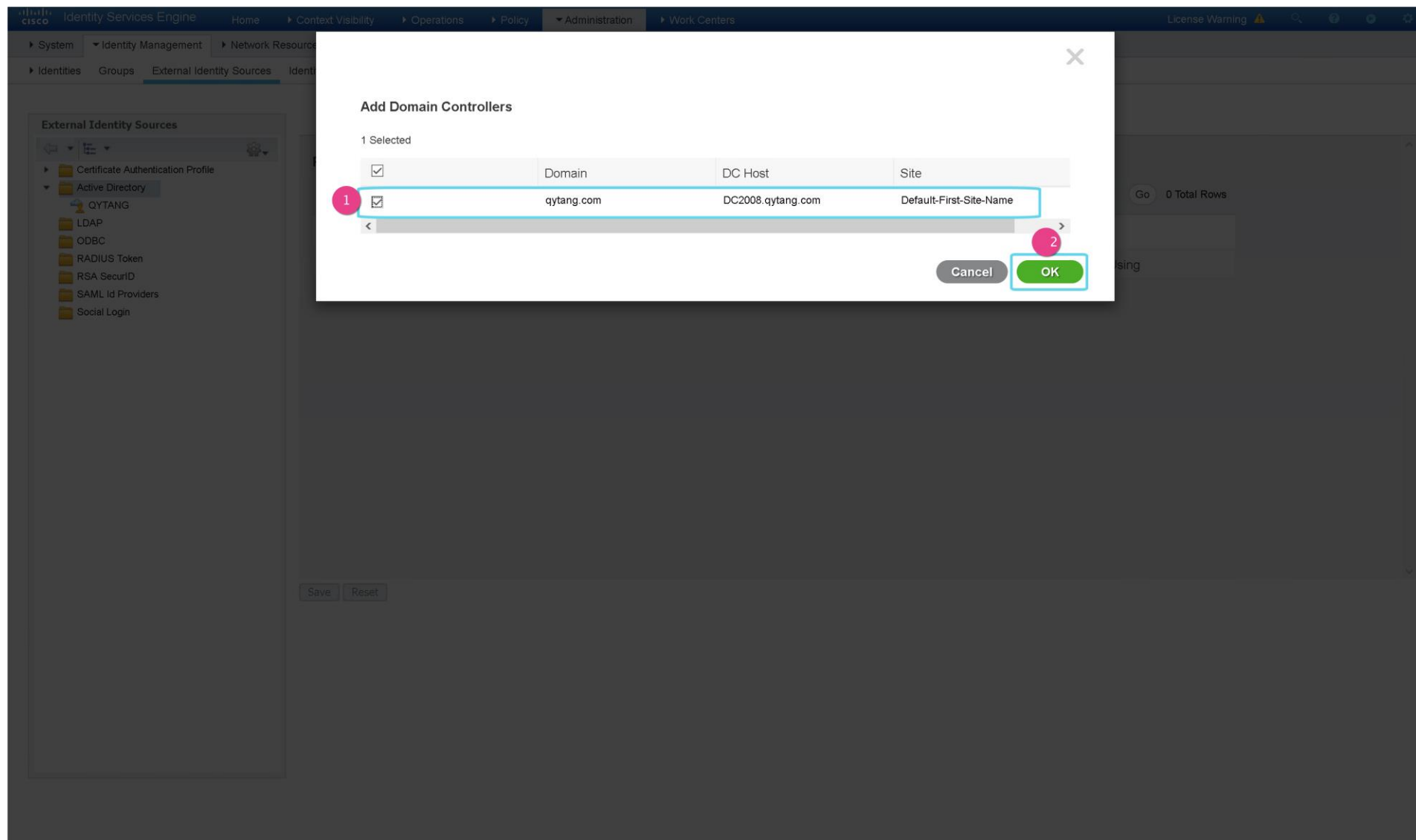
ISE Node	ISE Node Role	Status	Domain Controller	Site
<input type="checkbox"/> ISE24.qytang.com	STANDALONE	<input checked="" type="checkbox"/> Operational	DC2008.qytang.com	Default-First-Site-Name

Buttons: Save, Reset

ISE整合AD(添加PassiveID)

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation path is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The main navigation menu includes System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. The current page is titled "External Identity Sources" and is part of the "Administration" section. The left sidebar shows a tree view of external identity sources, including Certificate Authentication Profile, Active Directory, QYTANG, LDAP, ODBC, RADIUS Token, RSA SecurID, SAML Id Providers, and Social Login. The main content area is titled "PassiveID Domain Controllers" and has tabs for Connection, Whitelisted Domains, PassiveID (selected), Groups, Attributes, and Advanced Settings. The "PassiveID" tab is highlighted with a red circle labeled "1". Below the tabs, there is a table with columns: Domain, DC Host, Site, IP Address, and Monitor Using. The table is currently empty, with the text "No data found." displayed below it. Above the table, there are buttons for Refresh, Edit, Trash, Add DCs (highlighted with a red circle labeled "2"), Use Existing Agent, Config WMI, and Add Agent. The table also includes a "Rows/Page" dropdown set to 0, a search field with "0 / 0", and a "Go" button. At the bottom of the page, there are "Save" and "Reset" buttons.

ISE整合AD(添加PassiveID)



ISE整合AD(添加PassiveID)

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation pane on the left shows the hierarchy: External Identity Sources > Active Directory > QYTANG. The main content area is titled "PassiveID Domain Controllers" and shows a table with one entry selected. The "Edit" button is highlighted with a red circle labeled "2", and the selected row is highlighted with a red circle labeled "1".

PassiveID Domain Controllers

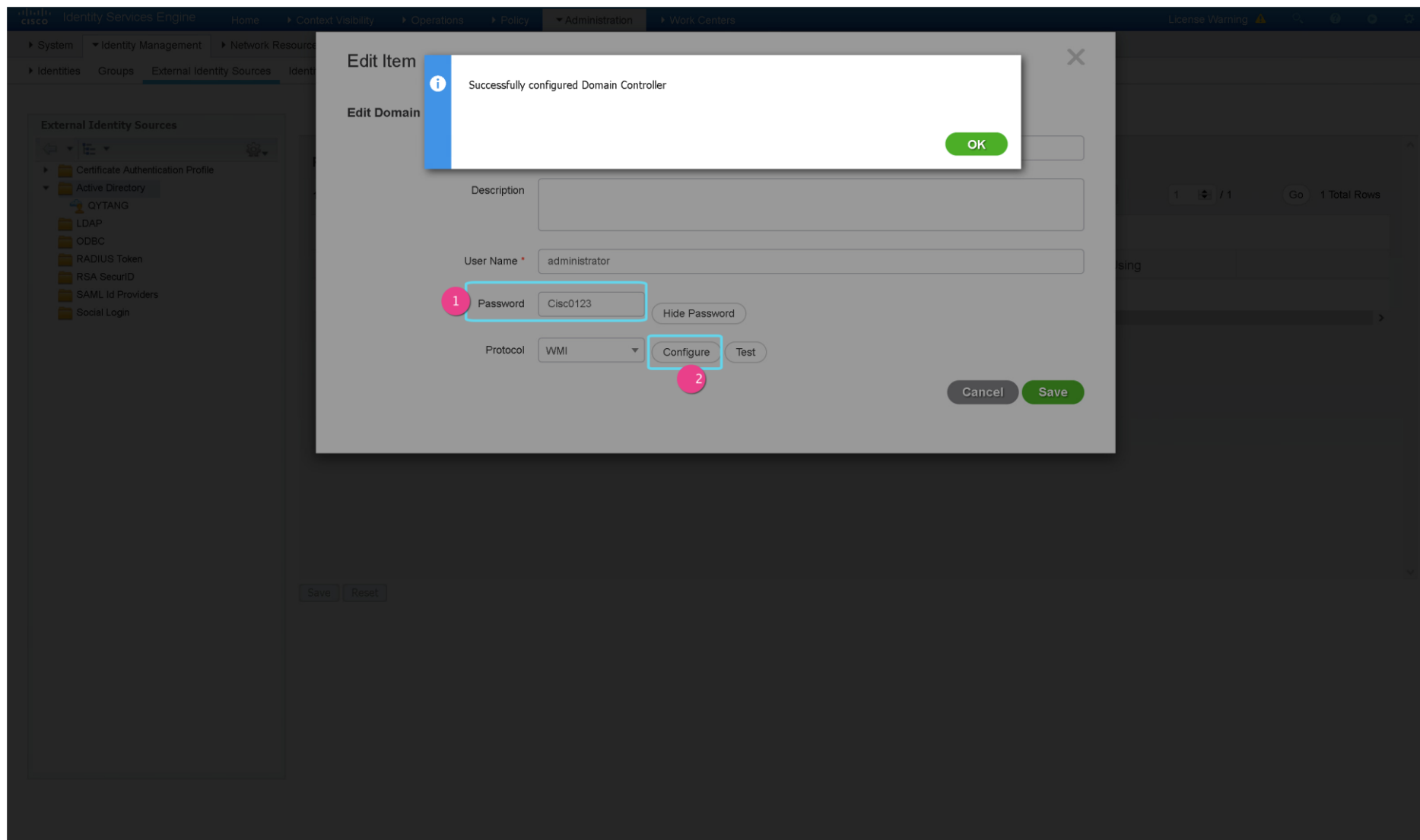
1 Selected Rows/Page 1 / 1 Go 1 Total Rows

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

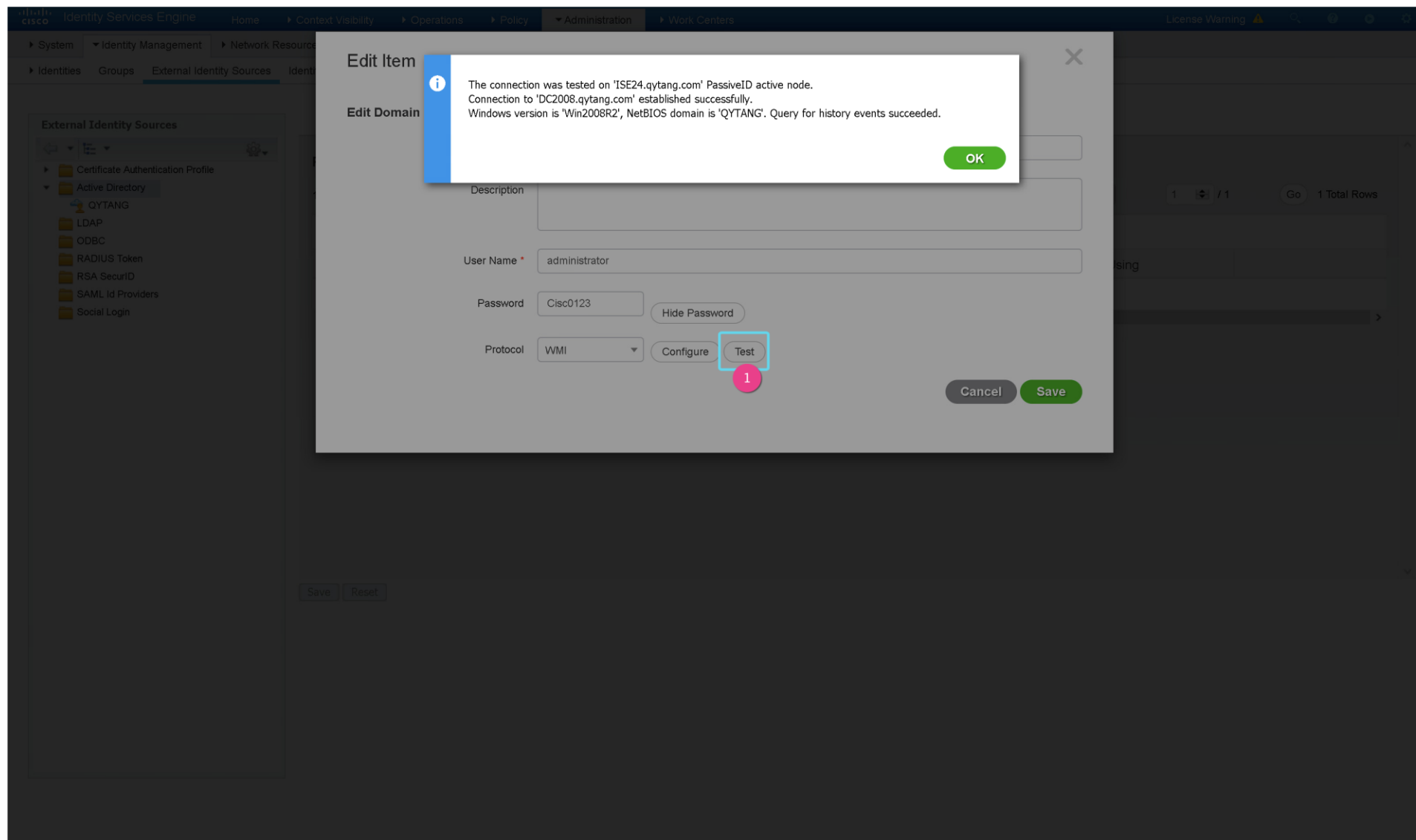
<input checked="" type="checkbox"/>	Domain	DC Host	Site	IP Address	Monitor Using
<input checked="" type="checkbox"/>	qytang.com	DC2008.qytang.com	Default-First-Site-Name	192.168.1.244	WMI

Save Reset

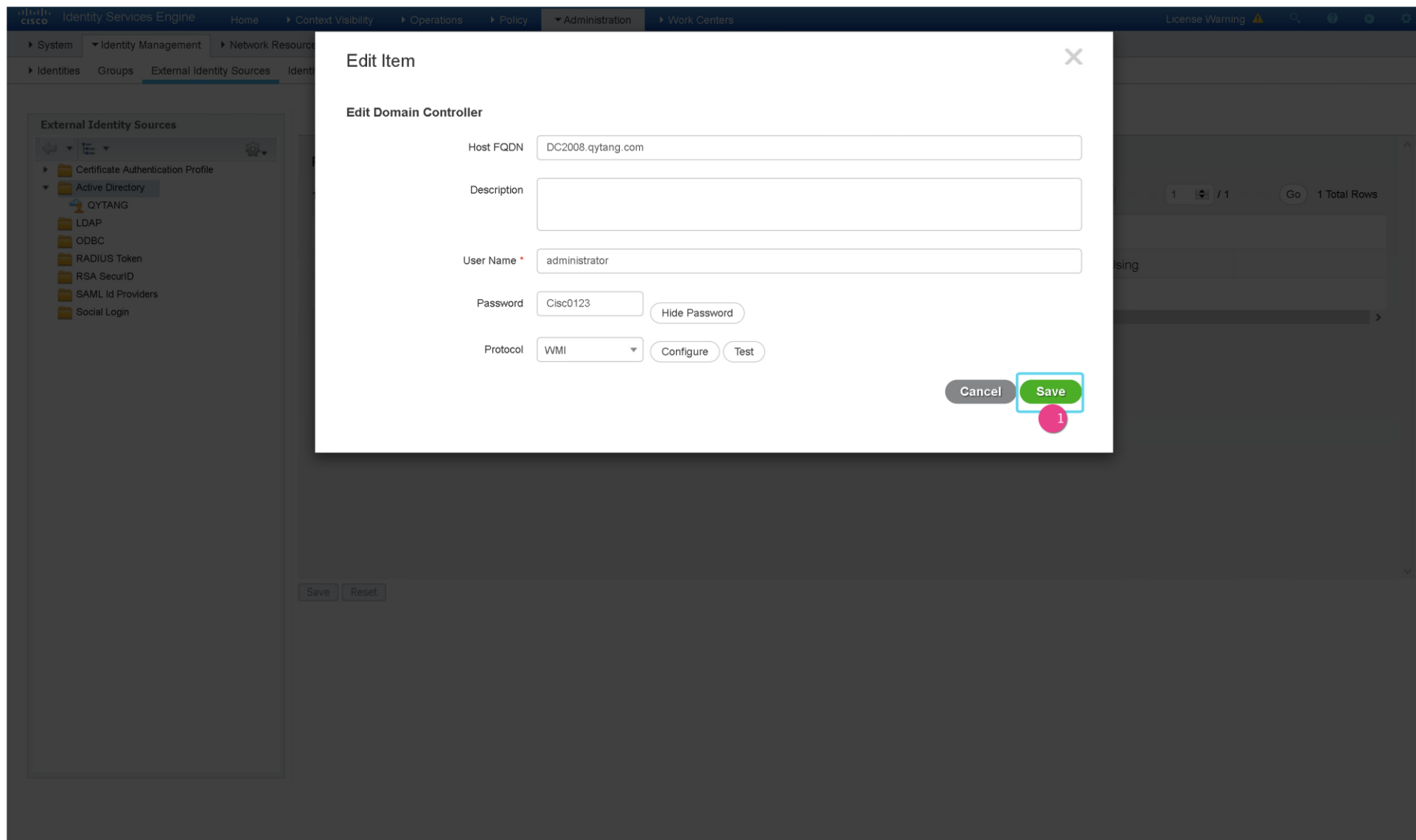
ISE整合AD(添加PassiveID)



ISE整合AD(添加PassiveID)



ISE整合AD(添加PassiveID)



ISE整合AD(添加PassiveID)

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The navigation pane on the left shows the hierarchy: External Identity Sources > Active Directory > QYTANG. The main content area is titled "PassiveID Domain Controllers" and shows a table with one entry for the domain "qytang.com".

Navigation: Home > Context Visibility > Operations > Policy > Administration > Work Centers

System: Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed Service > Threat Centric NAC

Identities > Groups > External Identity Sources > Identity Source Sequences > Settings

External Identity Sources

- Certificate Authentication Profile
- Active Directory
 - QYTANG
 - LDAP
 - ODBC
 - RADIUS Token
 - RSA SecurID
 - SAML Id Providers
 - Social Login

PassiveID Domain Controllers

0 Selected Rows/Page 1 / 1 Total Rows

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

Domain	DC Host	Site	IP Address	Monitor Using
<input type="checkbox"/> qytang.com	DC2008.qytang.com	Default-First-Site-Name	192.168.1.244	WMI

Save Reset

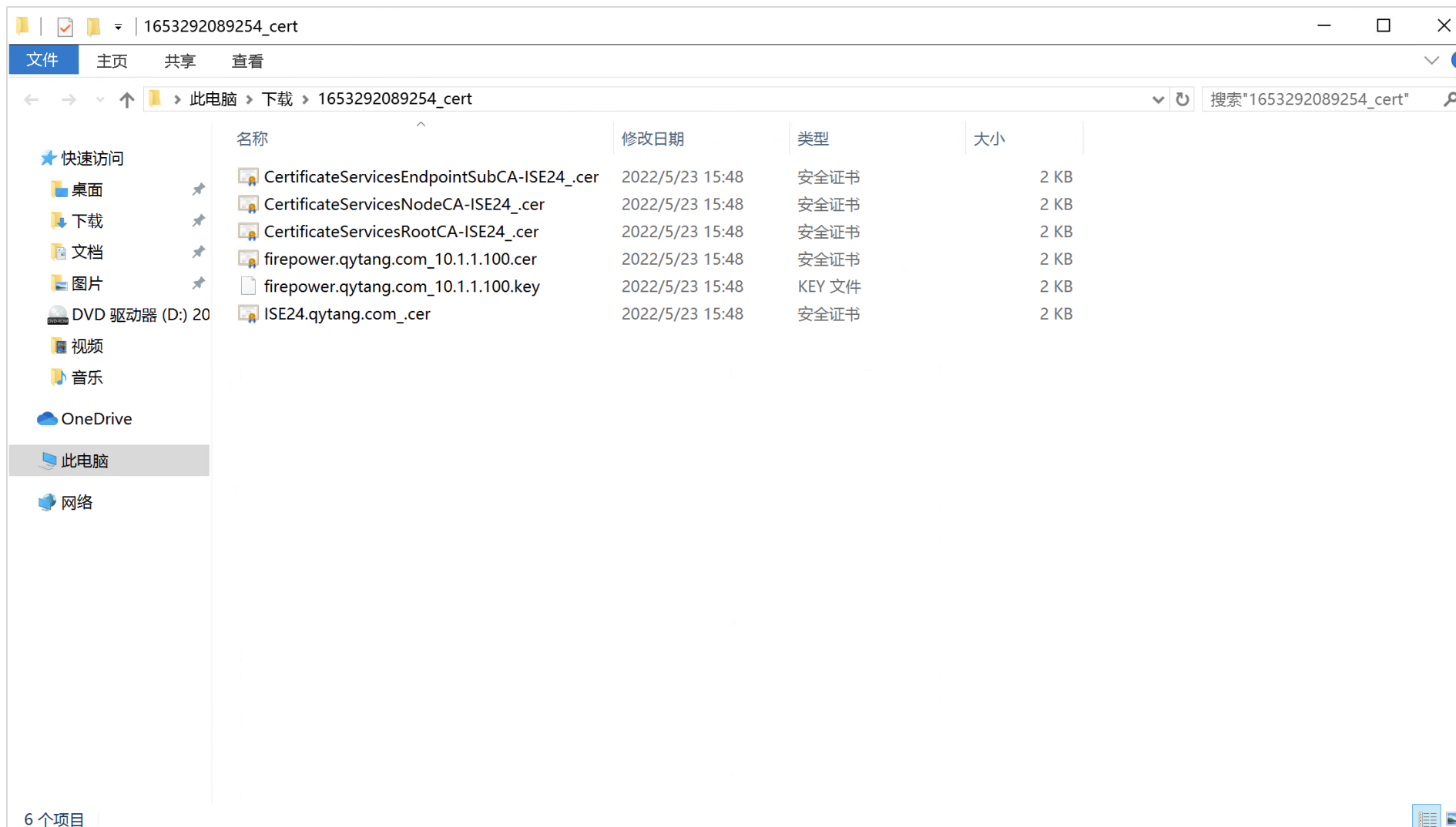
FMC与ISE之间的PxGrid(证书)

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console interface for generating pxGrid certificates. The navigation path is: Administration > pxGrid Services > Certificates. The configuration page is titled "Generate pxGrid Certificates" and includes the following fields and options:

- I want to:** A dropdown menu set to "Generate a single certificate (without a certificate signing request)".
- Common Name (CN):** A text input field containing "firepower.qytang.com".
- Description:** A text input field containing "qytang ise pxgrid cert".
- Certificate Template:** A dropdown menu set to "PxGrid_Certificate_Template".
- Subject Alternative Name (SAN):** A dropdown menu set to "IP address" with a text input field containing "10.1.1.100".
- Certificate Download Format:** A dropdown menu set to "Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate ch:".
- Certificate Password:** A password input field with masked characters.
- Confirm Password:** A password input field with masked characters.

At the bottom of the form, there are "Reset" and "Create" buttons. The "Create" button is highlighted with a pink circle. Below the form, a green status bar indicates "Connected to pxGrid ISE24.qytang.com".

FMC与ISE之间的PxGrid(证书)



FMC与ISE之间的PxGrid(证书)

Firepower Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** AMP Intelligence

Deploy 1 2 3 4 admin

AAA Server
Access List
Address Pools
Application Filters
AS Path
Cipher Suite List
Community List
Distinguished Name
DNS Server Group
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Cert Enrollment
External Cert Groups
External Certs
Internal CA Groups
Internal CAs
Internal Cert Groups
Internal Certs
Trusted CA Groups
Trusted CAs
Policy List
Port
Prefix List
Route Map

Trusted CAs

Add Trusted CA Filter

Trusted certificate authority (CA) object represents a CA public key certificate belonging to a trusted CA. You can use external CA objects in SSL policy, realm configurations and ISE/ISE-PIC connection.

Name	Value	
AAA-Certificate-Services	CN=AAA Certificate Services, ORG=Comodo CA L...	/
Actalis-Authentication-Root-CA	CN=Actalis Authentication Root CA, ORG=Actalis ...	/
AddTrust-External-CA-Root	CN=AddTrust External CA Root, ORG=AddTrust A...	/
AffirmTrust-Commercial	CN=AffirmTrust Commercial, ORG=AffirmTrust, C=...	/
AffirmTrust-Networking	CN=AffirmTrust Networking, ORG=AffirmTrust, C=...	/
AffirmTrust-Premium	CN=AffirmTrust Premium, ORG=AffirmTrust, C=US	/
AffirmTrust-Premium-ECC	CN=AffirmTrust Premium ECC, ORG=AffirmTrust, ...	/
Amazon-Root-CA-1	CN=Amazon Root CA 1, ORG=Amazon, C=US	/
Amazon-Root-CA-2	CN=Amazon Root CA 2, ORG=Amazon, C=US	/
Amazon-Root-CA-3	CN=Amazon Root CA 3, ORG=Amazon, C=US	/
Amazon-Root-CA-4	CN=Amazon Root CA 4, ORG=Amazon, C=US	/
Atos-TrustedRoot-2011	CN=Atos TrustedRoot 2011, ORG=Atos, C=DE	/
Autoridad-de-Certificacion-Firmaprofesional-CIF-A62634068	CN=Autoridad de Certificacion Firmaprofesional C...	/
Baltimore-CyberTrust-Root	CN=Baltimore CyberTrust Root, ORG=Baltimore, O...	/
Buypass-Class-2-Root-CA	CN=Buypass Class 2 Root CA, ORG=Buypass AS-...	/
Buypass-Class-3-Root-CA	CN=Buypass Class 3 Root CA, ORG=Buypass AS-...	/

Displaying 1 - 20 of 114 rows | Page 1 of 6

How To

FMC与ISE之间的PxGrid(证书)

Firepower Management Center
Objects / Object Management

Trusted CAs

Trusted certificate authority (CA) object represents a CA public key certificate belonging to a trusted CA. You can use external CA objects in SSL policy, realm configurations and ISE/ISE-PIC connection.

Import Trusted Certificate Authority

Name: (1)

Certificate Data or, choose a file: (2)

```
-----BEGIN CERTIFICATE-----
MIIFKjCCAxKgAwIBAgIQGLG4UQTtTIKvZtCVDgyW2jANBgkqhkiG9w0BAQsFADAv
MS0wKwYDVQQDDCRDZXJ0aWZpY2F0ZSB0ZXJ2aWVudD90IENBIC0gSVNF
MjQw
HhcNMjQwNDEyMDg1MTQyWWhcNMzlwNDEzMDg1MTQyWjAvMS0wKwYDVQQDDC
RDZXJ0
```

Encrypted, and the password is:

CertificateServicesRootCA-ISE24_.cer (3)

Name	Value
AAA-Certificate-Services	CN=AAA Certificate Services, ORG=Comodo CA L...
Actalis-Authentication-Root-CA	CN=Actalis Authentication Root CA, ORG=Actalis ...
AddTrust-External-CA-Root	CN=AddTrust External CA Root, ORG=AddTrust A...
AffirmTrust-Commercial	CN=AffirmTrust Commercial, ORG=AffirmTrust, C=...
AffirmTrust-Networking	CN=AffirmTrust Networking, ORG=AffirmTrust, C=...
AffirmTrust-Premium	CN=AffirmTrust Premium, ORG=AffirmTrust, C=US
AffirmTrust-Premium-ECC	CN=AffirmTrust Premium ECC, ORG=AffirmTrust, ...
Amazon-Root-CA-1	CN=Amazon Root CA 1, ORG=Amazon, C=US
Amazon-Root-CA-2	CN=Amazon Root CA 2, ORG=Amazon, C=US
Amazon-Root-CA-3	CN=Amazon Root CA 3, ORG=Amazon, C=US
Amazon-Root-CA-4	CN=Amazon Root CA 4, ORG=Amazon, C=US
Atos-TrustedRoot-2011	CN=Atos TrustedRoot 2011, ORG=Atos, C=DE
Autoridad-de-Certificacion-Firmaprofesional-C...	CN=Autoridad de Certificacion Firmaprofesional C...
Baltimore-CyberTrust-Root	CN=Baltimore CyberTrust Root, ORG=Baltimore, O...
Buypass-Class-2-Root-CA	CN=Buypass Class 2 Root CA, ORG=Buypass AS-...
Buypass-Class-3-Root-CA	CN=Buypass Class 3 Root CA, ORG=Buypass AS-...

Displaying 1 - 20 of 114 rows | Page 1 of 6

How To

FMC与ISE之间的PxGrid(证书)

Firepower Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** AMP Intelligence

Deploy 1 2 3 4 admin

Internal Certs

Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in SSL rules, ISE/ISE-PIC connection and captive portal configuration.

Name	Value
No records to display	

[Add Internal Cert](#)

No data to display | < < Page 1 of 1 > > | C

[How To](#)

FMC与ISE之间的PxGrid(证书)

Firepower Management Center
Objects / Object Management

Internal Certs

Add Internal Cert

Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in SSL rules, ISE/ISE-PIC connection and captive portal configuration.

Name

Add Known Internal Certificate

Name: qytang-firepower

Certificate Data or, choose a file: Browse..

```
-----BEGIN CERTIFICATE-----
MIIE9jTCCAiWgAwIBAgIQKdBHus+EQUCWqkNtISEBMzANBgkqhkiG9w0BAQsFADA3
MTUwMwYDVQQDDCxDZXJ0aWZpY2F0ZSB0ZXJ2aWNlcyBFbWw2ludCBTdWl
gQ0Eg
LSBJU0UyNDAeFw0yMjA1MjIwNzQ4MDhaFw0yNDA1MjIwNzQ4MDhaMB8HTAbB
```

Key or, choose a file: Browse..

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE9jA0BgoqhkiG9w0BDAEDMB0EFpBgvw3PPFuP9UDHNfrJyWsjowZAgIIAASC
BMhFbLFZ3jU6pArapBz2ktnV8QoLjMoiyGmyrVA/0UDmRHjDYtabMH2k3hUfq
zmbzwX1/cU3hpPrfsC/ELK38w53onq5k2/Ukt9H3gkt1DrG60j8fG5oYUoYzKkT
PJ9TvtTThbnkQ5nc66hqIKQy1B3Rv3rozdvKj9vqlxRkhmg.JsbZtnc6XicJ+fmrQ2
qKcmQikOd5HApnvoJOWK8Cnaeg0g5UwVETXZprNicHvzWoSxn8lvMXnlfchngH
```

Encrypted, and the password is:

Cancel Save

firepower.qytang.com_10.1.1.100.cer

firepower.qytang.com_10.1.1.100.key

No data to display | Page 1 of 1

How To

FMC与ISE之间的PxGrid(证书)

Firepower Management Center
Objects / Object Management

Overview Analysis Policies Devices **Objects** AMP Intelligence

Deploy admin

Internal Certs

Add Internal Cert

Internal certificate object represents a server public key certificate belonging to your organization. You can use internal certificate objects and groups in SSL rules, ISE/ISE-PIC connection and captive portal configuration.

Name	Value	
qytang-firepower	CN=firepower.qytang.com	

Displaying 1 - 1 of 1 rows | << Page 1 of 1 >>

[How To](#)

FMC与ISE之间的PxGrid(整合)

The screenshot shows the Cisco Firepower Management Center (FMC) configuration page for Identity Sources. The page is titled "Identity Sources" and includes a navigation bar with options like Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. The configuration fields are as follows:

- Service Type:** Identity Services Engine (2)
- Primary Host Name/IP Address:** ise24.qytang.com (3)
- Secondary Host Name/IP Address:** (empty)
- pxGrid Server CA:** qytang-ca (4)
- MNT Server CA:** qytang-ca (5)
- FMC Server Certificate:** qytang-firepower (6)
- ISE Network Filter:** ex. 10.89.31.0/24, 192.168.8.0/24
- Subscribe To:** Session Directory Topic (7) and SXP Topic (checked)
- * Required Field:** Test (8)

A "Status" dialog box is open, showing the following information:

- Status:** ISE connection status: Primary host: Failure
- Additional Logs:**

```
Primary host:
[INFO]: PXGrid v2 is enabled
[ERROR]: pxgrid 2.0: failed account activation.
accountState=PENDING
[ERROR]: Failed to contact pxGrid node at
'ise24.qytang.com': pxgrid2.0: Could not activate
account
```
- Buttons:** OK (10)

At the bottom of the page, there is a "How To" button.

FMC与ISE之间的PxGrid(整合)

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The current page is 'pxGrid Services' under 'Administration'. The top navigation bar includes: System, Identity Management, Network Resources, Device Portal Management, pxGrid Services, Feed Service, and Threat Centric NAC. Below the navigation bar, there are tabs for: All Clients, Web Clients, Capabilities, Live Log, Settings, Certificates, and Permissions. The main content area shows a table of clients with the following columns: Client Name, Client Description, Capabilities, Status, Client Group(s), Auth Method, and Log. The table contains 6 rows of data. The first row is selected, and its status is 'Pending'. A red circle '1' is placed next to the client name 't-fmc-9a7a95249b6711eb89300b...'. The 'Approve' button in the top toolbar is highlighted with a red circle '2'. The status of the selected client is 'Pending'. The bottom of the page shows a green bar with the text 'Connected to pxGrid ISE24.qytang.com'.

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
<input type="checkbox"/> ▶ ise-mnt-ise24		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
<input type="checkbox"/> ▶ ise-pubsub-ise24		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
<input type="checkbox"/> ▶ ise-fanout-ise24		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
<input type="checkbox"/> ▶ ise-bridge-ise24		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
<input type="checkbox"/> ▶ ise-admin-ise24		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
<input checked="" type="checkbox"/> ▶ t-fmc-9a7a95249b6711eb89300b...		Capabilities(0 Pub, 0 Sub)	Pending		Certificate	View

FMC与ISE之间的PxGrid(整合)

The screenshot shows the Cisco Firepower Management Center (FMC) web interface. The main navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', 'AMP', and 'Intelligence'. The secondary navigation bar includes 'Cloud Services', 'Realms', 'Realm Sequences', 'Identity Sources', 'High Availability', 'eStreamer', 'Host Input Client', and 'Smart Software Satellite'. The 'Identity Sources' page is active, showing configuration options for 'Identity Services Engine'. A 'Test' button is highlighted with a red circle and the number 1. A 'Status' dialog box is open, showing the 'ISE connection status: Primary host: Success' message, which is also highlighted with a red circle and the number 2. The dialog box also displays a list of 'Additional Logs' for the primary host, including messages about PXGrid v2 being enabled, account activation, and successful connection to ISE24.qytang.com:8910. The 'OK' button in the dialog box is highlighted with a red circle and the number 3. A 'How To' button is visible at the bottom of the page.

Firepower Management Center
System / Integration / Identity Sources

Overview Analysis Policies Devices Objects AMP Intelligence

Cloud Services Realms Realm Sequences Identity Sources High Availability eStreamer Host Input Client Smart Software Satellite

You have unsaved changes [Cancel](#) [Save](#)

Identity Sources

Service Type None Identity Services Engine

Primary Host Name/IP Address *

Secondary Host Name/IP Address

pxGrid Server CA * +

MNT Server CA * +

FMC Server Certificate * +

ISE Network Filter

Subscribe To:

Session Directory Topic

SXP Topic

* Required Field

Status

ISE connection status: Primary host: Success

Additional Logs

Primary host:
[INFO]: PXGrid v2 is enabled
[INFO]: pxgrid 2.0: account activate succeeded
[INFO]: Successful connection to ISE24.qytang.com:8910
[INFO]: These ISE Services are up: SessionDirectory, SXP, EndpointProfile, SecurityGroups, AdaptiveNetworkControl

How To

FMC与ISE之间的PxGrid(整合)

Firepower Management Center
System / Integration / Identity Sources

Overview Analysis Policies Devices Objects AMP Intelligence

Cloud Services Realms Realm Sequences Identity Sources High Availability eStreamer Host Input Client Smart Software Satellite

You have unsaved changes [Cancel](#) [Save](#)

Identity Sources

Service Type None Identity Services Engine

Primary Host Name/IP Address *

Secondary Host Name/IP Address

pxGrid Server CA * +

MNT Server CA * +

FMC Server Certificate * +

ISE Network Filter

Subscribe To:

Session Directory Topic

SXP Topic

* Required Field

[How To](#)

FMC与ISE之间的PxGrid(整合)

Identity Services Engine Administration Work Centers

pxGrid Services Feed Service Threat Centric NAC

All Clients Web Clients Capabilities Live Log Settings Certificates Permissions

Enable Disable Approve Group Decline Delete Refresh Total Pending Approval(0)

1 - 7 of 7 Show 25 per page Page 1

Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
ise-mnt-ise24		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
ise-pubsub-ise24		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
ise-fanout-ise24		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
ise-bridge-ise24		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
ise-admin-ise24		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
fmc-9a7a95249b6711eb89300ba...		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View
t-fmc-9a7a95249b6711eb89300b...		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View

Connected to pxGrid ISE24.qytang.com



乾颐堂

4. FMC策略

创建Identity策略

Firepower Management Center
Policies / Access Control / Identity

Overview Analysis **Policies** Devices Objects AMP Intelligence

Deploy admin

Object Management | Access Control

Compare Policies **New Policy**

Identity Policy	Domain	Status	Last Modified
There are no policies created. Add a new policy			

How To

创建Identity策略

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title "Firepower Management Center", and sub-navigation for "Policies / Access Control / Identity". The main navigation menu contains "Overview", "Analysis", "Policies", "Devices", "Objects", "AMP", and "Intelligence". The "Policies" tab is active. On the right, there are search, deploy, and user options (admin). Below the navigation, there are links for "Object Management" and "Access Control", and buttons for "Compare Policies" and "New Policy".

The main content area shows a table with columns: "Identity Policy", "Domain", "Status", and "Last Modified". A message states: "There are no policies created. [Add a new policy](#)".

A "New Identity policy" dialog box is open in the center. It contains the following fields and buttons:

- Name:** A text input field containing "qytang-id-policy". A red circle with the number "1" is positioned to the left of this field.
- Description:** An empty text input field.
- Buttons:** "Cancel" and "Save". The "Save" button is highlighted with a red circle and the number "2".

At the bottom center of the interface, there is a "How To" button.

创建Identity策略

Firepower Management Center
Policies / Access Control / Identity Policy Editor

Overview Analysis **Policies** Devices Objects AMP Intelligence

qytang-id-policy Save Cancel

Enter Description

Rules Active Authentication

+ Add Category **+ Add Rule**

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules										
This category is empty										
Standard Rules										
This category is empty										
Root Rules										
This category is empty										

No data to display |<< Page 1 of 1 >>| C

[How To](#)

创建Identity策略

Firepower Management Center
Policies / Access Control / Identity Policy Editor

Overview Analysis Policies Devices Objects AMP Intelligence

qytang-id-policy

You have unsaved changes [Save](#) [Cancel](#)

Enter Description

Rules Active Authentication

+ Add Category + Add Rule Search Rules

Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Source Ports	Dest Ports	Realm	Action	Auth Protocol
Administrator Rules										
This category is empty										
Standard Rules										
1 qytang-rule-1	ftd1-inside-zone (Routed)	any	10.1.1.0/24	any	any	any	any	qytangad (AD)	Passive Authentication	none
Root Rules										
This category is empty										

Displaying 1 - 1 of 1 rules |<< Page 1 of 1 >>| C

How To

Access策略

Firepower Management Center
Policies / Access Control / Policy Editor

Overview Analysis **Policies** Devices Objects AMP Intelligence

QYTANG-Policy

You have unsaved changes [Analyze Hit Counts](#) [Save](#) [Cancel](#)

[Inheritance Settings](#) | [Policy Assignments \(1\)](#)

Rules [Security Intelligence](#) [HTTP Responses](#) [Logging](#) [Advanced](#) Prefilter Policy: [Default Prefilter Policy](#) SSL Policy: [None](#) Identity Policy: [qytang-id-policy](#)

[Filter by Device](#) Show Rule Conflicts [+ Add Category](#) [+ Add Rule](#)

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applicat...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action						
Mandatory - QYTANG-Policy (1-4)																			
Inside-DMZ (1-2)																			
1	inside-to-dmz	ftd1-inside-zon	ftd1-dmz-zone	10.1.1.0/24	192.168.1.241 192.168.1.244	Any	Any	Any	Any	Any	Any	Any	Allow						
2	dmz-to-inside	ftd1-dmz-zone	ftd1-inside-zone	192.168.1.241 192.168.1.244	10.1.1.0/24	Any	Any	Any	Any	Any	Any	Any	Allow						
Inside-Outside (3-3)																			
3	permit-ad-user-all	ftd1-inside-zon	Any	Any	Any	qytangad/ft	Any	Any	Any	Any	Any	Any	Allow						
DMZ-Outside (4-4)																			
4	DNS	ftd1-dmz-zone	ftd1-outside-zone	192.168.1.244	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any	Any	Allow						
Default - QYTANG-Policy (-)																			
There are no rules in this section. Add Rule or Add Category																			
Default Action													Access Control: Block All Traffic						

Displaying 1 - 4 of 4 rules | Page 1 of 1 | Rules per page: 100

[How To](#)

Access策略

Firepower Management Center
Policies / Access Control / Policy Editor

Overview Analysis **Policies** Devices Objects AMP Intelligence

QYTANG-Policy
Enter Description

Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: qytang-id-policy

Filter by Device Search Rules Show Rule Conflicts Add Category Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applica...	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action						
Mandatory - QYTANG-Policy (1-4)																			
Inside-DMZ (1-2)																			
1	inside-to-dmz	ftd1-inside-zon	ftd1-dmz-zone	10.1.1.0/24	192.168.1.241 192.168.1.244	Any	Any	Any	Any	Any	Any	Any	Allow						
2	dmz-to-inside	ftd1-dmz-zone	ftd1-inside-zon	192.168.1.241 192.168.1.244	10.1.1.0/24	Any	Any	Any	Any	Any	Any	Any	Allow						
Inside-Outside (3-3)																			
3	permit-ad-user-all	ftd1-inside-zon	Any	Any	Any	qytangad/fpgroup	Any	Any	Any	Any	Any	Any	Allow						
DMZ-Outside (4-4)																			
4	DNS	ftd1-dmz-zone	ftd1-outside-zo	192.168.1.244	Any	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any	Allow						
Default - QYTANG-Policy (-)																			
There are no rules in this section. Add Rule or Add Category																			
Default Action													Access Control: Block All Traffic						
Displaying 1 - 4 of 4 rules																	Page 1 of 1		Rules per page: 100

How To

Access策略

Firepower Management Center
Deploy / Deployment

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy 1 2 admin

1 device selected
Deploy time: Estimate Deploy

Search using device name, type, domain, group or status

<input checked="" type="checkbox"/>	Device	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
> <input checked="" type="checkbox"/>	QYTANG-FTD 1		FTD		Apr 14, 2022 3:22 AM		Pending

[How To](#)

Access策略

The screenshot displays the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes the Cisco logo, the title 'Firepower Management Center', and several menu items: Overview, Analysis, Policies, Devices, Objects, AMP, and Intelligence. On the right side of the navigation bar, there is a search icon, a 'Deploy' button with a notification icon, a settings gear, a help icon, and the user name 'admin'.

Below the navigation bar, there is a search bar with the placeholder text 'Search using device name, type, domain, group or status'. To the right of the search bar, it indicates '1 device selected' and 'Deploy time: Estimate', with a 'Deploy' button.

The main content area features a table with the following columns: Device, Inspect Interruption, Type, Group, Last Deploy Time, Preview, and Status. The table contains one row for the device 'QYTANG-FTD', which is currently in a 'Pending' status.

A 'Deployment Confirmation' dialog box is open in the center of the screen. The dialog box contains the text: 'You have selected 1 device to deploy. Are you sure you want to go ahead?'. At the bottom of the dialog box, there are two buttons: 'Deploy' and 'Cancel'. The 'Deploy' button is highlighted with a red circle and a blue border.

At the bottom center of the interface, there is a 'How To' button.

Access策略

Firepower Management Center
Deploy / Deployment

Overview Analysis Policies Devices Objects AMP Intelligence

Deploy

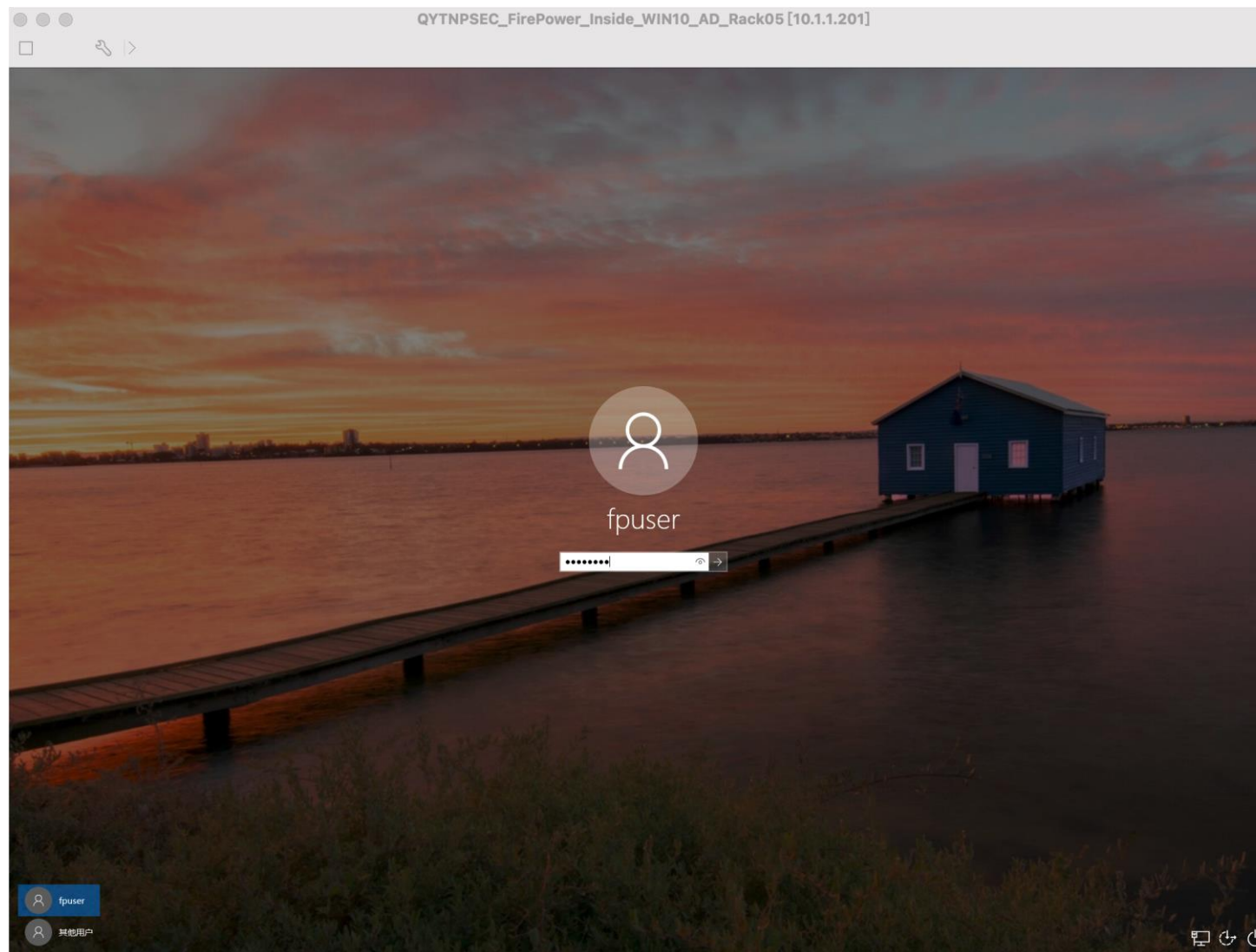
Deploy

Search using device name, type, domain, group or status

Device	Inspect Interruption	Type	Group	Last Deploy Time	Preview	Status
> <input checked="" type="checkbox"/> QYTANG-FTD		FTD		Apr 14, 2022 3:22 AM		Completed

How To

测试(登录域)



测试(查看Current Active Session)

The screenshot displays the Cisco Identity Services Engine (ISE) interface. The breadcrumb trail at the top indicates the navigation path: Home > Context Visibility > Operations > Policy > Administration > Work Centers (1). The left sidebar shows the navigation menu with 'Reports' (4) and 'Passive ID Reports' (5) expanded, and 'Current Active Sessions' (6) selected. The main content area shows the 'Current Active Sessions' report for the period from 2022-05-23 00:00:00.0 to 2022-05-23 17:01:13.0. A table displays the session details, with the first row (7) highlighted:

Initiated	Updated	Session Time	Identity	Endpoint ID	Security Group
Mon May 23 16:59:51 CST 2022	Mon May 23 16:59:51 CST 2022		fpuser	10.1.1.201	

The table also includes a search filter for Identity, Endpoint ID, and Security Group. The bottom right corner shows 'Rows/Page' set to 1 and '1 Total Rows'.

测试(访问互联网)

← → ↻ baidu.com/s?ie=utf-8&f=8&rsrv_bp=1&rsrv_idx=1&tn=baidu&wd=qytang&fenlei=256&rsrv_pq=bc918a8600054a0e&rsrv_t=124c1ZuRHclNX7h%2BhlazM%2ByDWk8Bk%2BkA8hKd61Jc76YQNg7xu8tZkxwK1HJ&rlqiang=en&rsrv_enter=1&rsrv_dl=tb&rsrv_sug3=7&rsrv_sug1=1&rsrv_sug7=1... 百度一下

百度为您找到相关结果约295,000个

山西网科防火墙接入方式之透明模式 - 百度文库
2页 发布时间: 2018年07月01日
QYTANG(config)# int e0/1 QYTANG(config-if-eth0/1)# zone I2-trust QYTANG(config-if-eth0/1)# n o shutdown QYTANG(config-if-eth0/1)# exit QYTANG(config)# int e0/2 QYT...

乾颐堂Python网络快速强化班 - 乾颐堂网络实验室
第11周: 5月13-19 Python网络编程 网络监控与自动化运维 第12周: 5月20-26 Python网络编程 网络监控与自动化运维 乾颐堂客服热线: 400-618-8070 乾颐堂官网: www.qytang.com 乾颐...
乾颐堂网络实验室

专注思科培训_Python培训_CCIE培训_HCIE培训 - 乾颐堂网络...
【乾颐堂网络实验室】专注思科培训,华为培训,Python培训【来电咨询: 400-618-8070】 涵盖CCNA培训、CCNP培训、CCIE培训、HCIE培训、HCIP培训、HCIA培训、CCIE安全培训、DC数据中心培训及思科华为考...
乾颐堂网络实验室

河南泉源堂智慧药房连锁有限责任公司 - 爱企查
2022年5月12日 官网: www.qytang.cn 地址: 郑州经济技术开发区航海东路与第二十五大街交叉口联东U谷第一期东区35号楼2层35-2-1 简介: 河南泉源堂智慧药房连锁有限责任公司成立于2021年03月18日,注册...
爱企查

仓库- 现任明教教主-乾颐堂 (qytang) - Gitee.com
@qytang 乾颐堂创始人秦桐网名现任明教教主! 关注私信 0 Stars 37 Watches 381 Followers 0 Following <http://weibo.com/xrmjiz> <http://weibo.com/xrmjiz> 概览仓库34星选集...
gitee

其他人还在搜
37tang 彩名堂 鸡场 Tang Duy Tan Xtandi 黄糖 qy1005 qy是谁 trakatan KHITAN

乾颐堂现任明教教主网络入门到实战课程! - 乾颐堂网络实验室
思科,华为, Python学习 CCNA|CCNP|CCIE|HCIA|HCIP|HCIE 路由交换|安全|DC数据中心|无线|云计算 乾颐堂客服热线: 400-618-8070 乾颐堂官网: www.qytang.com 乾颐堂网络实验室 我们为您想的更多
new.qytang.com/Timetable/View/... 百度快照

现任明教教主-乾颐堂 (qytang) - Gitee.com
qytang_Python 乾颐堂Python学习 Python 164040 Python_Network_2018_HTTP_2423 PyQYT 乾颐堂乾颐堂Python网络编程PyQYT项目 Python 3817 VIP_LDAP3 4513 DevNet2019 2215 E1...
Gitee

qytang的空间 - 播视网
qytang的个人空间<http://rjji.bozhong.com/286106.html> [收藏][复制][分享][RSS] 空间首页 动态 记录 日志 相册 主题 分享 好友 个人资料 头像 加为好友 给我留言 打个招呼 发...
播视网

百度热搜
1 拜登启动印太经济框架 13国加入
2 朝鲜元帅国葬出殡 金正恩为其抬棺
3 “动态清零”可持续且必须坚持
4 北京24小时新增本土感染者63例
5 河南隔一天测一次核酸 费用谁出?
6 清华在校女博士报考协警未被录取
7 拜登保镖在韩国打人后紧急回国
8 日本首相: 日美将监视中国海军活动
9 世卫发布猴痘疫情暴发预警
10 订单转移东南亚 外贸寒冬来了吗
11 王心凌回应又火了
12 张文宏: 新冠疫情短期内不会结束
13 麻报行程致疫情在京扩散 工头致歉
14 3米长抹香鲸2次搁浅沙滩死亡
15 居民错过核检被要求补缴前24轮费用

测试(查看日志)

Firepower Management Center Overview Analysis Policies Devices Objects AMP Intelligence

QYTANG-Policy Enter Description Analyze Hit Counts Save Cancel

Inheritance Settings | Policy Assignments (1)

Rules Security Intelligence HTTP Responses Logging Advanced Prefilter Policy: Default Prefilter Policy SSL Policy: None Identity Policy: qytang-id-policy

Filter by Device Search Rules Show Rule Conflicts Add Category Add Rule

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applications	Source Ports	Dest Ports	URLs	Source SGT	Dest SGT	Action	
Mandatory - QYTANG-Policy (1-4)														
Inside-DMZ (1-2)														
1	inside-to-dmz	ftd1-inside-zo	ftd1-dmz-zone	10.1.1.0/24	192.168.1.241 192.168.1.244	Any	Any	Any	Any	Any	Any	Any	Allow	
2	dmz-to-inside	ftd1-dmz-zone	ftd1-inside-zo	192.168.1.241 192.168.1.244	10.1.1.0/24	Any	Any	Any	Any	Any	Any	Any	Allow	
Inside-Outside (3-3)														
3	permit-ad-user	ftd1-inside-zo	Any	Any	Any	qytangad/fpc...	Any	Any	Any	Any	Any	Any	Allow	
DMZ-Outside (4-4)														
4	DNS	ftd1-dmz-zone	ftd1-outside-z	192.168.1.244	Any	Any				DNS_over_TCI DNS_over_UDI	Any	Any	Allow	
Default - QYTANG-Policy (-)														

1

- Cut
- Copy to
- Move to another policy
- Paste Above
- Paste Below
- Object Details...
- Edit...
- Delete
- State
- Insert new rule...
- Insert new category...
- 2 Show events

Default Action Access Control: Block All Traffic

1 Row Selected

Displaying 1 - 4 of 4 rules Page 1 of 1 Rules per page: 100

How To

测试(查看日志)

Firepower Management Center
Analysis / Connections / Events

Overview Analysis Policies Devices Objects AMP Intelligence

Bookmark This Page | Reporting | Dashboard | View Bookmarks | Search

Predefined Searches

Connection Events (switch workflow)

2022-05-23 04:14:41 - 2022-05-23 05:21:50 **II**
Expanding

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

Connections with Application Details **Table View of Connection Events**

Jump to...

	<input type="checkbox"/>	First Packet ×	Last Packet ×	Action ×	Reason ×	Initiator IP ×	Initiator Country ×	Initiator User ×	Responder IP ×	Responder Country ×	Security Intelligence × Category	Ingress Security Zone ×	Egress Security Zone ×	Source Port / ICMP Type
▼	<input type="checkbox"/>	2022-05-23 05:20:27	2022-05-23 05:21:29	Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	65.55.44.109	USA		ftd1-inside-zone	ftd1-outside-zone	50700 / t
▼	<input type="checkbox"/>	2022-05-23 05:20:27		Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	65.55.44.109	USA		ftd1-inside-zone	ftd1-outside-zone	50700 / t
▼	<input type="checkbox"/>	2022-05-23 05:20:24		Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	40.74.108.123	JPN		ftd1-inside-zone	ftd1-outside-zone	50699 / t
▼	<input type="checkbox"/>	2022-05-23 05:20:23	2022-05-23 05:20:24	Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	20.190.144.160	KOR		ftd1-inside-zone	ftd1-outside-zone	50698 / t
▼	<input type="checkbox"/>	2022-05-23 05:20:23		Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	20.190.144.160	KOR		ftd1-inside-zone	ftd1-outside-zone	50698 / t
▼	<input type="checkbox"/>	2022-05-23 05:19:55	2022-05-23 05:20:25	Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	142.251.42.234	USA		ftd1-inside-zone	ftd1-outside-zone	50696 / t
▼	<input type="checkbox"/>	2022-05-23 05:19:55	2022-05-23 05:20:25	Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	142.251.42.234	USA		ftd1-inside-zone	ftd1-outside-zone	50697 / t
▼	<input type="checkbox"/>	2022-05-23 05:19:50	2022-05-23 05:21:29	Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	65.55.44.109	USA		ftd1-inside-zone	ftd1-outside-zone	50695 / t
▼	<input type="checkbox"/>	2022-05-23 05:19:50		Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	65.55.44.109	USA		ftd1-inside-zone	ftd1-outs	Right-click for menu
▼	<input type="checkbox"/>	2022-05-23 05:19:49	2022-05-23 05:19:58	Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	20.42.65.92	USA		ftd1-inside-zone	ftd1-outside-zone	50694 / t
▼	<input type="checkbox"/>	2022-05-23 05:19:49		Allow		10.1.1.201		fpuser (qytangad\fpuser, LDAP)	20.42.65.92	USA		ftd1-inside-zone	ftd1-outside-zone	50694 / t

Page 1 of 1 > | Displaying rows 1-11 of 11 rows

[View](#)

[View All](#)

javascriptvoid(0)