



# FortiSwitch Cookbook

**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<https://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTINET TRAINING & CERTIFICATION PROGRAM**

<https://www.fortinet.com/support-and-training/training.html>

**NSE INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD CENTER**

<https://fortiguard.com/>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



August 18, 2020

FortiSwitch Cookbook

# TABLE OF CONTENTS

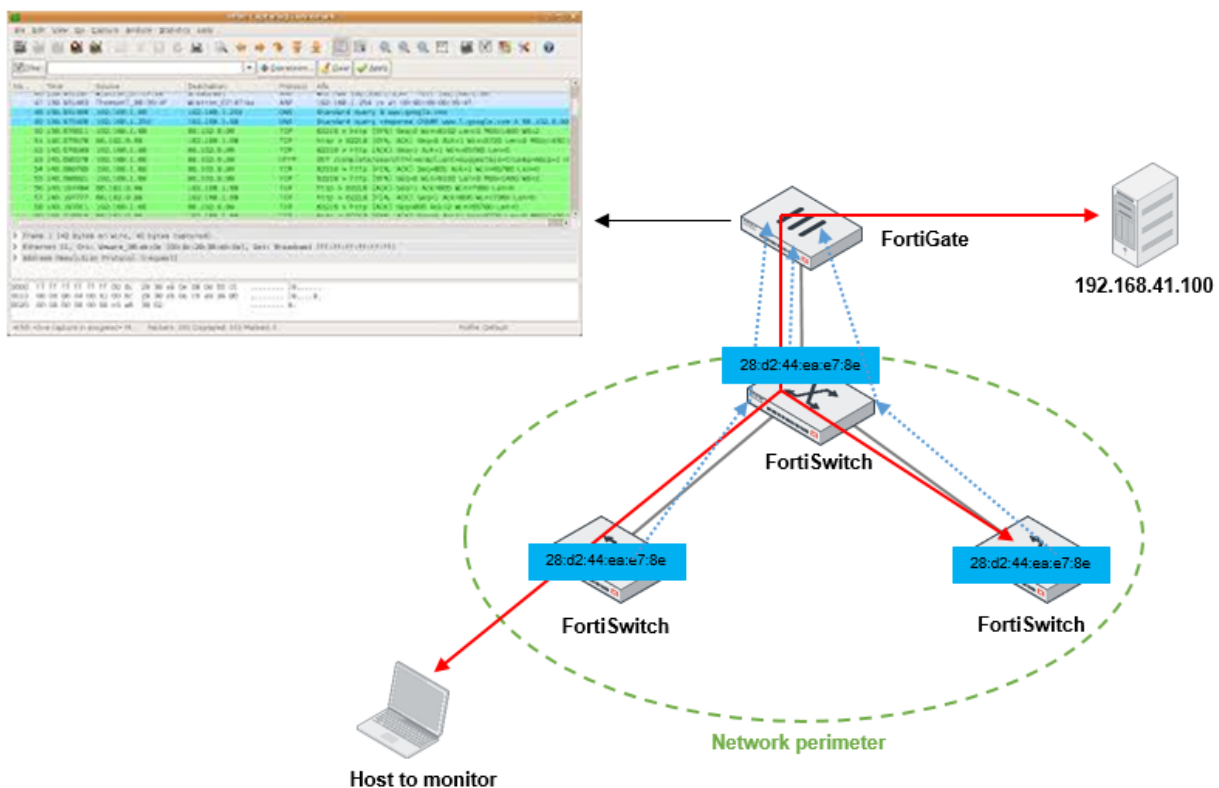
<b>Capturing packets from a sniffer VLAN in a FortiLink setup</b>	<b>4</b>
Remote sampling of a MAC address	4
Remote sampling of a FortiSwitch port	5
<b>Setting up port-based 802.1x authentication in a FortiLink setup</b>	<b>6</b>
Configuring the FortiGate and FortiSwitch units	6
Configuring the RADIUS server	13
Troubleshooting	22
Configuring Windows 10	26
<b>Enterprise FortiSwitch secure access</b>	<b>32</b>
Logging	32
FortiLink configuration	33
MCLAG configuration	37
IDF configuration	40
HA configuration	41
Validation	45
Security Fabric visibility	46
Bonus—FortiSwitch access	47

# Capturing packets from a sniffer VLAN in a FortiLink setup

This cookbook article documents how to capture packets on a VLAN that is being used as the network sniffer (also known as the packet analyzer) and then send the packets to a remote destination.

To capture packets (mirror traffic) on the FortiSwitch fabric, you need to decide what traffic you want to examine. The traffic can be specific switch ports, MAC addresses, or IP addresses. Then you can decide where to send the packet capture (mirrored traffic) to. The destination can be the FortiGate unit, where you can use the local FortiGate packet capture facility, or the destination can be somewhere else in the network (such as across the network through the FortiGate unit or a device directly connected to the FortiSwitch fabric).

## Remote sampling of a MAC address



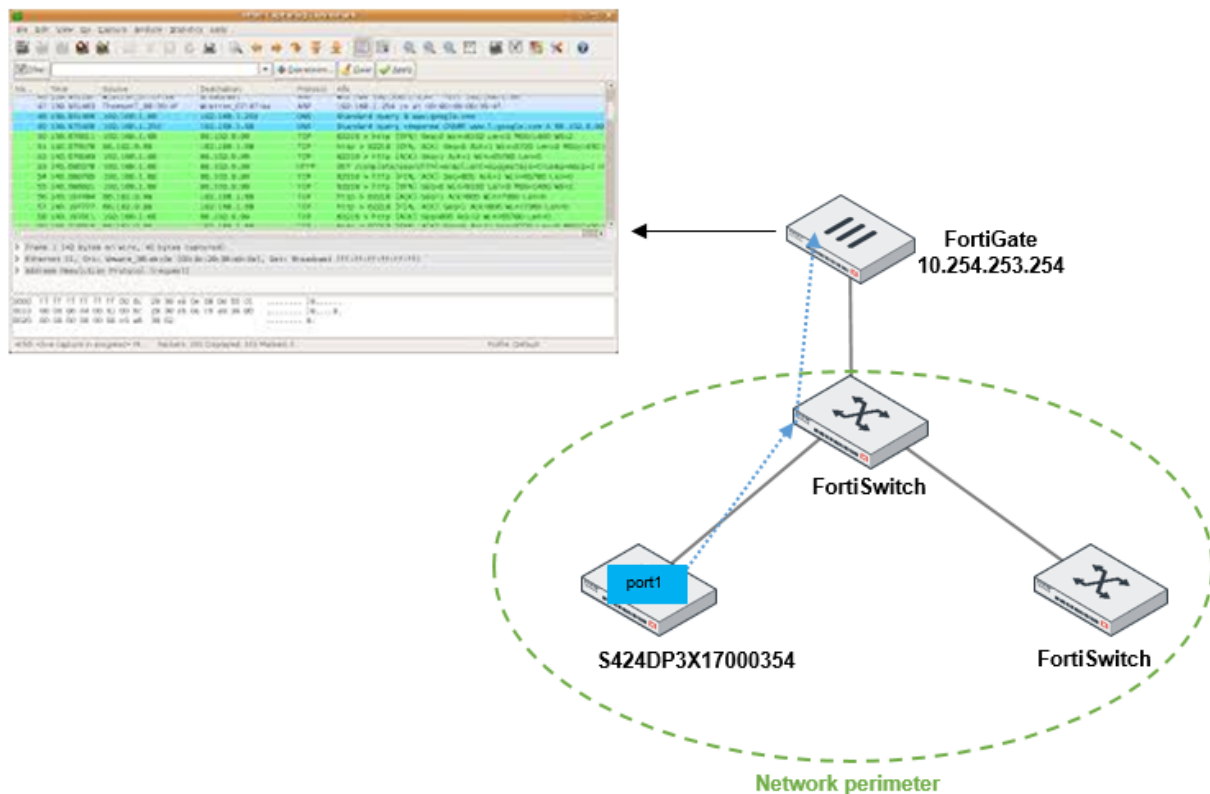
The following is a basic FortiOS configuration for remote sampling:

```
config switch-controller traffic-sniffer
  set erspan-ip 192.168.41.100 // the target IP address for the traffic, which is
    routed through the FortiGate unit
  config target-mac
    edit 28:d2:44:ea:e7:8e // a specific MAC address you want to examine
  next
```

```
end
end
```

In this example, the IP address is a remote end station (such as a desktop PC connected to a network, which is accessed through the FortiGate unit). The traffic is delivered to the FortiGate unit and then routed to the PC where you can use a packet analyzer to examine it. Specific targeted MAC addresses or IP addresses are only sampled when the traffic enters the FortiSwitch fabric (the network perimeter), so you only see one copy of the frame in the sampling.

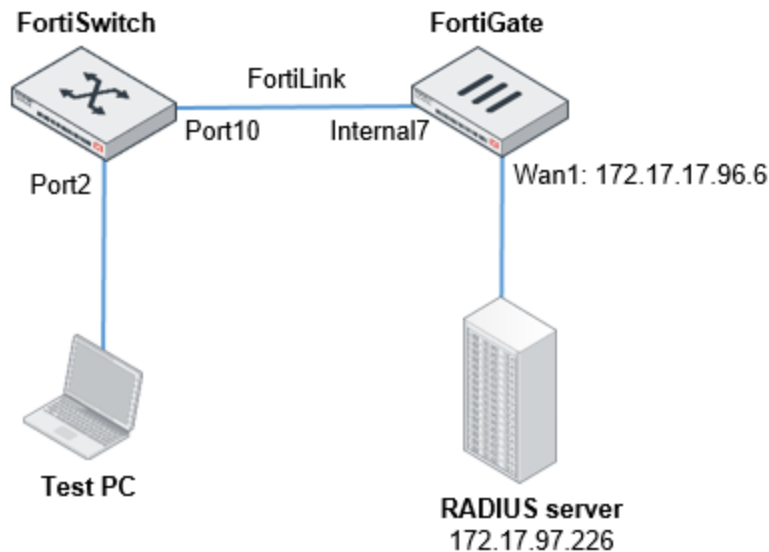
## Remote sampling of a FortiSwitch port



One common use case is to enable sniffing on a FortiSwitch port for quick debugging.

```
FortiGate-100E # config switch-controller traffic-sniffer
set erspan-ip 10.254.253.254 // the traffic is sent only to the FortiGate unit
config target-port
edit "S424DP3X17000354"
set in-ports "port1" // mirror all traffic to/from the switch port to
FortiGate
set out-ports "port1"
next
end
end
```

## Setting up port-based 802.1x authentication in a FortiLink setup



This cookbook article documents how to set up port-based 802.1x authentication. The following tasks are covered:

- [Configuring the FortiGate and FortiSwitch units on page 6](#)
- [Configuring the RADIUS server on page 13](#)
- [Configuring Windows 10 on page 26](#)

802.1x is an IEEE Standard for port-based Network Access Control (PNAC).

The following are the main parts of 802.1x authentication:

- A supplicant—the user or client that wants to be authenticated
- An authentication server—the actual server doing the authentication, typically a RADIUS server. It decides whether to accept the end user's request for full network access.
- An authenticator—a network device that provides a data link between the client and the network and can allow or block network traffic between the two, such as an Ethernet switch or wireless access point

802.1x uses the Extensible Authentication Protocol (EAP) to facilitate communication from the supplicant to the authenticator and from the authenticator to the authentication server.

## Configuring the FortiGate and FortiSwitch units

This section shows how to configure port-based 802.1x authentication with managed FortiSwitch ports when using FortiLink and how to troubleshoot the configuration.

1. Log on to your FortiGate unit.
2. Go to *User & Device > RADIUS Servers* and select *Create New*.
3. Make the following changes:
  - In the Name field, enter a name for your RADIUS server. The name can match the Windows server name to make it easier to identify.
  - Select *Specify* for the authentication method and select *MS-CHAP-v2*.
  - In the NAS IP field, enter the IP address of your RADIUS server.
  - In the Primary Server area, enter the IP address of your RADIUS server again.
  - In the Secret field, enter the secret password that you configured in the RADIUS client settings.

4. Select *Test Connectivity*.  
You should get a green response saying that the connectivity is successful.  
**NOTE:** The Test User Credentials button does not work with MS-CHAP-v2. The button is designed to function only with the insecure Password Authentication Protocol (PAP). With MS-CHAP-v2 configured, you will always receive a failure message if you select this button.
5. To complete a successful user test, run a command from the FortiOS command line:

```
FortiGate# diagnose test authserver radius RADIUSSERVERNAME mschap2
username password
```

The following is the successful output of this command:

```
FWF60D4615010908 (root) # diagnose test authserver radius Radius-Server mschap2 testuser1 !.....
authenticate 'testuser1' against 'mschap2' succeeded, server=primary assigned_rad_session_id=1890019100 session_timeout=0 secs idle_timeout=0 secs!
```

6. Create a user group:
  - a. Go to *User & Device > User Groups* and select *Create New*.
  - b. In the Group field, enter a name for the user group.
  - c. Select *Firewall* as the type.
  - d. Select *OK* to create the user group.

### 7. Create the FortiSwitch/FortiLink VLAN interface.

- Go to *WiFi & Switch Controller* > *FortiSwitch VLANs* and select *Create New*.  
The following figure shows the configured FortiSwitch/FortiLink VLAN interface.

Name	VLAN ID	IP/Netmask	Access	Ref.
LAGuestVlan	31	172.16.31.254/255.255.255.0	Ping	1
LAGuestVlan	33	172.16.33.254/255.255.255.0	Ping	1
LAGuestVlan	34	172.16.34.254/255.255.255.0	Ping	5
LALanSecure	32	172.16.32.254/255.255.255.0	Ping HTTPS SSH Port HTTP Wireless Controller	3
vswinteract	1	0.0.0.0/0.0.0.0		8

- Check the configuration in the FortiOS CLI:

```
FWF60D4615010908 # show system interface LAGuest
config system interface
edit "LAGuest"
set vdom "root"
set ip 172.16.34.254 255.255.255.0
set allowaccess ping
set device-identification enable
set device-identification-active-scan enable
set role lan
set snmp-index 12
set switch-controller-dhcp-snooping enable
set interface "internal17"
set vlanid 34
next
end

FWF60D4615010908 # show system interface LALanSecure
config system interface
edit "LALanSecure"
set vdom "root"
set ip 172.16.32.254 255.255.255.0
set allowaccess ping https ssh http capwap
```



```
    set alias "--HQ Secure LAN"
    set device-identification enable
    set device-identification-active-scan enable
    set fortiheartbeat enable
    set role lan
    set snmp-index 14
    set switch-controller-dhcp-snooping enable
    set interface "internal7"
    set vlanid 32
  next
end
```

### 8. Configure the 802.1x settings in the FortiOS CLI:

```
config switch-controller 802-1X-settings
  set link-down-auth set-unauth
  set reauth-period 60
  set max-reauth-attempt 2
end
```

### 9. Configure the 802.1x security policy in the FortiOS CLI:

```
config switch-controller security-policy 802-1X
  edit "LASecure_802-1X-policy"
    set user-group "Radius-Group"
    set mac-auth-bypass disable
    set open-auth disable
    set eap-passthru enable
    set guest-vlan enable
    set guest-vlan-id "LAGuest" // same as auth-fail-vlan
    set guest-auth-delay 60
    set auth-fail-vlan enable // use a specific VLAN upon authentication failure
    set auth-fail-vlan-id "LAGuest"
    set radius-timeout-overwrite enable
  next
end
```

If you want to reduce the time delay in recovering from auth-fail-vlan when an 802.1X failure happens, reduce the max-reauth-attempt and guest-auth-delay settings.

### 10. Apply the port security policy to the FortiSwitch port in the FortiOS CLI:

```
config switch-controller managed-switch
  edit "FS108D3W15000509"
    set fsw-wan1-peer "internal7"
    set fsw-wan1-admin enable
    set version 1
    set dynamic-capability 71836
    config ports
      edit "port2"
        set poe-capable 1
        set vlan "LALanSecure"
        set allowed-vlans "LAGuest"
        set port-security-policy "LASecure_802-1X-policy" // use "port-based"
          authentication
        set export-to "root"
      next
    next
end
```

```

end
next
end

```

11. Configure the firewall policy for the FortiSwitch connection to the RADIUS server, as shown in the following figure:

The screenshot shows the 'Edit Policy' configuration page in the FortiLink web interface. The left sidebar contains a navigation menu with the following items: root, Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects (selected), IPv4 Policy (selected), Proxy Policy, Authentication Rules, Addresses, Wildcard FQDN Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Proxy Options, Traffic Shapers, Traffic Shaping Policy, Security Profiles, VPN, User & Device, WiFi & Switch Controller, Log & Report, and Monitor. The main content area is titled 'Edit Policy' and contains the following configuration fields:

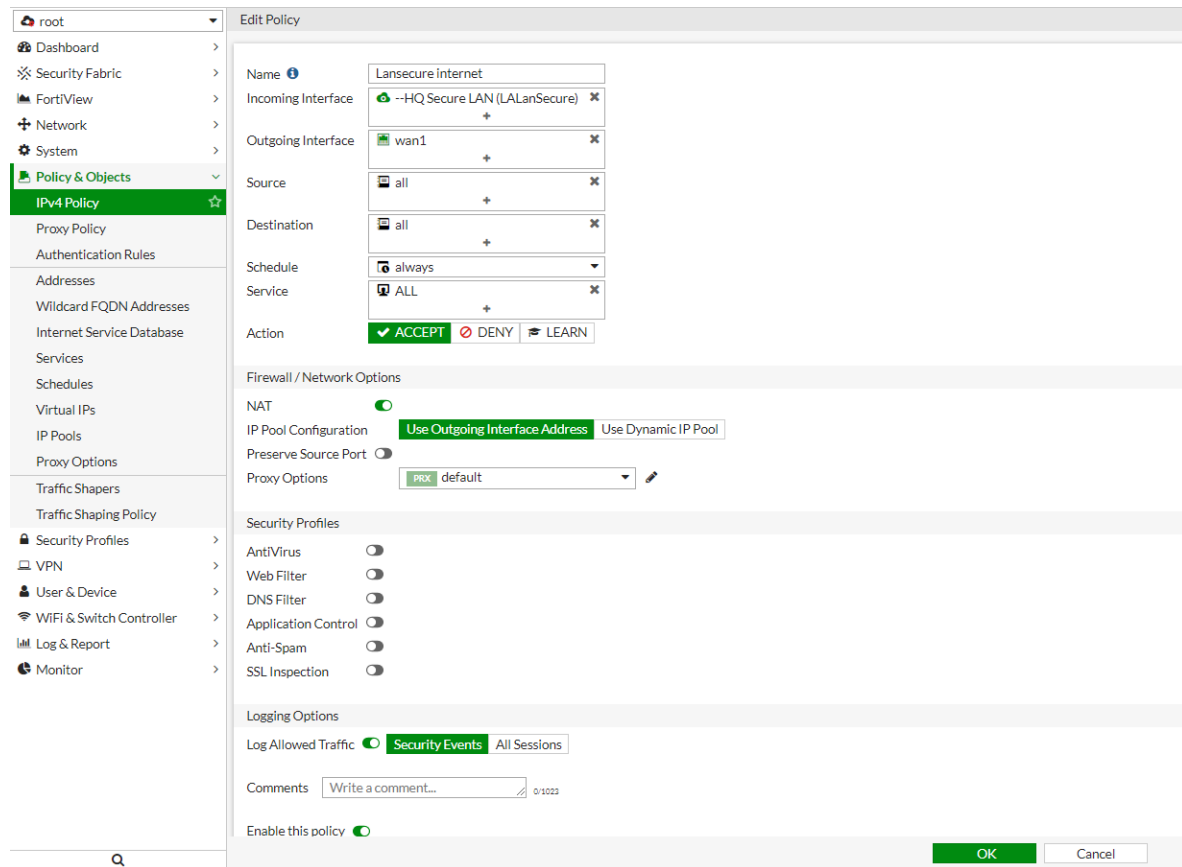
- Name:** 8021x
- Incoming Interface:** any
- Outgoing Interface:** wan1
- Source:** 169.254.1.0/24
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY, LEARN

Below the main configuration fields, there are several sections with expandable options:

- Firewall / Network Options:**
  - NAT:** (checked)
  - IP Pool Configuration:** Use Outgoing Interface Address (checked), Use Dynamic IP Pool
  - Preserve Source Port:** (unchecked)
  - Proxy Options:** PROX default
- Security Profiles:**
  - AntiVirus: (unchecked)
  - Web Filter: (unchecked)
  - DNS Filter: (unchecked)
  - Application Control: (unchecked)
  - Anti-Spam: (unchecked)
  - SSL Inspection: (unchecked)
- Logging Options:**
  - Log Allowed Traffic:** (checked) Security Events (checked), All Sessions
- Comments:** Write a comment... (0/1023)
- Enable this policy:** (checked)

At the bottom right of the page, there are 'OK' and 'Cancel' buttons.

**12. Configure the firewall policy for the VLAN interface to the Internet, as shown in the following figure:**



**To troubleshoot your configuration:**

1. In the FortiOS CLI, verify that the connection from the FortiGate unit to the FortiSwitch unit is up:

```
exec switch-controller get-conn-status
```

2. In the FortiSwitchOS CLI, you can check if the authentication. The following output shows a successful authentication:

```
FS108D3W15000509 # diagnose switch 802-1x status port2
port2 : Mode: port-based (mac-by-pass disable)
Link: Link up
Port State: authorized ( )
Dynamic Authorized Vlan : 0
EAP pass-through mode : Enable
Native Vlan : 32
Allowed Vlan list: 32
Untagged Vlan list:
Guest Vlan : 34 Guest Auth Delay :120
Auth-Fail Vlan : 34
Sessions info:
54:e1:ad:4a:2d:6b Type=802.1x, PEAP, state=AUTHENTICATED, etime=0, eap_cnt=10
params:reAuth=600
```

The following output shows a failed authentication:

```
FS108D3W15000509 # diagnose switch 802-1x status port2
port2 : Mode: port-based (mac-by-pass disable)
  Link: Link up
  Port State: unauthorized ( )
  Dynamic Authorized Vlan : 0
  EAP pass-through mode : Enable
  Native Vlan : 32
  Allowed Vlan list: 32
  Untagged Vlan list:
  Guest Vlan : 34 Guest Auth Delay :120
  Auth-Fail Vlan : 34
  Sessions info:
  54:e1:ad:4a:2d:6b Type=802.1x, IDENTITY, state=HELD, etime=0, eap_cnt=5
    params:reAuth=600
```

```
FS108D3W15000509 # diagnose switch vlan list 32
```

```
VlanId Ports
```

```
32 port2 port10
```

After a wrong password being entered, port2 is removed from VLAN 32 (LALanSecure) and is replaced by VLAN 34(LAGuest).

```
FS108D3W15000509 # diagnose switch vlan list 32
VlanId Ports
```

```
32 port10
```

```
FS108D3W15000509 # diagnose switch vlan list 34
VlanId Ports
```

```
34 port1 port2 port10
```

After a successful authentication, port2 is moved to VLAN 32 (LALanSecure) and removed from VLAN 34 (LAGuest).

```
FS108D3W15000509 # diagnose switch vlan list 32
VlanId Ports
```

```
32 port2 port10
```

```
FS108D3W15000509 # diagnose switch vlan list 34
VlanId Ports
```

```
34 port1 port10
```

**NOTE:** When you replace an existing RADIUS server with a new one, the configuration is not updated in the FortiSwitch unit. Use the following procedure to update the RADIUS server configuration in the FortiSwitch unit:

1. Use the FortiGate unit to access the FortiSwitch using SSH.
2. Remove the configuration associated with the existing RADIUS server. Use the following commands to find the existing RADIUS server configuration:

```
show user group
show user radius
```

3. To synchronize the configuration with the FortiSwitch unit:

```
exe switch-controller trigger-config-sync
```

4. Verify that the FortiGate unit and the FortiSwitch unit are synchronized:

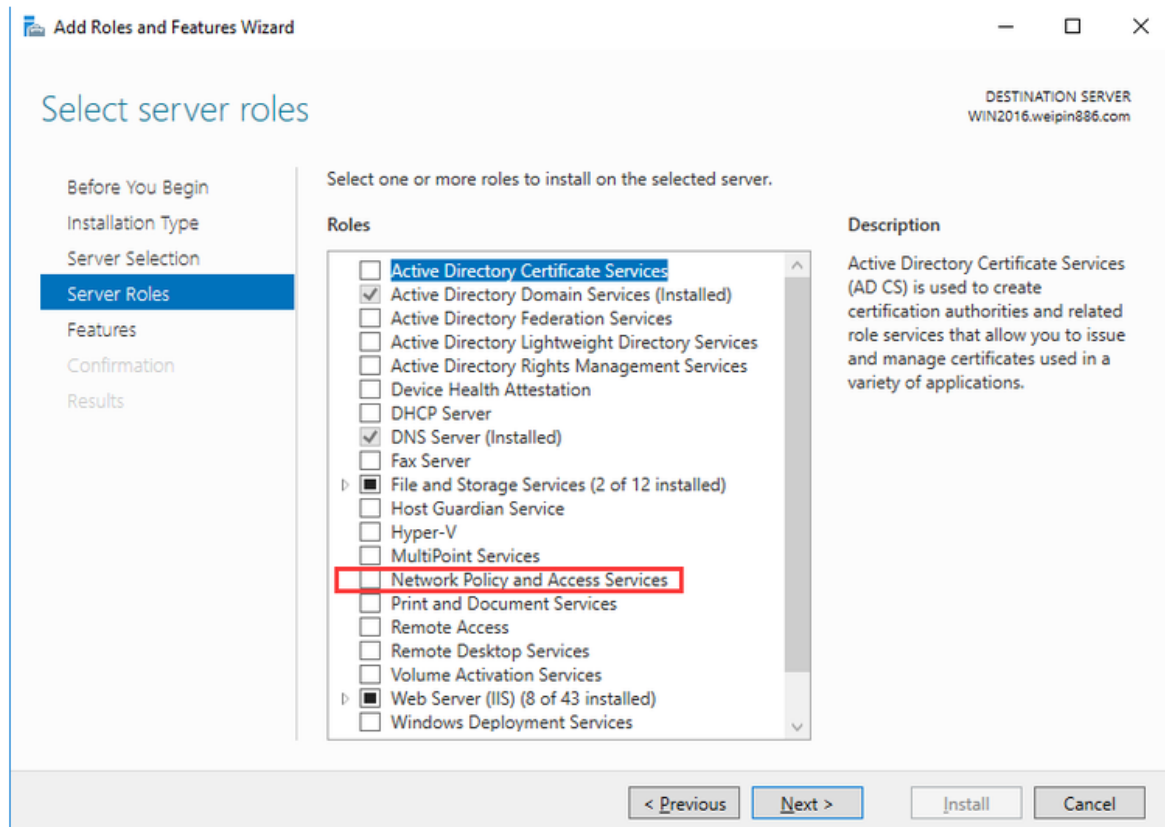
```
exe switch-controller get-sync-status all
```

## Configuring the RADIUS server

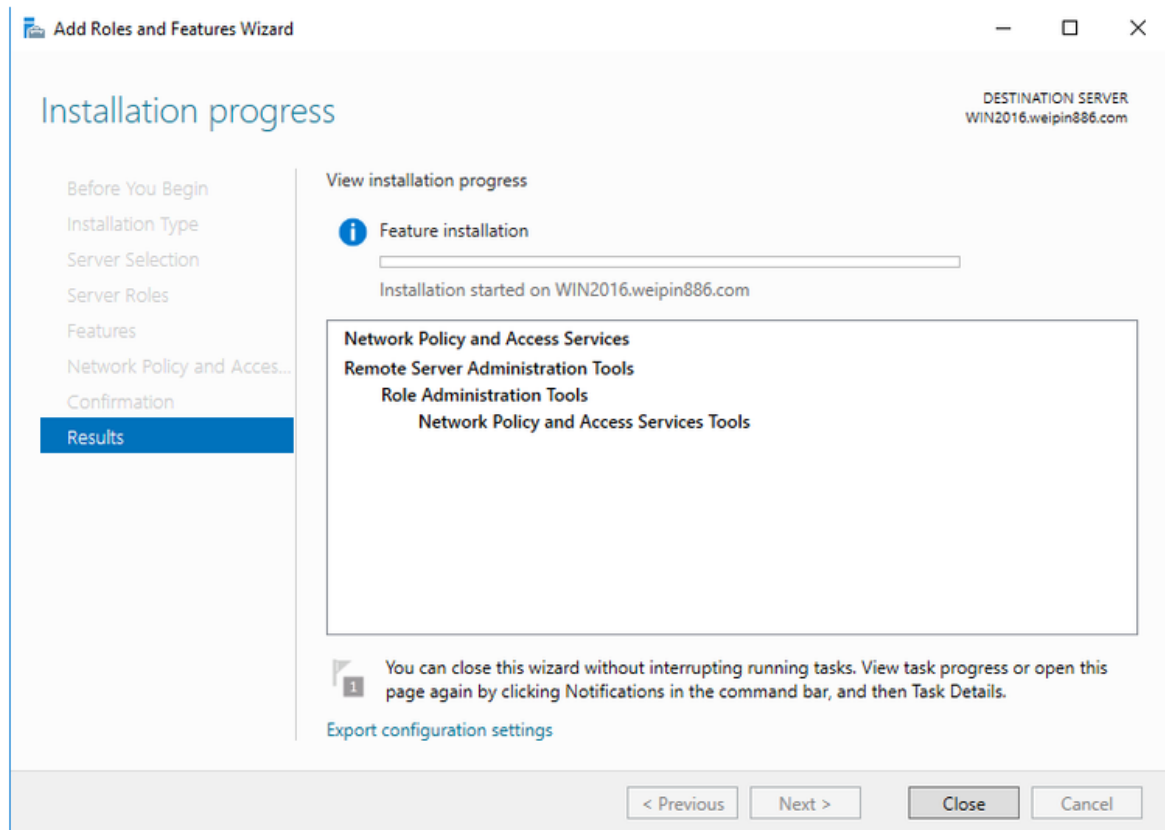
This section shows how to configure the RADIUS server to accept port-based 802.1x authentication. This example shows how to install and configure RADIUS in Windows Server 2016.

1. Log in to the Windows Server 2016 that you plan to use as your RADIUS server.
2. Launch the Server Manager and select *Manage* from the top right.
3. Select *Add Roles and Features* to launch the wizard.

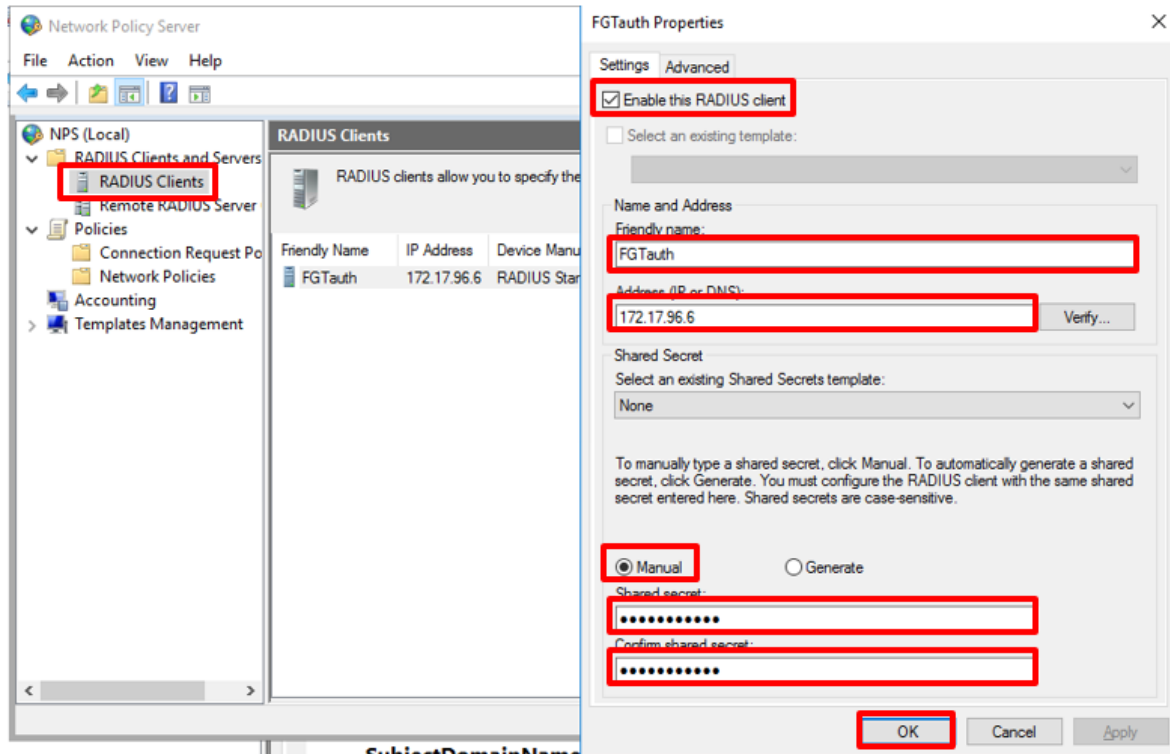
4. From the wizard page, select *Network Policy and Access Services*, as shown in the following figure:



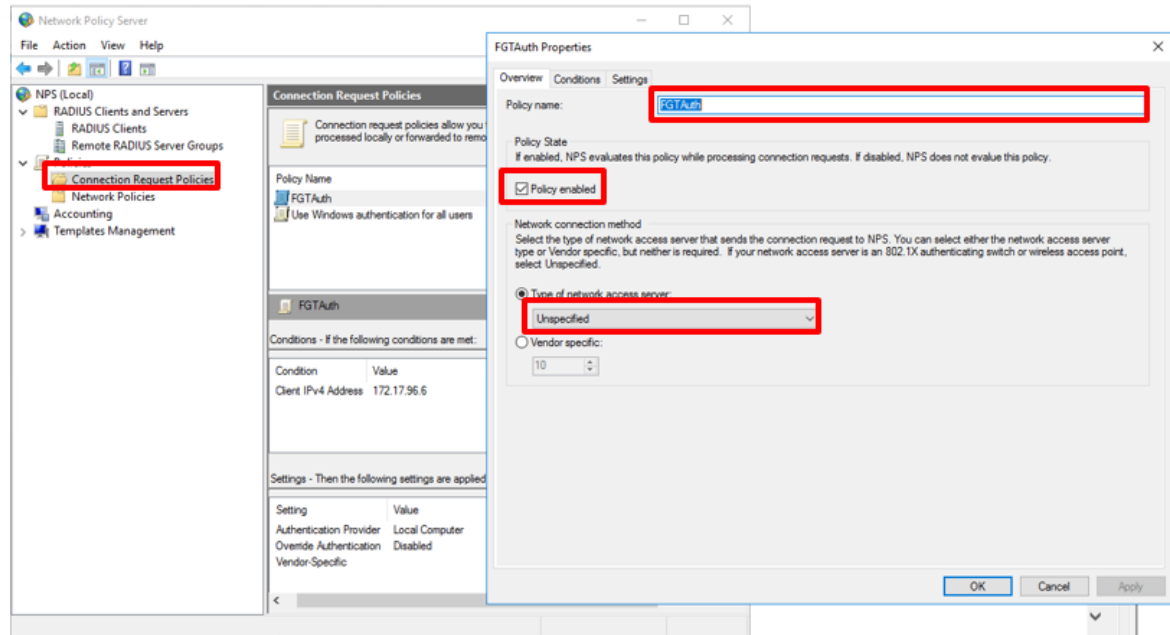
5. Select *Next* and then select *Finish* to start the installation. No reboot is required.



6. After the installation is complete, select *Tools* from the Server Manager and then select *Network Policy Server*.
7. Right-click on *RADIUS Clients* and select *New* to display the new RADIUS client dialog box. Use the following procedure to configure the RADIUS clients:
  - a. Select the *Enable the RADIUS client* checkbox.
  - b. Enter a name for your RADIUS server, such as `FGTAuth`.
  - c. Enter the IP address of the FortiGate unit that is used to access the RADIUS server. Typically, this is the interface in the FortiGate unit with the same network as the RADIUS server. Otherwise, this will be the IP address you have configured as the source-ip in the user RADIUS settings in FortiOS.
  - d. In the Shared Secret area, keep *Manual* selected and enter a password in the Shared secret field.  
**NOTE:** This password must match the FortiGate RADIUS server settings.
  - e. Select *OK*.

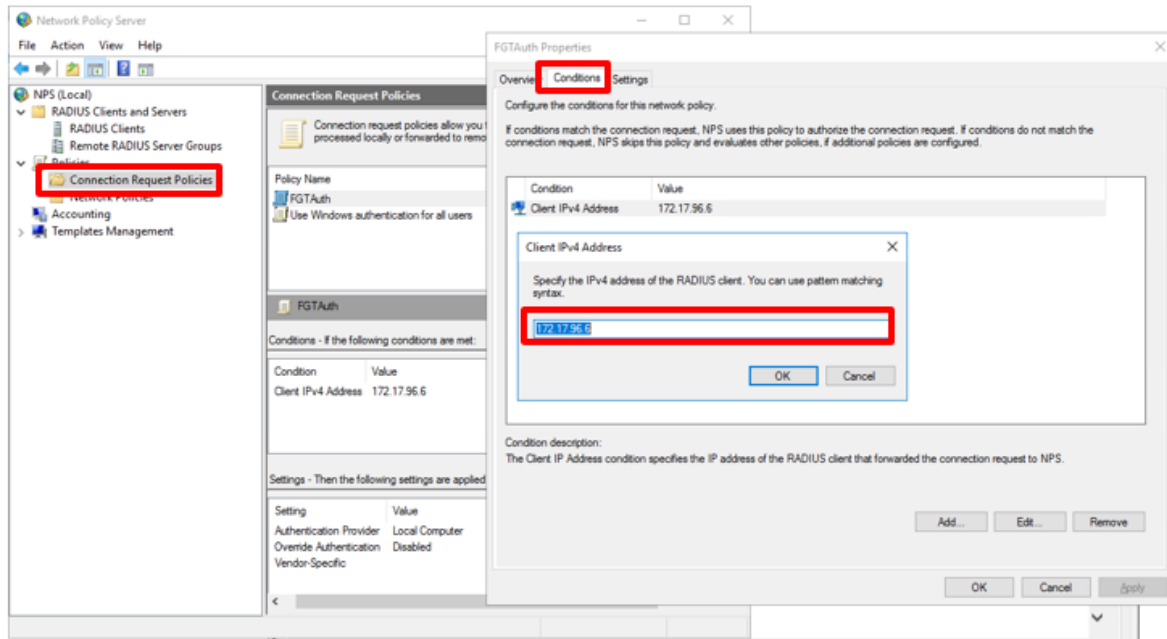


8. Under the Policies section of the NPS Snap-in, right-click *Connection Request Policies* and select *New*.
  - In the Overview tab, enter a name for the policy, such as *FGTAUTH*.
  - Select the *Policy enabled* check box.
  - Leave the type of network access server as *Unspecified*.

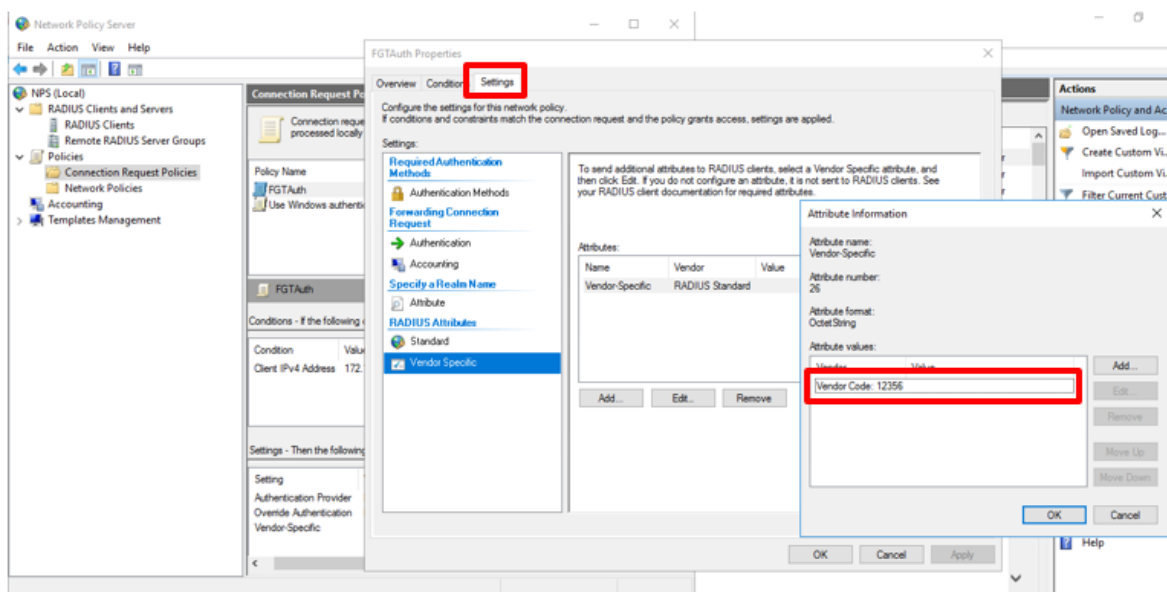




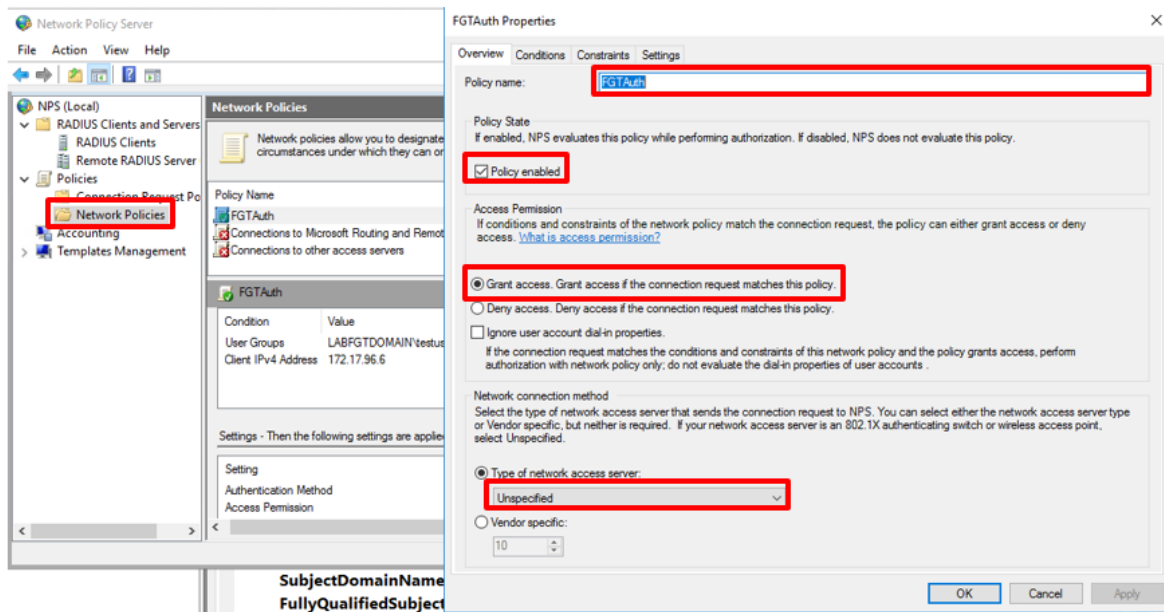
9. Select the *Conditions* tab.
  - a. Select *Add* and then select the *Client IPv4 Address* condition.
  - b. Select *Add* again and enter the IP address of the RADIUS client, which is the IP address of the FortiSwitch unit.
  - c. Enable the NAT to the firewall policy from the FortiLink interface to the interface in which the RADIUS server is routed. In this example, it is the wan1 interface with an IP address of 172.17.96.6.



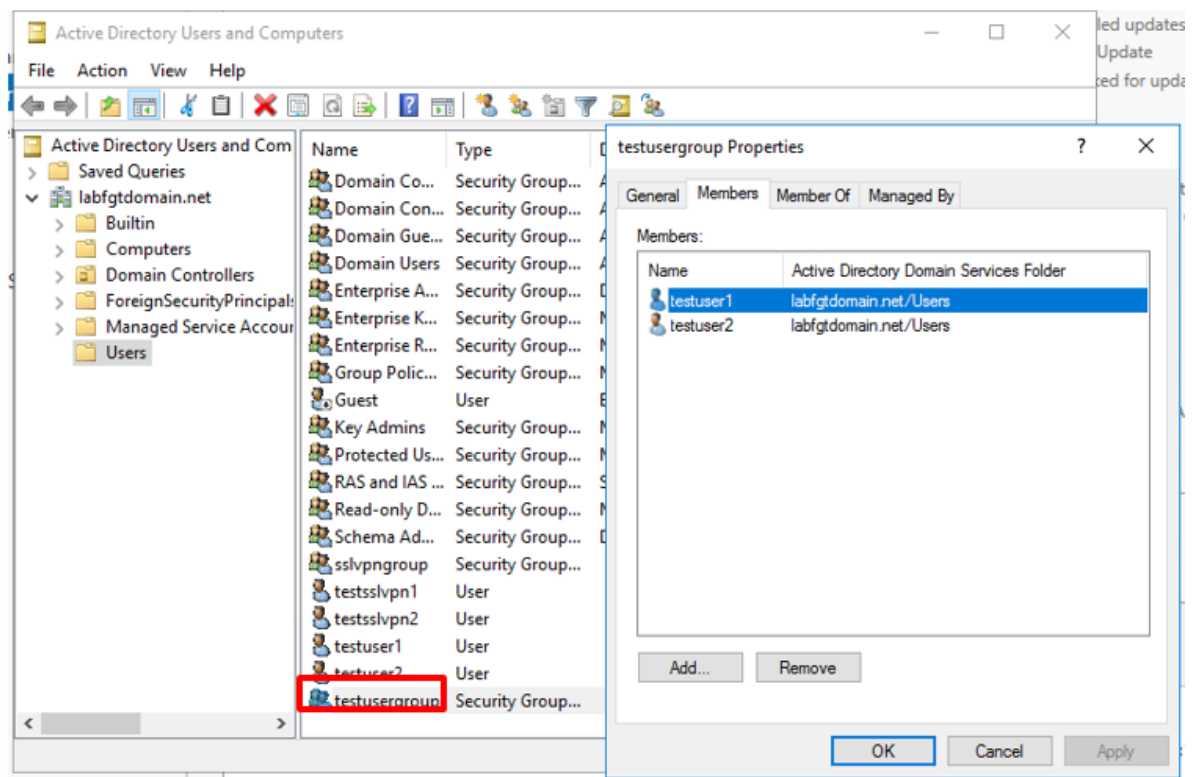
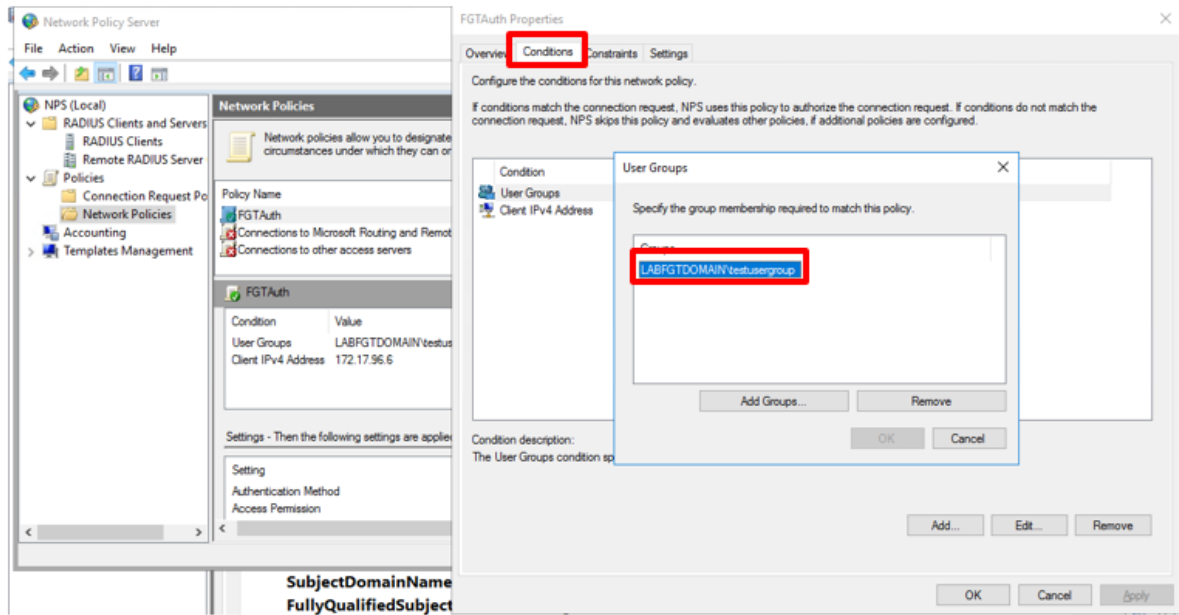
10. Select the *Settings* tab.
  - a. Select *Vendor Specific* and then select *Add*.
  - b. Scroll to the very bottom of the list and select *Vendor-Specific*.
  - c. Select *Add*.



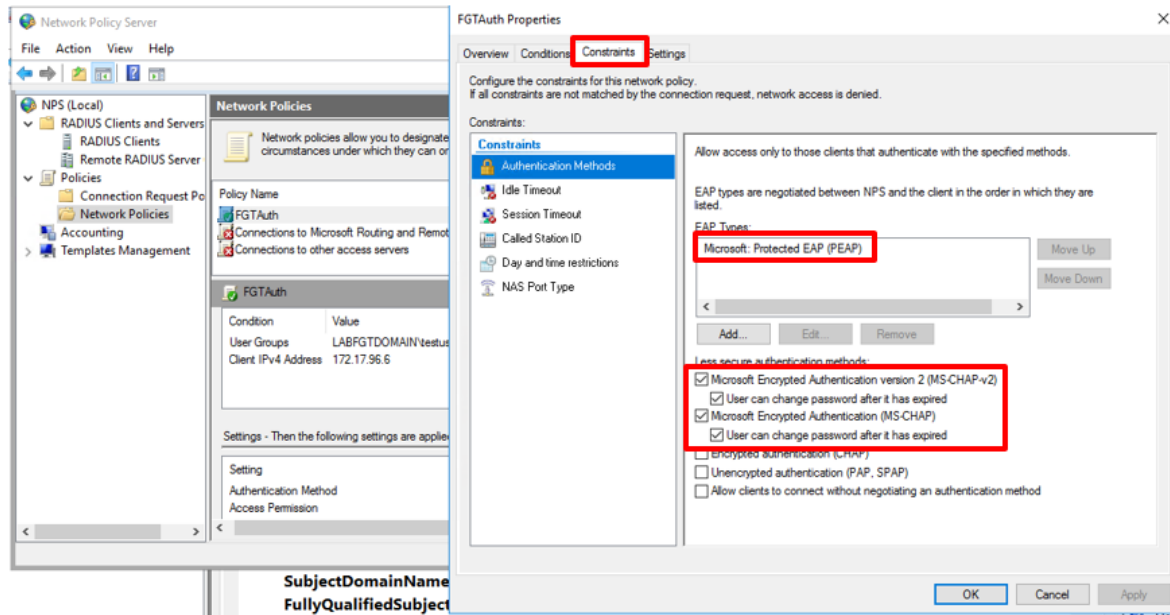
11. Configure a network policy.
  - a. From the Network Policy Server Snap-in, right-click on *Network Policies* and select *New*.
  - b. Enter a name for the policy, such as `FGTAuth`.
  - c. On the Overview tab, make sure that *Policy enabled* checkbox is selected.
  - d. Verify that *Grant access* is selected.
  - e. Verify that the type of network access server is set to *Unspecified*.



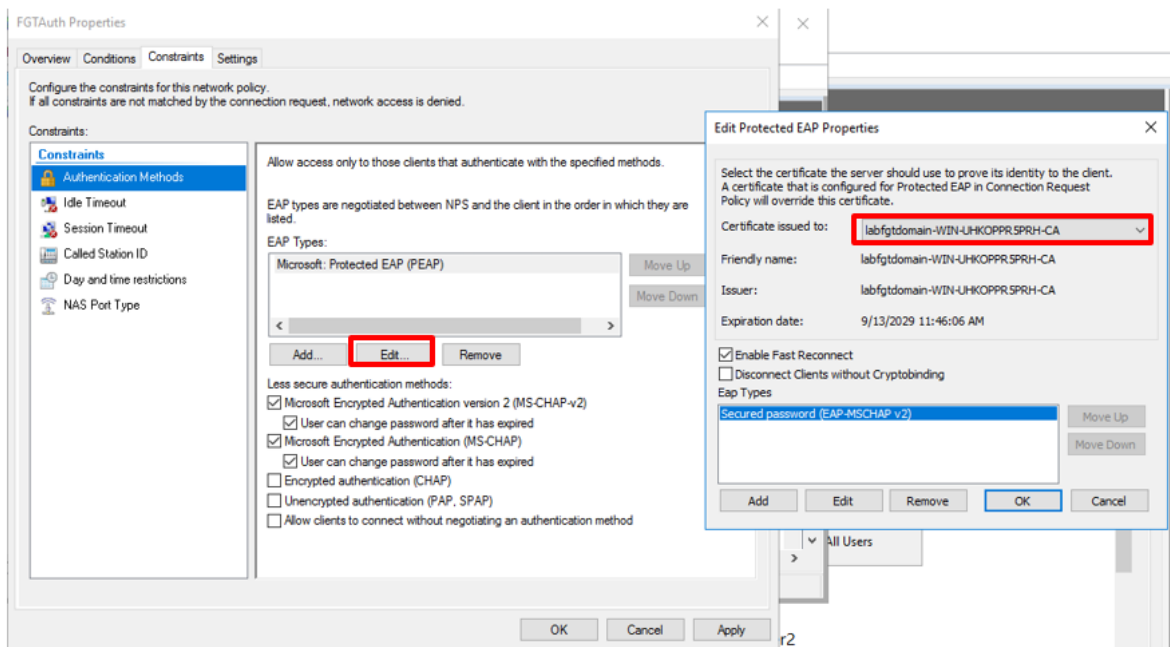
12. Select the Conditions tab.
  - a. Select *Add*.
  - b. Select *Windows Groups* and then select *Add*.
  - c. Select *Add Groups*.
  - d. Enter the name of the group in AD that you want to allow for 802.1x connections.
  - e. Select *OK*.



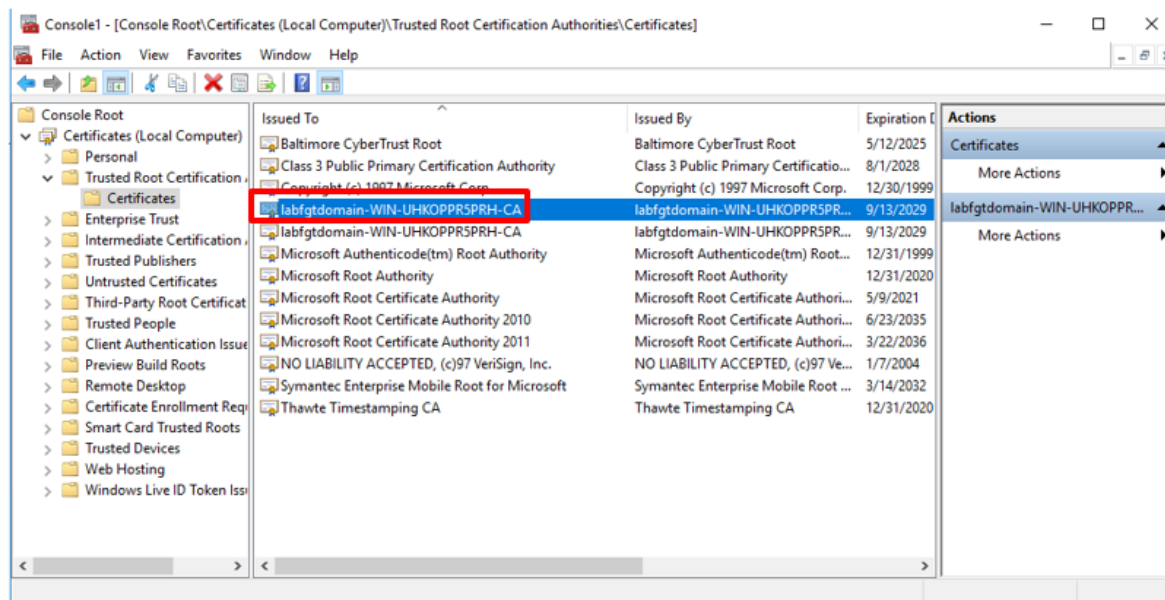
13. In the Constraints tab, verify that the following check boxes are selected, select *Apply*, and then select *OK* to complete the policy.



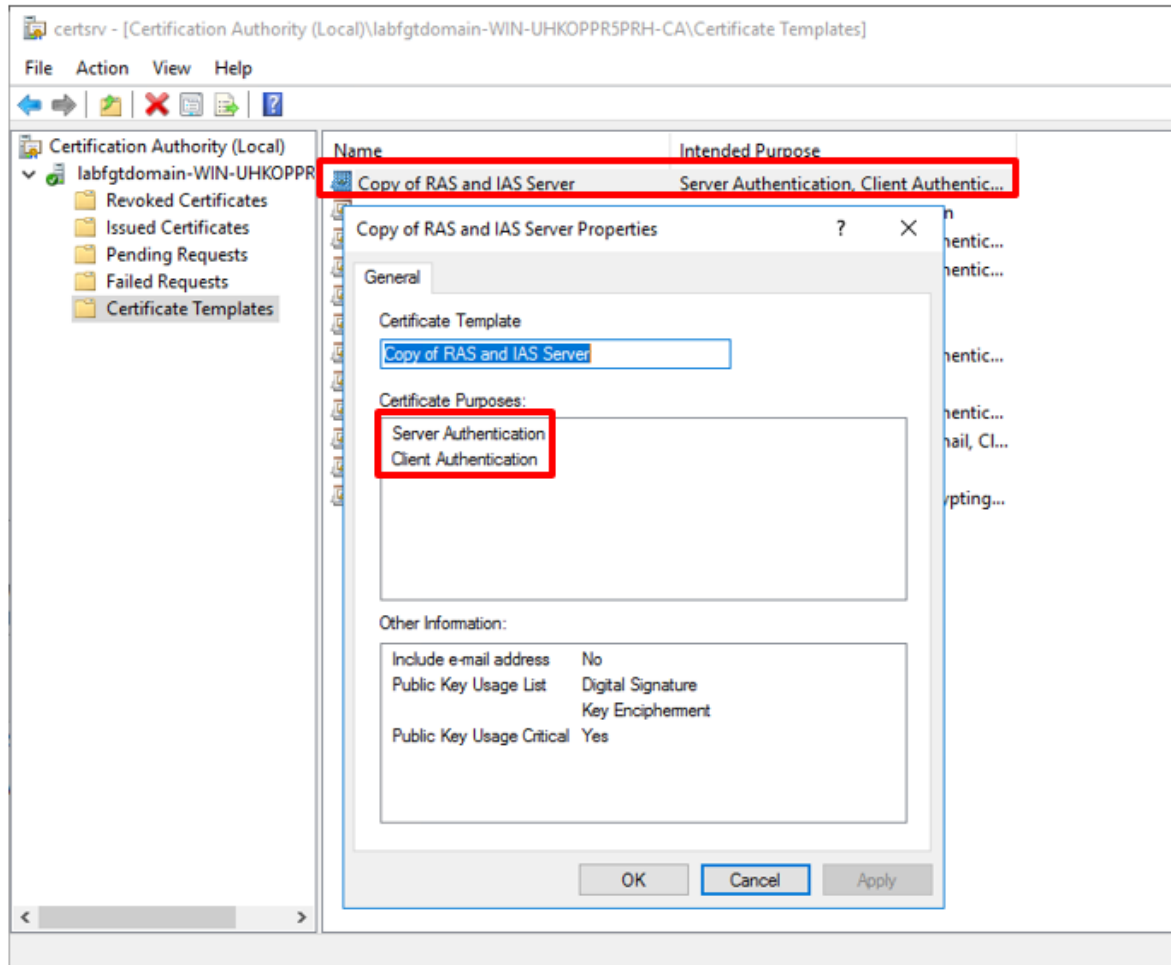
14. To verify the server certificate used by Microsoft Protocol EAP (PEAP), select *Edit*, and then select the certificate for the server to prove its identity to the client.



15. Download the certificate that you selected and save it in the Trusted Root Certificate Authorities directory of the local PC.



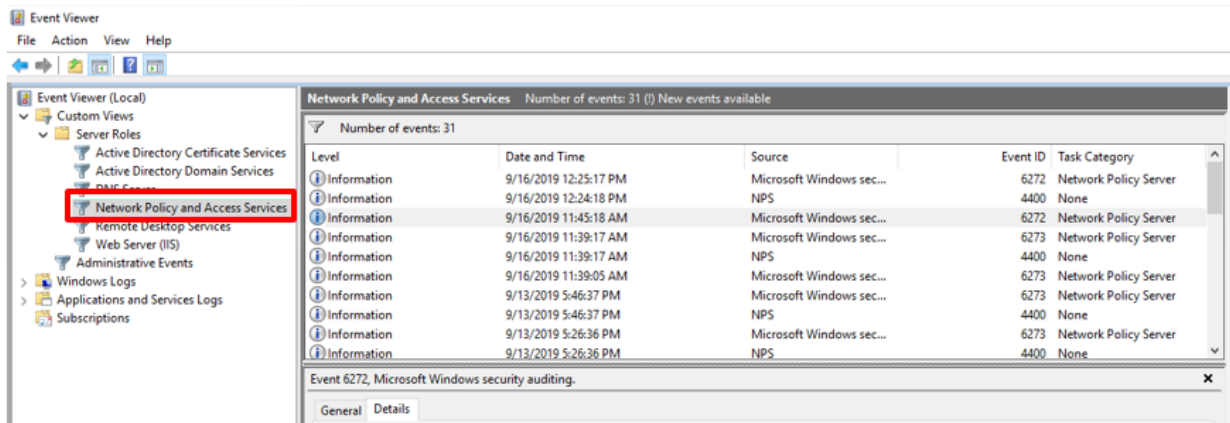
- Under Certification Authority (Local), make certain that the settings match those in the following figure. Otherwise, you will receive an authentication failure with the following reason: "The client could not be authenticated because the Extensible Authentication Protocol (EAP) Type cannot be processed by the server."



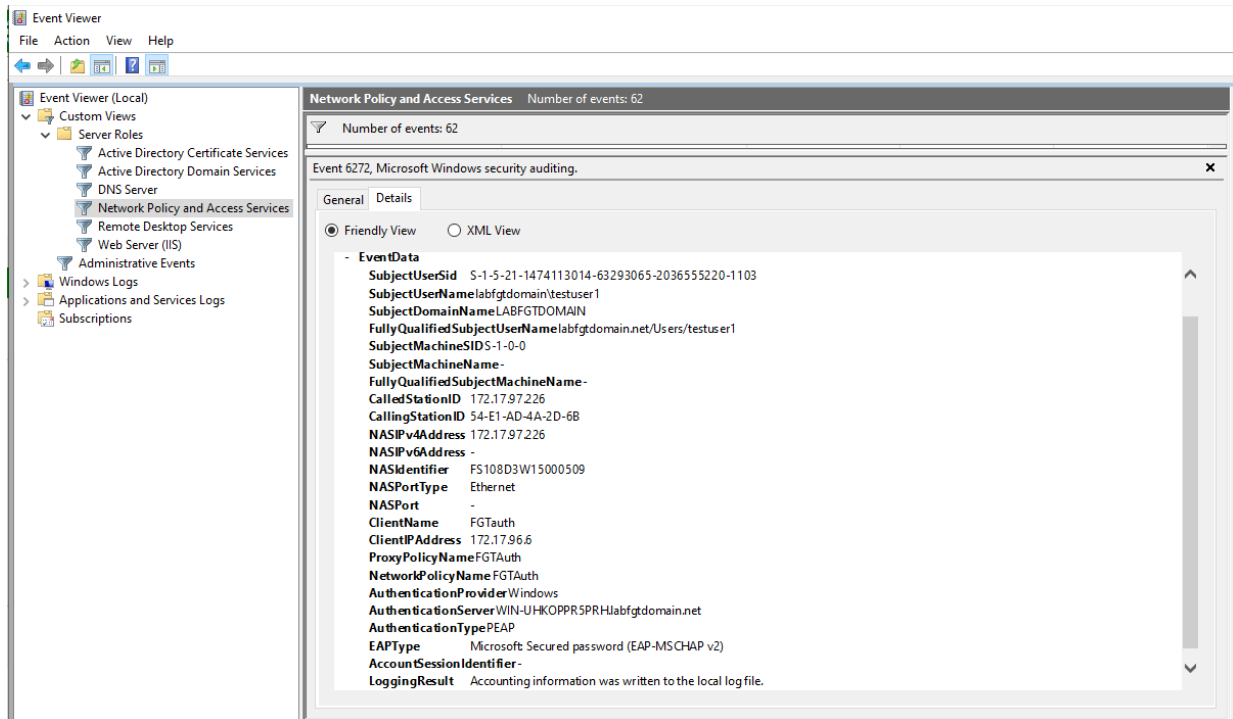
## Troubleshooting

The best way to troubleshoot 802.1x connections is by looking at the Event Viewer of the Windows Server. Under Server Roles, check the output of the Network Policy and Access Services.

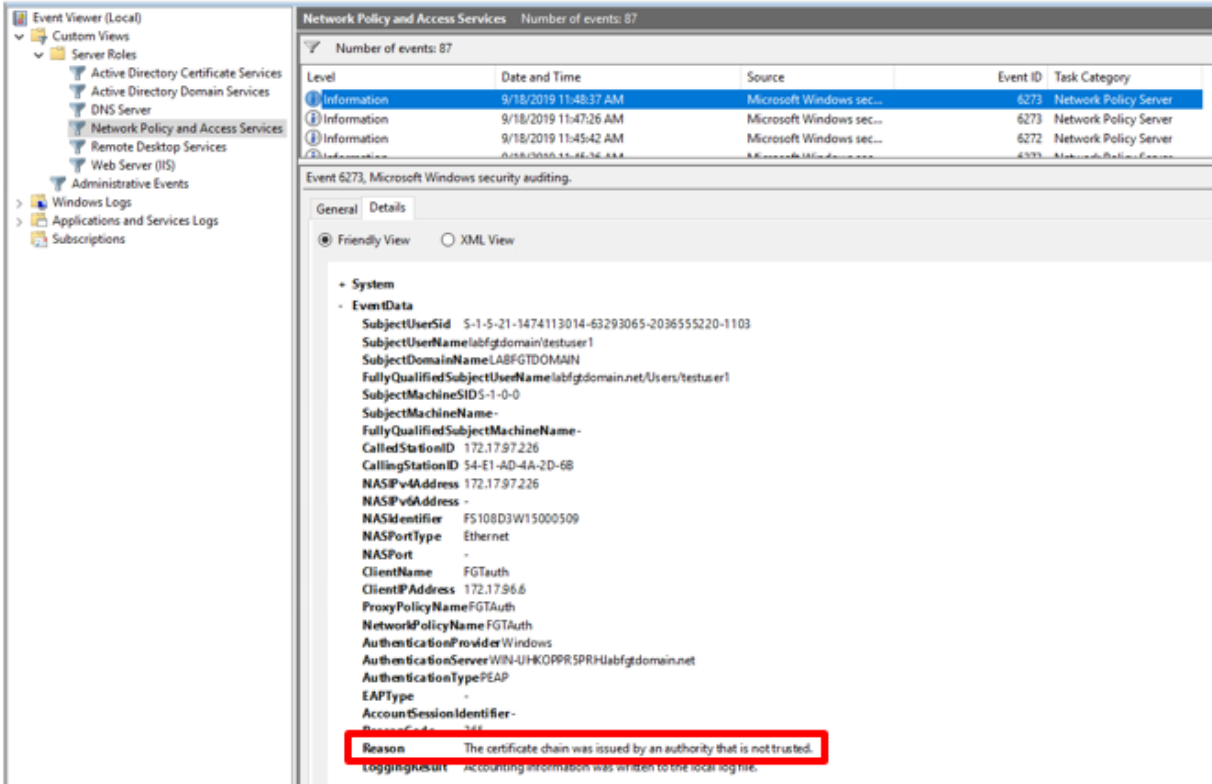
The following figure shows the successful output of an 802.1x connection from the PC:



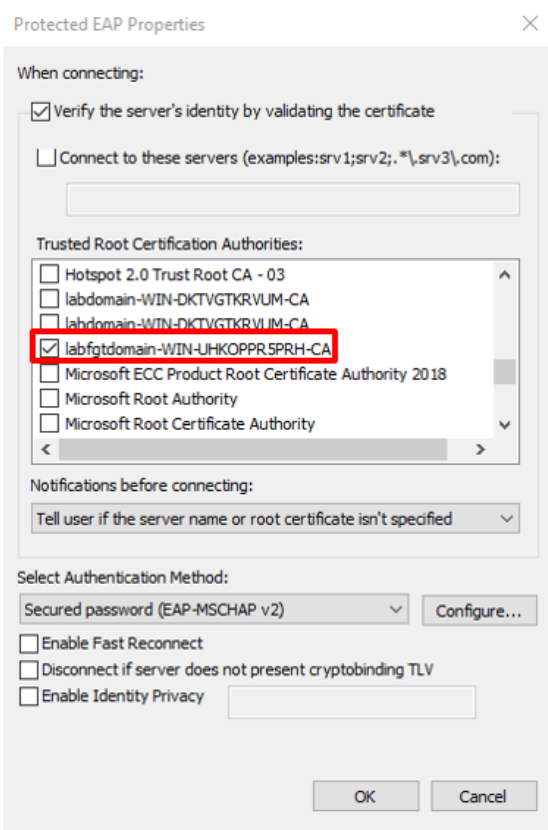
## Setting up port-based 802.1x authentication in a FortiLink setup



### Issue 1: The certificate chain was issued by an authority that is not trusted.



To fix this issue, import the CA certificate into the local machine and add it to the Trusted Root Certification Authorities.





## Issue 2: The specified user does not exist.

The screenshot displays the Windows Event Viewer interface. On the left, the 'Event Viewer (Local)' tree is expanded to 'Network Policy and Access Services'. The main pane shows a list of events, with Event 6273 selected. The 'Details' tab for this event is active, showing a 'Friendly View' of the event data. The 'Reason' field is highlighted with a red box, indicating the error message: 'The specified user account does not exist.' Below this, the 'LoggingResult' field shows 'Accounting information was written to the local log file.'

Level	Date and Time	Source	Event ID	Task Category
Information	9/18/2019 11:48:37 AM	Microsoft Windows sec...	6273	Network Policy Server
Information	9/18/2019 11:47:26 AM	Microsoft Windows sec...	6273	Network Policy Server
Information	9/18/2019 11:45:42 AM	Microsoft Windows sec...	6272	Network Policy Server

Event 6273, Microsoft Windows security auditing.

General Details

☒ Friendly View ☐ XML View

System

EventData

SubjectUserSid S-1-0-0

SubjectUserName Rajat Goyal

SubjectDomainName LABFGTDOMAIN

FullyQualifiedSubjectUserName LABFGTDOMAIN\Rajat Goyal

SubjectMachineSid S-1-0-0

SubjectMachineName -

FullyQualifiedSubjectMachineName -

CallingStationID 172.17.97.226

CallingStationID 54-E1-AD-4A-2D-68

NASIPv4Address 172.17.97.226

NASIPv6Address -

NASIdentifier FS108D3W15000509

NASPortType Ethernet

NASPort -

ClientName FGTAUTH

ClientIP Address 172.17.96.6

ProxyPolicyName FGTAUTH

NetworkPolicyName -

AuthenticationProvider Windows

AuthenticationServer WIN-UHKOOPRSPRHlabfgtdomain.net

AuthenticationType EAP

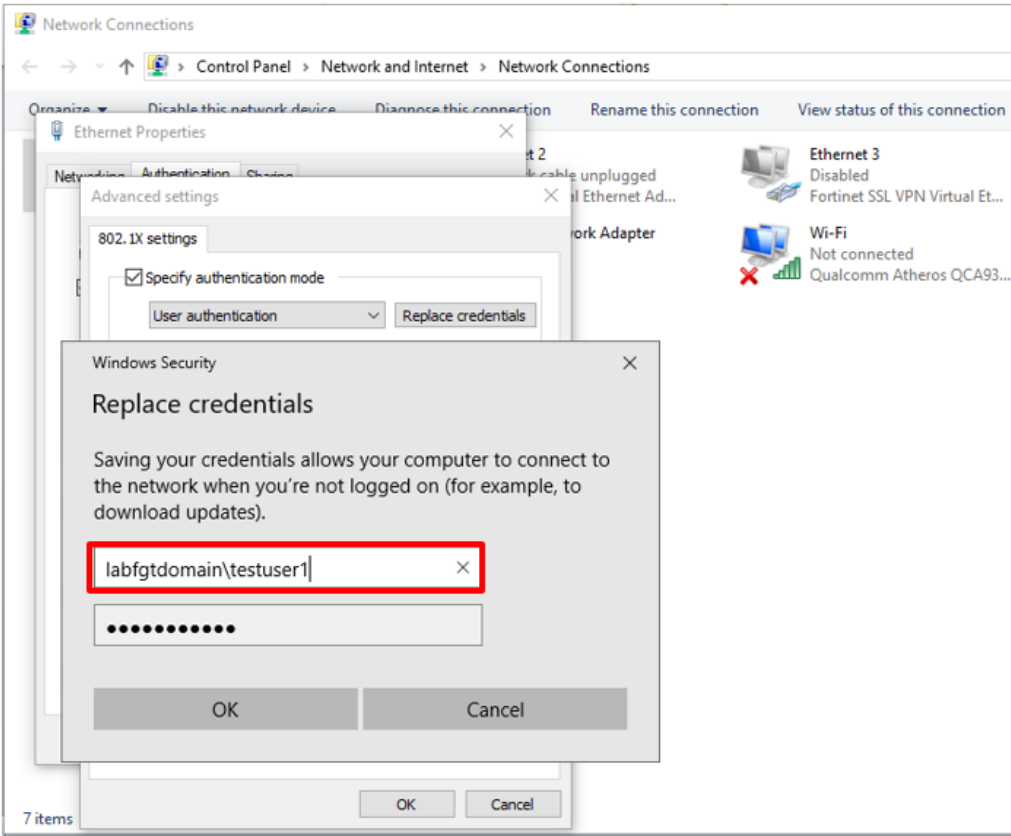
EAPType -

AccountSessionIdentifier -

Reason The specified user account does not exist.

LoggingResult Accounting information was written to the local log file.

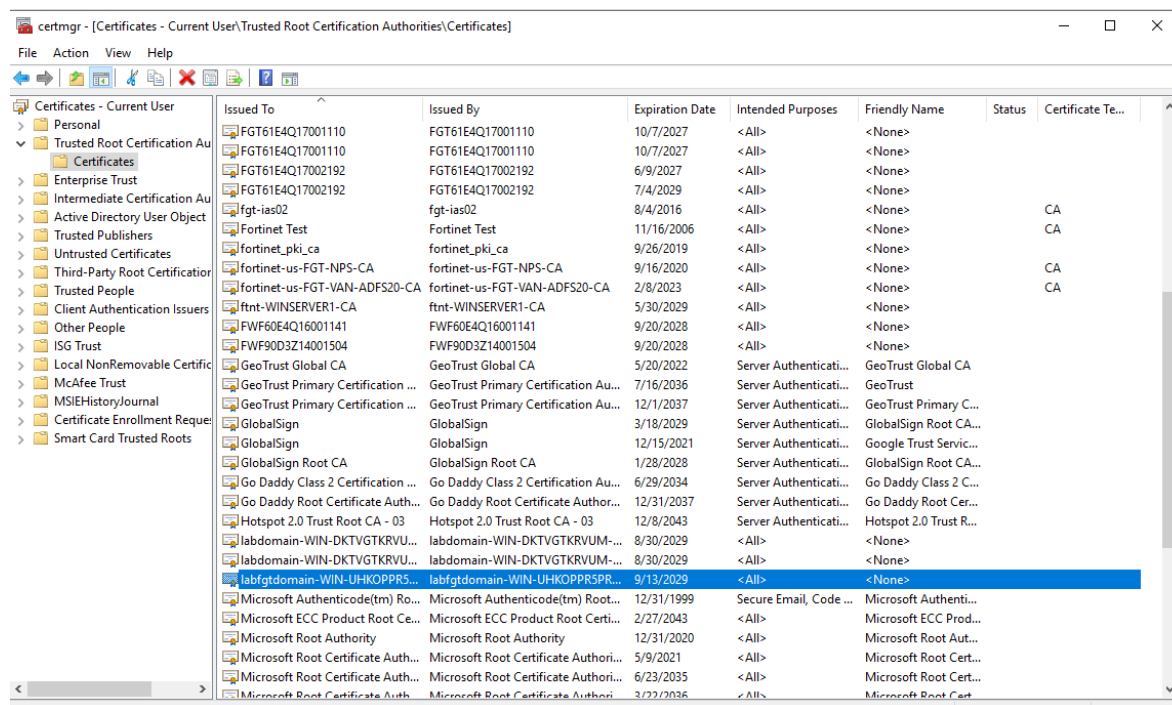
To fix this issue, under *Advanced settings*, you can specify whether you want user authentication, computer authentication, or both.



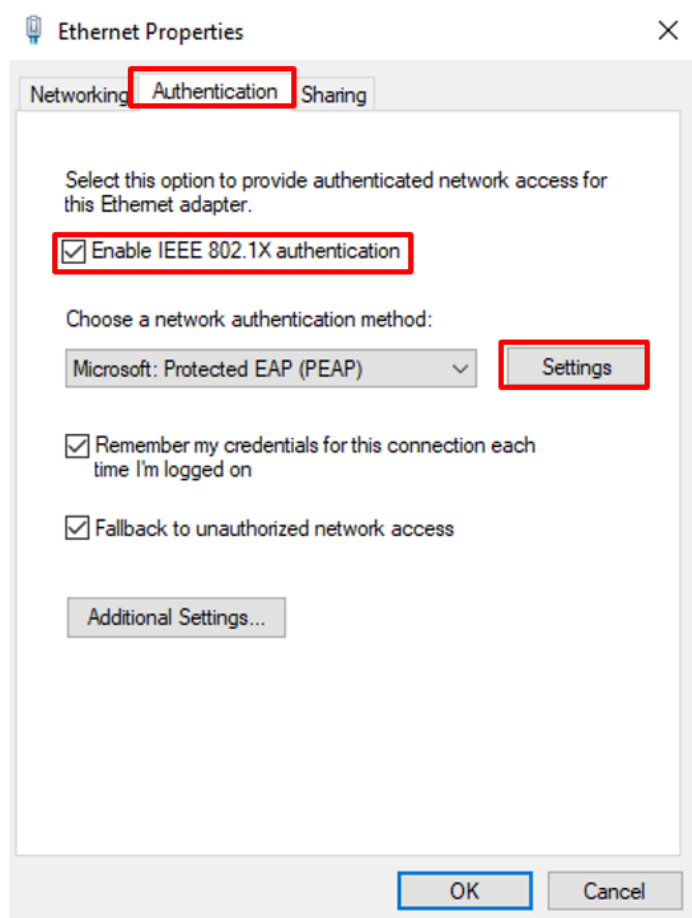
## Configuring Windows 10

This section shows how to configure Windows 10 for 802.1x user authentication.

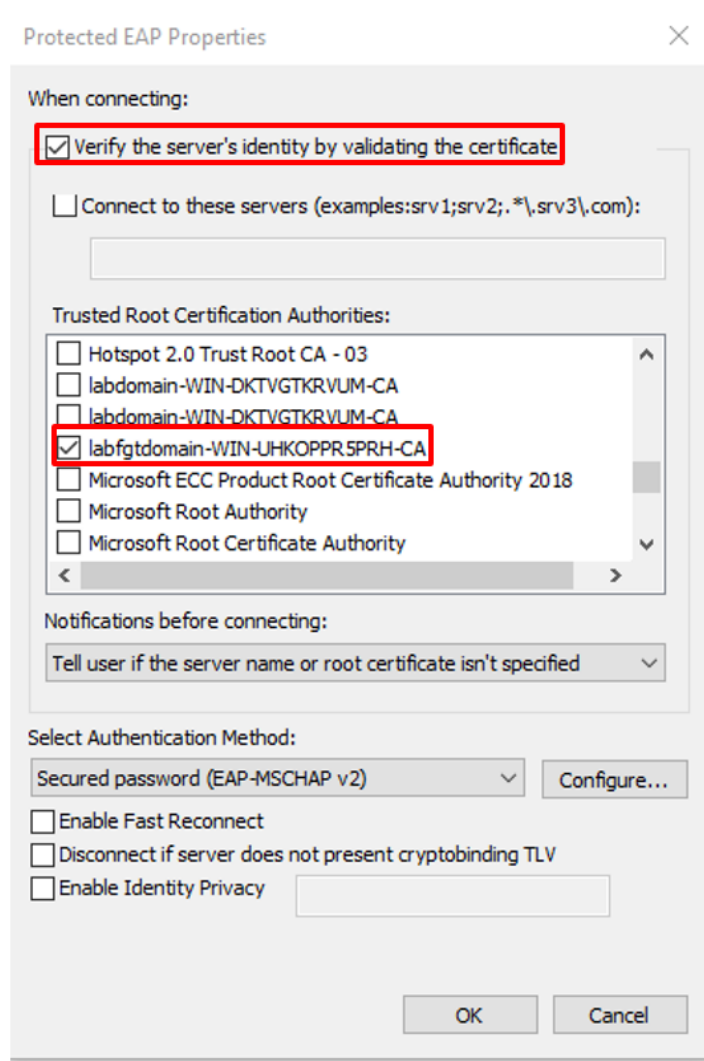
1. Select *Start*, right-click *Computer*, select *Manage*, and then select *Services and Applications*.
2. In the details pane, double-click *Services* and then do one of the following:
  - To configure the startup type, right-click *Wired AutoConfig*, and then select *Properties*. In *Startup type*, select *Automatic* and then select *Start*.
  - To start the service for the current session only, right-click *Wired AutoConfig* and then select *Start*.
3. Install the RADIUS server's certificate to the PC, as shown in the following figure:



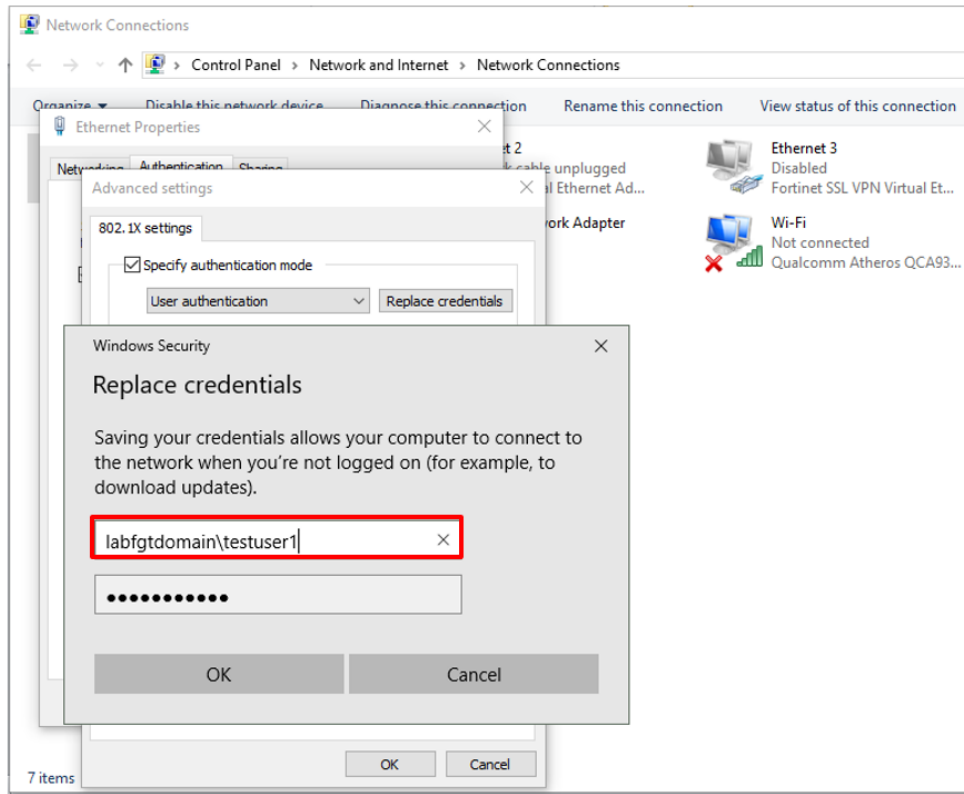
4. In the properties of the network connection, navigate to the Authentication tab, and make sure the *Enable IEEE 802.1X authentication* check box is selected.
5. Select *Settings*.



6. To select the Certificate Authority (CA) that the RADIUS server's certificate uses, import the CA certificate into the local machine and save it in the Trusted Root Certification Authorities directory. If you purchased an SSL certificate from a major CA (such as Verisign or GoDaddy), Windows should have the CA loaded and listed already.



7. Under *Advanced settings*, you can specify whether you want user authentication.



8. Make sure the Wired AutoConfig service is set up for automatic startup, as shown in the following figure. The Wired AutoConfig service allows Windows to interact with 802.1x.

Windows Search	Provides co...	Running	Automatic (D...	Local Syste...
Windows Time	Maintains d...	Running	Manual (Trig...	Local Service
Windows Update	Enables the ...	Running	Manual (Trig...	Local Syste...
Windows Update Medic Ser...	Enables rem...		Manual	Local Syste...
WinHTTP Web Proxy Auto-...	WinHTTP i...	Running	Manual	Local Service
Wired AutoConfig	The Wired ...	Running	Automatic	Local Syste...
WLAN AutoConfig	The WLANS...		Manual	Local Syste...
WMI Performance Adapter	Provides pe...		Manual	Local Syste...
Work Folders	This service ...		Manual	Local Service
Workstation	Creates and...	Running	Automatic	Network S...
WLAN AutoConfig	This service		Manual	Local Service

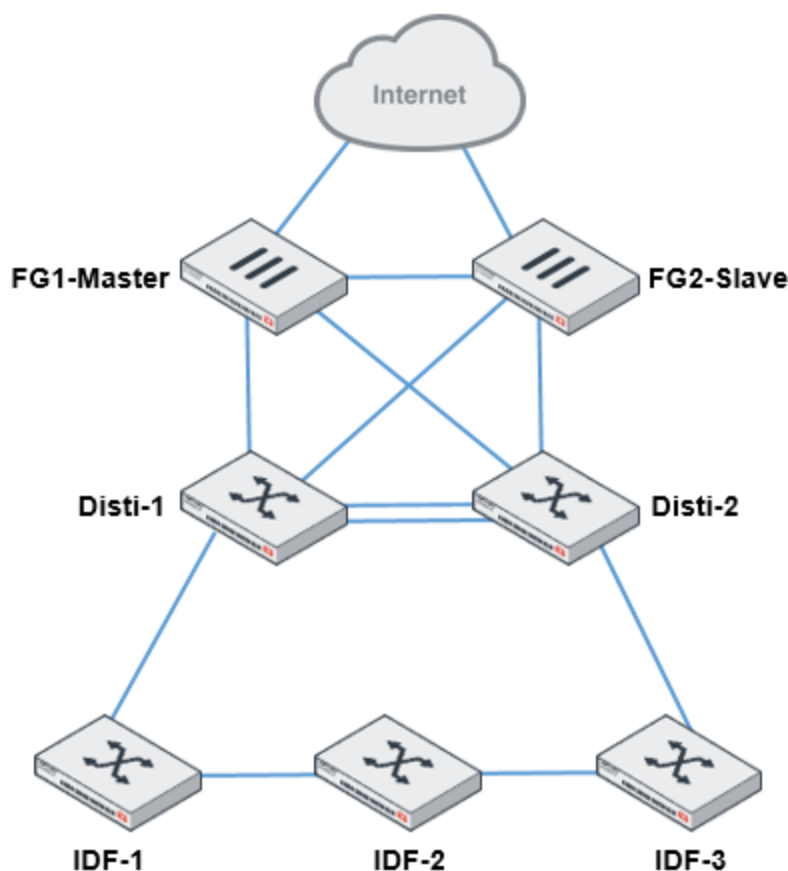
9. To verify that the PC successfully connects, check the network connections. Look for the Ethernet port and make sure that there is no "Authentication failed" message.
10. When the authentication succeeds, you should get an IP address from the right VLAN, as shown in the following figure:

```
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . : 
  Description . . . . . : Realtek PCIe GbE Family Controller
  Physical Address. . . . . : 54-E1-AD-4A-2D-6B
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::e128:8157:b61e:8ec2%8(Preferred)
  IPv4 Address. . . . . : 172.16.32.1(Preferred)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : Monday, September 16, 2019 11:45:52 AM
  Lease Expires . . . . . : Monday, September 23, 2019 11:45:50 AM
  Default Gateway . . . . . : 172.16.32.254
  DHCP Server . . . . . : 172.16.32.254
  DHCPv6 IAID . . . . . : 55894445
  DHCPv6 Client DUID. . . . . : 00-01-00-01-20-E5-55-95-54-E1-AD-4A-2D-6B
  DNS Servers . . . . . : 208.91.112.53
                        : 208.91.112.52
  NetBIOS over Tcpip. . . . . : Enabled
```

11. When the authentication fails, you should get the IP address from the auth-fail-vlan VLAN, as shown in the following figure:

```
Ethernet adapter Ethernet:
  Connection-specific DNS Suffix . : 
  Description . . . . . : Realtek PCIe GbE Family Controller
  Physical Address. . . . . : 54-E1-AD-4A-2D-6B
  DHCP Enabled. . . . . : Yes
  Autoconfiguration Enabled . . . . : Yes
  Link-local IPv6 Address . . . . . : fe80::e128:8157:b61e:8ec2%8(Preferred)
  IPv4 Address. . . . . : 172.16.34.1(Preferred)
  Subnet Mask . . . . . : 255.255.255.0
  Lease Obtained. . . . . : Monday, September 16, 2019 2:12:19 PM
  Lease Expires . . . . . : Monday, September 23, 2019 2:12:19 PM
  Default Gateway . . . . . : 172.16.34.254
  DHCP Server . . . . . : 172.16.34.254
  DHCPv6 IAID . . . . . : 55894445
  DHCPv6 Client DUID. . . . . : 00-01-00-01-20-E5-55-95-54-E1-AD-4A-2D-6B
  DNS Servers . . . . . : 208.91.112.53
                        : 208.91.112.52
  NetBIOS over Tcpip. . . . . : Enabled
```

## Enterprise FortiSwitch secure access



This cookbook article documents a highly resilient 2-tier FortiSwitch architecture (faster convergence) that take advantage of the full performance (bandwidth utilization) offered by MLAG (multichassis LAG).

The FortiGates, for the exercise, are under FortiOS 6.0.1 and FortiSwitch at 6.0 or 3.6.6 (depending on platform compatibility). FortiSwitch must be at least at 3.6.4 in order to deploy MLAG with access ring.

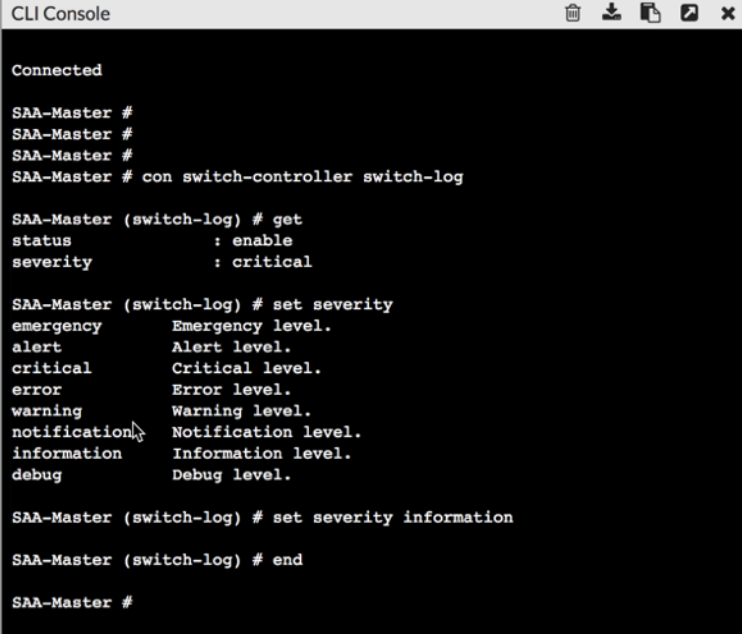
Also ensure that the FortiSwitch models used for MLAG supports the feature: [FortiSwitch Datasheet](#)

In the end, the topology above will be deployed.

## Logging

Increase the level of logging to follow the deployments steps.





```
CLI Console
Connected
SAA-Master #
SAA-Master #
SAA-Master #
SAA-Master # con switch-controller switch-log

SAA-Master (switch-log) # get
status          : enable
severity        : critical

SAA-Master (switch-log) # set severity
emergency       Emergency level.
alert           Alert level.
critical        Critical level.
error           Error level.
warning         Warning level.
notification    Notification level.
information     Information level.
debug           Debug level.

SAA-Master (switch-log) # set severity information

SAA-Master (switch-log) # end

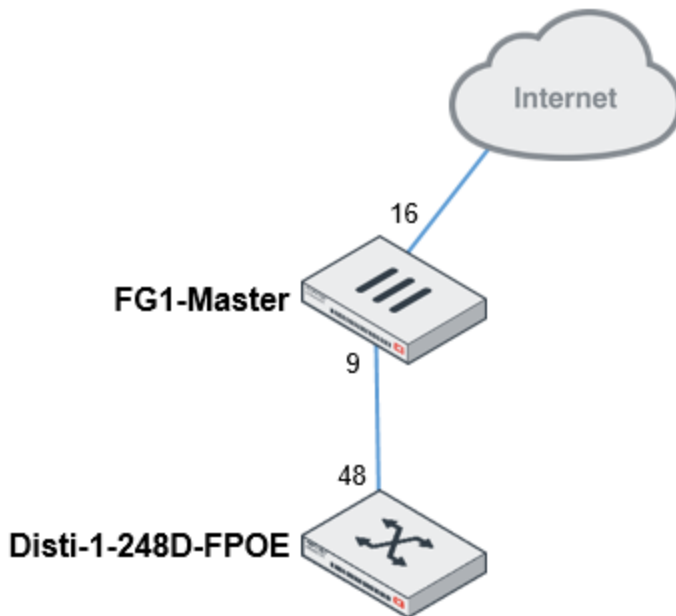
SAA-Master #
```

## FortiLink configuration

1. From *Network > Interfaces*, create a 802.3ad port
2. Add the two member ports that will form the LAG and will be interconnected from the FortiGate-Master to the distribution 1 and 2.
3. Select the addressing mode *"Dedicated to FortiSwitch."*
4. By default, the FortiLink segment is configured in an APIPA address range. In the present context, we will make sure that this segment is routable in order to validate certain metrics on the FortiSwitch GUI. Ensure in an enterprise context that this environment is accessible only through legitimate and restricted privileges.
5. For the purpose of the exercise, we will ensure that FortiSwitch are not automatically authorized to validate certain steps. But it is quite possible to speed up the process and allow automatic authorization.
6. Make sure at first that split interface is enabled (until MCLAG configuration).

The screenshot shows the FortiGate 600D SAA-Master web interface. The left sidebar contains a menu with categories: Favorites, Dashboard, Security Fabric, FortiView, Network (selected), Interfaces (selected), DNS, Packet Capture, SD-WAN, Performance SLA, SD-WAN Rules, Static Routes, Policy Routes, RIP, OSPF, BGP, Multicast, System, Policy & Objects, and Security Profiles. The main content area is titled 'New' and shows the configuration for a new interface named 'FLink'. The configuration includes: Interface Name (FLink), Alias (empty), Type (802.3ad Aggregate), Interface Members (port9 and port10), Tags (Add Tag Category button), Addressing mode (Manual, DHCP, Dedicated to FortiSwitch), IP/Network Mask (192.168.169.1/24), Connected Devices (None), Automatically authorize devices (disabled), FortiLink split interface (enabled), Status, and Comments (empty).

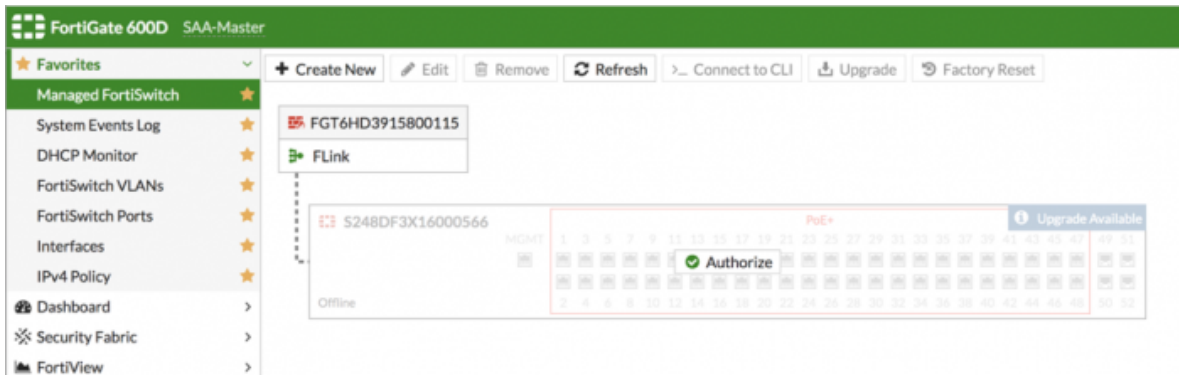
7. Connect the FG1-Master to Disti-1 (port9 to port48).



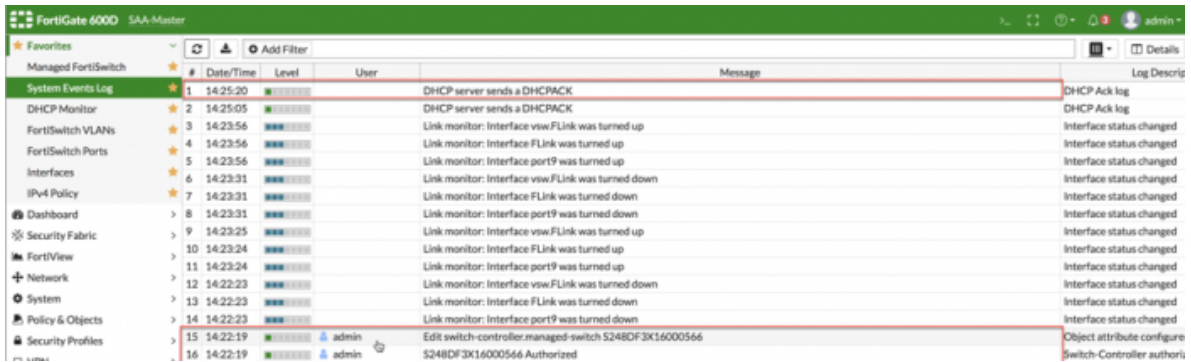
8. Confirm the discovery of the FortiSwitch unit in the logs.



9. Authorize the Disti-1 thereafter.



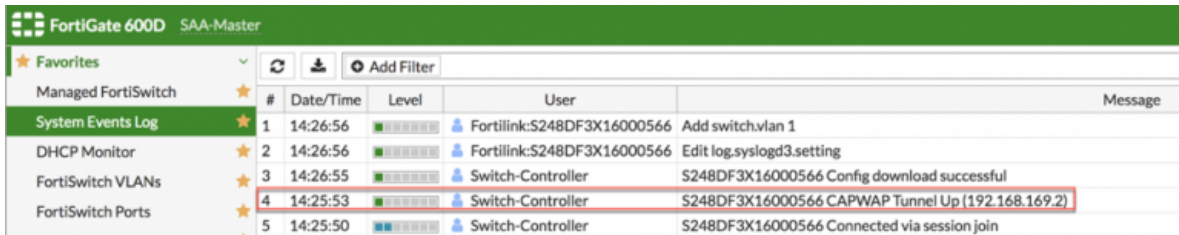
10. At this point, the switch will reboot and will be converted from standalone to managed mode.



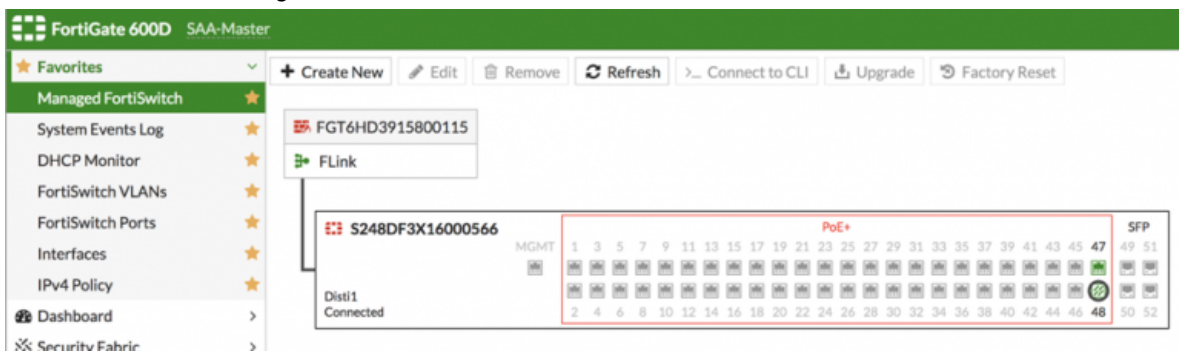
11. The switch receives an IP address in the previously configured segment.



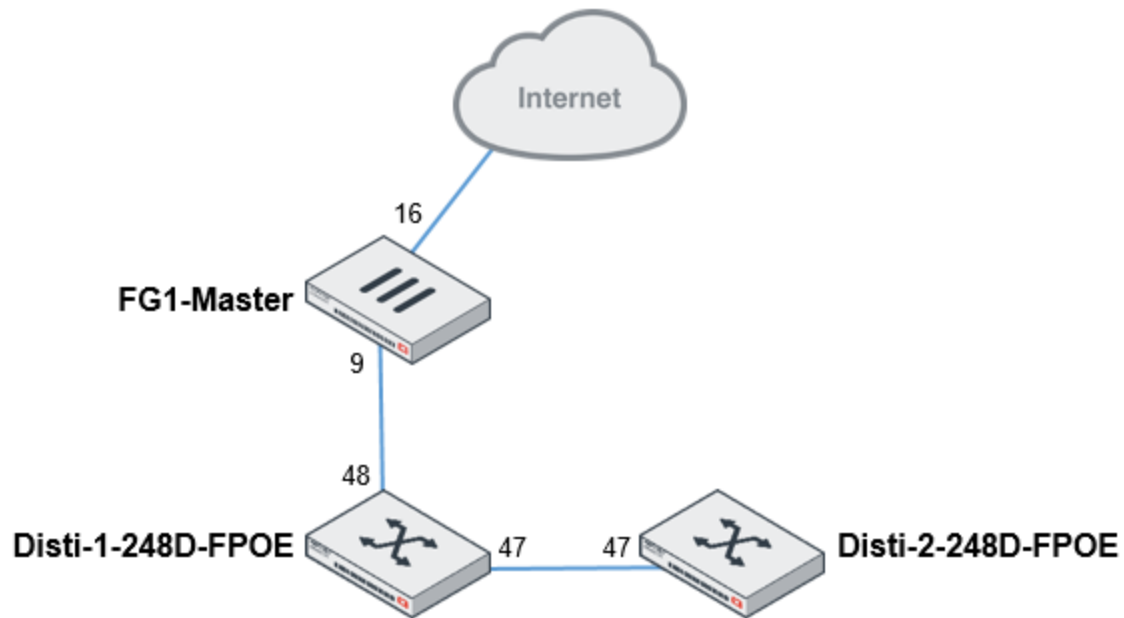
12. The CAPWAP tunnel will appear as UP in the logs.



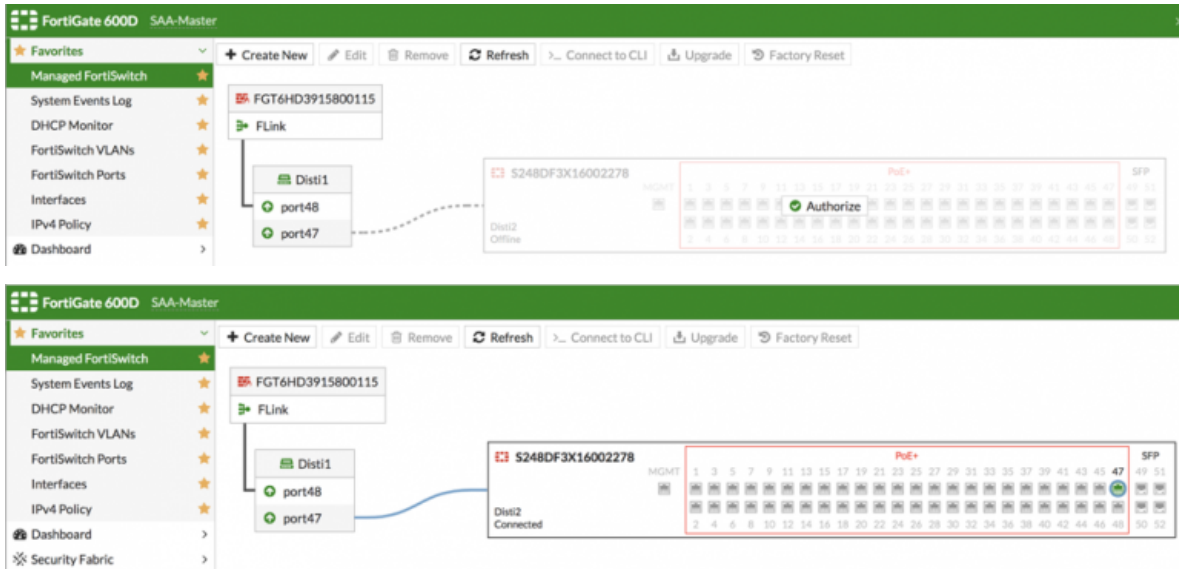
13. Dist1-1 will now be managed.



14. Link the Distribution 1 to Distribution 2 as follows:



15. Allow the addition of the Disti2.



## MCLAG configuration

1. Connect in CLI to Disti2.



2. Enable MCLAG-ICL on the trunk toward Disti-1.

```
Disti2 # config switch trunk
Disti2 (trunk) # edit
name Trunk name.
8DF3X16000566-0

Disti2 (trunk) # edit 8DF3X16000566-0

Disti2 (8DF3X16000566-0) # set mclag-icl enable

Disti2 (8DF3X16000566-0) # end
WARNING: One or more trunk members has ACL configured.
Disti2 #
```

3. Which will result in the following confirmation at log level:

FortiGate 600D SAA-Master					
Add Filter					
	#	Date/Time	Level	User	Message
System Events Log	1	14:43:15	INFO	Fortilink:S248DF3X16002278	MCLAG: ICL ACL change ingress-port-bitmap=0xffffffff, egress-block-port-bitmap=0xffffffff
DHCP Monitor	2	14:43:15	INFO	Fortilink:S248DF3X16002278	Edit switch.trunk 8DF3X16000566-0

4. Connect to the Disti-1 in the CLI:



5. Enable MCLAG-ICL on the trunk toward Disti-2.

```
Disti1 # config switch trunk
Disti1 (trunk) # edit
name Trunk name.
8DF3X16002278-0
__FoRtI1LiNk0__

Disti1 (trunk) # edit 8DF3X16002278-0

Disti1 (8DF3X16002278-0) # set mclag-icl enable

Disti1 (8DF3X16002278-0) # end
WARNING: One or more trunk members has ACL configured.
Disti1 #
```

★ Favorites						
Managed FortiSwitch						
	#	Date/Time	Level	User	Message	
System Events Log	1	14:46:35	✓	Fortilink:S248DF3X16002278	MCLAG: ICL ACL change ingress-port-bitmap=0x1fffffffffff, egress-block-port-bitmap=0x0	
DHCP Monitor	2	14:46:35	✓	Fortilink:S248DF3X16000566	MCLAG: ICL ACL change ingress-port-bitmap=0x1fffffffffff, egress-block-port-bitmap=0x0	
FortiSwitch VLANs	3	14:46:34	✓	Fortilink:S248DF3X16000566	MCLAG: ICL ACL change ingress-port-bitmap=0x1fffffffffff, egress-block-port-bitmap=0x1fffffffffff	
FortiSwitch Ports	4	14:46:33	✓	Fortilink:S248DF3X16000566	Edit switch.trunk 8DF3X16002278-0	

- Disable the split interface from FortiLink and enable automatic authorization.

**FortiGate 600D SAA-Master**

★ Favorites

- Managed FortiSwitch
- System Events Log
- DHCP Monitor
- FortiSwitch VLANs
- FortiSwitch Ports
- Interfaces**
- IPv4 Policy
- Dashboard
- Security Fabric
- FortiView
- Network
- System
- Policy & Objects
- Security Profiles
- VPN
- User & Device
- WiFi & Switch Controller
- Log & Report
- Monitor

### Edit Interface

Interface Name: FLink

Alias:

Link Status: Up

Type: 802.3ad Aggregate

Interface Members: port9 port10   
 +

Tags:   
  Add Tag Category

Address

Addressing mode: Manual DHCP **Dedicated to FortiSwitch**

IP/Network Mask: 192.168.169.1/255.255.255.0

Connected Devices: 2 FortiSwitch(s)

Automatically authorize devices

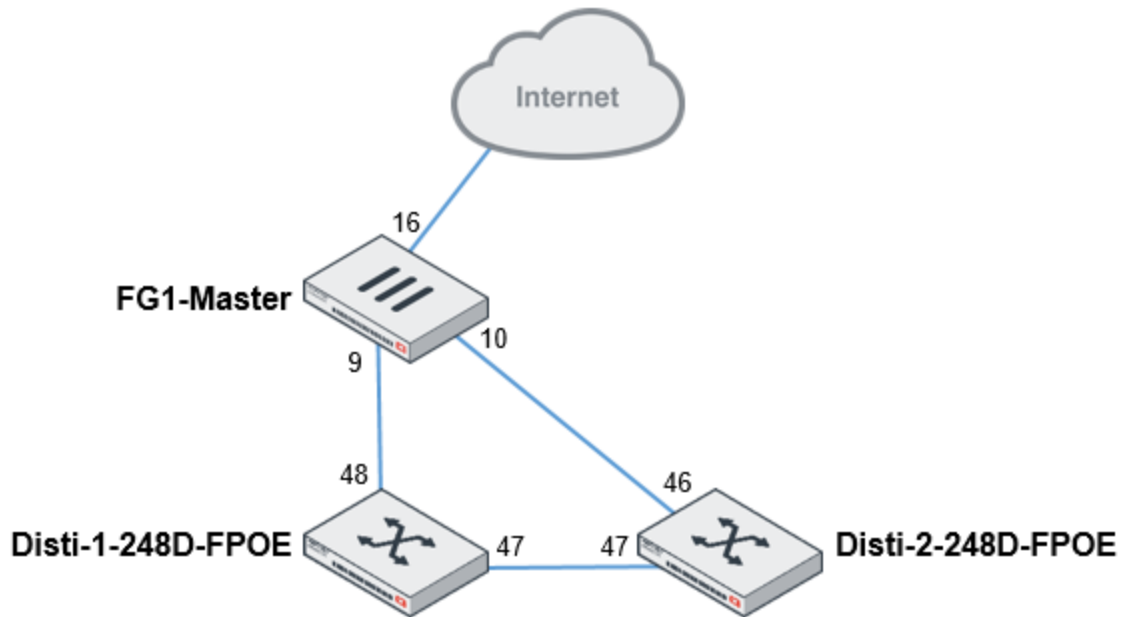
FortiLink split interface

Status

Comments:

Interface State: Enabled Disabled

- Close the loop from the Dist-2 to the second port of the FortiLink LAG of the FortiGate Master.



8. Resulting FortiSwitch presentation:

FortiGate 600D SAA-Master

Managed FortiSwitch

System Events Log

DHCP Monitor

FortiSwitch VLANs

FortiSwitch Ports

Interfaces

IPv4 Policy

Dashboard

Security Fabric

FortiView

Network

System

Policy & Objects

Security Profiles

FGT6HD3915800115

FLink

S248DF3X16000566

MGMT

PoE+

SFP

Disti1 Connected

S248DF3X16002278

MGMT

PoE+

SFP

Disti2 Connected

9. You can validate the consistency at the MCLAG level using the following command:

```

SAA-Master # diag switch-controller dump mclag
icl          Dumps MCLAG inter-chassis-link(ICL).
list         Dumps MCLAG list.
peer-consistency-check  Checks MCLAG peer consistency.

SAA-Master # diag switch-controller dump mclag peer-consistency-check
Managed Switch : S248DF3X16000566  0

Running diagnostic, it may take sometime...

mclag-trunk-name  peer-config lacp-state  stp-state  local-ports
-----
BDF3X16002278-0*  OK          UP          OK          port47
__PortLink0__    OK          UP          OK          port48

Managed Switch : S248DF3X16002278  0

Running diagnostic, it may take sometime...

mclag-trunk-name  peer-config lacp-state  stp-state  local-ports
-----
BDF3X16000566-0*  OK          UP          OK          port47
__PortLink0__    OK          UP          OK          port46
  
```

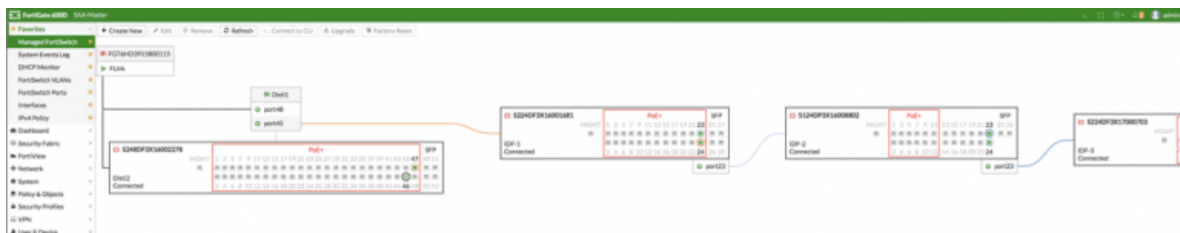
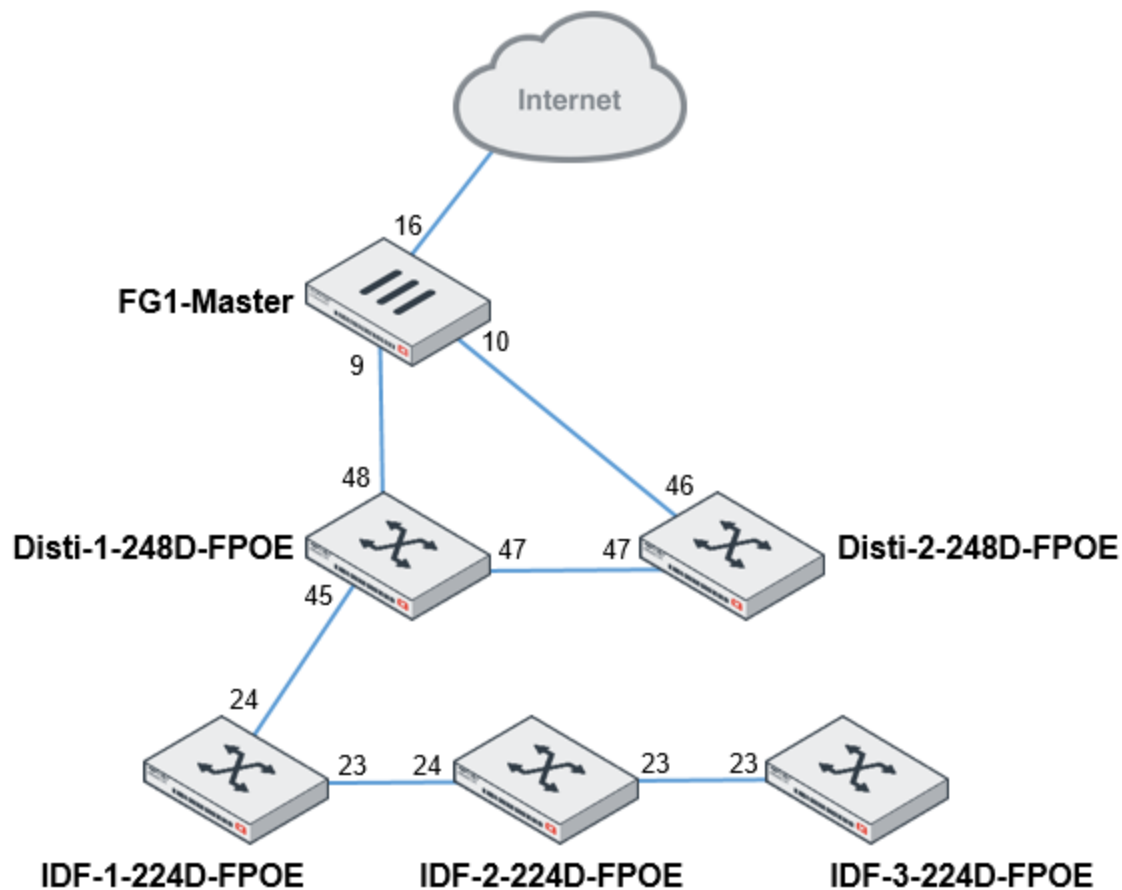


10. Several other commands allow you to diagnose the feature:

- On FortiGate: `diagnose netlinkaggregate name fortalink`
- On FortiSwitch Disti: `diagnose switch trunk list __FoRtI1LiNk0__`
- On FortiSwitch Disti: `diagnose switch mclag list __FoRtI1LiNk0__`
- On FortiSwitch Disti: `diagnose switch mclag icl`

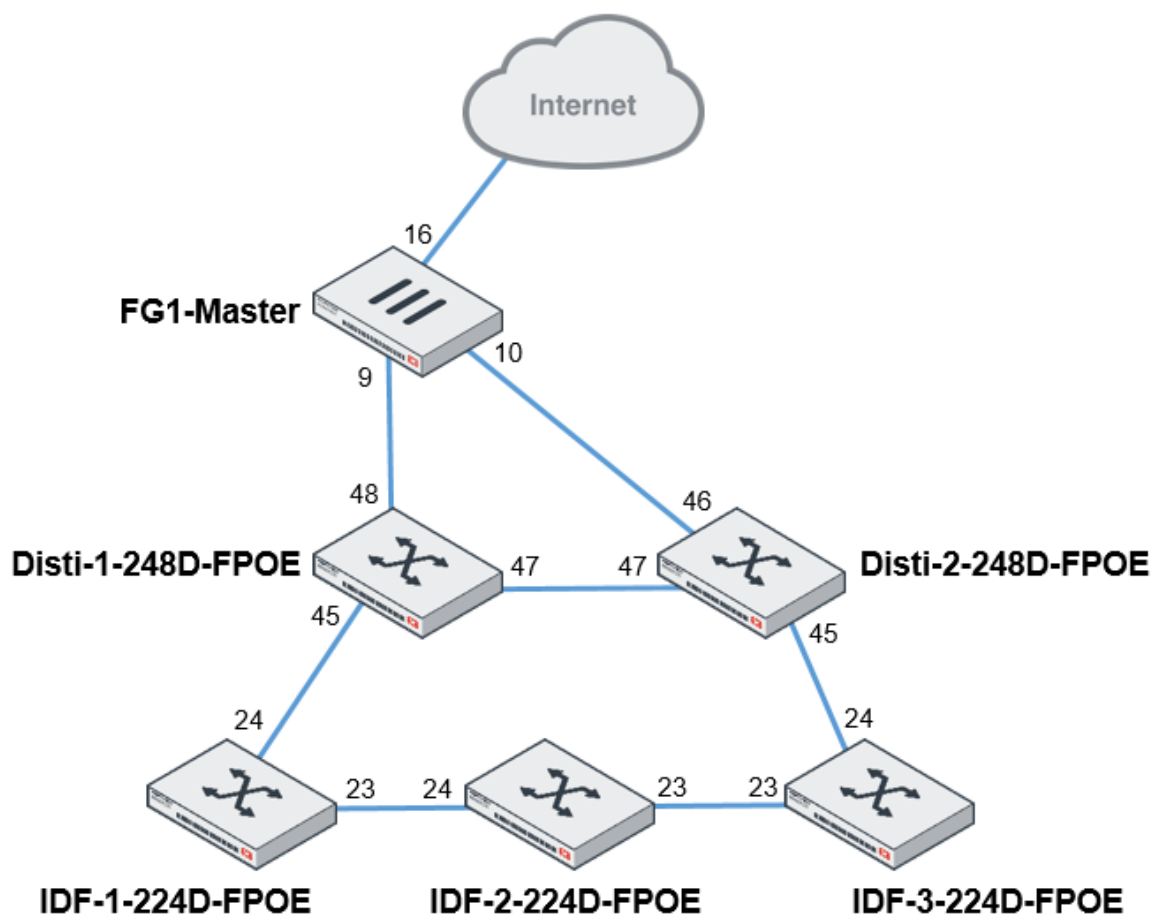
## IDF configuration

1. Interconnect the Disti-1, cascading the switches that make up the stack of the IDF, as follows:



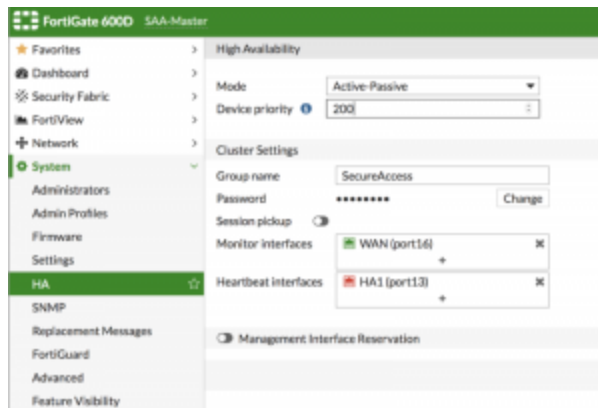
2. All that remains is to connect the IDF-3 to the Disti-2.





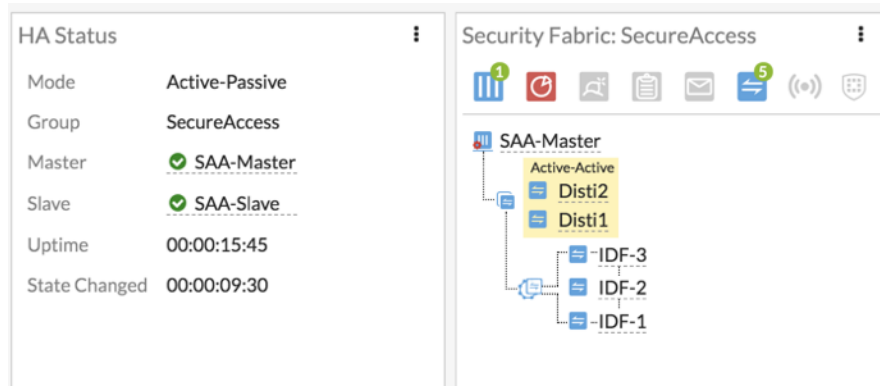
## HA configuration

## 1. Configure HA in active-passive mode.

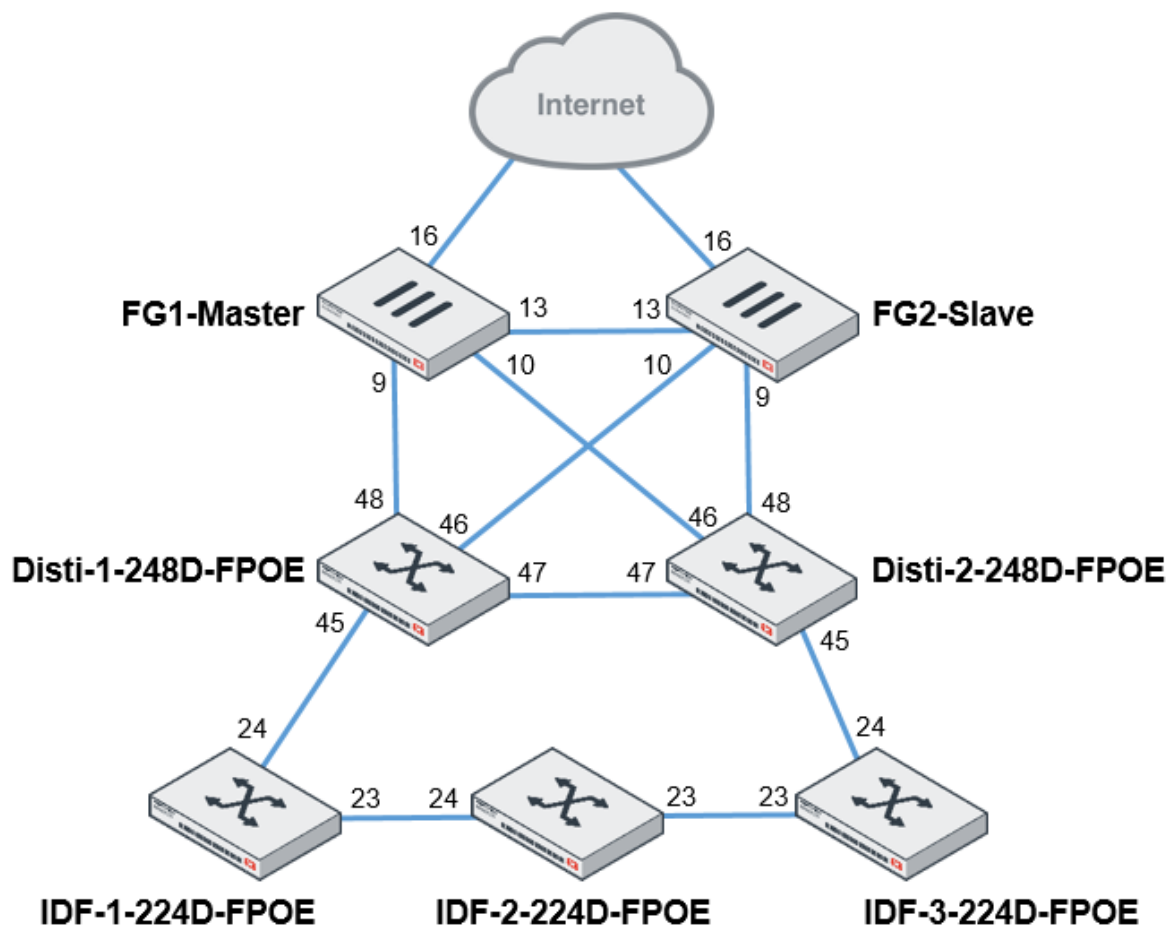


## 2. Make sure the configuration is well synchronized

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput	Checksum
FortiGate 600D	200	SAA-Master	FGT6HD3915800115	Master	1h 15m 57s	152	102.00 kbps	dc8b6e54e3ad771fcdeef39445121446
FortiGate 600D	100	SAA-Slave	FGT6HD3915800031	Slave	11m 10s	106	85.00 kbps	dc8b6e54e3ad771fcdeef39445121446



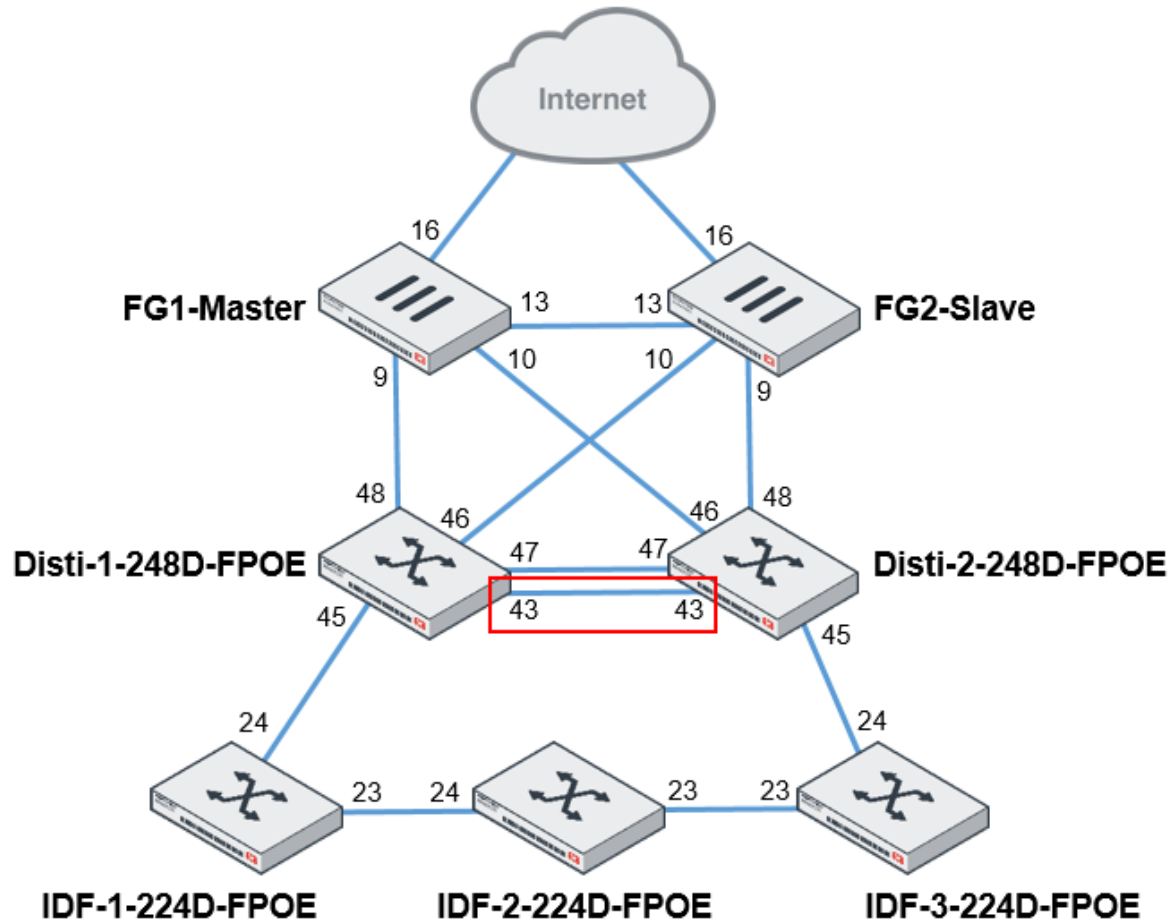
## 3. Connect the balance of the links in order to coherently replicate the wiring of the FortiGate Master and FortiGate Slave, as follows:



4. This configuration results in the managed FortiSwitch units.



5. Finalize by doubling the ICL links between the two distribution switches.



6. Validate the automatic integration into the trunk (LAG).

FortiGate 600D SAA-Master			
Favorites			
Managed FortiSwitch	+	Create New	✖
System Events Log	★	✎	Edit
DHCP Monitor	★	✖	Delete
FortiSwitch VLANs	★	🔍	Search
FortiSwitch Ports	★		
Interfaces	★		
IPv4 Policy	★		
Dashboard			
Security Fabric			
FortiView			
Network			
System			
Policy & Objects			
Security Profiles			
VPN			
User & Device			
WiFi & Switch Controller			
Log & Report			
Monitor			

Port	Description	Native VLAN
port31	vsw.FLink	
port32	vsw.FLink	
port33	vsw.FLink	
port34	vsw.FLink	
port35	vsw.FLink	
port36	vsw.FLink	
port37	vsw.FLink	
port38	vsw.FLink	
port39	vsw.FLink	
port40	vsw.FLink	
port41	vsw.FLink	
port42	vsw.FLink	
port43	S248DF3K16002278	
port44	vsw.FLink	
port45	S224DF3K16001681	
port46	FGT64D3F158000031	
port47	S248DF3K16002278	
port48	FGT64D3F158000115	

```
Distil #
Distil # config switch trunk

Distil (trunk) # edit 8DF3X16002278-0

Distil (8DF3X16002278-0) # sho
config switch trunk
    edit "8DF3X16002278-0"
        set mode lacp-active
        set auto-isl 1
        set mclag-icl enable
        set members "port47" "port43"
    next
end

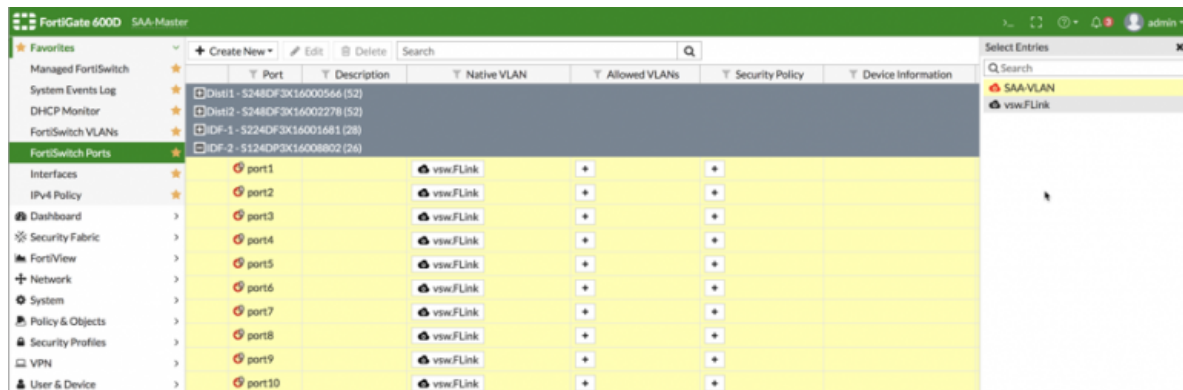
Distil (8DF3X16002278-0) #
```

## Validation

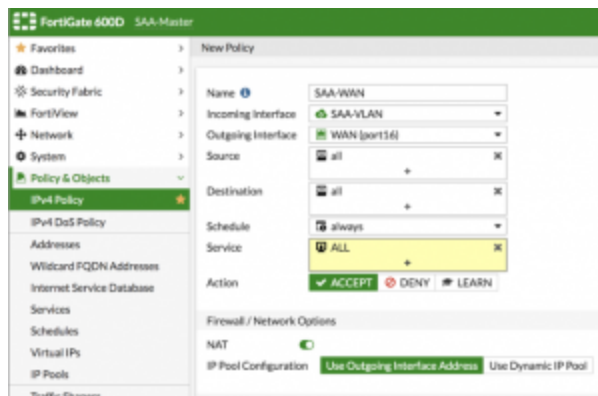
1. To ensure the robustness of the topology, create a test VLAN that will be assigned, for example, to one of the IDF switches.

The screenshot shows the FortiGate 6000 SAA-Master configuration page. The left sidebar contains a navigation menu with options like Favorites, Managed FortiSwitch, System Events Log, DHCP Monitor, FortiSwitch VLANs, FortiSwitch Ports, Interface, IPv4 Policy, Dashboard, Security Fabric, FortiView, Network, System, Policy & Objects, Security Profiles, VPN, User & Device, WiFi & Switch Controller, Log & Report, and Monitor. The main configuration area is titled 'New' and shows the configuration for a new interface named 'SAA-VLAN'. The configuration includes the following fields and options:

- Interface Name: SAA-VLAN
- Alias: (empty)
- Type: VLAN
- Interface: FLink
- VLAN ID: 15
- Color: Change
- Tags: Role: LAN, Add Tag Category
- Address: Addressing mode: Manual, IPv4 Network Mask: 10.15.15.1/24
- Administrative Access: IPv4 (HTTP, HTTPS, CAPWAP, RADIUS Accounting, SSH, SNMP, FortiTelemetry, PING, RMON Access, FTN)
- DHCP Server: Address Range (Create New, Edit, Delete), Starting IP: 10.15.15.2, End IP: 10.15.15.254, Netmask: 255.255.255.0, Default Gateway: Same as Interface IP, DNS Server: Same as System DNS, Same as Interface IP



2. Allow access to the Internet.

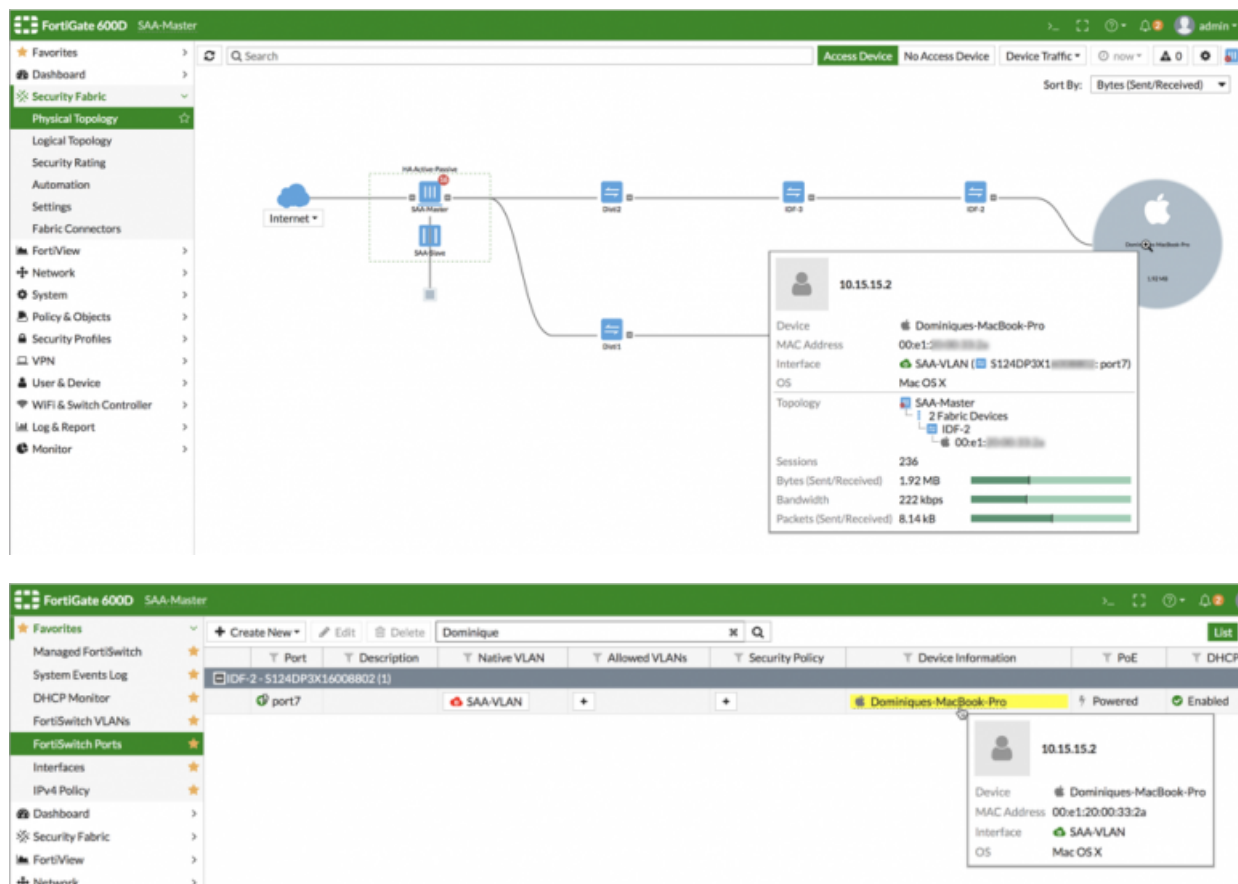


3. You should be able to reboot the FortiGate-Master, remove some links (Disti1 port to IDF-1 in this case), generate HA balancing using the loss of the monitored link (WAN), and see at most only the loss of some packets:

```
64 bytes from 1.1.1.1: icmp_seq=26 ttl=55 time=9.086 ms
64 bytes from 1.1.1.1: icmp_seq=27 ttl=55 time=11.223 ms
64 bytes from 1.1.1.1: icmp_seq=28 ttl=55 time=12.373 ms
64 bytes from 1.1.1.1: icmp_seq=29 ttl=55 time=10.972 ms
64 bytes from 1.1.1.1: icmp_seq=30 ttl=55 time=12.373 ms
64 bytes from 1.1.1.1: icmp_seq=31 ttl=55 time=9.944 ms
64 bytes from 1.1.1.1: icmp_seq=32 ttl=55 time=11.564 ms
64 bytes from 1.1.1.1: icmp_seq=33 ttl=55 time=10.968 ms
64 bytes from 1.1.1.1: icmp_seq=34 ttl=55 time=9.797 ms
64 bytes from 1.1.1.1: icmp_seq=35 ttl=55 time=11.991 ms
64 bytes from 1.1.1.1: icmp_seq=36 ttl=55 time=8.921 ms
64 bytes from 1.1.1.1: icmp_seq=37 ttl=55 time=9.766 ms
64 bytes from 1.1.1.1: icmp_seq=38 ttl=55 time=11.234 ms
64 bytes from 1.1.1.1: icmp_seq=39 ttl=55 time=10.779 ms
64 bytes from 1.1.1.1: icmp_seq=40 ttl=55 time=9.670 ms
Request timeout for icmp_seq 41
64 bytes from 1.1.1.1: icmp_seq=42 ttl=55 time=10.278 ms
64 bytes from 1.1.1.1: icmp_seq=43 ttl=55 time=8.658 ms
64 bytes from 1.1.1.1: icmp_seq=44 ttl=55 time=9.864 ms
64 bytes from 1.1.1.1: icmp_seq=45 ttl=55 time=10.438 ms
64 bytes from 1.1.1.1: icmp_seq=46 ttl=55 time=15.925 ms
64 bytes from 1.1.1.1: icmp_seq=47 ttl=55 time=10.320 ms
```

## Security Fabric visibility

With the Security Fabric, in addition to extend your control and protection, you get unparalleled end-to-end visibility:



## Bonus—FortiSwitch access

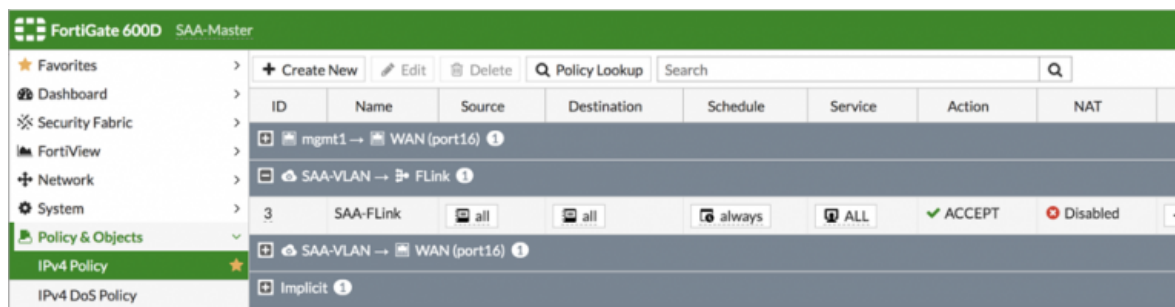
1. To access the FortiSwitch unit, configure a policy in the CLI.

```
SAA-Master # config firewall policy
SAA-Master (policy) # edit 0
new entry '0' added

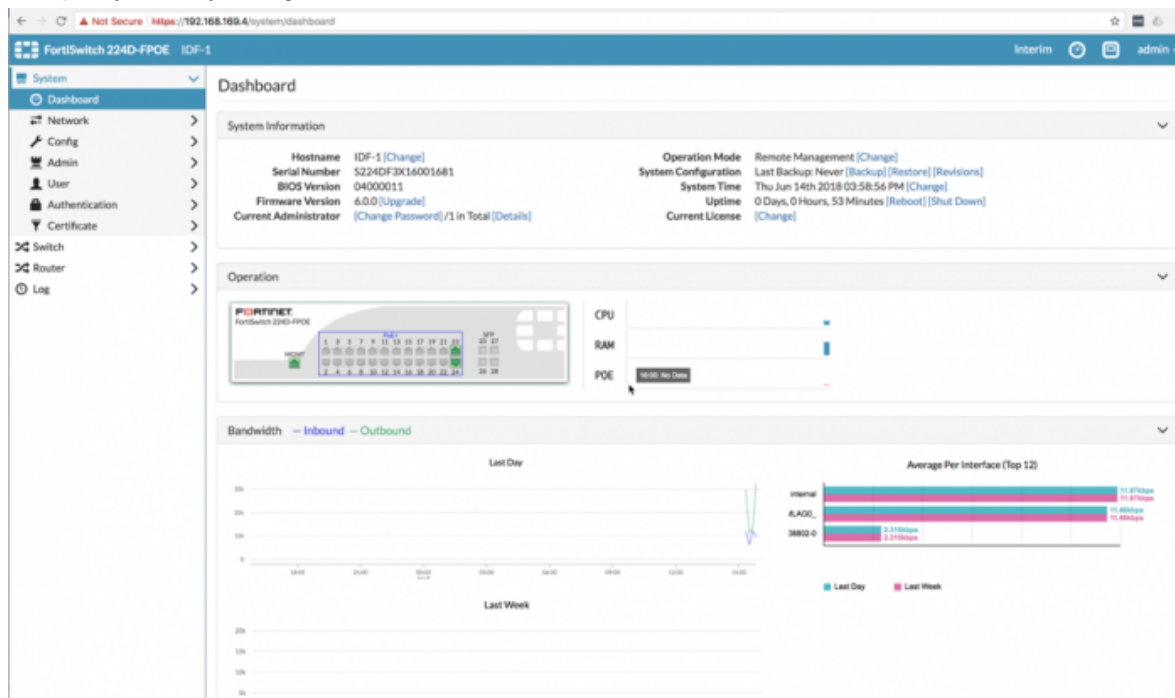
SAA-Master (0) # set srcintf SAA-VLAN
SAA-Master (0) # set srcaddr all
SAA-Master (0) # set dstintf FLink
SAA-Master (0) # set dstaddr all
SAA-Master (0) # set action accept
SAA-Master (0) # set service ALL
SAA-Master (0) # set schedule always
SAA-Master (0) # end
SAA-Master #
```

2. The configured policy appears in the GUI.





3. This policy allows you to get access to the FortiSwitch unit.



4. The hardware configuration is as follows:







**FORTINET®**



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.