

iMaster NCE-Campus

Interoperability With Fortinet Test Report

Issue	01
Date	2025-10-10

Contents

1 Overview.....	1
2 Test Environment.....	2
2.1 Topology.....	2
2.2 Devices and Software	3
3 Configuring iMaster NCE-Campus.....	4
3.1 Configuring Authentication and Authorization.....	4
4 Interconnecting iMaster NCE-Campus with FortiManager	8
4.1 Applying for and Importing the Certificate	8
4.2 Configuring Interconnection.....	12
4.3 Configuring a Security Policy.....	15
5 Test Cases	20
5.1 Interconnecting iMaster NCE-Campus with FortiManager	20
5.2 Reporting User Login and Logout Messages.....	22
5.3 Changing the Authorized Security Group.....	26
5.4 Communication Failure Between FortiManager and iMaster NCE-Campus.....	28

1 Overview

iMaster NCE-Campus functions as the EcoGrid server to interconnect with third-party firewalls to report online users and security groups to the firewalls. Then policies can be configured on the third-party firewalls based on the synchronized data to control traffic.

iMaster NCE-Campus functions as a security policy management platform to provide secure network access for end users and devices. It stores user and security group information. iMaster NCE-Campus also provides user and security group information to external authorized parties through EcoGrid.

iMaster NCE-Campus EcoGrid is an open and extensible security product integration framework (SPIF). It uses the publish/subscribe model to publish context for ecosystem partners to use. Ecosystem partners can obtain information such as user identities from iMaster NCE-Campus. In this way, security policies in the ecosystem become more efficient.

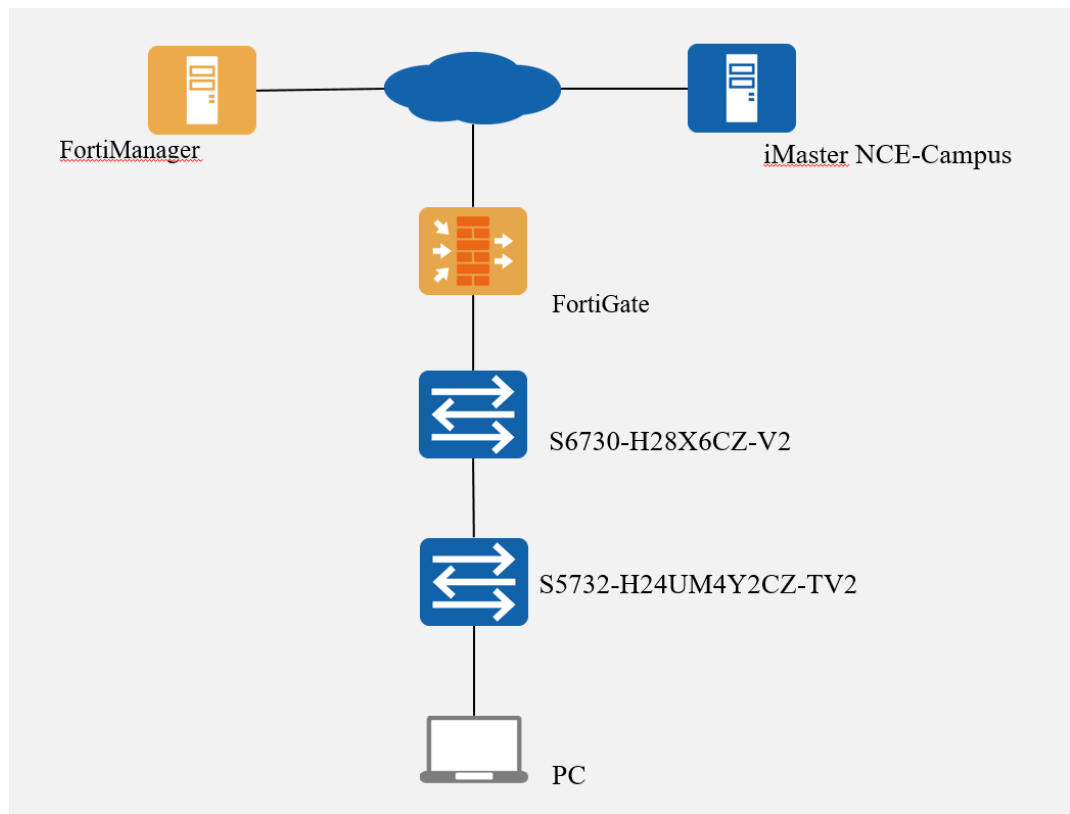
FortiManager functions as a client to interconnect with iMaster NCE-Campus EcoGrid. It synchronizes information such as sessions and security groups from iMaster NCE-Campus through EcoGrid. Then, FortiManager synchronizes the entries to FortiGate security devices to implement traffic control.

2 Test Environment

2.1 Topology

2.2 Devices and Software

2.1 Topology



2.2 Devices and Software

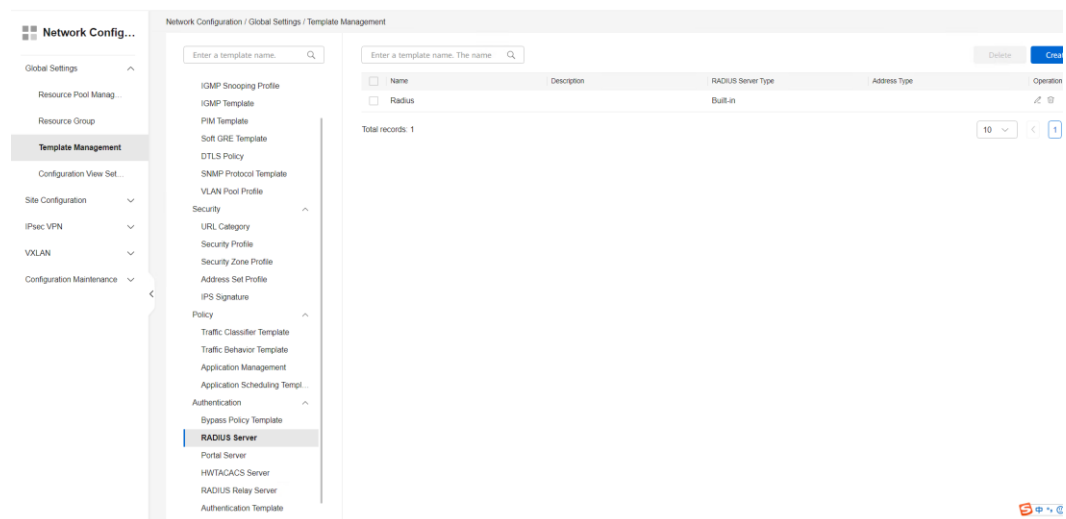
Device	Model	Software Version	Quantity	Remarks
Fortinet-Forti Manager	FortiManager	FortiManager-v7.4.6	1	pxGrid client
Fortinet-Forti Gate	FortiGate	FortiGate-200F v7.2.9	1	pxGrid client
Huawei Switch	S6730-H28X6CZ-V2	V600R025C00SPC 500	1	Border
	S5732-H24UM4Y 2CZ-TV2	V600R025C00SPC 500	1	Edge
iMaster NCE-Campus	iMaster NCE-Campus	V300R025C00SPC 100	1	AAA Server

3 Configuring iMaster NCE-Campus

3.1 Configuring Authentication and Authorization

3.1 Configuring Authentication and Authorization

1. Configure authentication.



Admission Management / Admission Policy / Free Mobility

Security Group Resource Group Policy Control IP-Group Entry Subscription IP-Group Entry

Enter a keyword. Security Group Type: All Import Export Delete Create

<input type="checkbox"/>	Name T1	ID T1	Description	Security Group Type
<input type="checkbox"/>	> newSec	5		Normal
<input type="checkbox"/>	> sec_group	4		Normal
<input type="checkbox"/>	> sec_group_deny	1		Normal
<input type="checkbox"/>	> sec_group_permit	6		Normal
<input type="checkbox"/>	> unknown	0	--	Normal

Total records: 5

3. Create a user and user group.

iMaster NCE-Campus Workbench Dashboard 192.168.1.1

Deploy Task Center Resource Center m@h.com

Admission Management / Admission Resource / Admission User Management

User Management Role Management Blacklist Management External Group Management

User MAC Account PPSK User Operation Log User Group IP Address ...

Enter a user group name. Enter a keyword. Advanced Search Custom Field Enable Disable Transfer Delete Create

<input type="checkbox"/>	Username T1	User Group	Role	Description T1	Email T1	Phone Number T1	User Expiration T1	User Status T1	Last Login T1	Operation
<input type="checkbox"/>	pa@h.com	ROOT-Quest	ROOT-Quest					Enabled		

Total records: 1

4. Create an authentication rule, an authorization rule, and an authorization result (security group authorization).

Admission Management / Admission Policy / Authentication and Authorization

Authentication Rule Authorization Result Authorization Rule Policy Element Multi-level RADIUS Relay Network Access Policy

Enter a name. Clear Filter Disable Enable Create

<input type="checkbox"/>	Priority T1	Name T1	Authentic...	Access Mode T1	Matching Condition	Data Sour...	Authentic...	Hits T1	Access Pa...	Enabling S...	Operation
<input type="checkbox"/>	1	wired	User access...	Wired		<Data sour...	PAP (local a...	0	--	Enabled	
<input type="checkbox"/>	1	Default	HACA portal...	Wired/Wirel...		<Data sour...	EAP-TLS (o...	0	--	Enabled	

Total records: 2

Admission Man...

Admission Overview

SDP Controller

Admission Resource

Admission User Man...

Guest Management

VIP Management

External Data Source

Client Management

Admission Device

Certificate Authentica...

Passive Identity Service

Admission Policy

Page Management

Authentication and ...

HWTACACS Authent...

Free Mobility

VAS

Admission Management / Admission Policy / Authentication and Authorization

Authentication Rule | Authorization Result | Authorization Rule | Policy Element | Multi-level RADIUS Relay | Network Access Policy

Authorization results are delivered only after they are bound to sites. For details, see [Online Help](#).

Enter a keyword.

<input type="checkbox"/>	Name T1	Service Type T1	Description T1	VIP Users T1	ACL T1	IPv6ACL T1	Authorized Us... T1	Security Group T1	VLAN T1	Download Rate... T1	Upload Rate (... T1	DSCP T1	Operation
<input type="checkbox"/>	Permit Access	All	It is a default a...	No	--	--	--	--	--	0	0	--	D
<input type="checkbox"/>	Deny Access	All	It is a default a...	No	--	--	--	--	--	0	0	--	D
<input type="checkbox"/>	pxGrid	Access service		No	--	--		sec_group	--	0	0	--	D E O

Total records: 3

20

Admission Man...

Admission Overview

SDP Controller

Admission Resource

Admission User Man...

Guest Management

VIP Management

External Data Source

Client Management

Admission Device

Certificate Authentica...

Passive Identity Service

Admission Policy

Admission Management / Admission Policy / Authentication and Authorization

Authentication Rule | Authorization Result | Authorization Rule | Policy Element | Multi-level RADIUS Relay | Network Access Policy

Enter a name.

Clear Hits

Disable

Enable

<input type="checkbox"/>	Priority T1	Name T1	Authenticati... T1	Access Mode T1	Matching Condition	Authorizatio... T1	Description T1	Hits T1	Enabling St... T1	Op
<input type="checkbox"/>	1	wired	User access ...	Wired		pxGrid		0	Enabled	D
<input type="checkbox"/>	N	Default	HACA Portal...	WiredWirele...		pxGrid	--	0	Enabled	D

Total records: 2

4 Interconnecting iMaster NCE-Campus with FortiManager

[4.1 Applying for and Importing the Certificate](#)

[4.2 Configuring Interconnection](#)

[4.3 Configuring a Security Policy](#)

4.1 Applying for and Importing the Certificate

1. Apply for and import certificates through iMaster NCE-Campus and a third-party client (iMaster NCE-Campus as the CA).
 - a. Log in to iMaster NCE-Campus as the system administrator, choose **System > Security Management > Certificate Authority Service** from the main menu, and choose **PKI Management > CA** from the navigation pane. Click **Add**, enter the required information, and click **Next**.
 - b. On the **Set Associate Profile** page, select **END_ENTITY_PREDEFINED_MULTI_KEY_TYPES_50YEARS**, and select the check box before the profile on the right to set it as the default profile. Click **Next**.

CA>Create CA

⚡ If you want to issue a response protection identity certificate in the next step or when uploading the CA certificate, select at least one profile whose certificate level is "End entity" in the associate profile list.

Set Associate Profile

Enter an associate profile name

Name	Certificate Level	Profile usage	Predefined
<input checked="" type="checkbox"/> END_ENTITY_PREDEFINED_MULTI_KEY_TYPES_50YEARS	End entity	Normal	Yes
<input type="checkbox"/> END_ENTITY_PREDEFINED_WEB_TLS	End entity	Normal	Yes
<input type="checkbox"/> END_ENTITY_PREDEFINED_MULTI_KEY_TYPES	End entity	Normal	Yes
<input type="checkbox"/> END_ENTITY_PREDEFINED_ECDSA256	End entity	Normal	Yes
<input type="checkbox"/> SUB_CA_PREDEFINED_ECDSA384	Subordinate CA	Normal	Yes
<input type="checkbox"/> ROOT_CA_PREDEFINED_ECDSA384	Root CA	Normal	Yes
<input type="checkbox"/> END_ENTITY_PREDEFINED_RSA3072	End entity	Normal	Yes
<input type="checkbox"/> END_ENTITY_PREDEFINED_RSA2048	End entity	Normal	Yes
<input type="checkbox"/> SUB_CA_PREDEFINED_RSA4096_60YEARS	Subordinate CA	Normal	Yes
<input type="checkbox"/> SUB_CA_PREDEFINED_RSA4096	Subordinate CA	Normal	Yes

Total records: 12

Set Default Profile

Enter a default profile name

Name	Profile usage	Operation
<input checked="" type="checkbox"/> END_ENTITY_PREDEFINED_MULTI_KEY_TYPES_50YEARS	Normal	Delete

Reset Cancel Previous Next

- c. Set Set CA certificate to TLS trust certificate and Issue response protection identity certificate to No, and click Submit.

System

Certificate Authority...

CA>Create CA

Set CA certificate to TLS trust certificate ☐ Yes ☒ No

Issue response protection identity certificate ☐ Yes ☒ No

- d. Enable the end entity certificate application function.
- Choose **System > Security Management > Certificate Authority Service** from the main menu and choose **Global Configuration > Function Management** from the navigation pane.
 - Click **Enable**. In the dialog box that is displayed, click **OK**.

iMaster NCE-Campus

Workbench

Resource Center Maintenance System

Function Management

Function Item	Description	Status	Operation
End entity certificate application	Apply for an end entity certificate using the basic information or CSR file	Enable	Disable

- e. Generate a CSR file on the third-party client and import it to iMaster NCE-Campus.

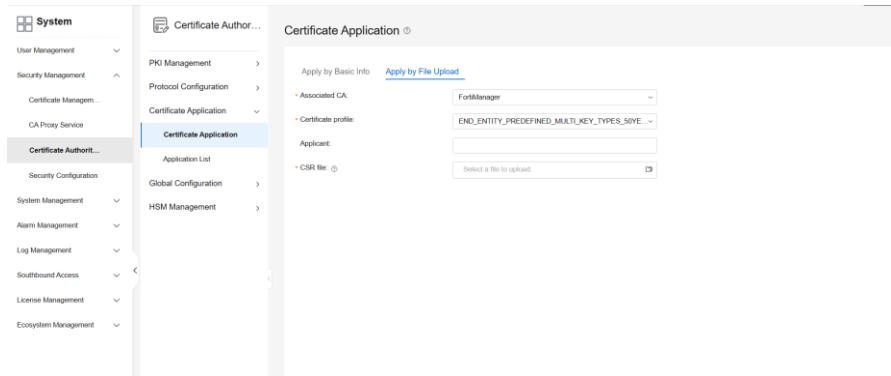
Generate a CSR file on FortiManager. The algorithm type in the file must be the same as that in the profile on iMaster NCE-Campus.

The first screenshot shows the FortiManager interface with the 'Certificate' section selected. The 'Generate CSR' button is highlighted in the left sidebar. The main panel displays a list of certificates, including 'Local CA Certificate (1)', 'Remote CA Certificate (1)', and 'Certificate (1)'. The 'Certificate (1)' entry is highlighted.

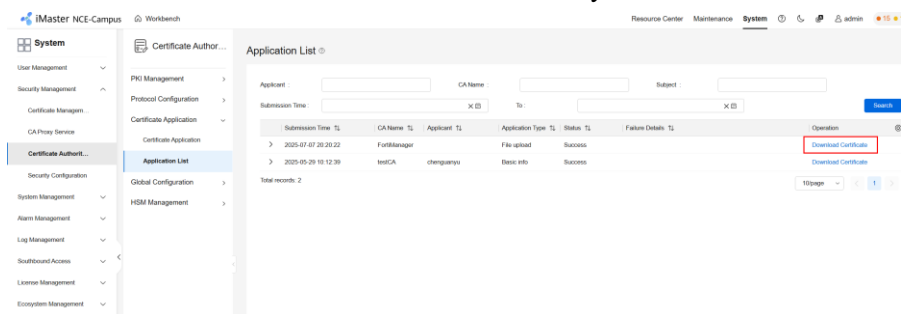
The second screenshot shows the 'Generate Certificate Signing Request' dialog box. The 'Subject Information' section is expanded, showing fields for 'Subject Name', 'Domain Name', 'Email Address', and 'Subject Alternative Name'. The 'Key Size' is set to 2048 bits. The 'Key Type' is set to RSA.

The third screenshot shows the FortiManager interface with the 'Certificate' section selected. The 'Certificate (1)' entry is highlighted in the list. The 'Generate CSR' button is highlighted in the left sidebar.

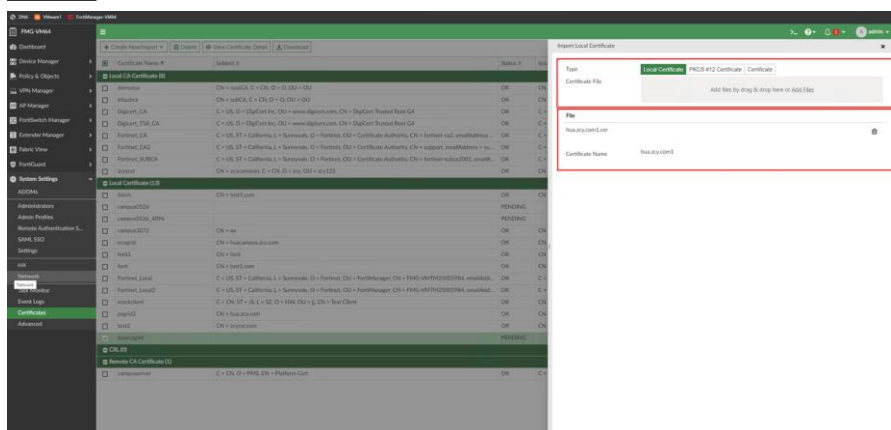
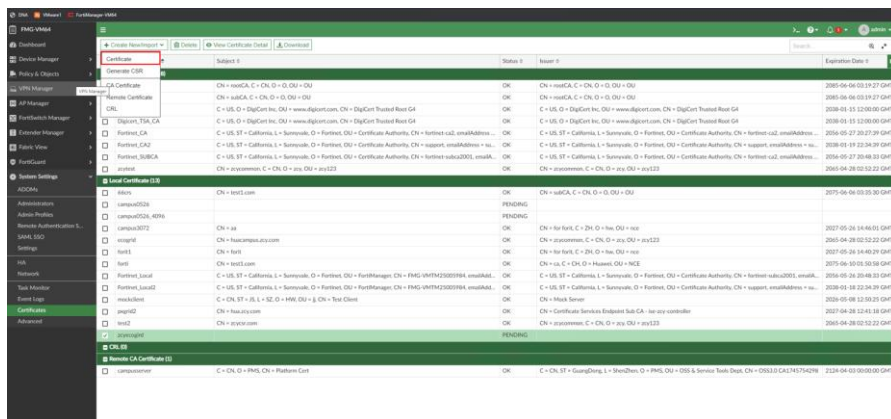
- Choose **System > Security Management > Certificate Authority Service** from the main menu and choose **Certificate Application > Certificate Application** from the navigation pane.
- Click the **Apply by File Upload** tab, import the CSR file generated by the third-party device, and click **Submit**.



- iii. Choose **System > Security Management > Certificate Authority Service** from the main menu and choose **Certificate Application > Application List** from the navigation pane. Click **Download Certificate** in the row that contains the desired certificate to download the certificate to your local PC.



- iv. Import the certificate downloaded in the previous step to the third-party client and activate the certificate.



iMaster NCE-Campus | Workbench | Resource Center | Maintenance | System | admin

System

- User Management
- Security Management
- Certificate Management
 - Service Certificate Management
 - All Certificates
 - Shared CRLs
 - Certificate Update
 - Settings
- CA Policy Service
- Certificate Authority
- Security Configuration
- System Management
- Alarm Management
- Log Management
- Southbound Access
- Licence Management
- Ecosystem Management

APIGWService Certificates [In Use]

Identify Certificates | Trust Certificates | Certificate Revocation Lists

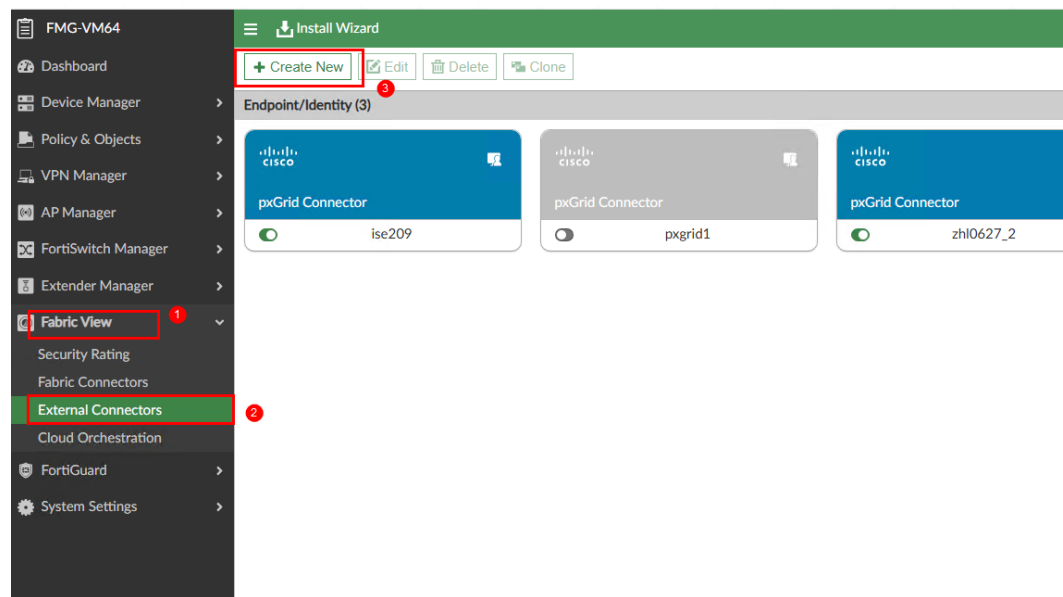
Certificate Alias: Q

<	Certificate A.	Issued By	Used By	Effective From	Expires On	Added On	Type	Remarks	Certificate S.	Operation
>	checkpoint.cn	CN=www.chec.	CN=www.chec.	2025-07-04 09.	2025-07-04 19.	2025-07-04 19.	-		Normal	[Edit] [Delete]
>	aggrCCA	CN=campus..	CN=campus..	2025-07-04 09.	2065-07-04 09.	2025-07-04 09.	-		Normal	[Edit] [Delete]
>	Dongguan2	CN=hwaeo..O	CN=ASPCA..	2025-06-21 11.	2025-06-21 11.	2025-06-27 09.	-		Normal	[Edit] [Delete]
>	ZhiCampus	CN=SHUTON..	CN=SHUTON..	2025-06-10 14.	2065-06-10 14.	2025-06-27 09.	-		Normal	[Edit] [Delete]
>	DONGGUAN6B	CN=D G O B ..	CN=D G O B ..	2025-06-21 15.	2075-06-21 15.	2025-06-21 15.	-		Normal	[Edit] [Delete]
>	zyxelw2	CN=SHUTON..	CN=huaw.zyx.com	2025-06-10 14.	2075-06-10 14.	2025-06-10 14.	-		Normal	[Edit] [Delete]
>	kentrix	CN=NICE..O	CN=nice.com	2025-06-10 09.	2075-06-10 09.	2025-06-10 09.	-		Normal	[Edit] [Delete]
>	trust-car	CN=CSSS D C.	CN=CSSS D C.	2025-06-08 08.	2124-05-18 09.	2025-06-09 21.	-		Normal	[Edit] [Delete]

Total records: 8

10page < 1 >

Configure the following options and click *OK*



Search...



MAC Address
Threat Feed

User ClearPass



Create New Fabric Connector - User pxGrid (2/2)

Connector Settings

Name

Status

This field is required.

pxGrid Connector

Server

CA Certificate

Click to select

Client Certificate

Click to select

Revision

Change Note *

0/1023

Revision History

Revert

View Diff

Search...

	Revision #	Changed by	Date/Time	Entry Key	Entry name	Action	Change Note	
No record found.								
								0

Back

Apply & Refresh

OK

Cancel

Activate Windows

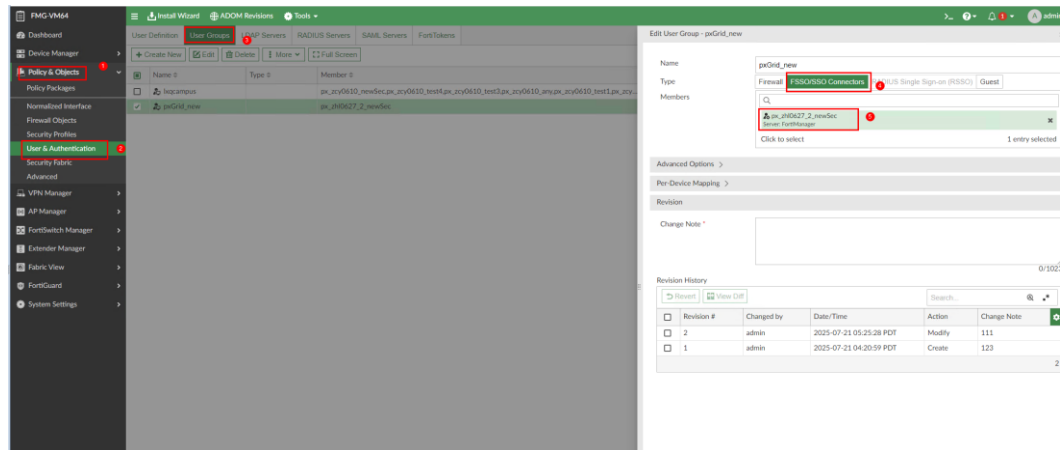
Go to System in Control Panel to activate Windows.

Activate Windows

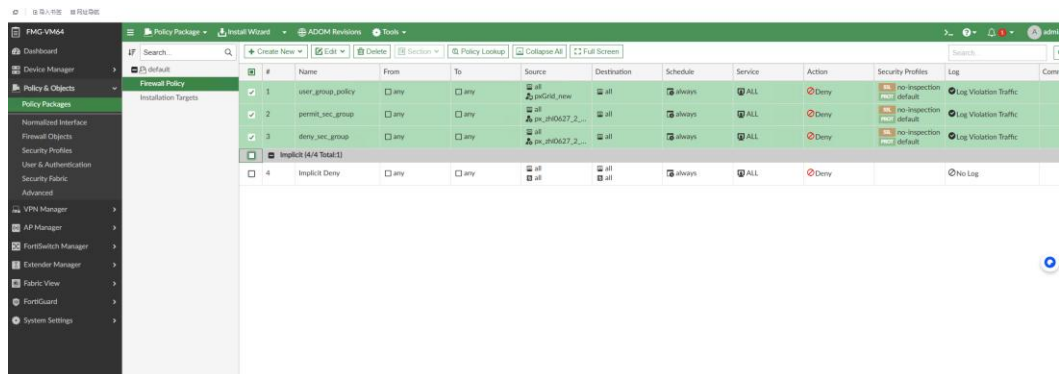
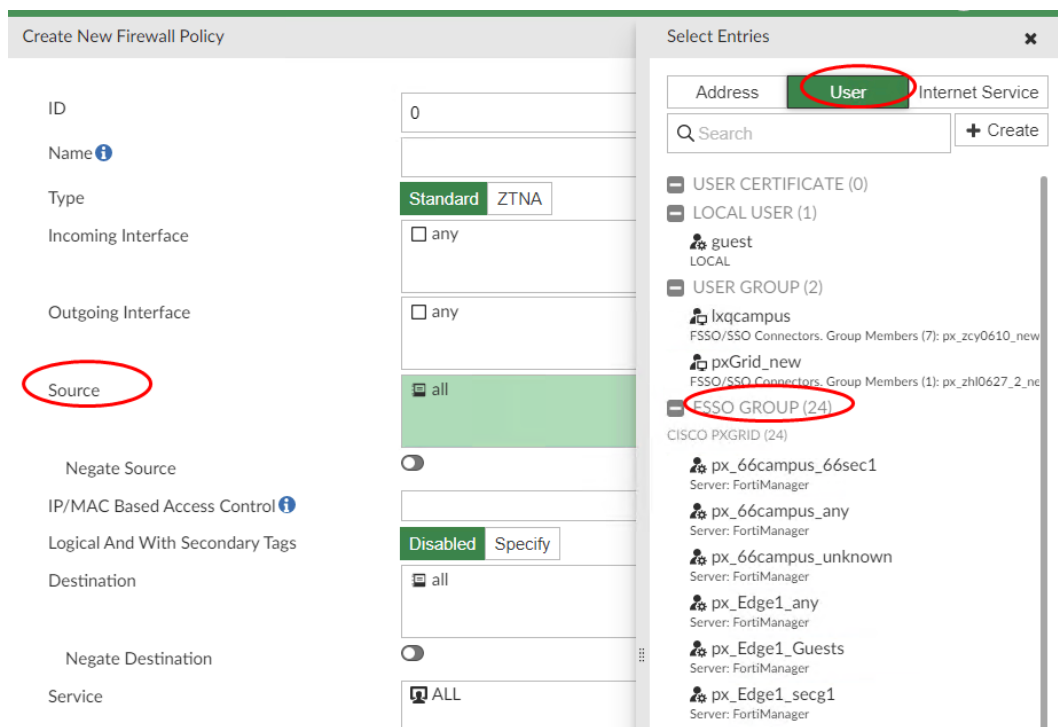
Go to Settings to activate Windows.

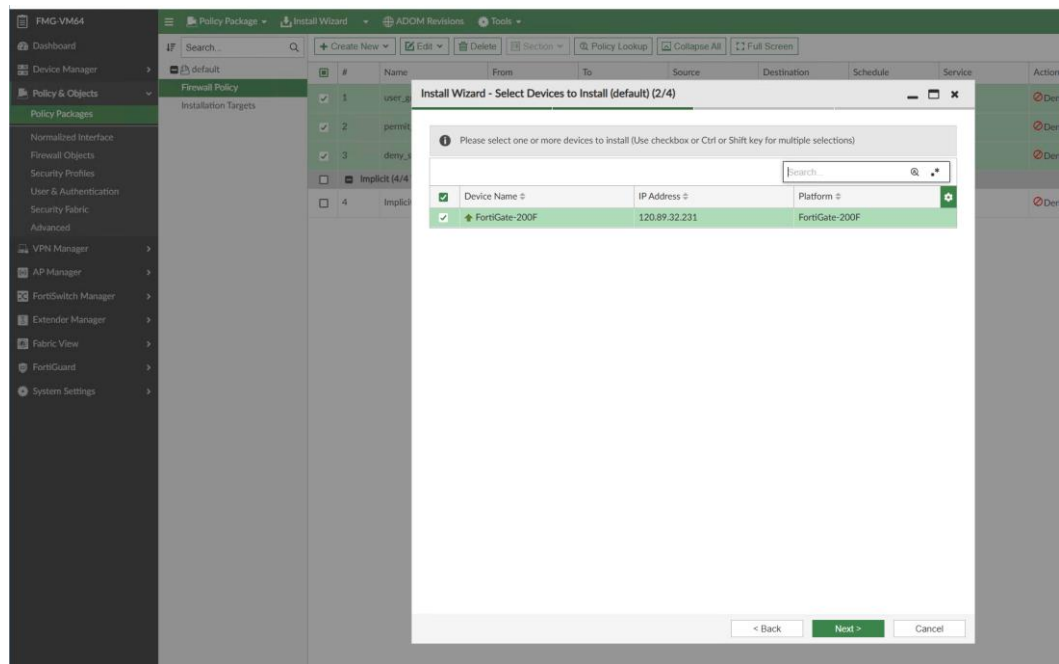
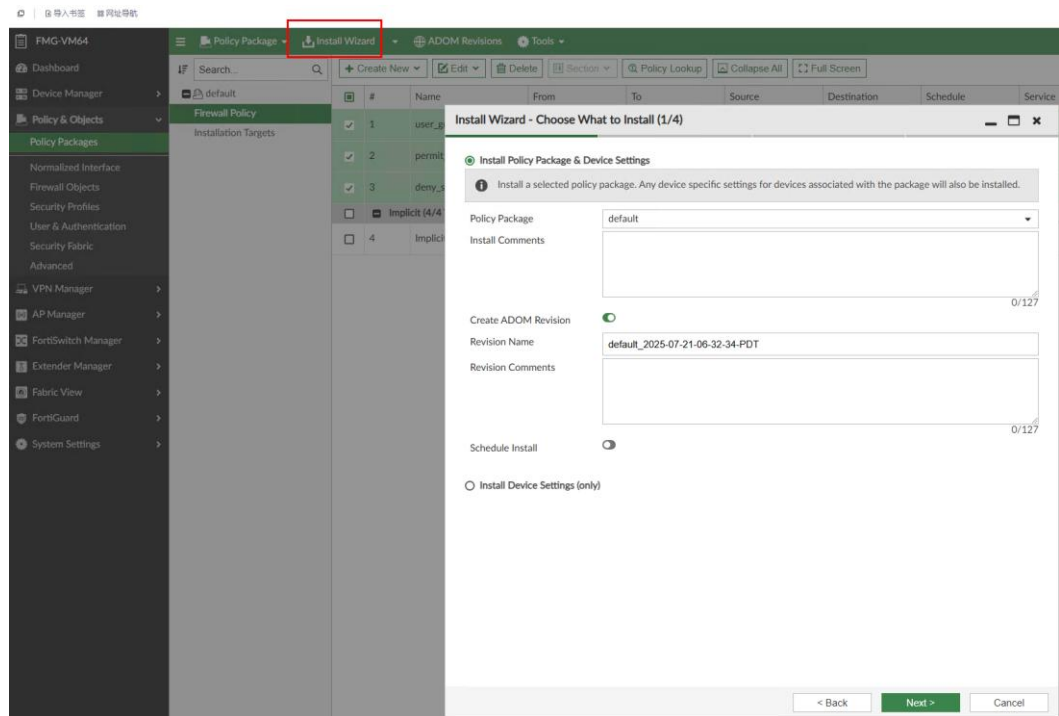
4.3 Configuring a Security Policy

1. Choose **Policy & Objects > User & Authentication > User Groups** and create a new group. Set the type as FSSO/Cisco TrustSec, and select pxGrid user as a member.



2. Create a policy with the **pxGrid_new** user group and install the policy on FortiGate.





Install Wizard - Validate Devices (default) (3/4)

Installation Preparation

Total: 2/2

Success: 2

Warning: 0

Error: 0

Show Details

✓ Interface Validation

✓ Policy and Object Validation

✓ Ready to Install

Install Preview

Policy Package Diff

Search...

✓	Device Name	Status	Action
✓	FortiGate-200F	Connection Up	

< Back

Install

Cancel

Install Wizard - Installation Progress (default) (4/4)

✓ Installed successfully.

100%

Total: 1/1, Success: 1, Warning: 0, Error: 0

Show Details

View Installation Log

View Progress Report

Search...

#	Name	Time Used	Status
1	FortiGate-200F	24s	install and save finished status=OK

Finish

Close

Policies on the FortiGate device

FortiGate-200F

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 Access Control List

IPv4 DoS Policy

Authentication Rules

Addresses

ZTNA

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

System

Security Fabric

Log & Report

View

Show in CLI

Policy lookup

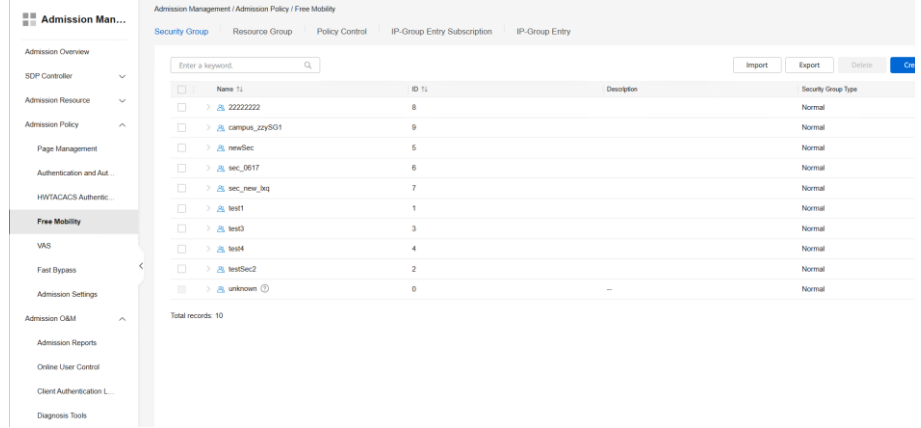
Search

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
user_group_policy	ipGrid_new	all	always	ALL	DENY			All
permit_sec_group	ip_chi0627_2_sec_group_permit	all	always	ALL	ACCEPT	Disabled	no-inspection	All
deny_sec_group	ip_chi0627_2_sec_group_deny	all	always	ALL	DENY			All
Implicit								
Implicit Deny	all	all	always	ALL	DENY			Disabled

5 Test Cases

- 5.1 Interconnecting iMaster NCE-Campus with FortiManager
- 5.2 Reporting User Login and Logout Messages
- 5.3 Changing the Authorized Security Group
- 5.4 Communication Failure Between FortiManager and iMaster NCE-Campus

5.1 Interconnecting iMaster NCE-Campus with FortiManager

Test Scenario	Interconnecting iMaster NCE-Campus with FortiManager
Test Objective	To verify that iMaster NCE-Campus is successfully interconnected with FortiManager.
Test Procedure	<p>1. Configure the interconnection by referring to section 4.2. Expected result 1 is achieved.</p> <p>2. A security group is created and online users are generated on the controller.</p> 

The security group created on the controller and the online users generated on the controller are synchronized to FortiManager, and the entries are synchronized to the FortiGate device.

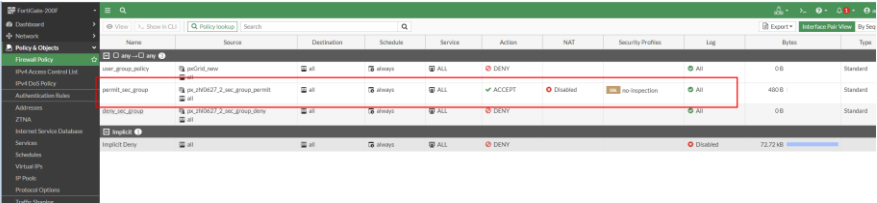
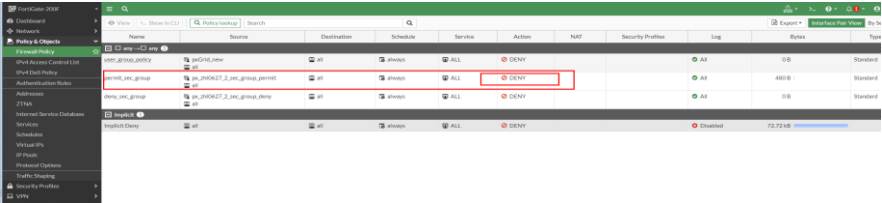
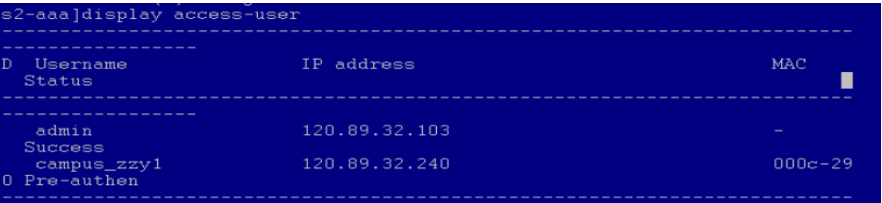
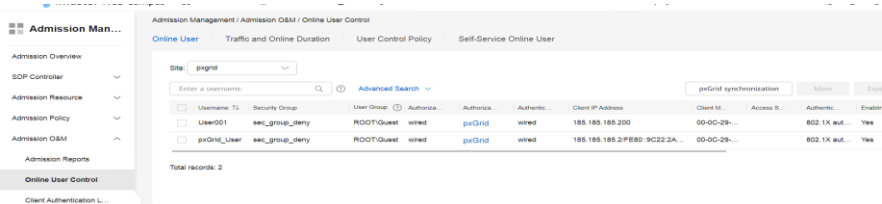
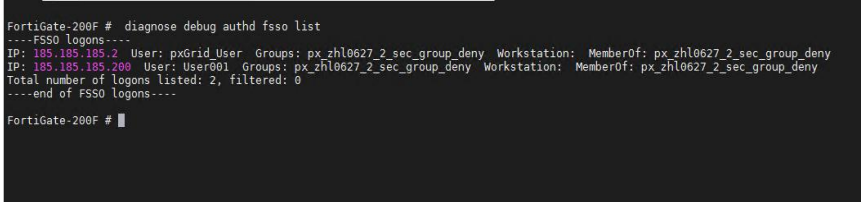
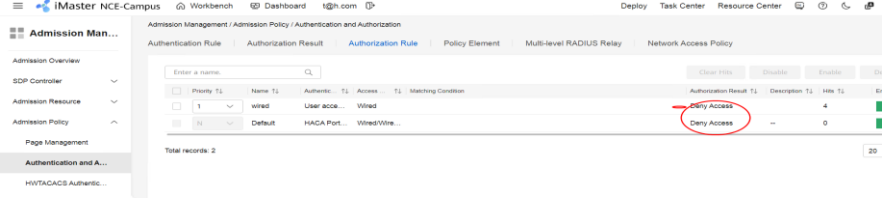
```

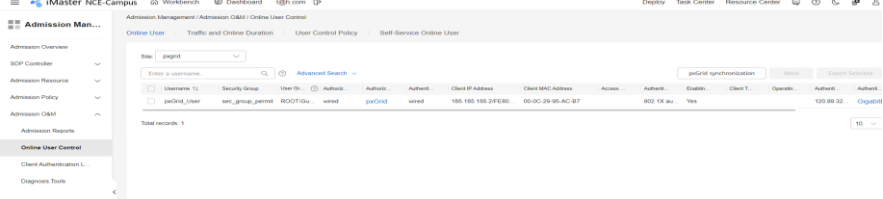
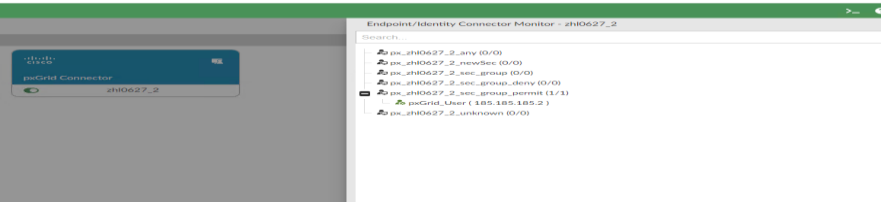
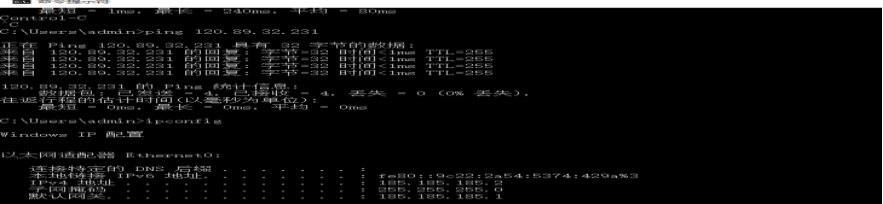
FortiGate-200F # diagnose debug authd fsso list
....FSO logons....
IP: 120.89.32.236 User: campus_zzy1 Groups: px_zhl0627_2_campus_zzySG1 Workstation:
IP: 120.89.32.237 User: ise209zzy1 Groups: px_ise209_ise209SG1 Workstation:
Total number of logons listed: 2, filtered: 0
----end of FSO logons----
FortiGate-200F #

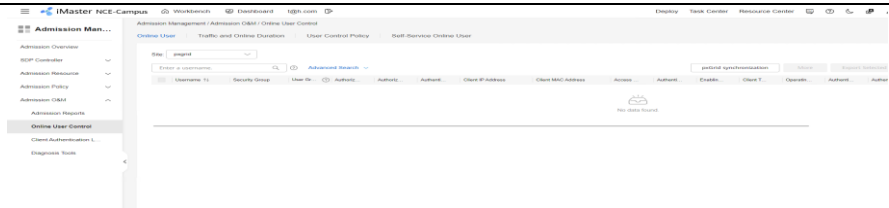
```

5.2 Reporting User Login and Logout Messages

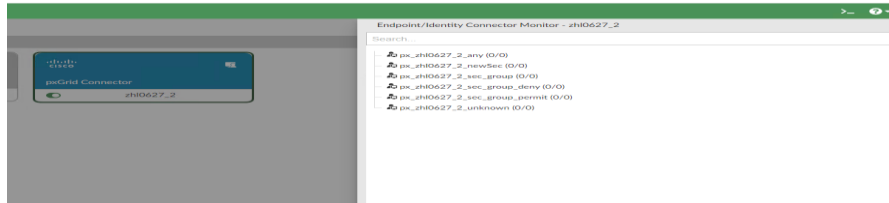
Test Scenario	Reporting new online users and offline users on iMaster NCE-Campus in real time
Test	To verify that new online users and offline users can be reported in real time on

Objective	iMaster NCE-Campus.
Test Procedure	<div>1. Configure security policies by referring to section 4.3.</div> <div>2. Add an online user on iMaster NCE-Campus and authorize the security group sec_group_permit (the security group has been synchronized to FortiManager). Expected result 1 is achieved.</div> <div></div> <div>3. Modify the security policy and the endpoint cannot access the network. Expected result 2 is achieved.</div> <div></div> <div>4. The user on iMaster NCE-Campus goes offline. Expected result 3 is achieved.</div> <div></div> <div>5. Modify the authorization rule and change the authorization result to deny access. Then, CoA is performed. Expected result 4 is achieved.</div> <div></div> <div></div> <div></div>
Expected	1. The online user is synchronized to FortiManager, and entries are

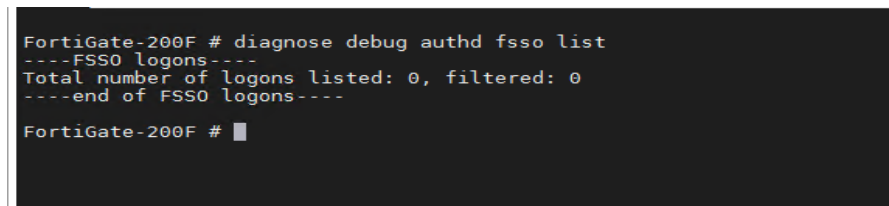
d Result	<p>synchronized to the FortiGate device. The endpoint can access 120.89.32.231.</p> <p>2. The endpoint cannot access 120.89.32.231.</p> <p>3. The online user is deleted from FortiManager, and the entries are deleted from the FortiGate device.</p> <p>4. The user goes offline, the online user is deleted from FortiManager, and the entries are deleted from the FortiGate device.</p>
Test Result	<p>1. The online user is synchronized to FortiManager, and entries are synchronized to the FortiGate device.</p> <p>Online User page of the controller</p>  <p>Entries synchronized to the FortiGate device</p>  <p>Online users on FortiManager</p>  <p>The endpoint can access 120.89.32.231</p>  <p>2. The endpoint cannot access 120.89.32.231.</p>  <p>3. The online user is deleted from FortiManager, and the entries are deleted from the FortiGate device.</p> <p>Controller user goes offline</p>



Online user deleted from FortiManager

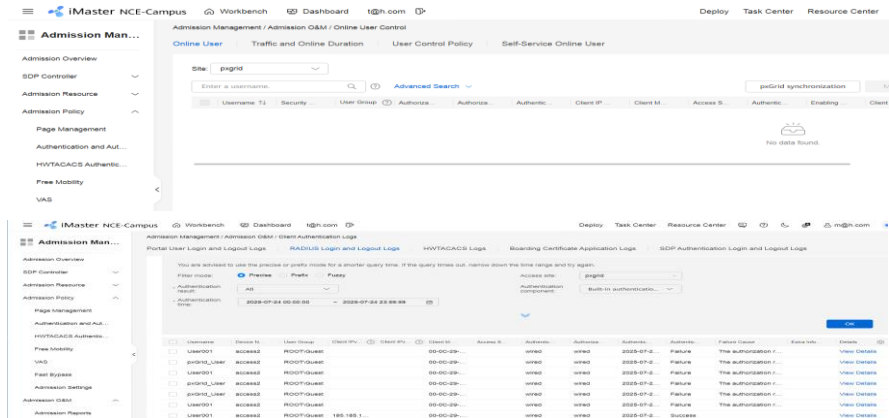


Entries deleted from the FortiGate device

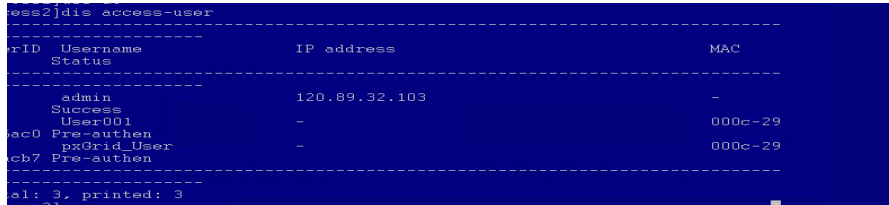


4. The user goes offline, the online user is deleted from FortiManager, and the entries are deleted from the FortiGate device.

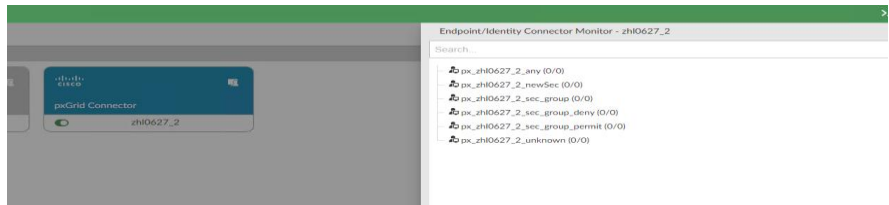
Controller user



Device

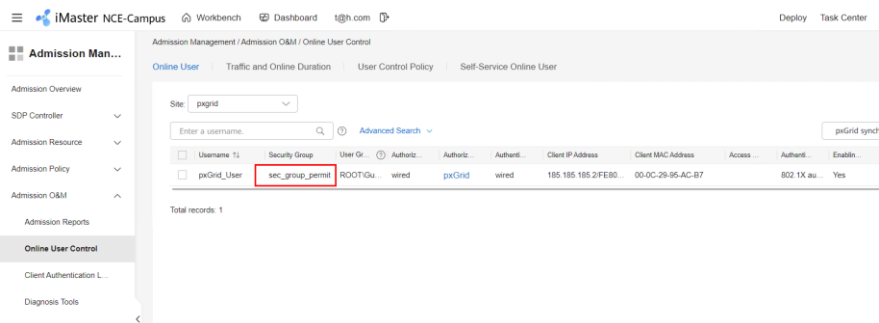
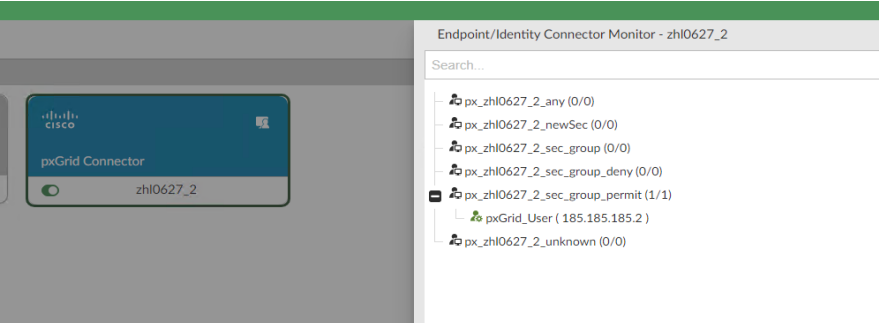


Online user deleted from FortiManager



	<p>Entries deleted from the FortiGate device</p> <pre> FortiGate-200F # diagnose debug authd fsso list ----FSSO logons---- Total number of logons listed: 0, filtered: 0 ----end of FSSO logons---- FortiGate-200F # </pre>
--	--

5.3 Changing the Authorized Security Group

Test Scenario	Reporting the security group authorization change of online users in real time on iMaster NCE-Campus
Test Objective	To verify that the security group authorization change of online users can be reported in real time on iMaster NCE-Campus.
Test Procedure	<p>1. Authorize the security group sec_group_permit to the user, and ensure that the endpoint can access 120.89.32.231.</p>   <pre> FortiGate-200F # diagnose debug authd fsso list ----FSSO logons---- IP: 185.185.185.2 User: pxGrid_User Groups: px_zhl0627_2_sec_group_permit Workstation: MemberOf: px_zhl0627_2_sec_group_permit Total number of logons listed: 1, filtered: 0 ----end of FSSO logons---- FortiGate-200F # </pre>

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log
user_group_policy	any	any	any	all	DENY			
permit_sec_group	any	any	any	all	ACCEPT	Disabled	no-inspection	
deny_sec_group	any	any	any	all	DENY			
Implicit Deny	any	any	any	all	DENY			

```
C:\Users\admin>ping 120.89.32.231

正在 Ping 120.89.32.231 具有 32 字节的数据:
来自 120.89.32.231 的回复: 字节=32 时间<1ms TTL=255
来自 120.89.32.231 的回复: 字节=32 时间<1ms TTL=255
来自 120.89.32.231 的回复: 字节=32 时间<1ms TTL=255
来自 120.89.32.231 的回复: 字节=32 时间<1ms TTL=255

120.89.32.231 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\admin>
```

2. Change the authorized security group of the online user on iMaster NCE-Campus to **sec_group_deny**. Expected result 1 is achieved.

#	Name	From	To	Source	Destination	Schedule	Service	Action	Security Profiles
1	user_group_policy	any	any	all	all	any	all	Deny	no-inspection
2	permit_sec_group	any	any	all	all	any	all	Accept	no-inspection
3	deny_sec_group	any	any	all	all	any	all	Deny	no-inspection
4	Implicit Deny	any	any	all	all	any	all	Deny	no-inspection

Name	Service Type	Description	VP Users	ACL	IPv4 ACL	Authorized Users	Security Group	VLAN	Downlink Rate	Uplink Rate	DSOP	Operation
Permit Access	All	It is a default a...	No	--	--	--	--	--	0	0	--	
Deny Access	All	It is a default a...	No	--	--	--	--	--	0	0	--	
paGrid	Access service	No	--	--	--	--	sec_group_deny	--	0	0	--	

Expected Result

1. The online user on FortiManager and the corresponding entries on the FortiGate device are changed, and the endpoint cannot access 120.89.32.231.

Test Result

Online User page of the controller

Admission Man...

Admission Overview

SDP Controller

Admission Resource

Admission Policy

Admission OAM

Admission Reports

Online User Control

Client Authentication L...

Admission Management / Admission OAM / Online User Control

Online User | Traffic and Online Duration | User Control Policy | Self-Service Online User

Site: pxgrid

Enter a username: Advanced Search

pxGrid synchronization | More | Export Selected | Export All

Username	Security Group	User Gr...	Authc...	Authc...	Client IP...	Client M...	Access...	Authc...	Enabl...	Client T...	Operat...	Authc...	Authc...	Loge T...	Call6 S...
pxGrid_U...	sec_group_deny	ROOT/Ga...	wired	pxGrid	wired	185.185.1...	00-0C-2B...	802.1X au...	Yes					120.89.32...	GigabitEthe...

Total records: 1

Online users on FortiManager

pxGrid Connector

zh10627_2

Endpoint/Identity Connector Monitor - zh10627_2

Search...

px_zhl0627_2_any (0/0)

px_zhl0627_2_newSec (0/0)

px_zhl0627_2_sec_group (0/0)

px_zhl0627_2_sec_group_deny (1/1)

pxGrid_User (185.185.185.2)

px_zhl0627_2_sec_group_permit (0/0)

px_zhl0627_2_unknown (0/0)

Corresponding entries changed on the FortiGate device

FortiGate-200F #

FortiGate-200F #

FortiGate-200F # diagnose debug authd fsso list

----FSO logons----

IP: 185.185.185.2 User: pxGrid User Groups: px_zhl0627_2_sec_group_permit Workstation: MemberOf: px_zhl0627_2_sec_group_permit

Total number of logons listed: 1, filtered: 0

----end of FSO logons----

FortiGate-200F # diagnose debug authd fsso list

----FSO logons----

IP: 185.185.185.2 User: pxGrid User Groups: px_zhl0627_2_sec_group_deny Workstation: MemberOf: px_zhl0627_2_sec_group_deny

Total number of logons listed: 1, filtered: 0

----end of FSO logons----

FortiGate-200F #

The endpoint cannot access 120.89.32.231

C:\Users\admin>ping 120.89.32.231

正在 Ping 120.89.32.231 具有 32 字节的数据:

来自 120.89.32.231 的回复: 字节=32 时间<1ms TTL=255

来自 120.89.32.231 的回复: 字节=32 时间<1ms TTL=255

来自 120.89.32.231 的回复: 字节=32 时间<1ms TTL=255

120.89.32.231 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),

往返行程的估计时间(以毫秒为单位):

最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\admin>ping 120.89.32.231

正在 Ping 120.89.32.231 具有 32 字节的数据:

请求超时。

请求超时。

请求超时。

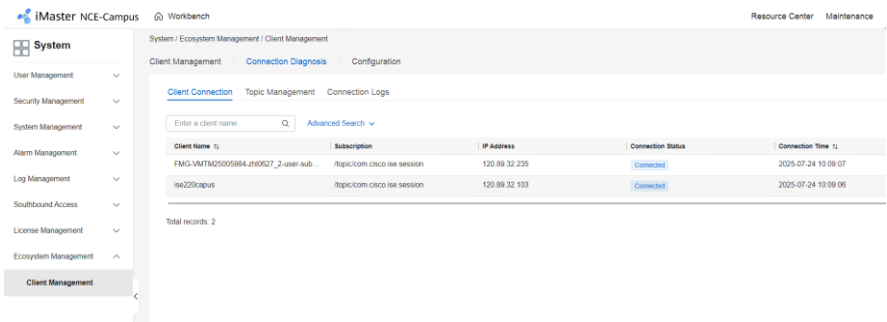
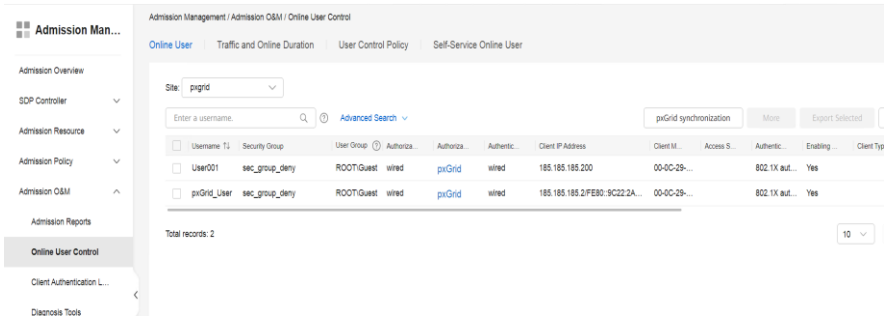
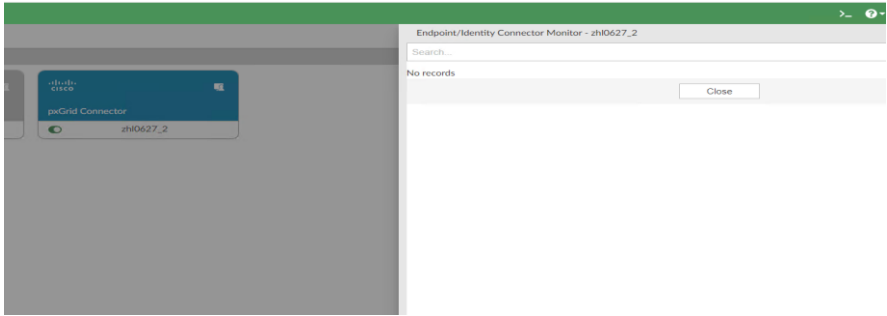
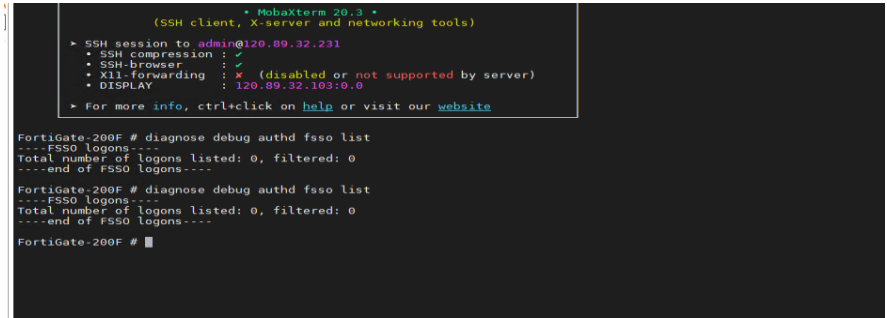
120.89.32.231 的 Ping 统计信息:

数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\admin>

5.4 Communication Failure Between FortiManager and iMaster NCE-Campus

Test	Communication failure between FortiManager and iMaster NCE-Campus
------	---

Scenario	
Test Objective	To verify that the users who go online during the communication failure between FortiManager and iMaster NCE-Campus can be synchronized to FortiManager after the fault is rectified.
Test Procedure	<p>1. Simulate a communication failure between FortiManager and iMaster NCE-Campus.</p>  <p>2. Add an online user on iMaster NCE-Campus and authorize the security group. Rectify the fault. Expected result 1 is achieved.</p>   
Expected Result	1. The channel is re-established, the online user is synchronized to FortiManager, and entries are synchronized to the FortiGate device.
Test	Controller channel

Result

System

User Management

Security Management

System Management

Alarm Management

Log Management

Southbound Access

License Management

Ecosystem Management

Client Management

System / Ecosystem Management / Client Management

Client Management

Connection Diagnosis

Configuration

Client Connection

Topic Management

Connection Logs

Enter a client name

Advanced Search

Client Name	Subscription	IP Address	Connection Status	Connection Time	Duration
FMG-VMTM25005684-zh0627_2-u	/topiccom/cisco/ise/session	120.89.32.235	Connected	2025-07-24 15:48:03	7m15s
ise220campus	/topiccom/cisco/ise/session	120.89.32.103	Connected	2025-07-24 10:09:06	5h46m12s

Total records: 2

20 pcs/page

Online user synchronized to FortiManager

pxGrid Connector

zh0627_2

Endpoint/Identity Connector Monitor - zh0627_2

px_zh0627_2_any (0/0)

px_zh0627_2_newSec (0/0)

px_zh0627_2_sec_group (0/0)

px_zh0627_2_sec_group_deny (2/2)

User001 (185.185.185.200)

px_zh0627_2_sec_group_permit (0/0)

px_zh0627_2_unknown (0/0)

Entries synchronized to the FortiGate device

```
FortiGate-200F # diagnose debug authd fsso list
----FSO logons----
IP: 185.185.185.2 User: pxGrid_User Groups: px_zhl0627_2_sec_group_deny Workstation: MemberOf: px_zhl0627_2_sec_group_deny
IP: 185.185.185.200 User: User001 Groups: px_zhl0627_2_sec_group_deny Workstation: MemberOf: px_zhl0627_2_sec_group_deny
Total number of logons listed: 2, filtered: 0
----end of FSSO logons----

FortiGate-200F #
```