



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/training-certification>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com



February 22, 2021

FortiSwitch Cookbook

TABLE OF CONTENTS

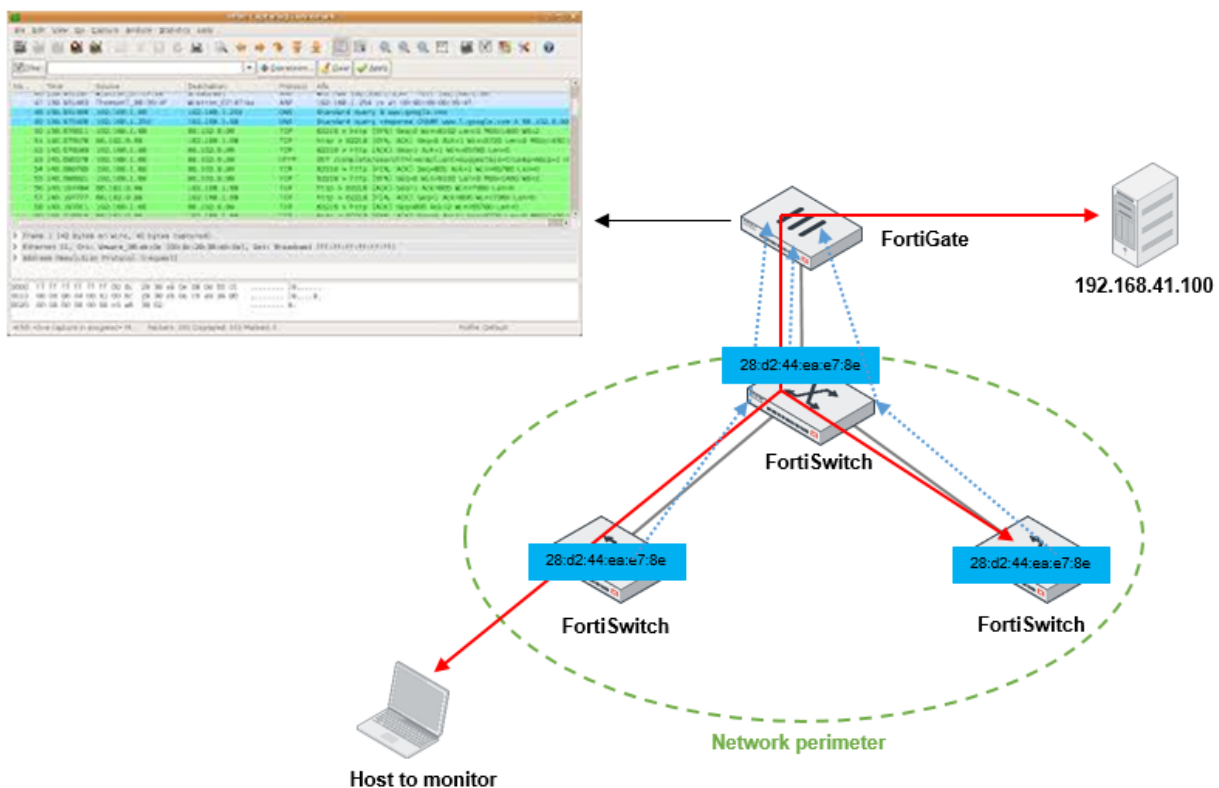
Capturing packets from a sniffer VLAN in a FortiLink setup	4
Remote sampling of a MAC address	4
Remote sampling of a FortiSwitch port	5
Setting up port-based 802.1x authentication in a FortiLink setup	6
Configuring the FortiGate and FortiSwitch units	6
Configuring the RADIUS server	13
Troubleshooting	21
Configuring Windows 10	25
Enterprise FortiSwitch secure access	31
Logging	31
FortiLink configuration	32
MCLAG configuration	36
IDF configuration	39
HA configuration	41
Validation	44
Security Fabric visibility	45
Bonus—FortiSwitch access	46
Interconnecting three sites with MCLAG	48
Adding the third site	49
Checking the topology	52
Relevant configuration	53
Carrying customer VLANs over a provider network	56
Configure the provider switches	57
Accept specific VLANs at the provider ingress	58
Assign different service tags at the provider ingress	59
Retag service VLANs	59
VLAN retagging/translation of regular 802.1Q traffic	61
MCLAG peer group managed with FortiLink over layer 3	62
Set up the FortiGate device	63
Configure the WAN router	65
Configure the site1_mclag1 switch	67
Authorize the site1_mclag1 switch	68
Configure the site1_mclag2 switch	70
Configure the FortiGate device	72
Configure the access switches	77
Finish the FortiSwitch configuration from the FortiGate device	78
Check the configuration	82

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:

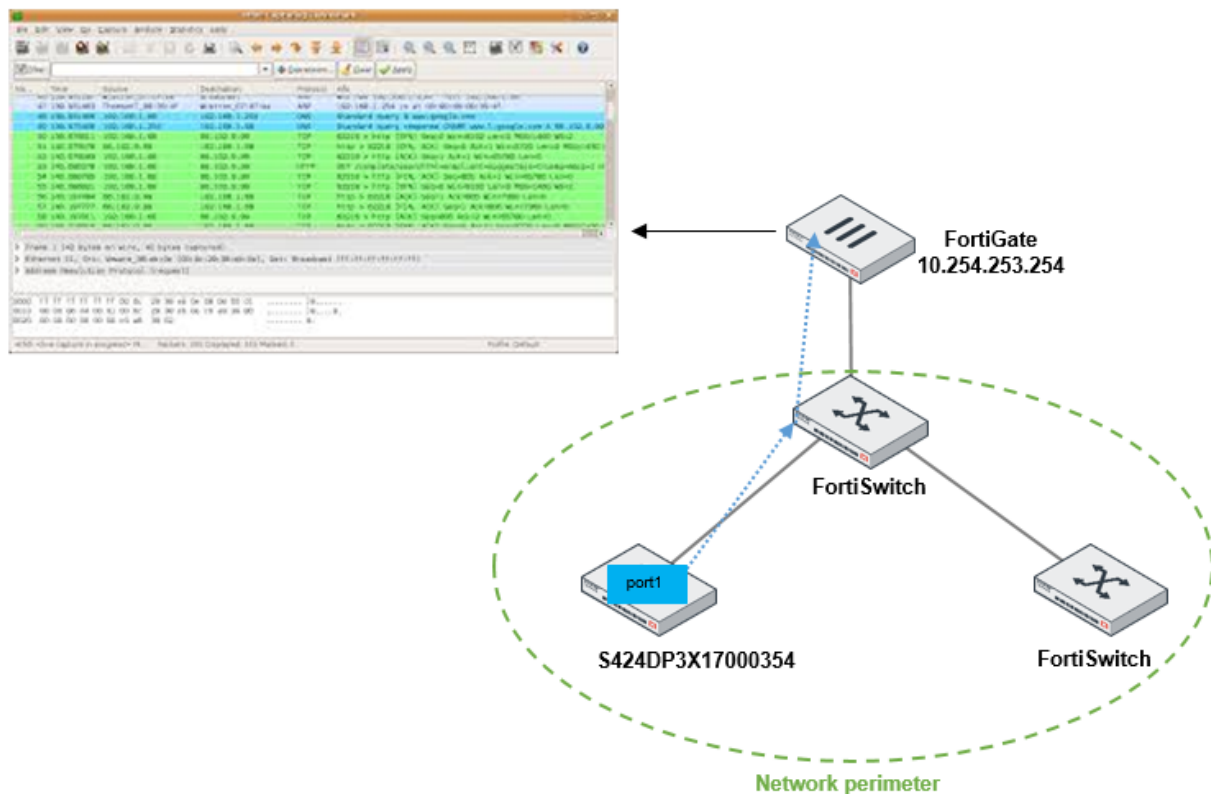
```
config switch-controller traffic-sniffer
  set erspan-ip 192.168.41.100 // the target IP address for the traffic, which is
    routed through the FortiGate unit
  config target-mac
    edit 28:d2:44:ea:e7:8e // a specific MAC address you want to examine
  next
```



```
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.

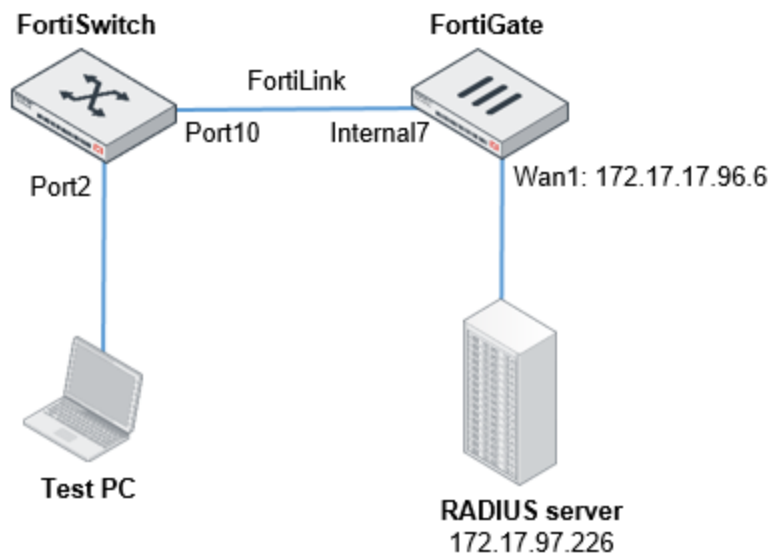
Remote sampling of a FortiSwitch port



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 25](#)

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 RADIUSERVERNAME 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.

The screenshot shows the 'Edit User Group' configuration page in the FortiLink GUI. The left sidebar shows the navigation menu with 'User & Device' selected. The main panel is titled 'Edit User Group' and contains the following fields:

- Name:** Radius-Group
- Type:** Firewall
- Members:** (empty list with a plus icon)
- Remote Groups:** (empty list with '+ Add', 'Edit', and 'Delete' buttons)
- Remote Server:** Radius-Server
- Group Name:** Any

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

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.

The screenshot shows the 'FortiSwitch VLANs' configuration page in the FortiLink GUI. The left sidebar shows the navigation menu with 'WiFi & Switch Controller' selected. The main panel displays a table of configured VLANs.

Name	VLAN ID	IP/Netmask	Access	Ref.
LAGuest	31	172.16.31.254/255.255.255.0	Ping	1
LAGuest	33	172.16.33.254/255.255.255.0	Ping	1
LAGuest	34	172.16.34.254/255.255.255.0	Ping	5
LAGuest	32	172.16.32.254/255.255.255.0	Ping	3
LAGuest	1	0.0.0.0/0.0.0.0	HTTPS SSH Port HTTP Wireless Controller	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 "internal7"
set vlandid 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
    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 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 (selected), Use Dynamic IP Pool
 - Preserve Source Port:** (unchecked)
 - Proxy Options:** PRX 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 (selected), 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:

The screenshot shows the FortiGate GUI's 'Edit Policy' window. The left sidebar shows the 'Policy & Objects' menu with 'IPv4 Policy' selected. The main window displays the configuration for a policy named 'Lansecure Internet'. The configuration includes the following fields and values:

- Name:** Lansecure Internet
- Incoming Interface:** --HQ Secure LAN (LanSecure)
- Outgoing Interface:** wan1
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ACCEPT (checked), DENY (unchecked), LEARN (unchecked)
- Firewall / Network Options:**
 - NAT:** checked
 - IP Pool Configuration:** Use Outgoing Interface Address (selected), Use Dynamic IP Pool (unchecked)
 - Preserve Source Port:** unchecked
 - Proxy Options:** default (selected)
- 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: unchecked
- Comments:** Write a comment... (0/1023)
- Enable this policy:** checked

The bottom of the window shows 'OK' and 'Cancel' buttons.

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
```

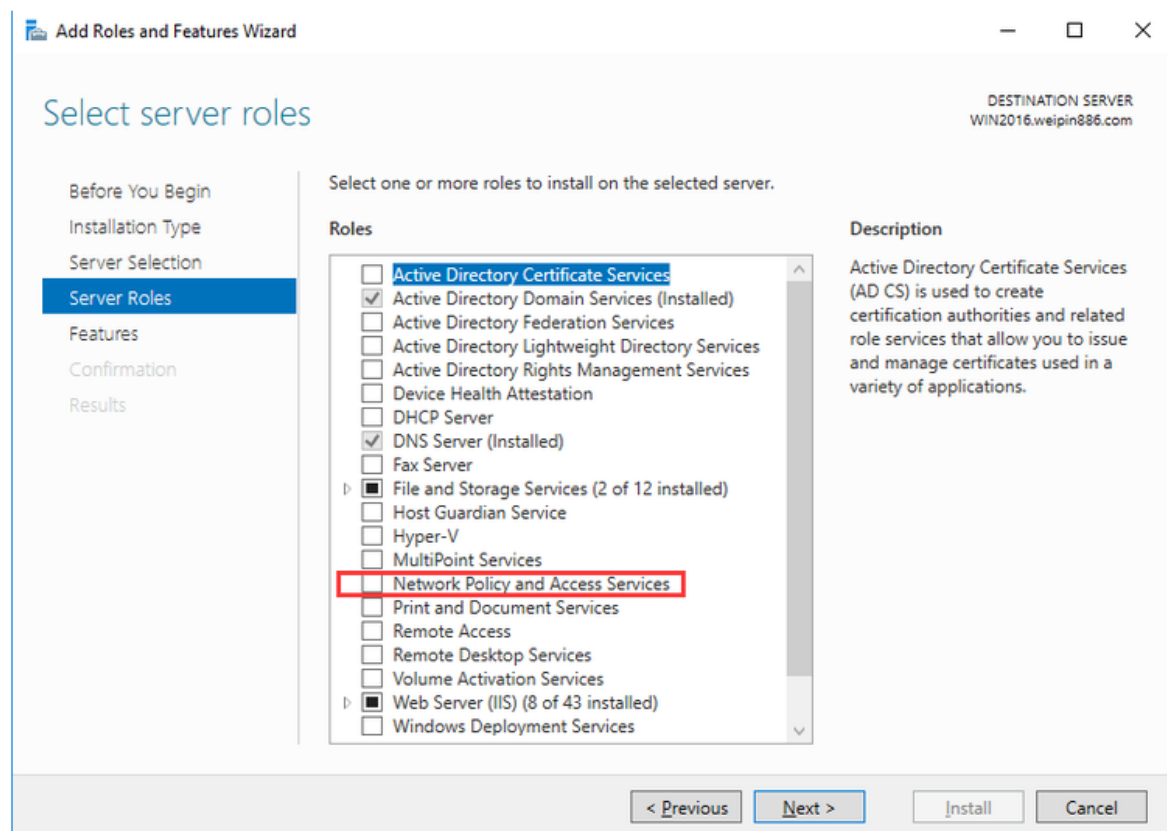
4. Verify that the FortiGate unit and the FortiSwitch unit are synchronized:

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

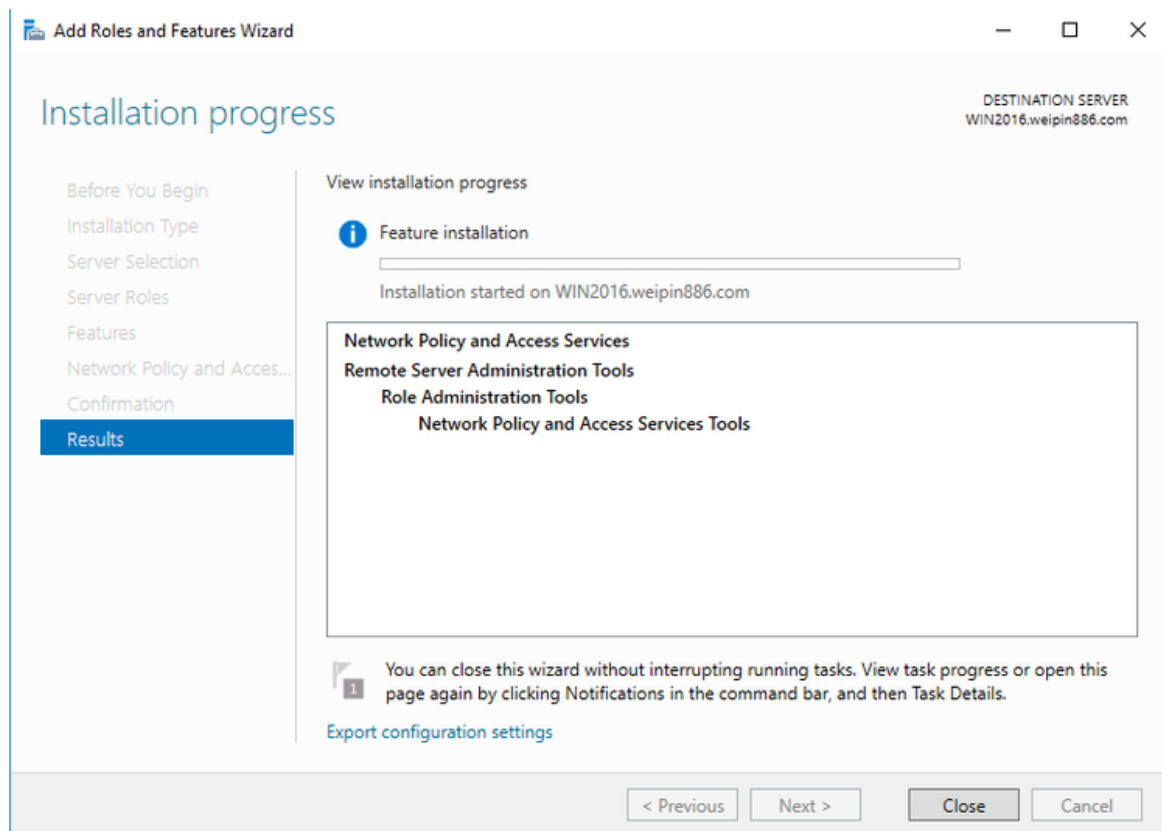
Configuring the RADIUS server

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.

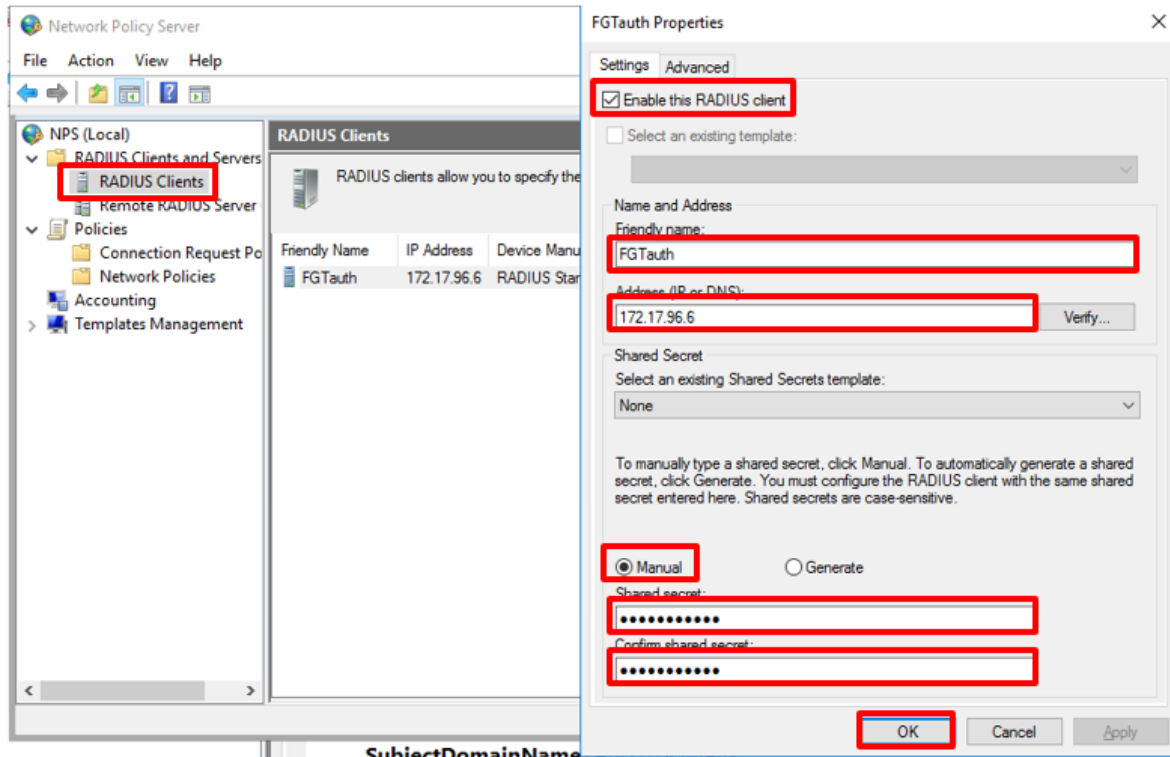
1. Log in to the Windows Server 2016 that you plan to use as your RADIUS server.
2. Launch the Server Manager and select *Manage* from the top right.
3. Select *Add Roles and Features* to launch the wizard.
4. From the wizard page, select *Network Policy and Access Services*, as shown in the following figure:



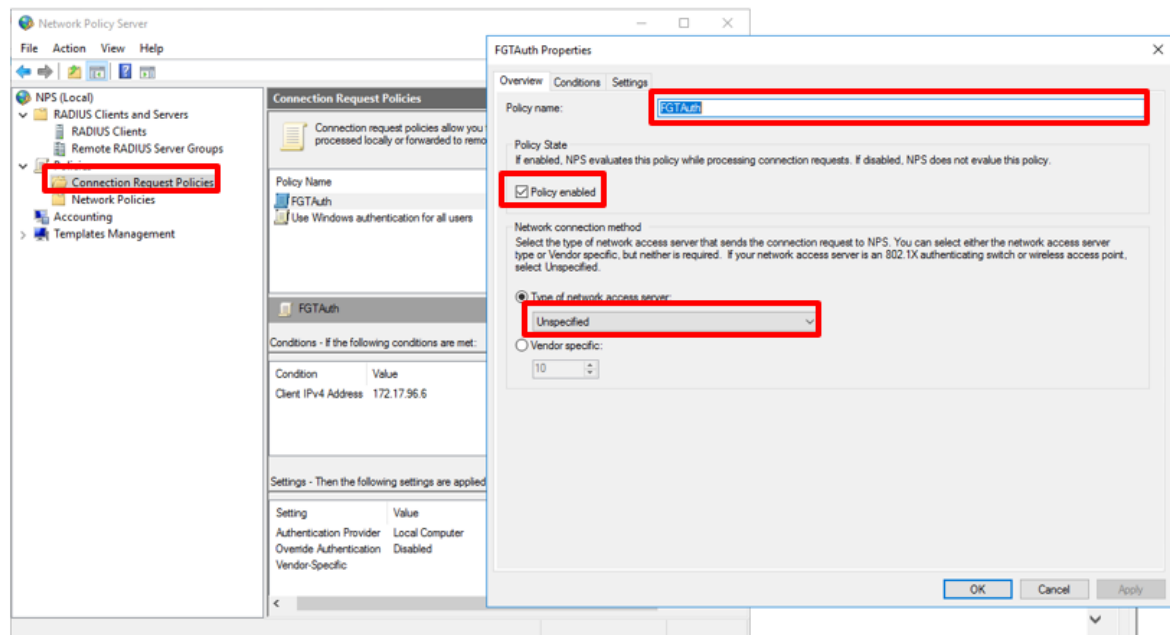
5. Select *Next* and then select *Finish* to start the installation. No reboot is required.



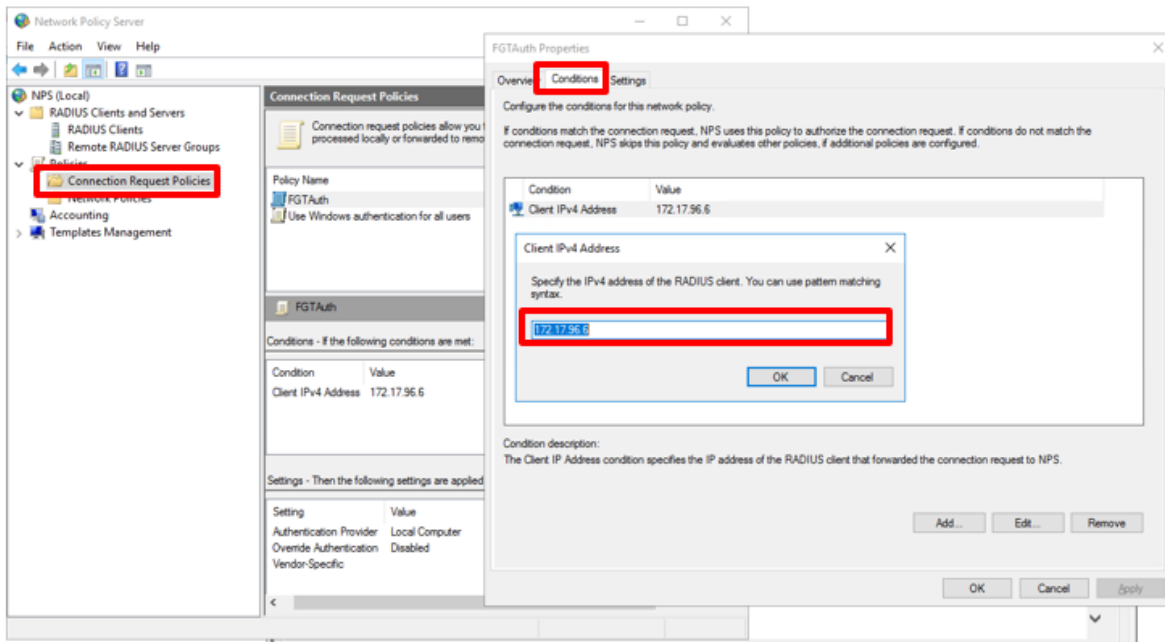
6. After the installation is complete, select *Tools* from the Server Manager and then select *Network Policy Server*.
7. Right-click on *RADIUS Clients* and select *New* to display the new RADIUS client dialog box. Use the following procedure to configure the RADIUS clients:
 - a. Select the *Enable 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*.



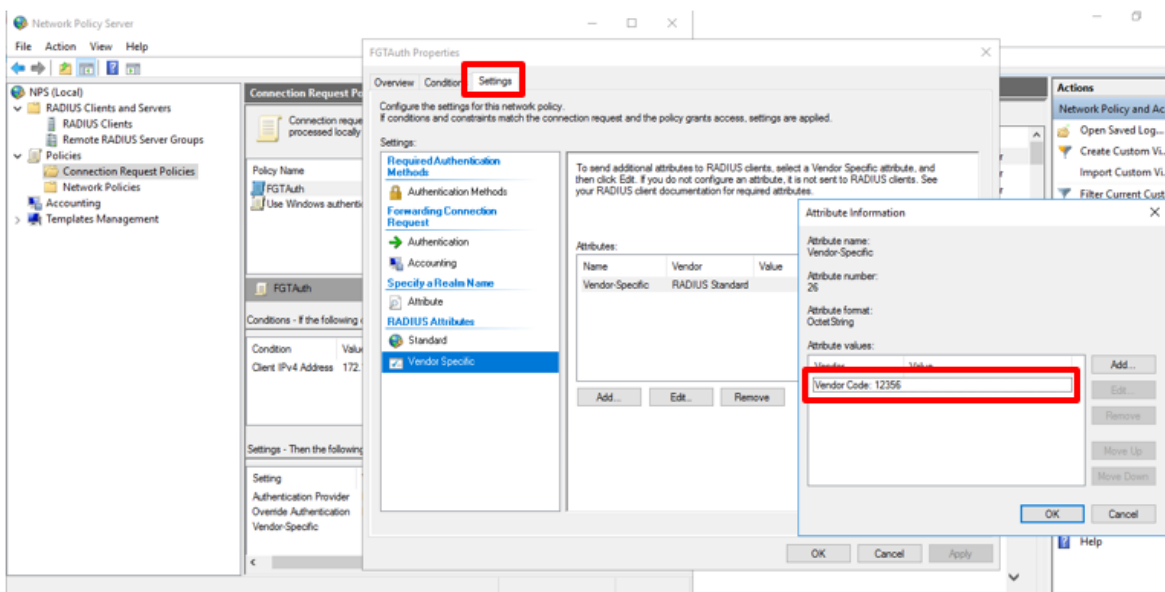
8. Under the Policies section of the NPS Snap-in, right-click *Connection Request Policies* and select *New*.
 - In the Overview tab, enter a name for the policy, such as `FGTAUTH`.
 - Select the *Policy enabled* check box.
 - Leave the type of network access server as *Unspecified*.



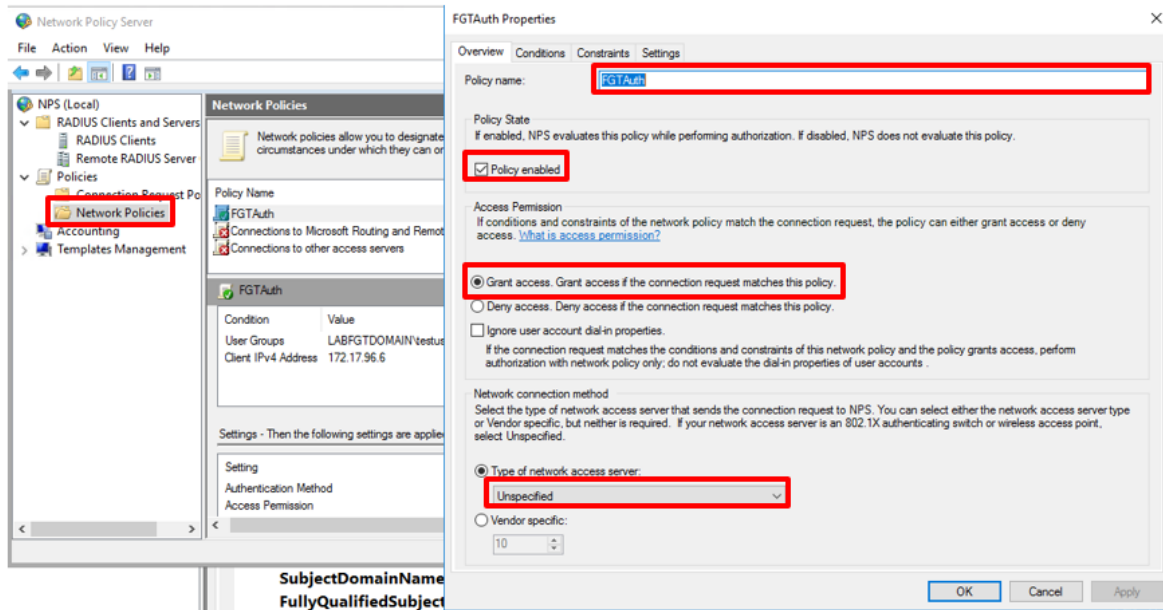
9. Select the *Conditions* tab.
 - a. Select *Add* and then select the *Client IPv4 Address* condition.
 - b. Select *Add* again and enter the IP address of the RADIUS client, which is the IP address of the FortiSwitch unit.
 - c. Enable the NAT to the firewall policy from the FortiLink interface to 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.



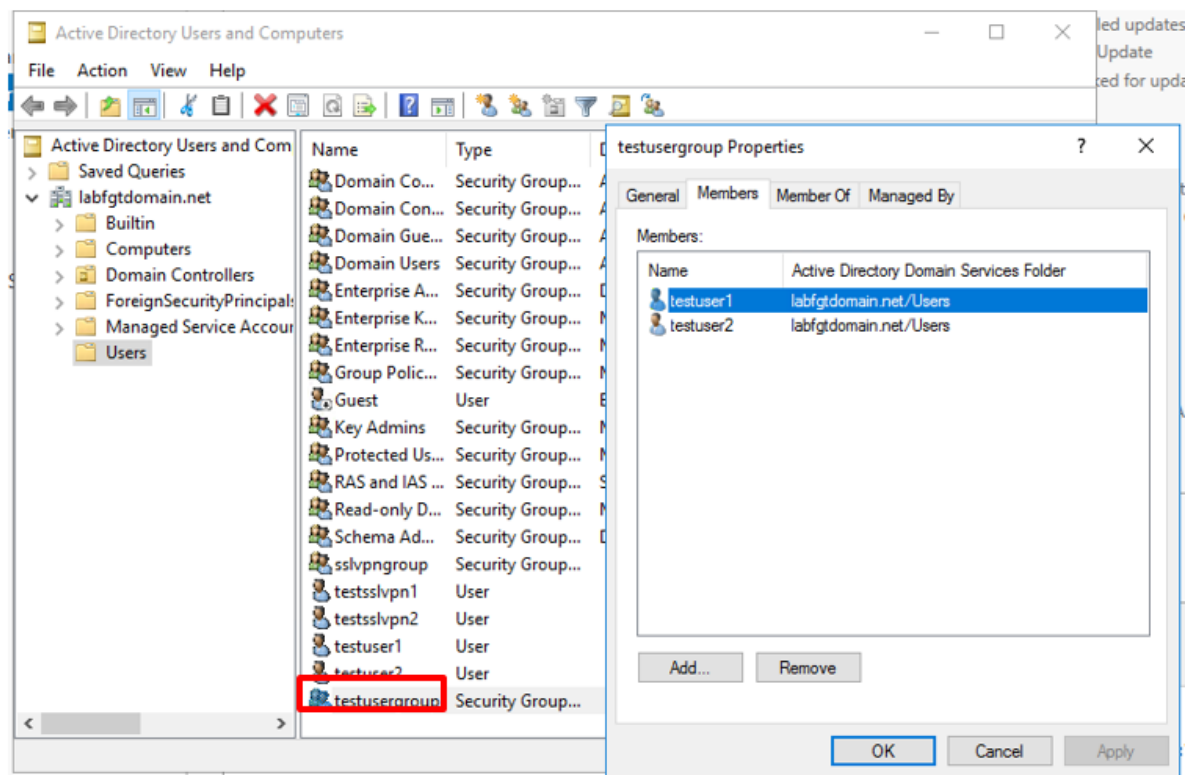
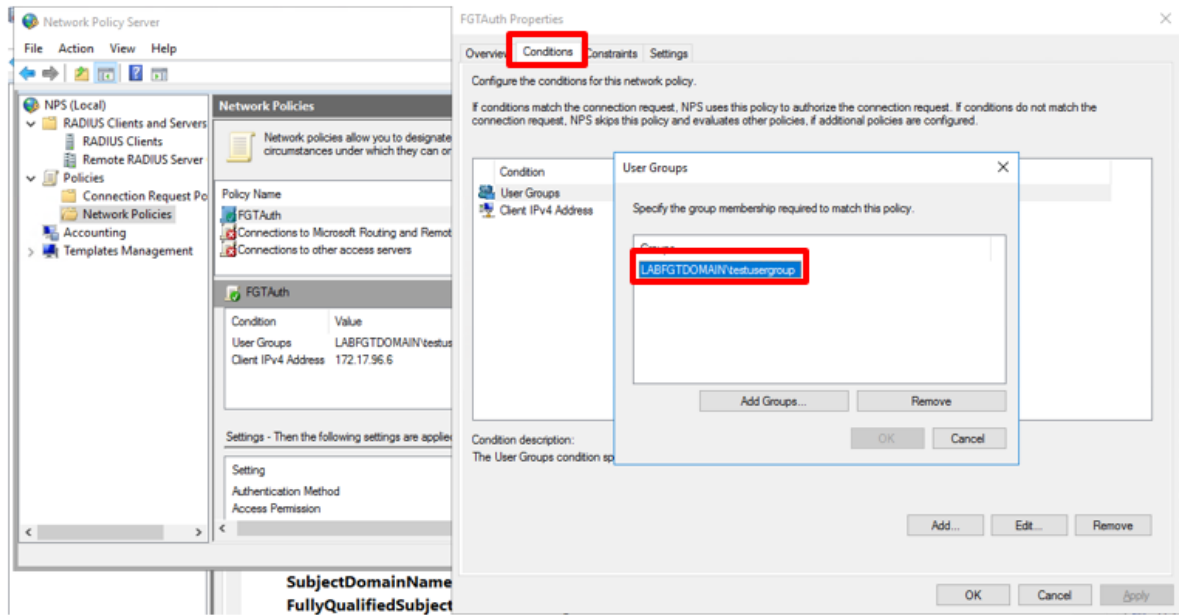
10. Select the *Settings* tab.
 - a. Select *Vendor Specific* and then select *Add*.
 - b. Scroll to the very bottom of the list and select *Vendor-Specific*.
 - c. Select *Add*.



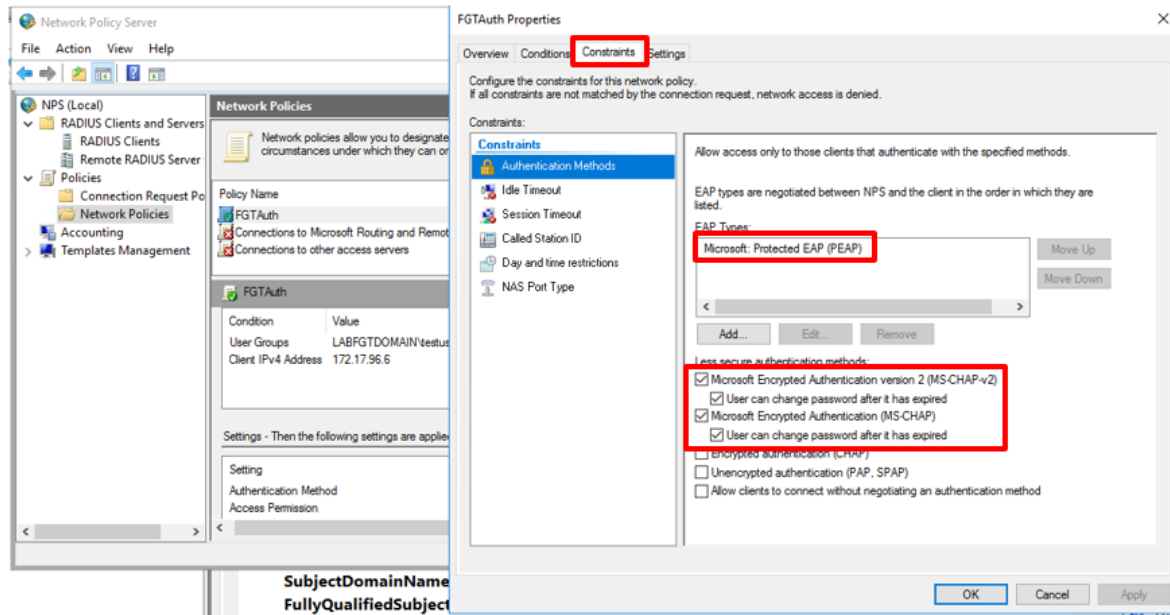
11. Configure a network policy.
 - a. From the Network Policy Server Snap-in, right-click on *Network Policies* and select *New*.
 - b. Enter a name for the policy, such as `FGTAuth`.
 - c. On the Overview tab, make sure that *Policy enabled* checkbox is selected.
 - d. Verify that *Grant access* is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



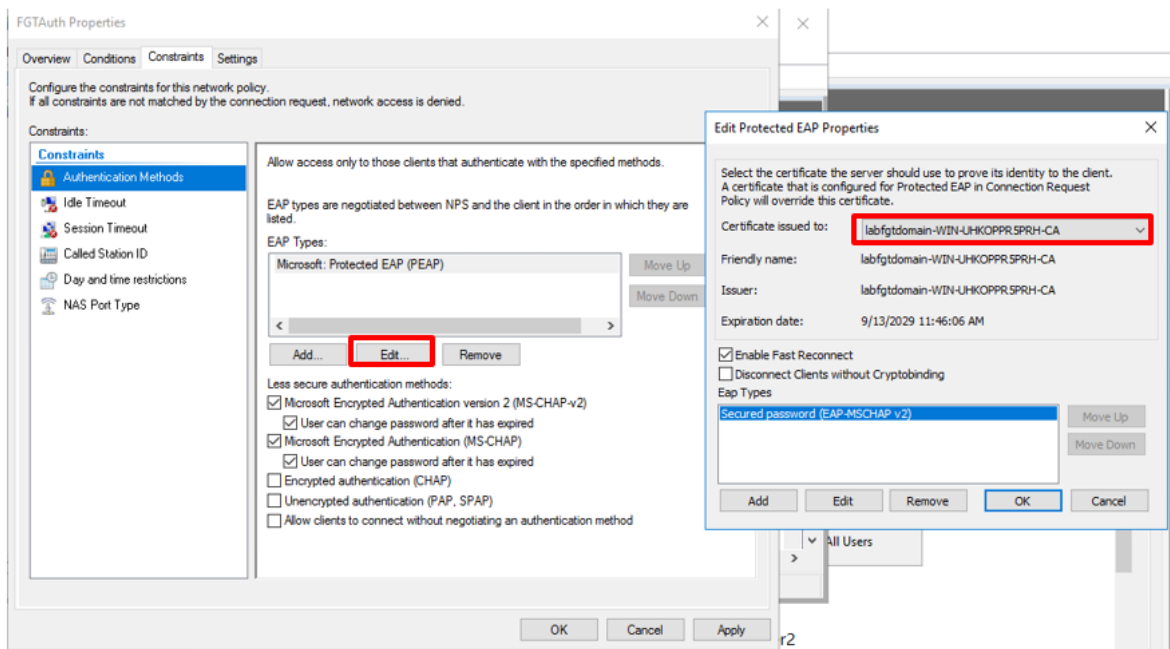
12. Select the Conditions tab.
 - a. Select *Add*.
 - b. Select *Windows Groups* and then select *Add*.
 - c. Select *Add Groups*.
 - d. Enter the name of the group in AD that you want to allow for 802.1x connections.
 - e. Select *OK*.



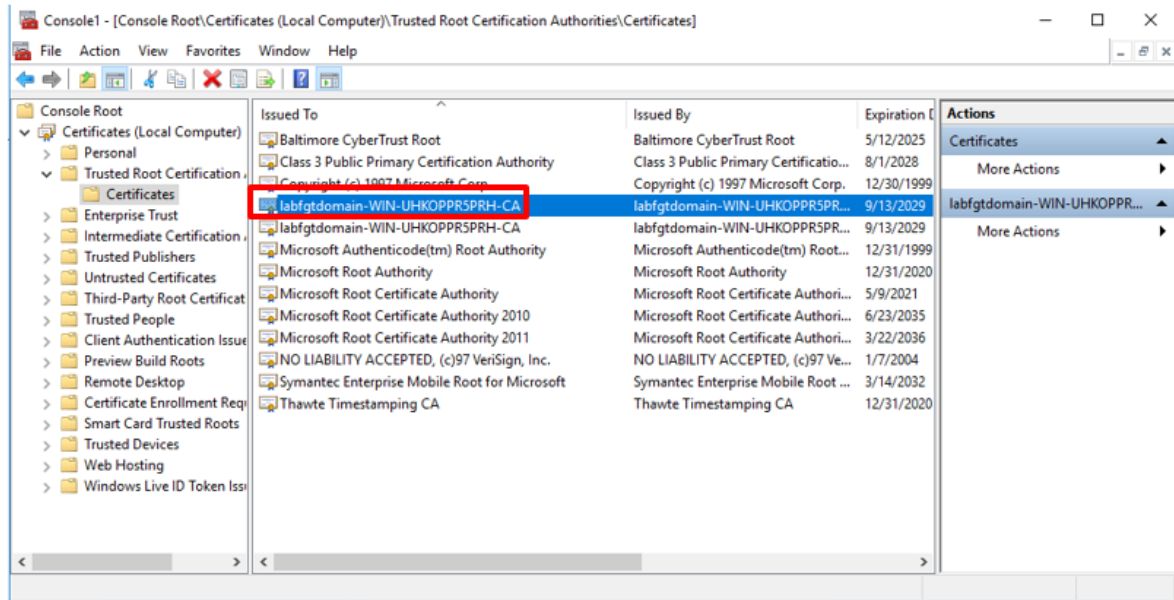
13. In the Constraints tab, verify that the following check boxes are selected, select *Apply*, and then select *OK* to complete the policy.



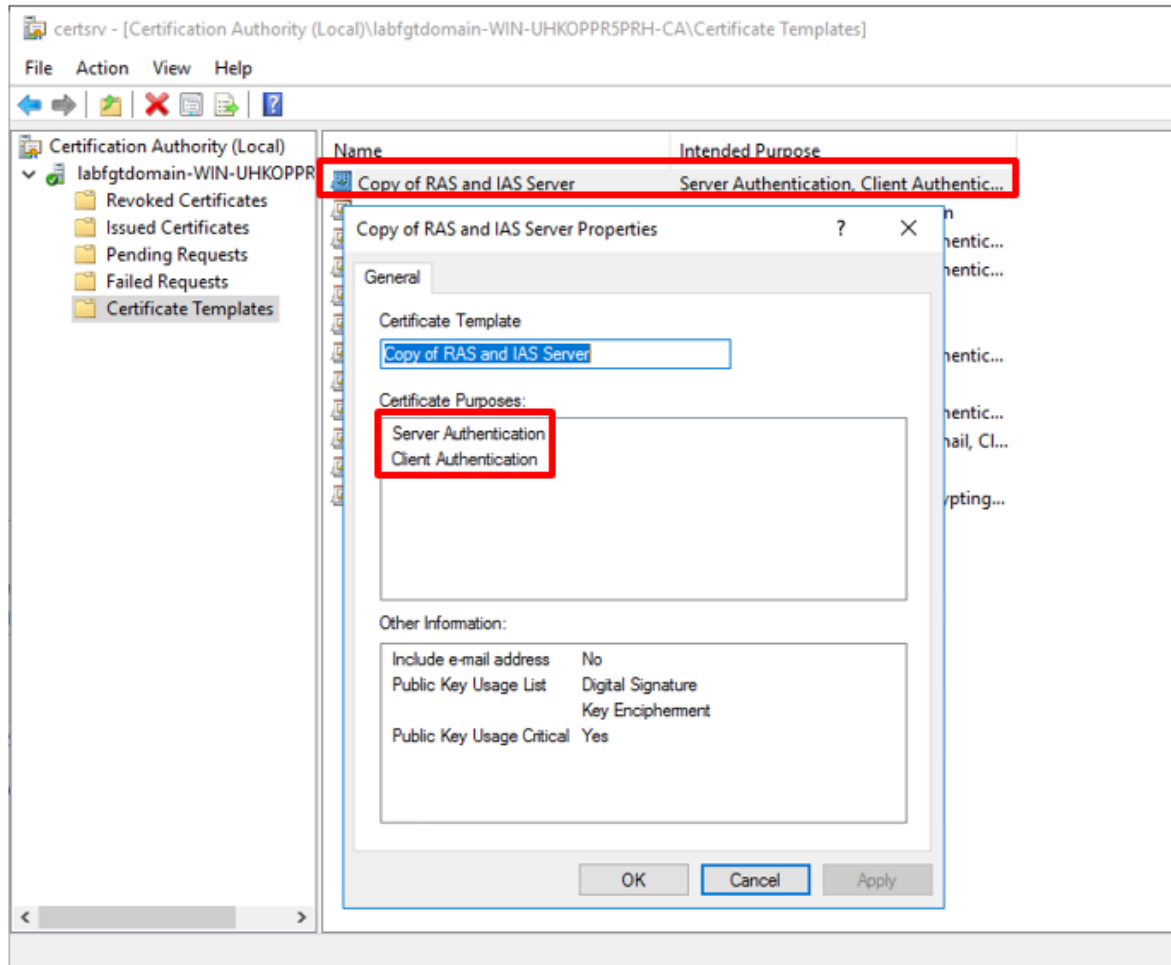
14. To verify the server certificate used by Microsoft Protocol EAP (PEAP), select *Edit*, and then select the certificate for the server to prove its identity to the client.



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



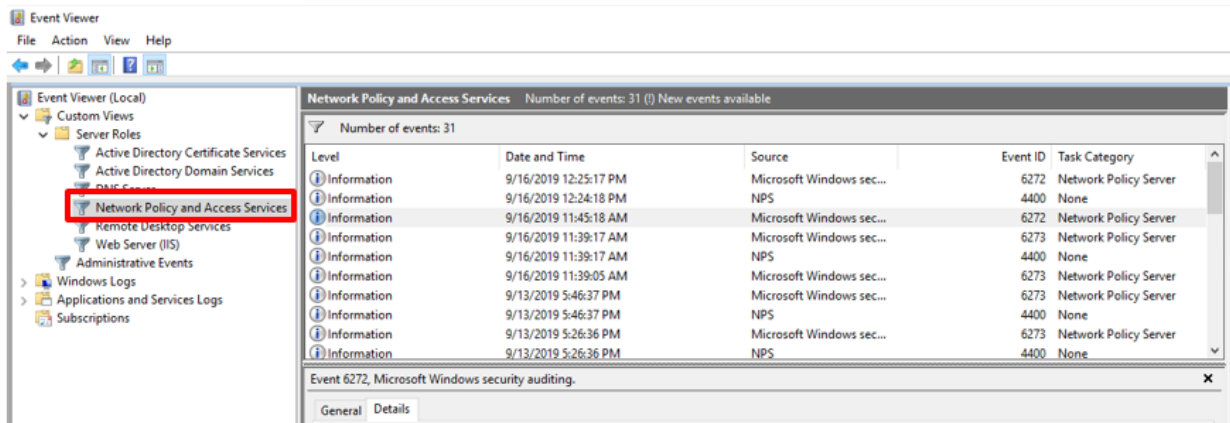
- Under Certification Authority (Local), make certain that the settings match those in the following figure. Otherwise, you will receive an authentication failure with the following reason: "The client could not be authenticated because the Extensible Authentication Protocol (EAP) Type cannot be processed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



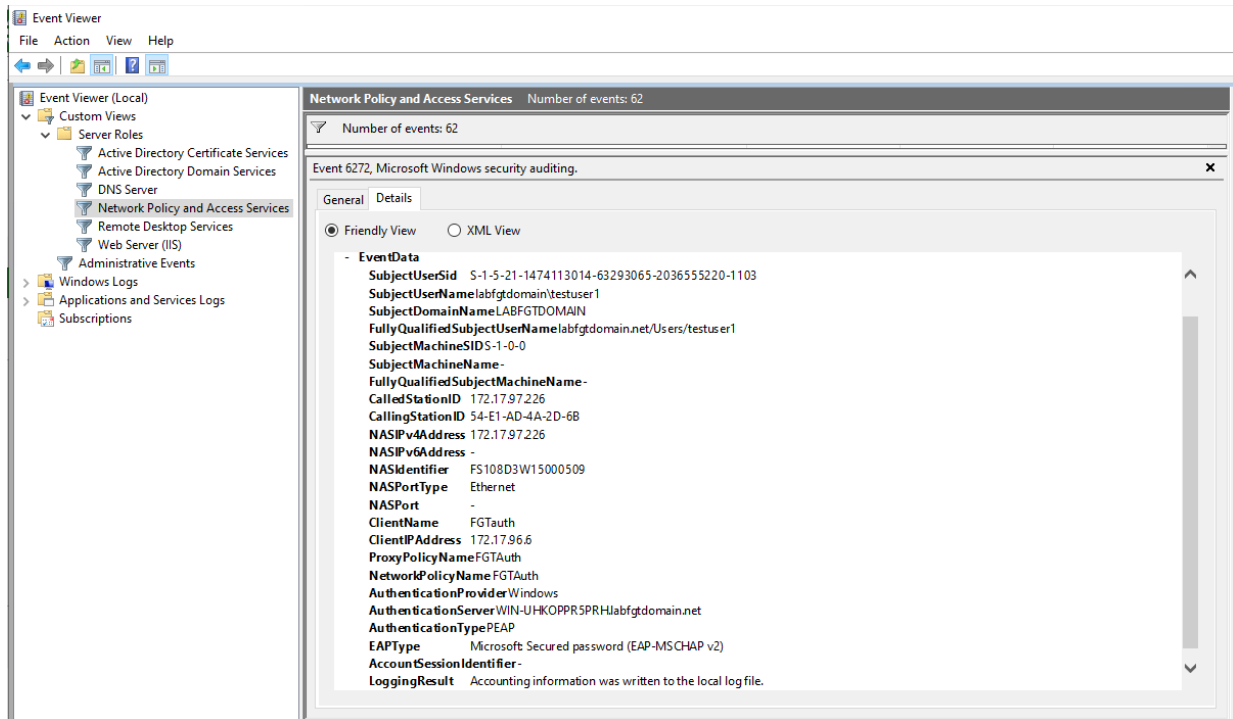
Troubleshooting

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.

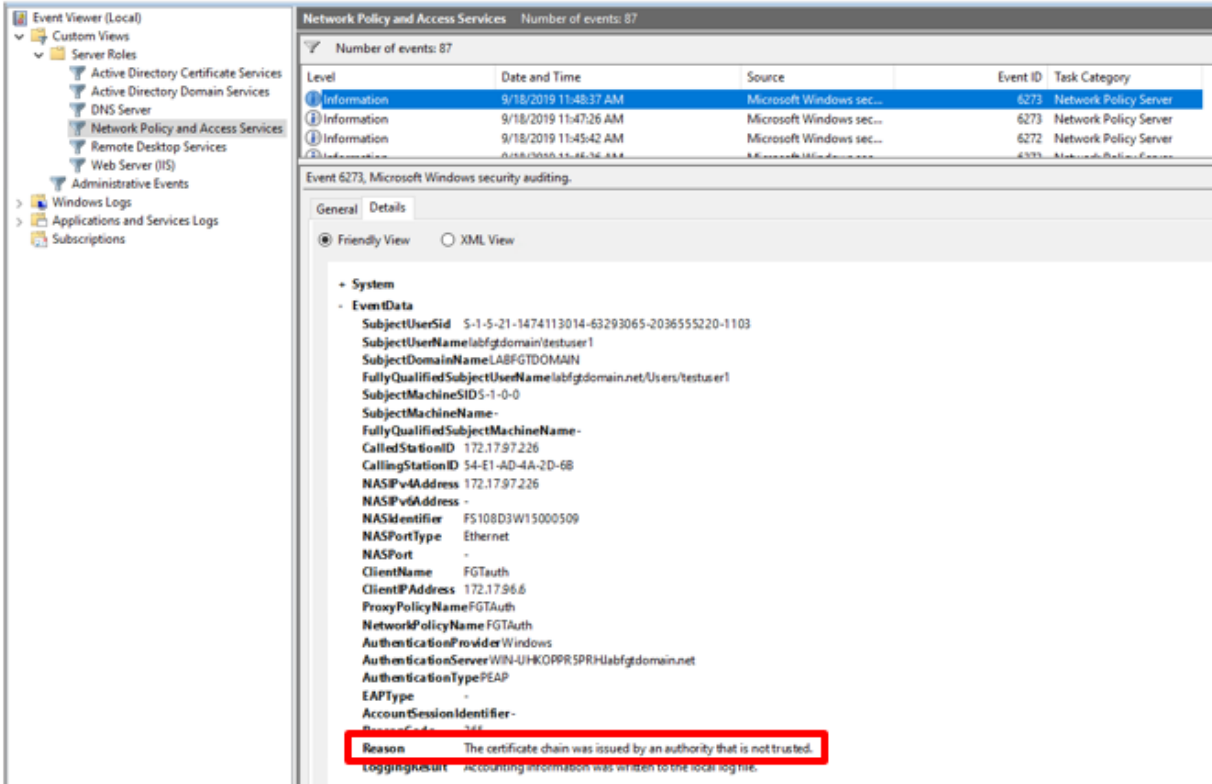
The following figure shows the successful output of an 802.1x connection from the PC:



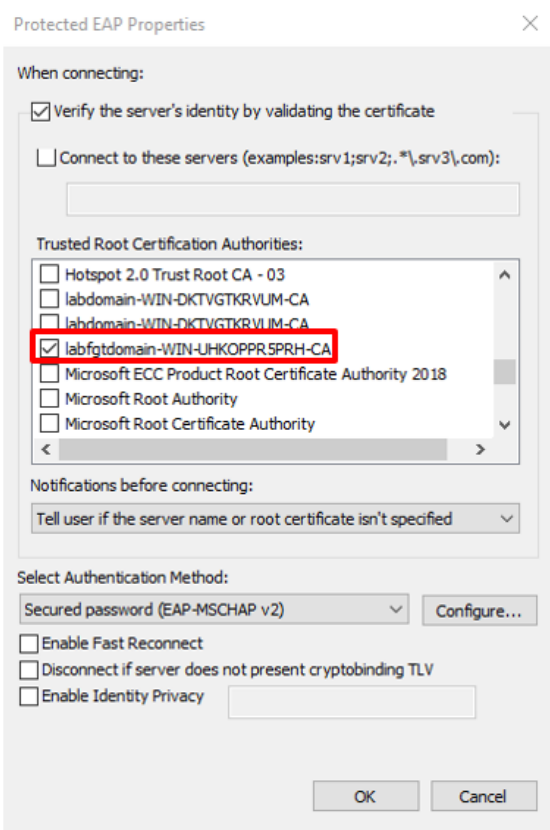
Setting up port-based 802.1x authentication in a FortiLink setup



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

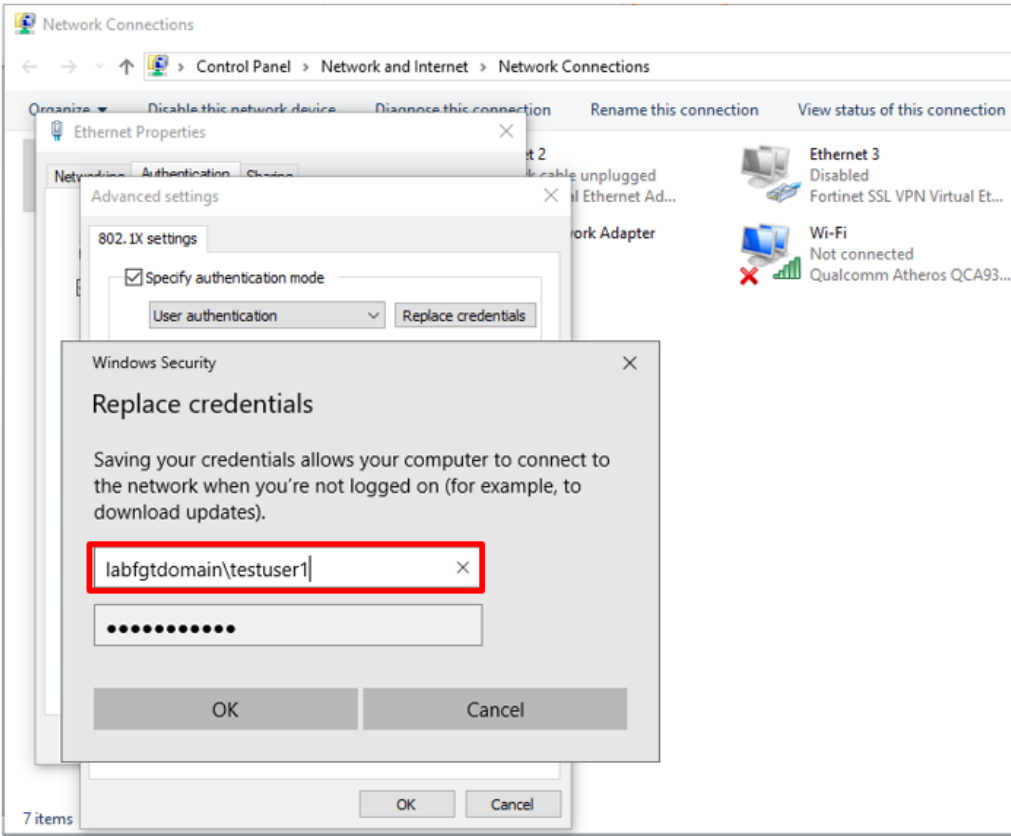
EAPType -

AccountSessionIdentifier -

Reason The specified user account does not exist.

LoggingResult Accounting information was written to the local log file.

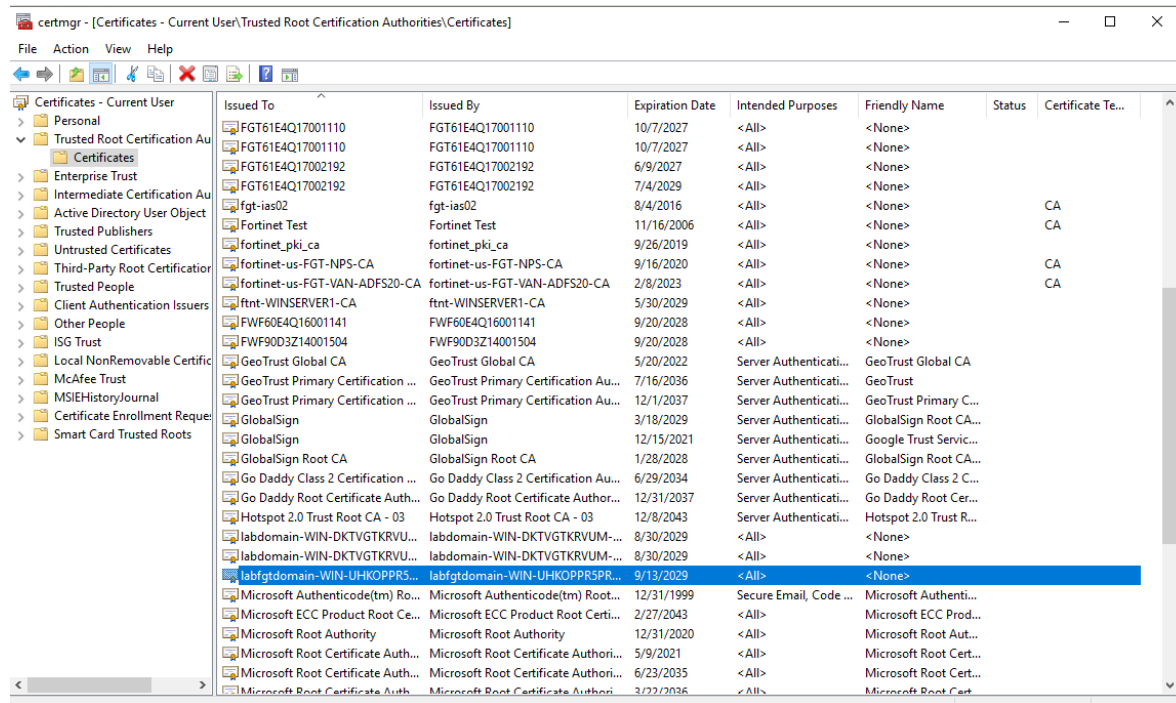
To fix this issue, under *Advanced settings*, you can specify whether you want user authentication, computer authentication, or both.



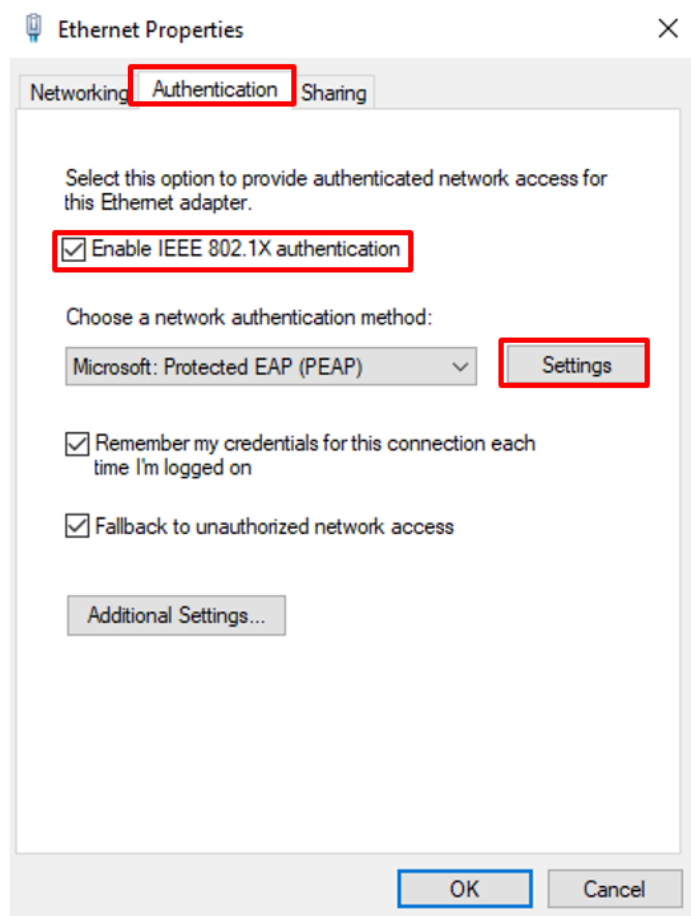
Configuring Windows 10

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

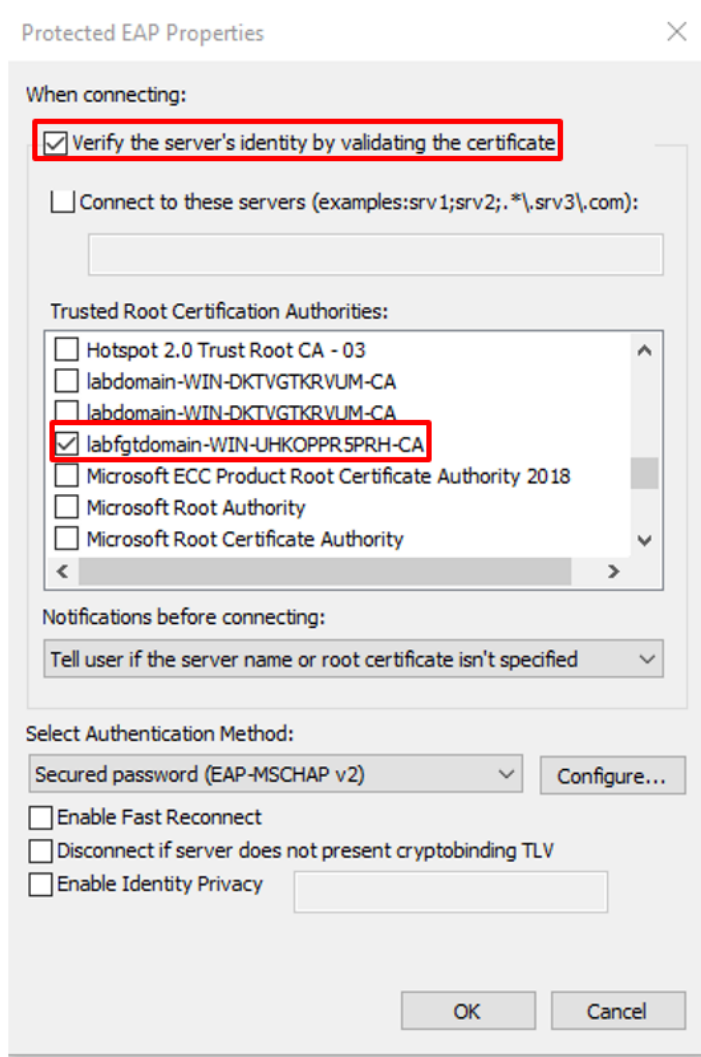
1. Select *Start*, right-click *Computer*, select *Manage*, and then select *Services and Applications*.
2. In the details pane, double-click *Services* and then do one of the following:
 - To configure the startup type, right-click *Wired AutoConfig*, and then select *Properties*. In *Startup type*, 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:



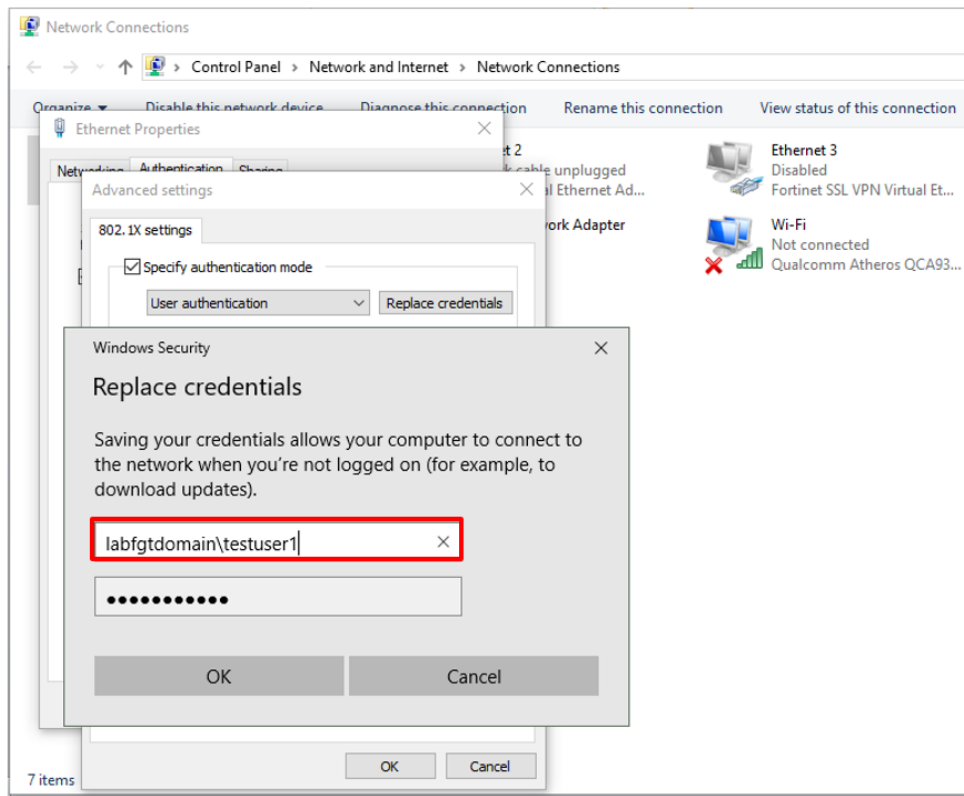
4. In the properties of the network connection, navigate to the Authentication tab, and make sure the *Enable IEEE 802.1X authentication* check box is selected.
5. Select *Settings*.



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

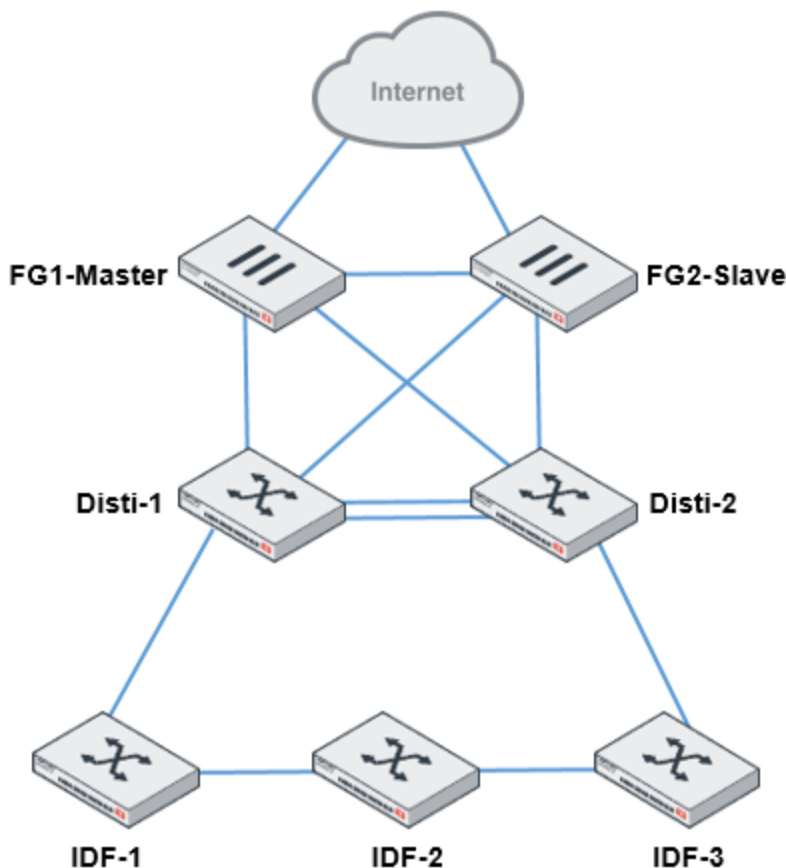
9. To verify that the PC successfully connects, check the network connections. Look for the Ethernet port and make sure that there is no "Authentication failed" message.
10. When the authentication succeeds, you should get an IP address from the right VLAN, as shown in the following figure:

```
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 MCLAG (multichassis LAG).

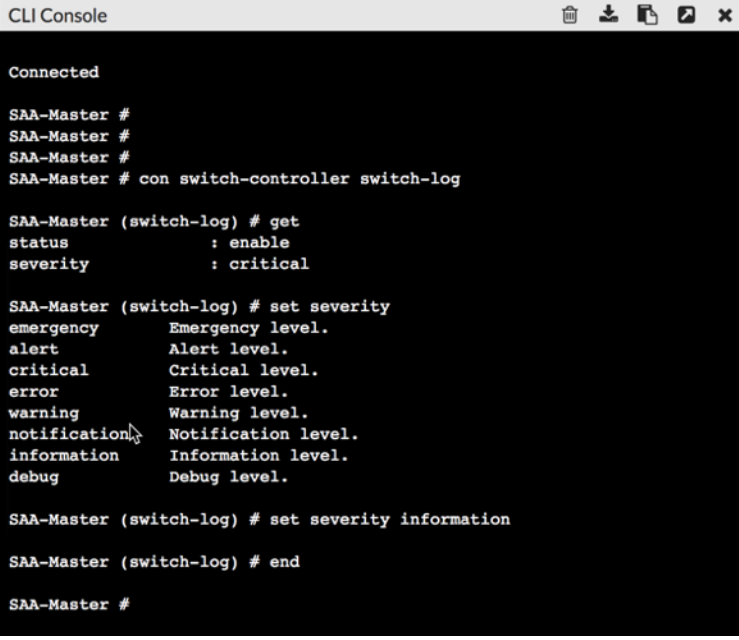
The FortiGates, for the exercise, are under FortiOS 6.0.1 and FortiSwitch at 6.0 or 3.6.6 (depending on platform compatibility). FortiSwitch must be at least at 3.6.4 in order to deploy MCLAG with access ring.

Also ensure that the FortiSwitch models used for MCLAG 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

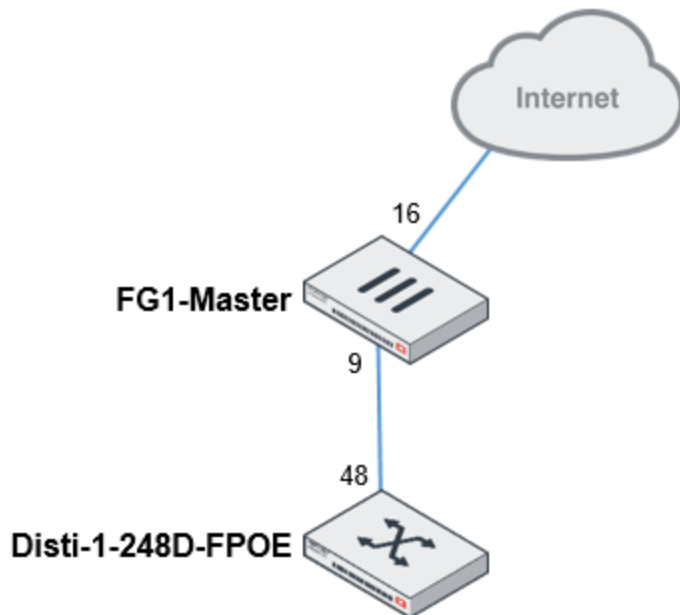
SAA-Master #
```

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 navigation menu with categories like Favorites, Dashboard, Security Fabric, FortiView, Network, Interfaces, 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 'Network' category is expanded, and the 'Interfaces' sub-category is selected. The main content area 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), Address (Addressing mode: Manual, DHCP, Dedicated to FortiSwitch; IP/Network Mask: 192.168.169.1/24; Connected Devices: None; Automatically authorize devices: off; FortiLink split interface: on), Status, and Comments (empty).

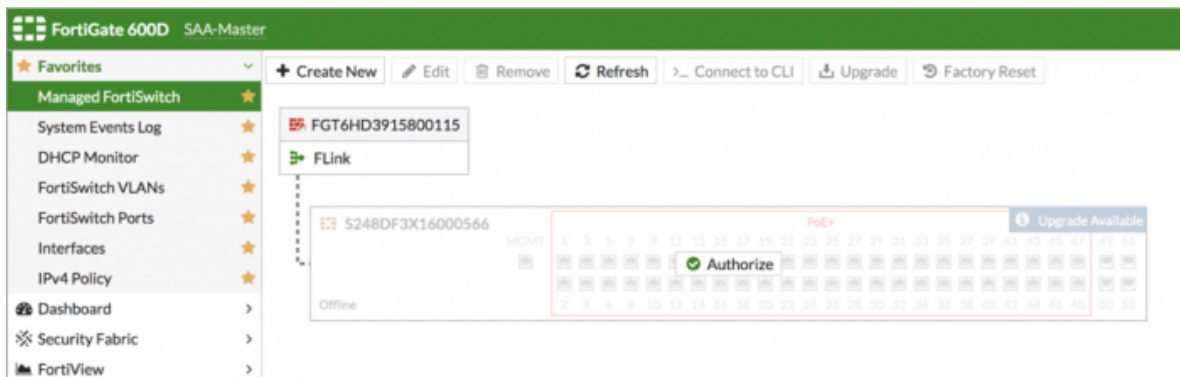
7. Connect the FG1-Master to Dist1-1 (port9 to port48).



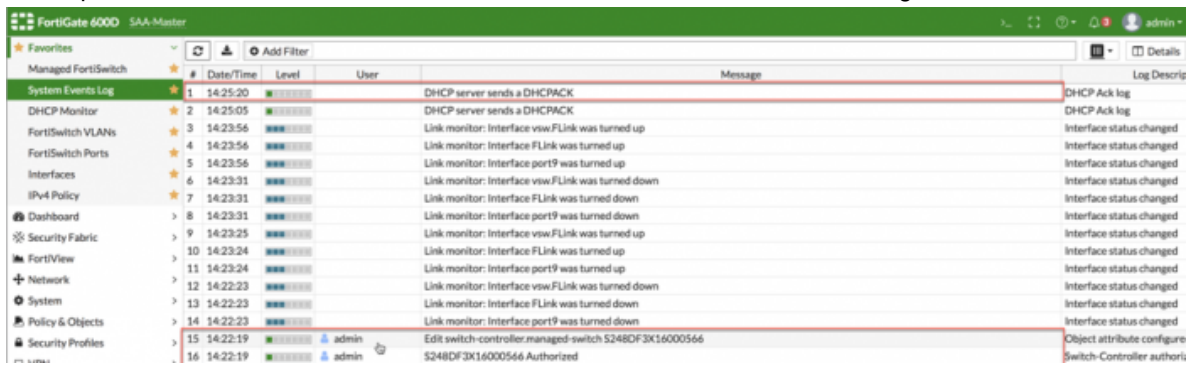
8. Confirm the discovery of the FortiSwitch unit in the logs.



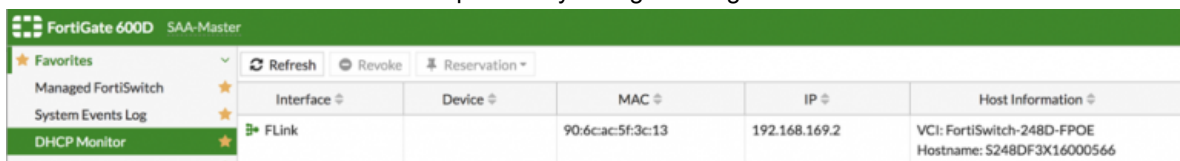
9. Authorize the Dist1-1 thereafter.



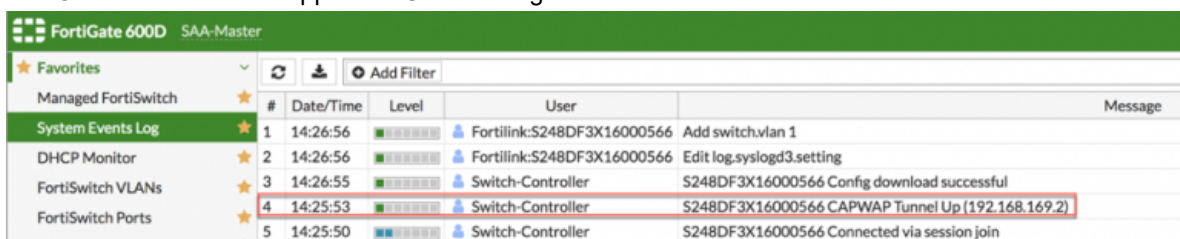
10. At this point, the switch will reboot and will be converted from standalone to managed mode.



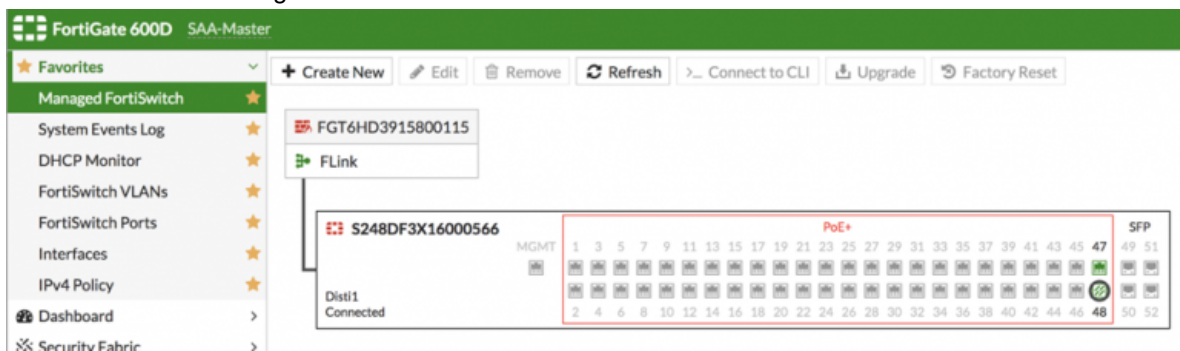
11. The switch receives an IP address in the previously configured segment.



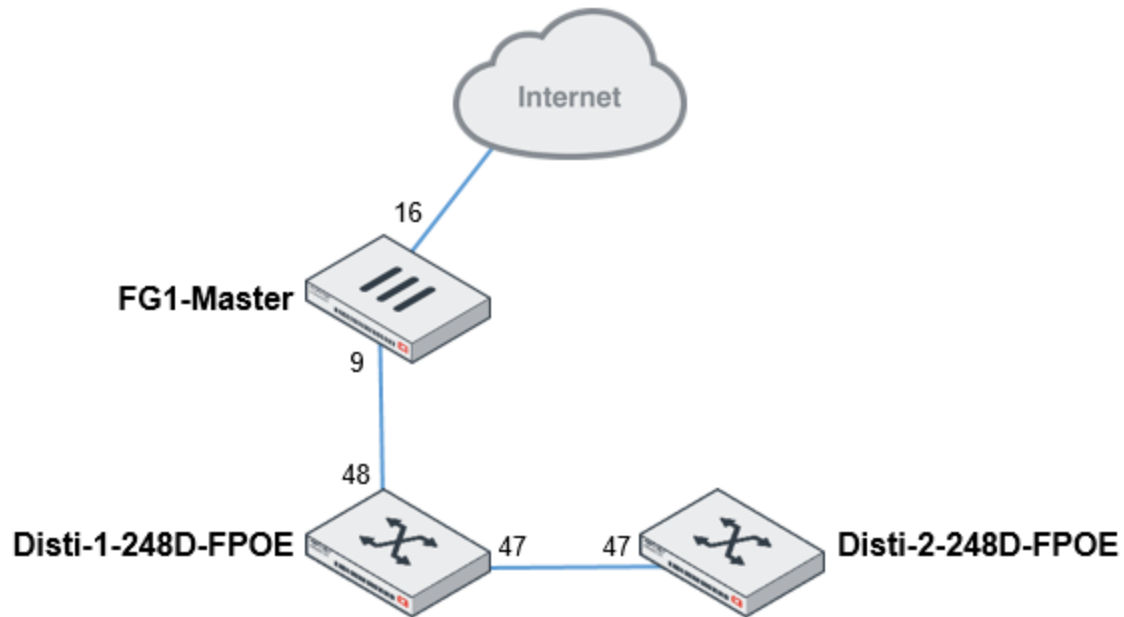
12. The CAPWAP tunnel will appear as UP in the logs.



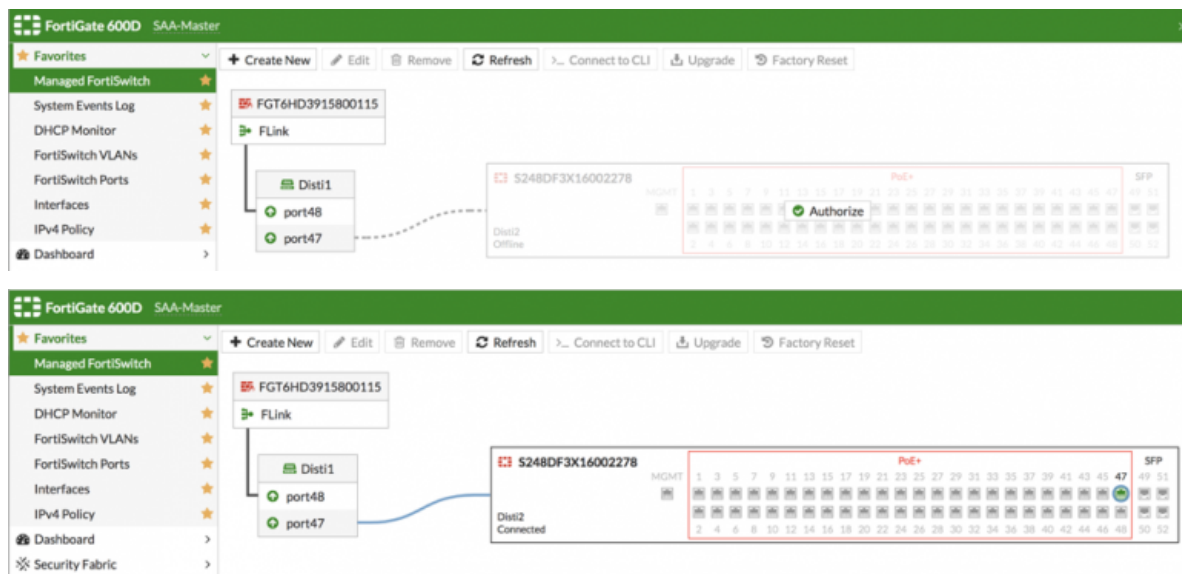
13. Dist1-1 will now be managed.



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	*****	FortiLink:S248DF3X16002278	MCLAG: ICL ACL change ingress-port-bitmap=0x1fffffffffff, egress-block-port-bitmap=0x1fffffffffff
DHCP Monitor	2	14:43:15	*****	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
__FortiLink0__

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 BDF3X16002278-0	

- 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

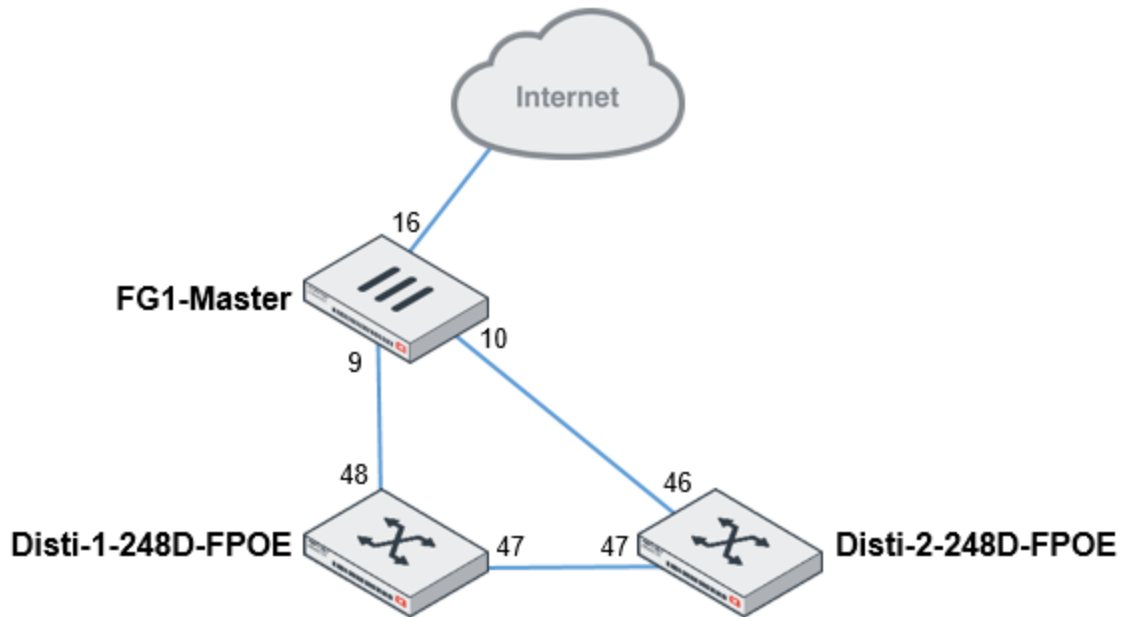
Enabled

Disabled

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

FortiSwitch Cookbook
Fortinet, Inc.

37



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

FortiSwitch S248DF3X16000566

MGMT

PoE+

SFP

Disti1 Connected

FortiSwitch 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
-----
S248DF3X16002278-0*  OK          UP          OK          port47
__FortiLink0__      OK          UP          OK          port48

Managed Switch : S248DF3X16002278  0

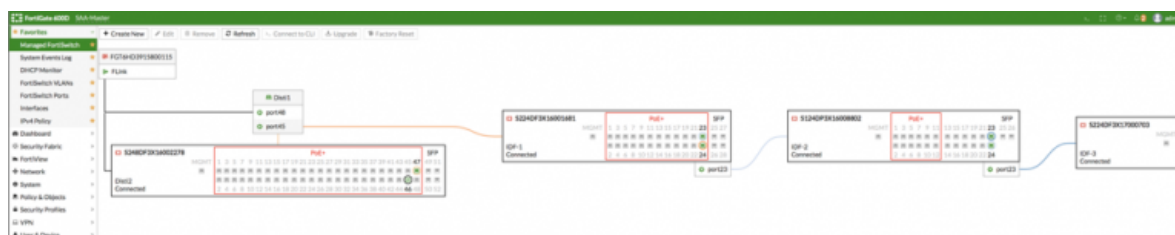
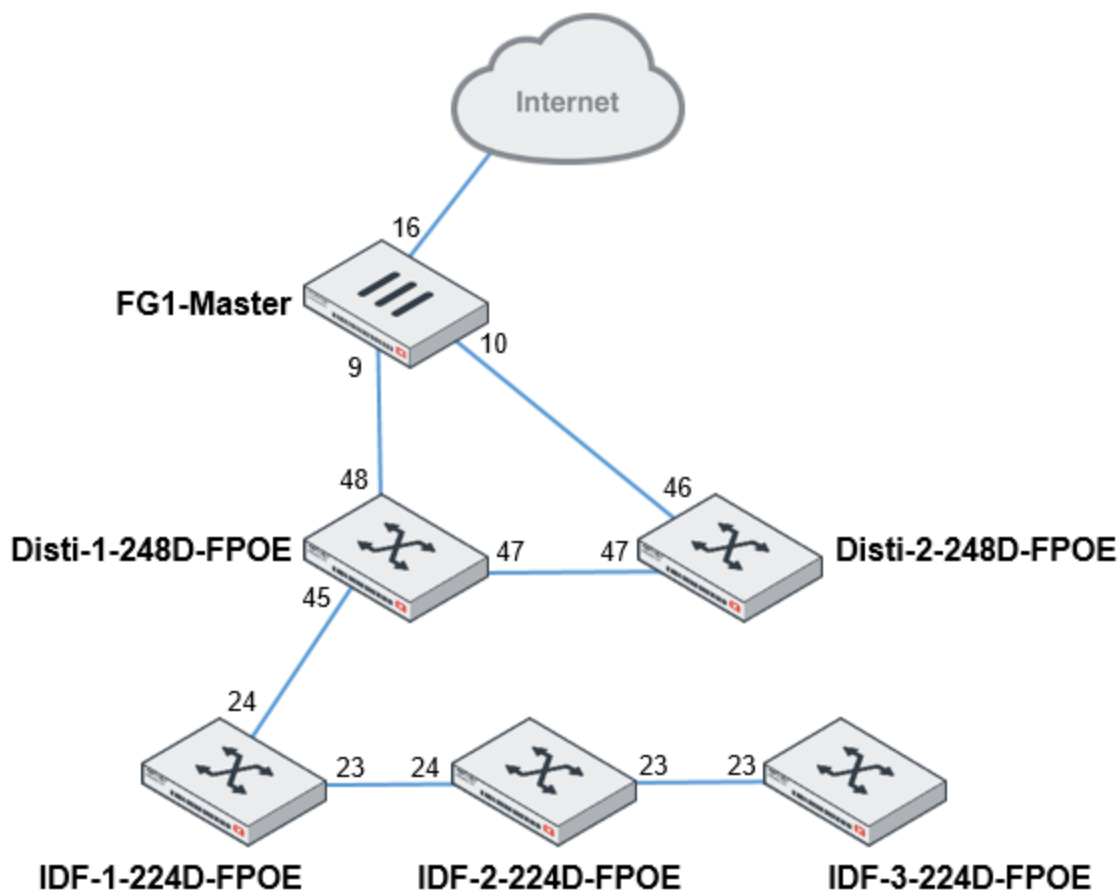
Running diagnostic, it may take sometime...

mclag-trunk-name  peer-config lacp-state  stp-state  local-ports
-----
S248DF3X16000566-0*  OK          UP          OK          port47
__FortiLink0__      OK          UP          OK          port46
  
```

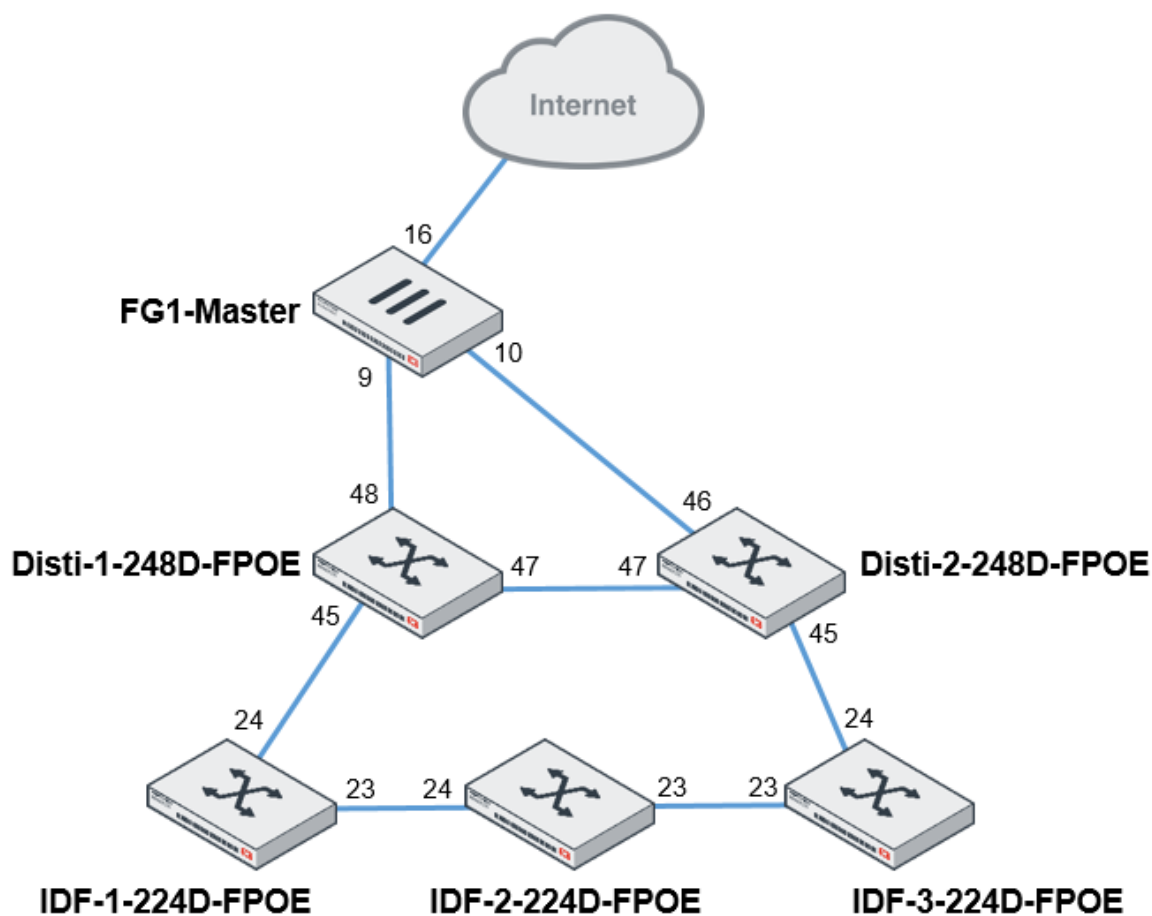
10. Several other commands allow you to diagnose the feature:
- On FortiGate: `diagnose netlinkaggregate name fortilink`
 - On FortiSwitch Disti: `diagnose switch trunk list __FoRtI1LiNk0__`
 - On FortiSwitch Disti: `diagnose switch mclag list __FoRtI1LiNk0__`
 - On FortiSwitch Disti: `diagnose switch mclag icl`

IDF configuration

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

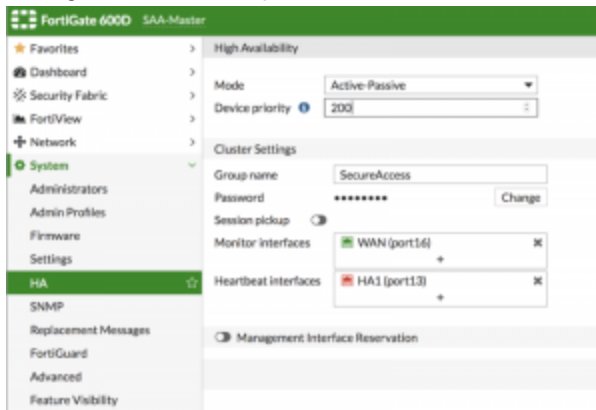


- 2.** All that remains is to connect the IDF-3 to the Distri-2.



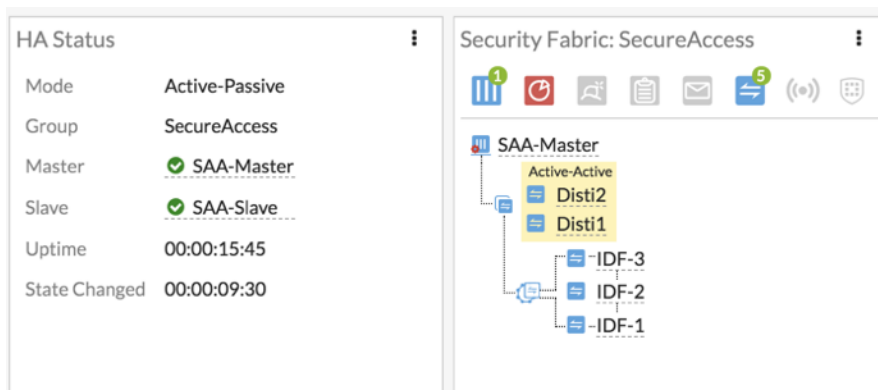
HA configuration

1. Configure HA in active-passive mode.

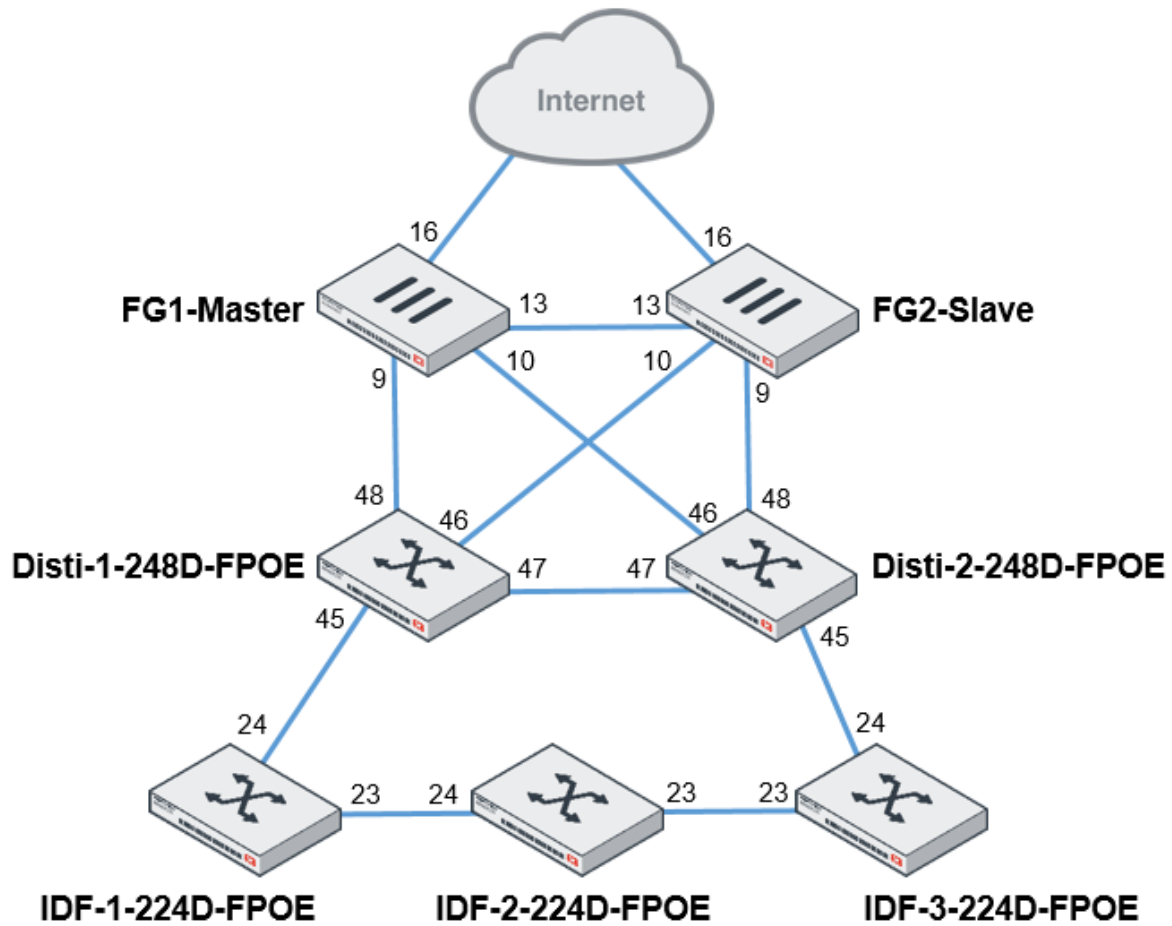


2. Make sure the configuration is well synchronized

Synchronized	Priority	Hostname	Serial No.	Role	Uptime	Sessions	Throughput	Checksum
FortiGate 6000	200	SAA-Master	FGT6HD3915800115	Master	1h 15m 57s	152	102.00 kbps	dc8b6e54e3ad771fcdceef39445121446
FortiGate 6000	100	SAA-Slave	FGT6HD3915800031	Slave	11m 10s	106	85.00 kbps	dc8b6e54e3ad771fcdceef39445121446



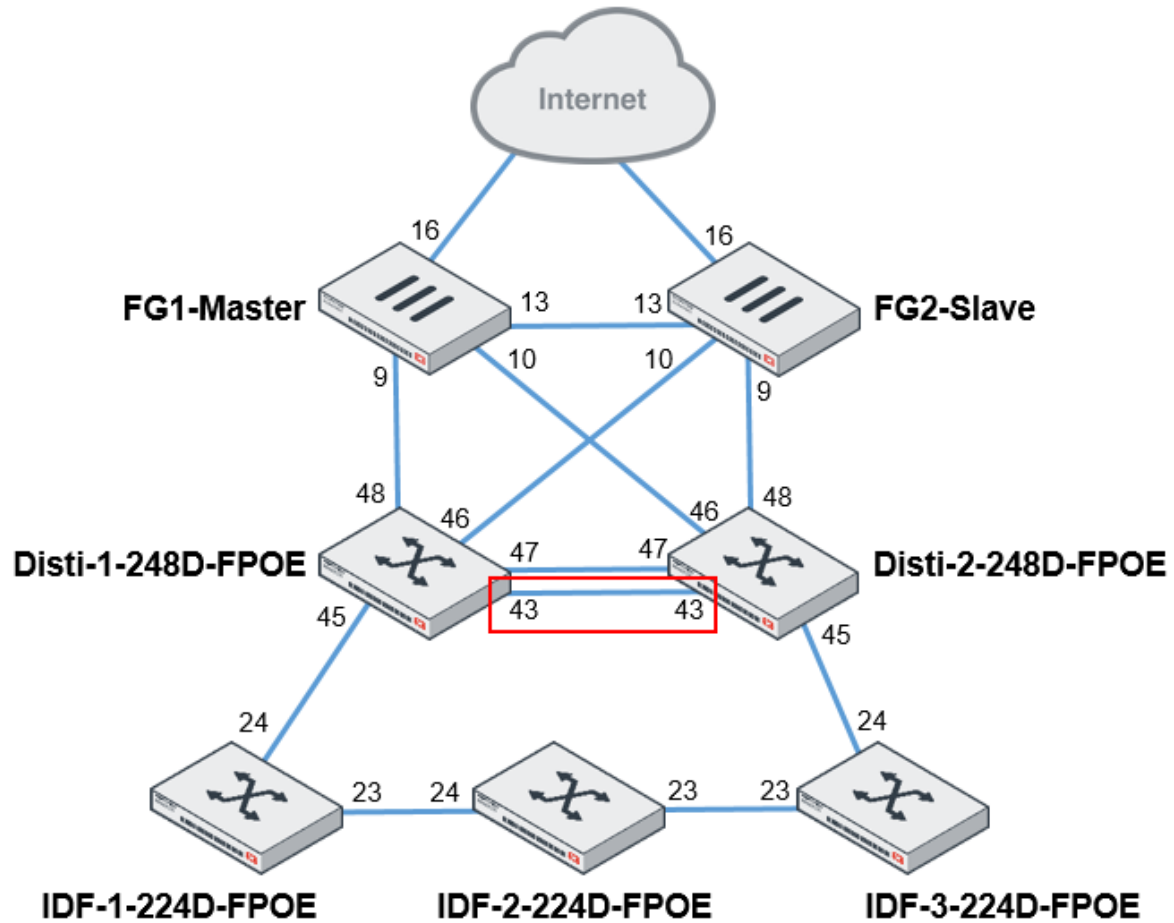
3. Connect the balance of the links in order to coherently replicate the wiring of the FortiGate Master and FortiGate Slave, as follows:



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	Edit Delete Search
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	>		

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		FGT6HD3P15800001
port47		S248DF3K16002278
port48		FGT6HD3P15800115

```
Distil #
Distil # config switch trunk

Distil (trunk) # edit 8DF3X16002278-0

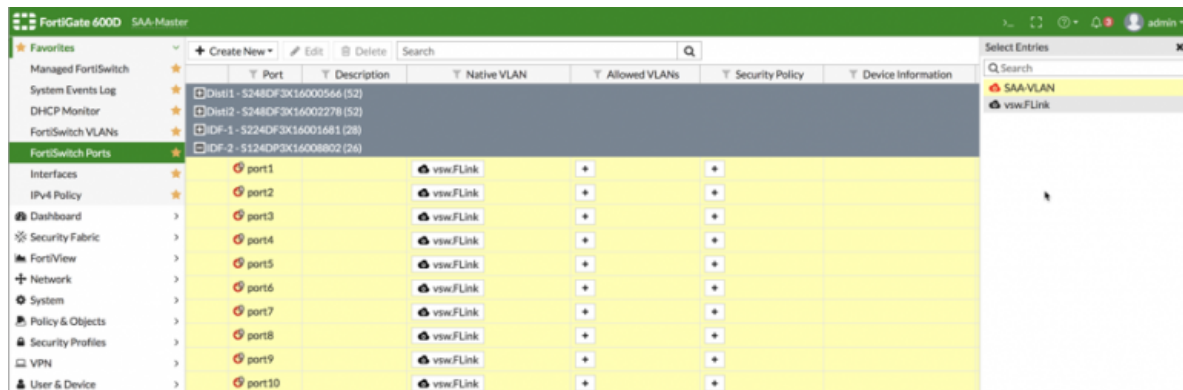
Distil (8DF3X16002278-0) # sho
config switch trunk
    edit "8DF3X16002278-0"
        set mode lacp-active
        set auto-isl 1
        set mclag-icl enable
        set members "port47" "port43"
    next
end

Distil (8DF3X16002278-0) #
```

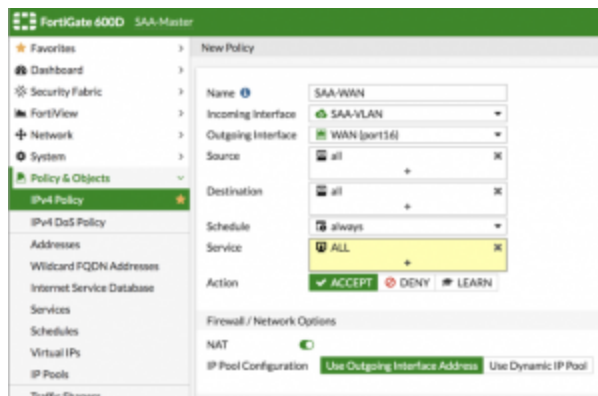
Validation

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: Interface Name (SAA-VLAN), Alias (empty), Type (VLAN), Interface (FLink), VLAN ID (15), and Color (Change). The 'Tags' section shows a role of 'LAN' and an 'Add Tag Category' button. The 'Address' section shows 'Addressing mode' set to 'Manual' and 'IPv4 Network Mask' set to '10.15.15.1/24'. The 'Administrative Access' section shows various protocols checked, including IPv4, HTTPS, HTTP, CAPWAP, SSH, RADIUS Accounting, PING, SNMP, FortiTelemetry, FPMG Access, and FTM. The 'DHCP Server' section is also visible, showing an 'Address Range' configuration with 'Starting IP' 10.15.15.2 and 'End IP' 10.15.15.254, and a 'Netmask' of 255.255.255.0. The 'Default Gateway' is set to 'Same as Interface IP' and the 'DNS Server' is set to 'Same as System DNS'.



2. Allow access to the Internet.



3. You should be able to reboot the FortiGate-Master, remove some links (Dist1 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:

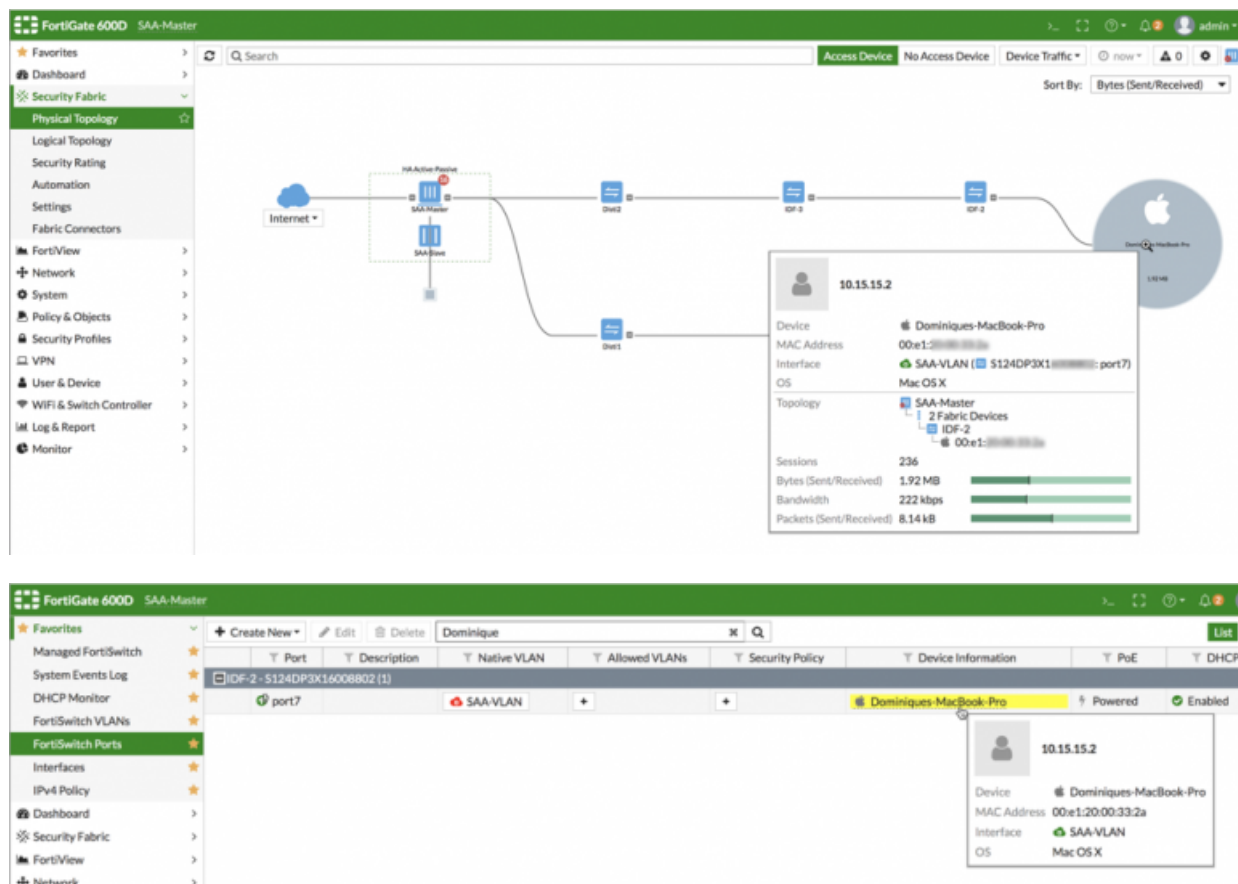
```

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:



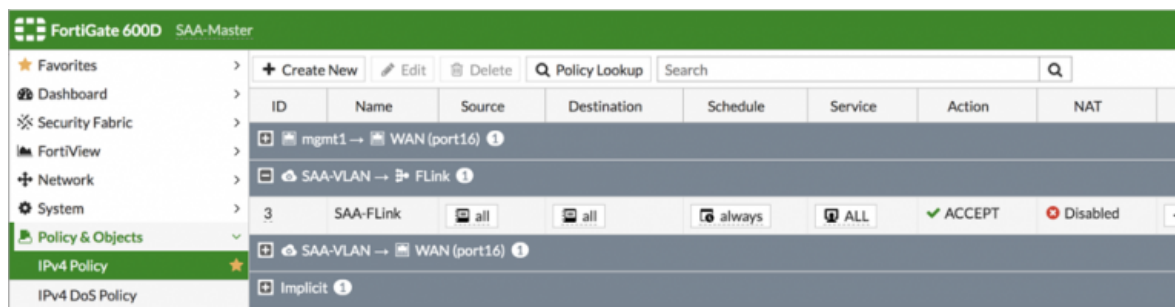
Bonus—FortiSwitch access

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

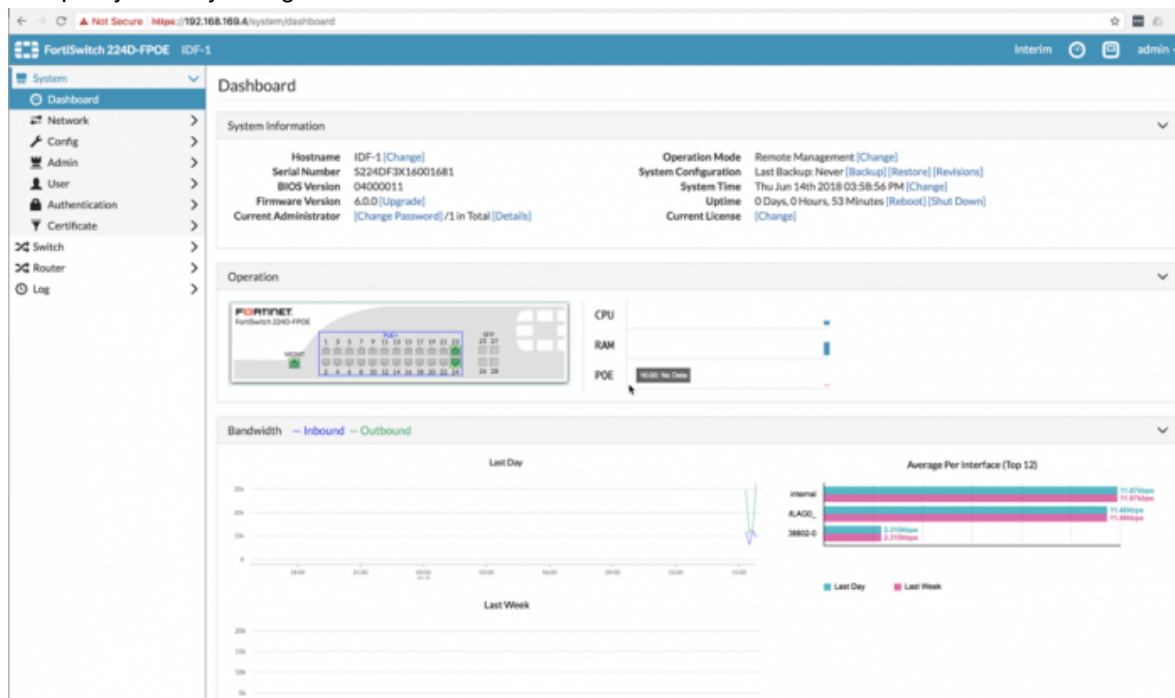
```
SAA-Master # config firewall policy
SAA-Master (policy) # edit 0
new entry '0' added

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.



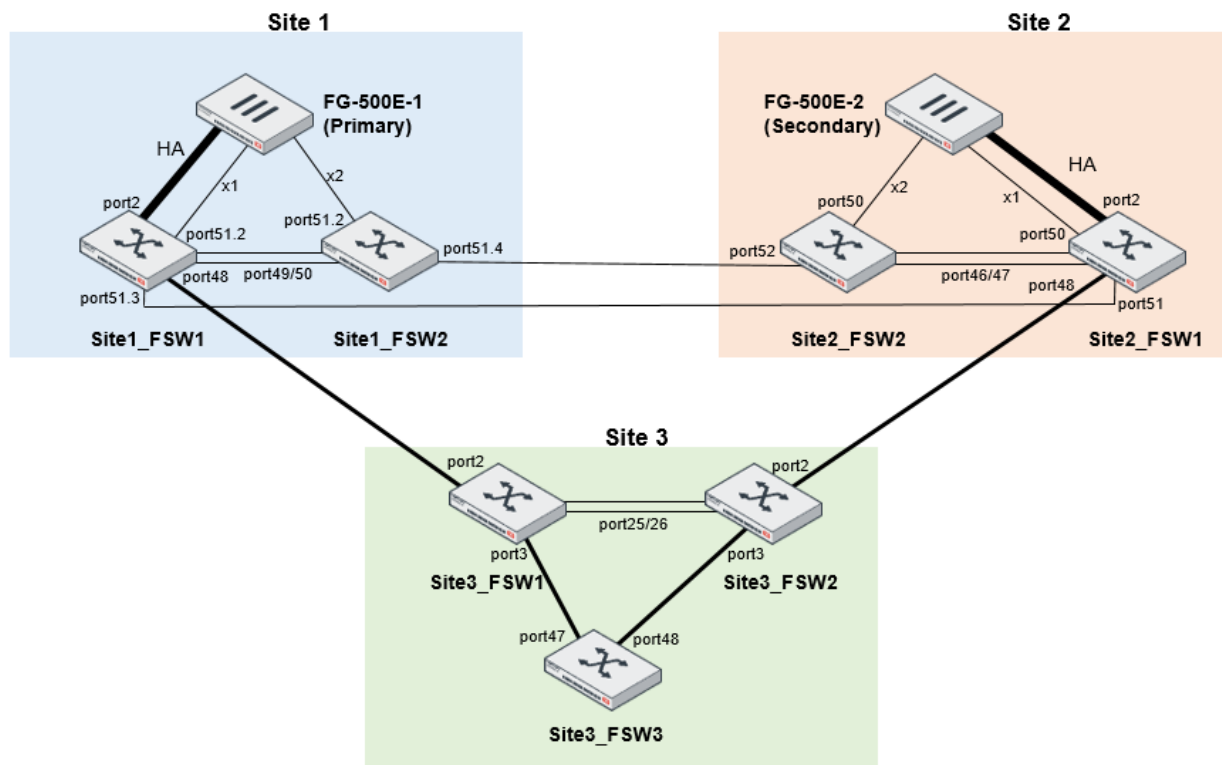
3. This policy allows you to get access to the FortiSwitch unit.



4. The hardware configuration is as follows:



Interconnecting three sites with MCLAG



This cookbook article describes how to add a third site that interconnects a third MCLAG peer group with the existing redundancy between two sites. The links between sites 1 and 3 and sites 2 and 3 are independent; therefore, loops are avoided by using the Spanning Tree Protocol (STP).

The following tasks are covered:

1. [Adding the third site on page 49](#)
2. [Checking the topology on page 52](#)
3. [Relevant configuration on page 53](#)

This cookbook article assumes that sites 1 and 2 are already deployed. See the “HA-mode FortiGate units in remote sites” section in the *FortiSwitch Managed by FortiOS 6.4* guide.

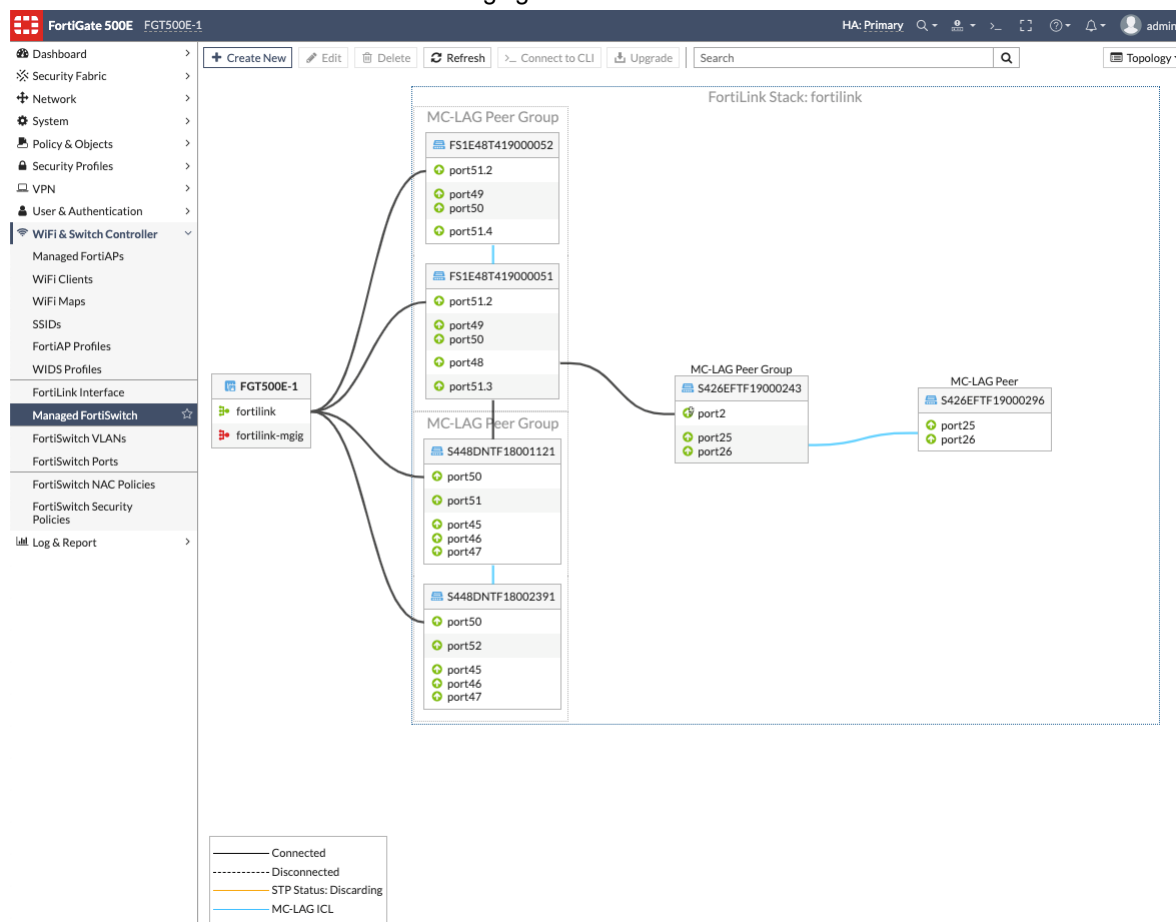
You can refer to the following topics for more information:

- [HA-mode FortiGate units in remote sites](#)
- [FortiSwitch Managed by FortiOS 6.4](#)
- [MCLAG topologies](#)

Adding the third site

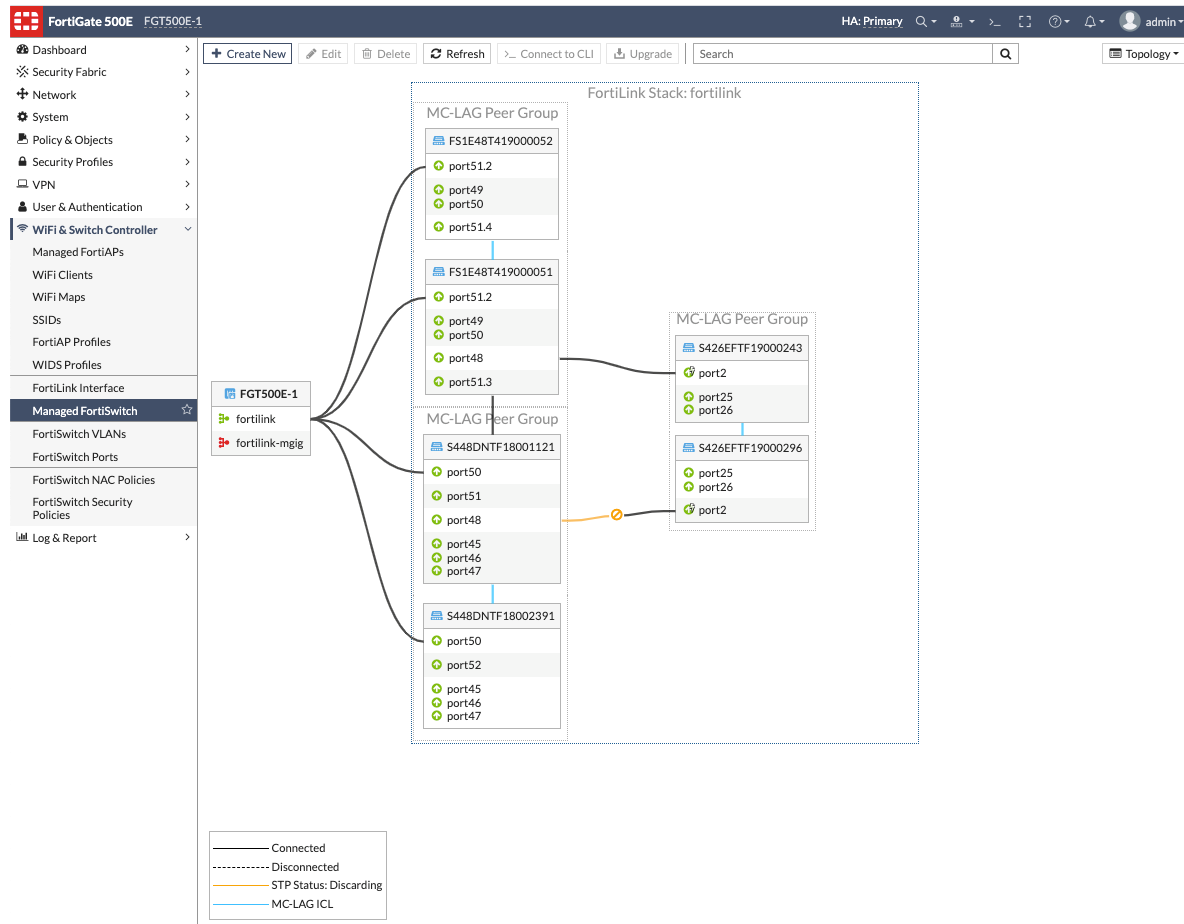
Perform the following steps on the primary FortiGate device:

1. Connect to the Site1_FSW1 and Site2_FSW1 CLI and use the `config switch auto-isl-port-group` command to group the ports going to site 3. See the “MCLAG topologies” section in the *FortiSwitch Managed by FortiOS 6.4* guide.
2. Connect the MCLAG peer switches Site3_FSW1 and Site3_FSW2 to site 1 only and authorize the two switches on the FortiGate device.
3. Connect to the Site3_FSW2 CLI and use the `config switch auto-isl-port-group` command to group the ports going to site 2. See the “MCLAG topologies” section in the *FortiSwitch Managed by FortiOS 6.4* guide.
4. Connect to the Site3_FSW1 CLI and use the `config switch auto-isl-port-group` command to group the ports going to site 1. The group name must be different than the one in the previous step. See the “MCLAG topologies” section in the *FortiSwitch Managed by FortiOS 6.4* guide.
5. In the primary FortiGate CLI, set the LLDP profile to `default-auto-mclag-icl` on the ports used for the MCLAG ICL in the Site3_FSW1 and Site3_FSW2 switches. Wait until the MCLAG peer group is formed between the two switches. See the following figure.

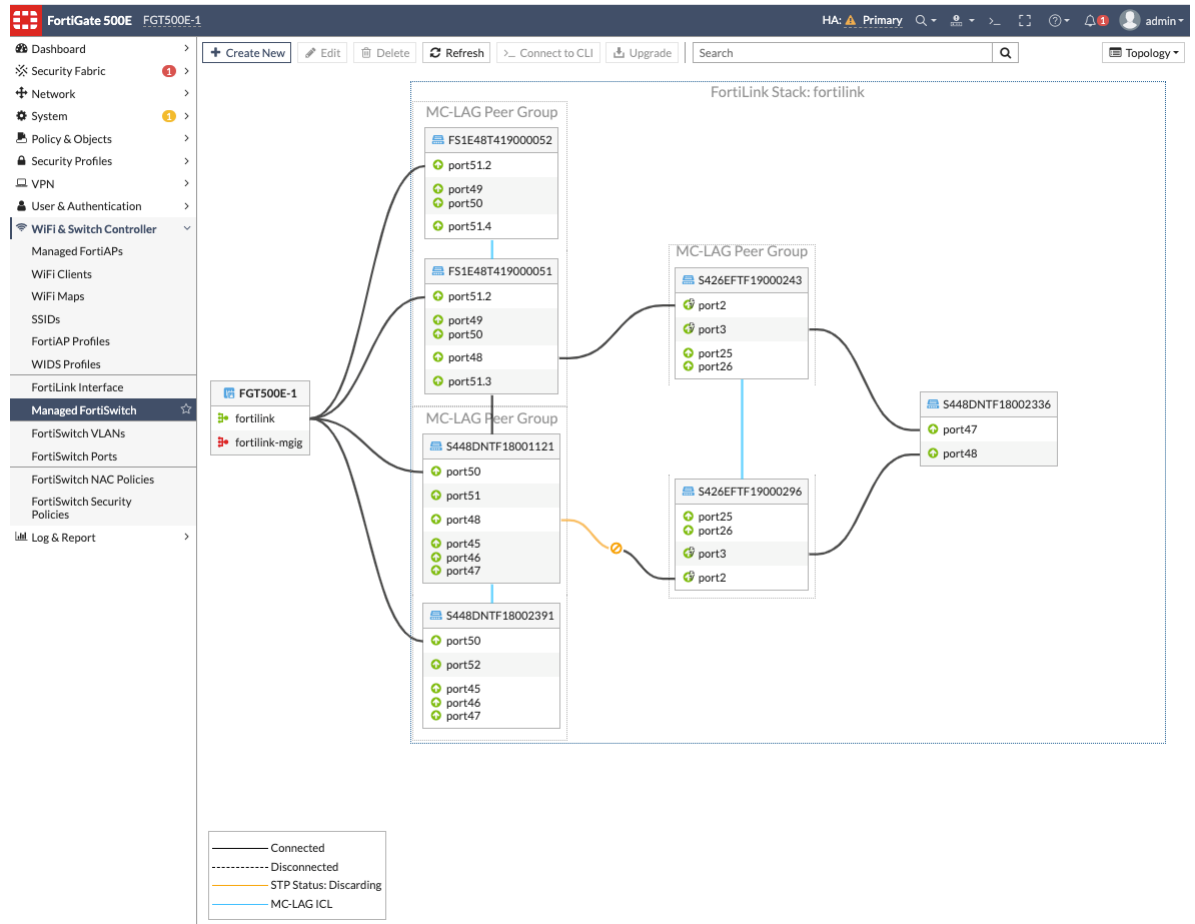


6. Connect Site3_FSW2 to Site2_FSW1 to form the connection between sites 2 and 3. Wait until the topology converges. See the following figure. The link between sites 1 and 3 is blocked by the Spanning Tree

Protocol to avoid forming a loop.

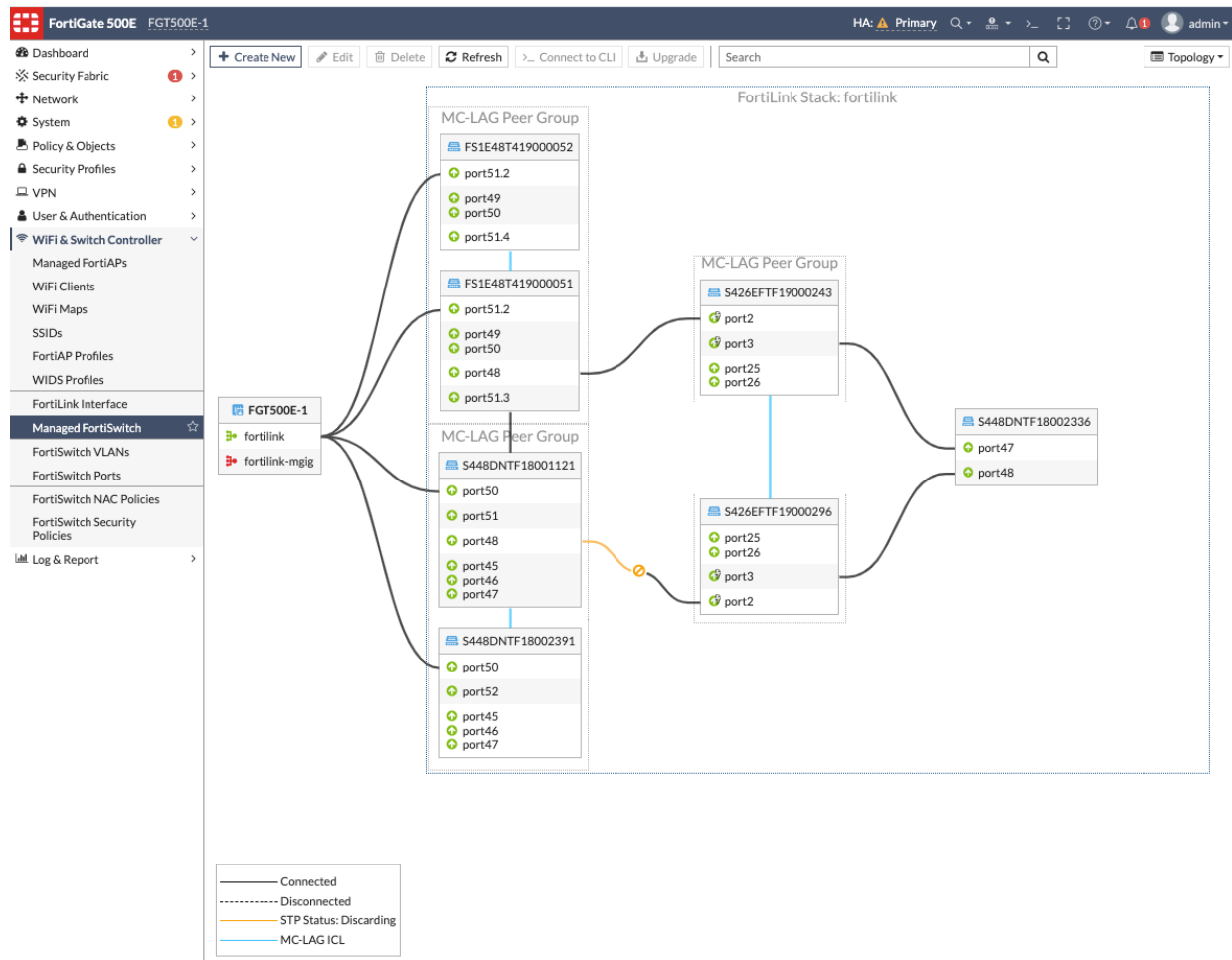


7. Connect to Site3_FSW3 and authorize it on the FortiGate device.



Checking the topology

The final topology is shown in the following figure.



You can use the FortiOS CLI to display the final topology as well.

```
FGT500E-1 # exec switch-controller get-conn-status
Managed-devices in current vdom root:
```

```
FortiLink interface : fortilink
SWITCH-ID      VERSION      STATUS      FLAG      ADDRESS      JOIN-TIME      NAME
FS1E48T419000051 v6.4.5 (461) Authorized/Up - 172.16.16.1 Wed Jan 13 23:00:12 2021 -
FS1E48T419000052 v6.4.5 (461) Authorized/Up - 172.16.16.2 Wed Jan 13 23:00:10 2021 -
S426EFTF19000243 v6.4.5 (461) Authorized/Up - 172.16.16.5 Wed Jan 13 23:00:50 2021 -
S426EFTF19000296 v6.4.5 (461) Authorized/Up - 172.16.16.6 Wed Jan 13 23:00:56 2021 -
S448DNTF18001121 v6.4.5 (461) Authorized/Up - 172.16.16.3 Wed Jan 13 23:00:53 2021 -
S448DNTF18002336 v6.4.5 (461) Authorized/Up - 172.16.16.199 Thu Jan 14 22:38:28 2021 -
S448DNTF18002391 v6.4.5 (461) Authorized/Up - 172.16.16.4 Wed Jan 13 23:00:52 2021 -
```

Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=config sync error, 3=L3
Managed-Switches: 7 (UP: 7 DOWN: 0)


```
FGT500E-1 # execute switch-controller get-physical-conn standard fortilink
This will display connectivity graph information for FortiLink from FortiGate's perspective
NOTE : If FortiSwitch is not authorized, no connectivity information will be shown
NOTE : If FortiSwitch is in idle state, no connectivity information will be shown
NOTE : If FortiSwitch ISL peer has inconsistent info, no connectivity information will be shown
```

```
FortiLink interface : fortilink
```

```
FortiGate(s)
FG5H0E5819900693(x1) <<----->> FS1E48T419000051(port51.2)
FG5H0E5819900693(x2) <<----->> FS1E48T419000052(port51.2)
FG5H0E5819900160(x1) <<----->> S448DNFTF18001121(port50)
FG5H0E5819900160(x2) <<----->> S448DNFTF18002391(port50)

Tier 1
FS1E48T419000051(port51.2) <<----->> FG5H0E5819900693(x1)
FS1E48T419000052(port51.2) <<----->> FG5H0E5819900693(x2)
S448DNFTF18001121(port50) <<----->> FG5H0E5819900160(x1)
S448DNFTF18002391(port50) <<----->> FG5H0E5819900160(x2)

Tier 2+
FS1E48T419000052(port49/_FlInK1_ICL0_) <<----->> FS1E48T419000051(port49/_FlInK1_ICL0_)
FS1E48T419000052(port50/_FlInK1_ICL0_) <<----->> FS1E48T419000051(port50/_FlInK1_ICL0_)
S426EFTTF19000243(port2/TO_SITE_1) <<----->> FS1E48T419000051(port48/TO_SITE_3)
S426EFTTF19000296(port25/_FlInK1_ICL0_) <<----->> S426EFTTF19000243(port25/_FlInK1_ICL0_)
S426EFTTF19000296(port26/_FlInK1_ICL0_) <<----->> S426EFTTF19000243(port26/_FlInK1_ICL0_)
S448DNFTF18001121(port48/TO_SITE_3) <<----->> S426EFTTF19000296(port2/TO_SITE_2)
S448DNFTF18001121(port51/To-SITE-1) <<----->> FS1E48T419000051(port51.3/To-SITE-2)
S448DNFTF18002336(port47/_FlInK1_MLAG0_) <<----->> S426EFTTF19000243(port3/8DNFTF18002336-0)
S448DNFTF18002336(port48/_FlInK1_MLAG0_) <<----->> S426EFTTF19000296(port3/8DNFTF18002336-0)
S448DNFTF18002391(port45/8DNFTF18001121-0) <<----->> S448DNFTF18001121(port45/8DNFTF18002391-0)
S448DNFTF18002391(port46/8DNFTF18001121-0) <<----->> S448DNFTF18001121(port46/8DNFTF18002391-0)
S448DNFTF18002391(port47/8DNFTF18001121-0) <<----->> S448DNFTF18001121(port47/8DNFTF18002391-0)
S448DNFTF18002391(port52/To-SITE-1) <<----->> FS1E48T419000052(port51.4/To-SITE-2)
```

Relevant configuration

Check the relevant FortiGate configuration:

```
FGT500E-1 # config switch-controller managed-switch
```

```
FGT500E-1 (managed-switch) # edit S426EFTTF19000243
```

```
FGT500E-1 (S426EFTTF19000243) # config ports
```

```
FGT500E-1 (ports) # edit port25
```

```
FGT500E-1 (port25) # show
```

```
config ports
```

```
edit "port25"
```

```
set lldp-profile "default-auto-mclag-icl"
```

```
next
```

```
end
```

```
FGT500E-1 (port25) # n
```

```
FGT500E-1 (ports) # edit port26
```

```
FGT500E-1 (port26) # show
```

```
config ports
```

```
edit "port26"
```

```
set lldp-profile "default-auto-mclag-icl"
```

```
next
```

```
end

FGT500E-1 (port26) # end

FGT500E-1 (S426EFTF19000243) # n

FGT500E-1 (managed-switch) # edit S426EFTF19000296

FGT500E-1 (S426EFTF19000296) # config ports

FGT500E-1 (ports) # edit port25

FGT500E-1 (port25) # show
config ports
    edit "port25"
        set lldp-profile "default-auto-mclag-icl"
    next
end

FGT500E-1 (port25) # n

FGT500E-1 (ports) # edit port26

FGT500E-1 (port26) # show
config ports
    edit "port26"
        set lldp-profile "default-auto-mclag-icl"
    next
end

FGT500E-1 (port26) # end

FGT500E-1 (S426EFTF19000296) # end
```

Check the relevant FortiSwitch configuration:

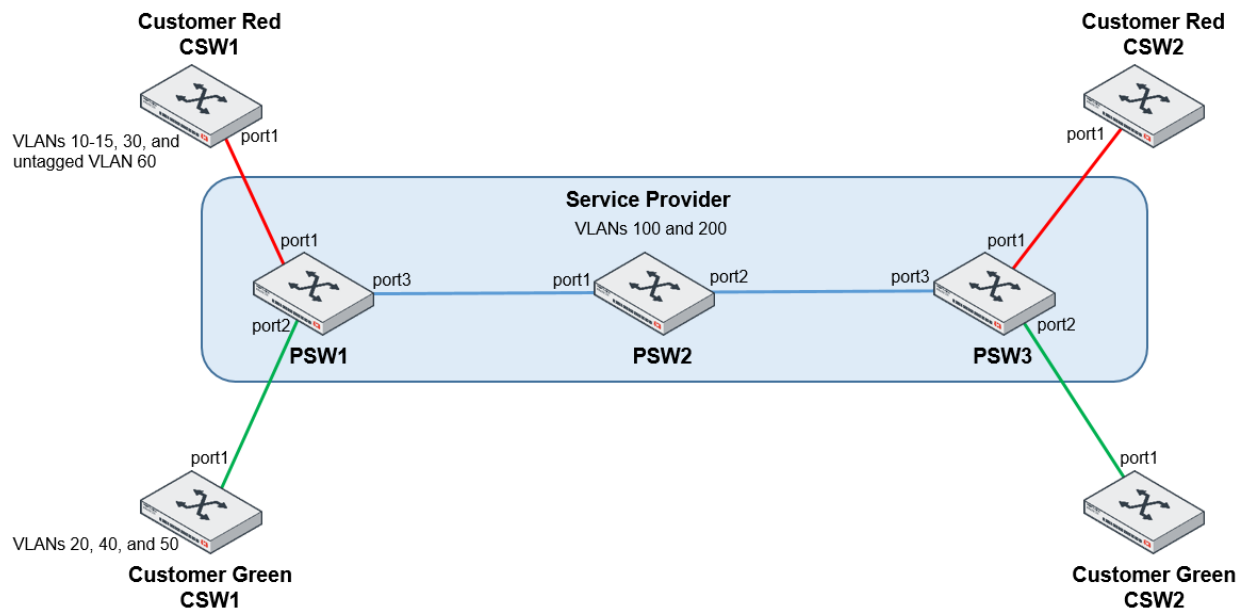
```
Site1_FSW1 # show switch auto-isl-port-group
config switch auto-isl-port-group
    edit "TO_SITE_3"
        set members "port48"
    next
end

Site2_FSW1 # show switch auto-isl-port-group
config switch auto-isl-port-group
    edit "TO_SITE_3"
        set members "port48"
    next
end

Site3_FSW1 # show switch auto-isl-port-group
config switch auto-isl-port-group
    edit "TO_SITE_1"
        set members "port2"
    next
end
```

```
Site3_FSW2 # show switch auto-isl-port-group
config switch auto-isl-port-group
  edit "TO_SITE_2"
    set members "port2"
  next
end
```

Carrying customer VLANs over a provider network



This cookbook article is for FortiSwitch units in standalone mode.

This cookbook article describes how to use VLAN stacking (QinQ) to carry customer VLANs over a service provider network. The following tasks are covered:

1. [Configure the provider switches on page 57](#)
2. [Accept specific VLANs at the provider ingress on page 58](#)
3. [Assign different service tags at the provider ingress on page 59](#)
4. [Retag service VLANs on page 59](#)
5. [VLAN retagging/translation of regular 802.1Q traffic on page 61](#)

There are two customers, Customer Red and Customer Green, each with two FortiSwitch units. They are connected to the three FortiSwitch units belonging to the service provider.

- Customer Red is using VLANs 10-15, VLAN 30, and untagged VLAN 60 to connect to port1 of the provider switches PSW1 and PSW3. The provider is using port3 to connect to Customer Red through VLANs 10-15, VLAN 30, and untagged VLAN 60.
- Customer Green is using VLANs 20, 40, and 50 to connect to port2 of the provider. The provider is using port3 to connect to Customer Green through VLANs 20, 40, and 50.

Provider switches

The service provider is using VLANs 100 and 200 to connect the three provider switches.

For the customer port, the provider switches PSW1 and PSW3 have QinQ enabled with all tags accepted at ingress. The switches has the “native-vlan” as the service VLAN for the customer port, and allowed-vlans are not used. The inner tag needs to be set or removed for untagged traffic on the customer port.

For the provider port, the provider switches PSW1 and PSW3 have QinQ disabled with regular allowed-vlans for each service VLAN. If the default VLAN TPID profile of 0x8100 is not being used, you need to specify the VLAN TPID profile with the `set vlan-tpid` command.

The provider switch PSW2 has QinQ disabled with regular allowed-vlans for each service VLAN. If the default VLAN TPID profile of 0x8100 is not being used, you need to specify the VLAN TPID profile with the `set vlan-tpid` command. For QinQ, use a VLAN TPID profile of 0x88a8.

Customer switches

The customer switches use simple 802.1Q VLANs. They are unaware of QinQ.

Configure the provider switches

You need to configure the provider switches PSW1, PSW2, and PSW3.

To configure the customer ports port1 and port2 of PSW1 and PSW3:

```
config switch interface
  edit "port1"
    set native-vlan 100
    config qnq
      set status enable
      set add-inner 60
      set remove-inner enable
    end
  next
end

config switch interface
  edit "port2"
    set native-vlan 200
    config qnq
      set status enable
    end
  next
end
```

You can use VLAN mapping to accept only specific customer VLANs. See [Accept specific VLANs at the provider ingress on page 58](#).

To configure the service provider port port3 of PSW1 and PSW3:

```
config switch interface
  edit "port3"
    set allowed-vlans 100,200
    set vlan-tpid "qnq"
  next
end
```

```
config switch vlan-tpid
  edit "qnq"
    set ether-type 0x88a8
  next
end
```

To configure the service provider ports port1 and port2 of PSW2:

```
config switch interface
  edit "port1"
    set allowed-vlans 100,200
    set vlan-tpid "qnq"
  next
end
```

```
config switch interface
  edit "port2"
    set allowed-vlans 100,200
    set vlan-tpid "qnq"
  next
end
```

```
config switch vlan-tpid
  edit "qnq"
    set ether-type 0x88a8
  next
end
```

Non-edge provider switches can use VLAN mapping to retag services VLANs. See [Retag service VLANs on page 59](#).

Accept specific VLANs at the provider ingress

Optionally, you can accept specific VLANs at the provider ingress on PSW1 and PSW3. To do this, use VLAN mapping inside QinQ. You need to enable `vlan-mapping-miss-drop` and specify each customer and the corresponding service tags. For example:

```
config vlan-mapping
  edit 1
    set match-c-vlan 10
    set new-s-vlan 100
  next
end
```

Service tags must be listed as allowed-vlans.

The following example accepts only VLAN 10.

```
config switch interface
  edit "port1"
    set native-vlan 100
    config qnq
      set status enable
      set vlan-mapping-miss-drop enable
```

```
        config vlan-mapping
            edit 1
                set match-c-vlan 10
                set new-s-vlan 100
            next
        end
    next
end
```

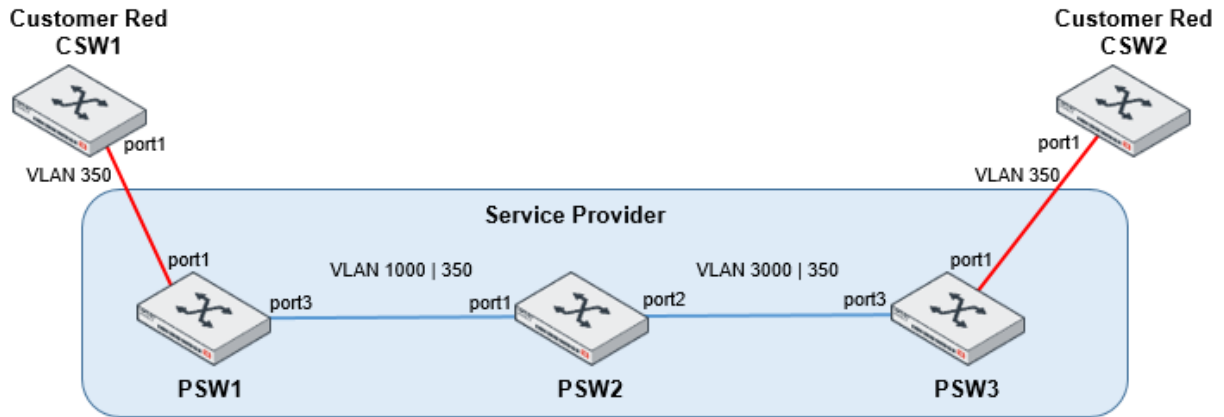
Assign different service tags at the provider ingress

Optionally, you can assign different service tags at the provider ingress on PSW1 and PSW3. To do this, use VLAN mapping inside QinQ. You need to specify each customer and the corresponding service tags. Service tags must be listed as allowed-vlans. Different service tags might be needed for QoS purposes.

```
config switch interface
    edit "port1"
        set native-vlan 100
        config qinq
            set status enable
            config vlan-mapping
                edit 1
                    set match-c-vlan 10
                    set new-s-vlan 100
                next
                edit 2
                    set match-c-vlan 20
                    set new-s-vlan 120
                next
            end
        end
    next
end
```

Retag service VLANs

The following figure shows the topology for the non-edge provider PSW2 receiving QinQ traffic from the provider edge switch PSW1 on port1 with customer VLAN 350 and service-tag 1000. The traffic is then sent out on port2 with service-tag 3000, preserving the customer VLAN. The reverse is done for traffic coming on port2 and leaving port1. In this example, the service VLAN retagging operation is done on the ingress port.



The following is the configuration of the provider port port1 of PSW2:

```
config switch interface
  edit "port1"
    set allowed-vlans 1-4094
    config vlan-mapping
      edit 1
        set direction ingress
        set match-c-vlan 350
        set action replace
        set new-s-vlan 3000
      next
    end
    set vlan-tpid "qng"
  next
end

config switch vlan-tpid
  edit "qng"
    set ether-type 0x88a8
  next
end
```

The following is the configuration of the provider port port2 of PSW2:

```
config switch interface
  edit "port2"
    set allowed-vlans 1-4094
    config vlan-mapping
      edit 1
        set direction ingress
        set match-c-vlan 350
        set action replace
        set new-s-vlan 1000
      next
    end
    set vlan-tpid "qng"
  next
end
```


You can also apply service VLAN retagging on egress. In this case, the match is done on the service tag. If you choose `action replace`, the new service VLAN must be specified. If you choose `action delete`, the service tag is removed, and the frame is forwarded with only the customer VLAN.

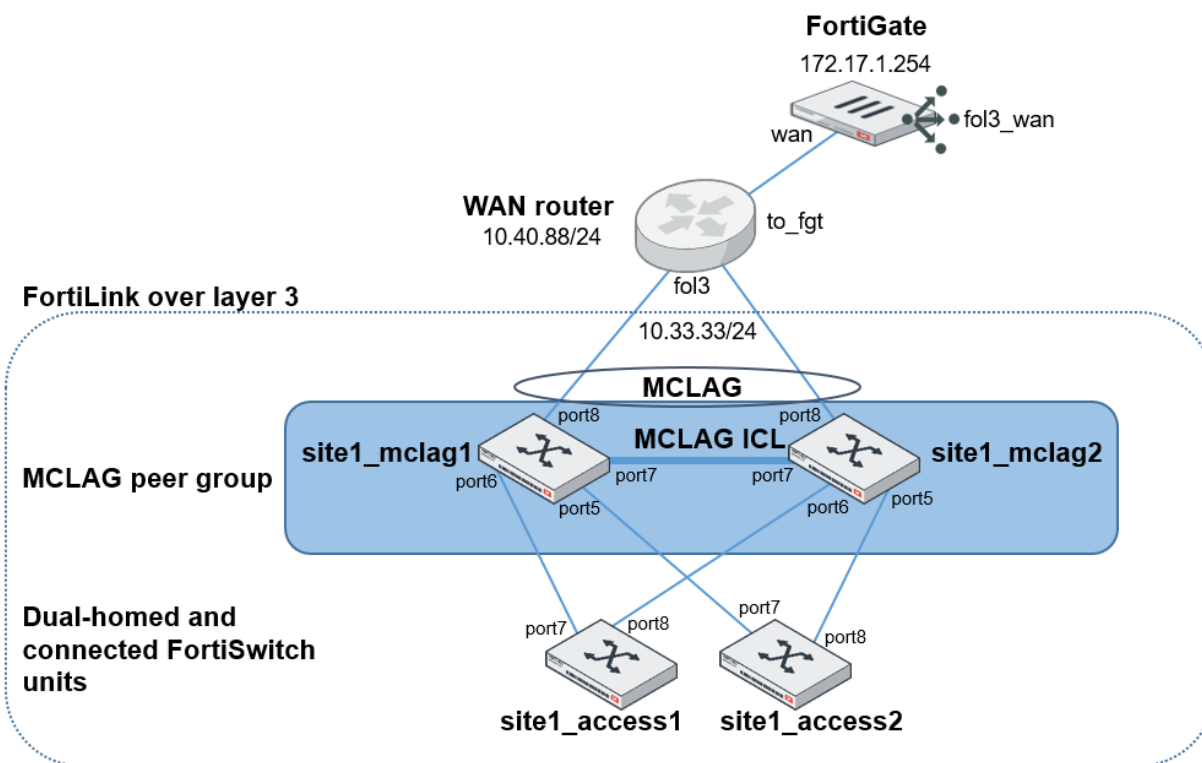
VLAN retagging/translation of regular 802.1Q traffic

You can use ACLs (to match the VLAN and set the action of the outer-vlan-tag) to retag or translate VLANs with regular 802.1Q traffic.

```
config switch acl ingress
  edit 1
    config action
      set outer-vlan-tag 2333
    end
    config classifier
      set vlan-id 350
    end
    set ingress-interface "mclag-761_419"
  next
end
```

On some FortiSwitch models, you can also apply an ACL on the prelookup and egress stages. The configuration is similar to the configuration in this section and is done under the `config switch acl prelookup` or `config switch acl egress` commands, respectively.

MCLAG peer group managed with FortiLink over layer 3



This cookbook article describes how to configure a multichassis link aggregation group (MCLAG) peer group that is managed with FortiLink over layer 3. The following tasks are covered:

1. [Set up the FortiGate device on page 63](#)
2. [Configure the WAN router on page 65](#)
3. [Configure the site1_mclag1 switch on page 67](#)
4. [Authorize the site1_mclag1 switch on page 68](#)
5. [Configure the site1_mclag2 switch on page 70](#)
6. [Configure the FortiGate device on page 72](#)
7. [Configure the access switches on page 77](#)
8. [Finish the FortiSwitch configuration from the FortiGate device on page 78](#)
9. [Check the configuration on page 82](#)

Assumptions

The following tasks must be done before starting this procedure:

- The FortiGate device is already configured with an interface towards the WAN router.
- The FortiGate device is already managing FortiSwitch units connected locally, and different VLANs are needed in the remote FortiSwitch units.

- The WAN router has an 802.3ad link aggregation group (LAG) connected to the FortiSwitch MCLAG peer group, and the WAN router is VLAN-capable. (An untagged VLAN is needed for FortiSwitch control, and tagged VLANs are needed for user data traffic.)

Configuration summary

Here is a summary of the procedure:

1. On the FortiGate device:
 - a. Configure the routing so the FortiGate unit can reach the FortiSwitch units.
 - b. Configure a dedicated FortiLink interface to control the FortiSwitch units connected to the FortiGate device from remote locations.
 - c. Configure a firewall policy to allow the connections from the FortiSwitch units.
2. On the WAN router, configure an untagged interface or VLAN on the LAG connected to the FortiSwitch units. Assign an IP address and DHCP service, including the Network Time Protocol (NTP) server and option 138 (the switch controller IP address).
3. On the site1_mclag1 FortiSwitch unit in the MCLAG peer group:
 - a. Enable FortiLink mode.
 - b. Set the switch-controller discovery type to DHCP.
 - c. Enable FortiLink over layer 3 on the switch interface connected to the WAN router and enable the Link Aggregation Control Protocol (LACP) on the newly formed trunk.
4. On the FortiGate device, authorize and name the site1_mclag1 FortiSwitch unit.
5. On the site1_mclag2 FortiSwitch unit in the MCLAG peer group:
 - a. Enable FortiLink mode.
 - b. Set the switch-controller discovery type to DHCP.
6. On the FortiGate device:
 - a. Authorize and name the site1_mclag2 FortiSwitch unit.
 - b. Enable the MCLAG peer group.
 - c. Connect to the CLI of the site1_mclag2 FortiSwitch unit and enable FortiLink over layer 3 on the switch interface connected to the WAN router. Enable LACP on the newly formed trunk.
 - d. Connect to the CLI of the site1_mclag1 FortiSwitch unit and enable MCLAG on the trunk connected to the WAN router.
7. On the access FortiSwitch units:
 - a. Enable FortiLink mode.
 - b. Set the switch-controller discovery type to DHCP.
8. On the FortiGate device:
 - a. Authorize and name the access FortiSwitch units.
 - b. Create FortiSwitch VLANs and assign them to FortiSwitch ports.

Set up the FortiGate device

1. Configure the routing so that the FortiGate device can reach the FortiSwitch units. For example, the following figure shows a static route to the network destination 10.33.33/24 used by the FortiSwitch units. The gateway IP address is 10.40.88.253, which is the address of the interface of the WAN router connected to the FortiGate unit.

FortiGate VM64-KVM FGT_Switch_Controller

Dashboard > Security Fabric > **Network** > Static Routes

Edit Static Route

Destination ⓘ Subnet Internet Service
10.33.33.0/255.255.255.0

Gateway Address
10.40.88.253

Interface
wan

Administrative Distance ⓘ
10

Comments
Write a comment... 0/255

Status
☒ Enabled ☐ Disabled

Advanced Options

2. Configure a dedicated FortiLink interface to control the FortiSwitch units connected to the FortiGate device from remote locations. Use the CLI to configure the dedicated FortiLink interface, and then the interface will be listed in the FortiLink interface list in the GUI. Set the interface type to `aggregate`, specify the IP address, enable FortiLink, and set the source IP address of the switch controller to use a fixed IP address from the FortiLink interface itself.

```
FGT_Switch_Controller # config system interface
FGT_Switch_Controller (interface) # edit fol3_wan
FGT_Switch_Controller (fol3_wan) # set vdom root
FGT_Switch_Controller (fol3_wan) # set type aggregate
FGT_Switch_Controller (fol3_wan) # set ip 172.17.1.254/24
FGT_Switch_Controller (fol3_wan) # set fortilink enable
FGT_Switch_Controller (fol3_wan) # set switch-controller-source-ip fixed
FGT_Switch_Controller (fol3_wan) # end
```

3. Configure a firewall policy to allow the connections from the FortiSwitch units. The service is CAPWAP (UDP port 5246). Configure the policy in the GUI first, specifying that the destination interface is the same as the source interface.

FortiGate VM64-KVM FGT_Switch_Controller

Dashboard > Security Fabric > Network > System > Policy & Objects > **Firewall Policy**

Edit Policy

Name ⓘ fsw_to_fol3_wan ID 5

Incoming Interface ⓘ wan Last used N/A

Outgoing Interface ⓘ wan First used N/A

Source ⓘ fsw Hit count 0

Destination ⓘ fol3_wan_IP Active sessions 0

Schedule ⓘ always

Service ⓘ ALL_ICMP, CAPWAP

Action ☒ ACCEPT ☐ DENY

Inspection Mode ☒ Flow-based ☐ Proxy-based

Firewall / Network Options

NAT ⓘ

Protocol Options ⓘ ☒ default

Security Profiles

AntiVirus ⓘ

Web Filter ⓘ

DNS Filter ⓘ

Application Control ⓘ

IPS ⓘ

File Filter ⓘ

SSL Inspection ⓘ no-inspection

Logging Options

Log Allowed Traffic ☒ Security Events ☐ All Sessions

Generate Logs when Session Starts ⓘ

Capture Packets ⓘ

OK Cancel

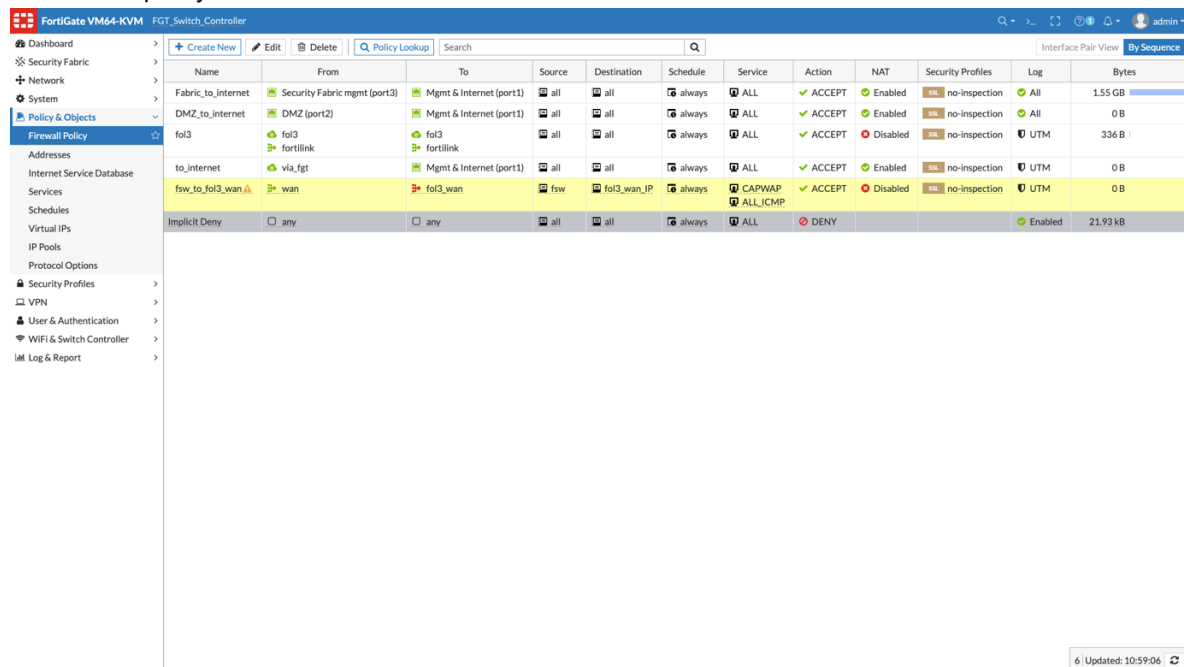
Then edit the policy in the CLI and change the destination interface to the FortiLink interface.

```

FGT_Switch_Controller # config firewall policy
FGT_Switch_Controller (policy) # edit 5
FGT_Switch_Controller (5) # show
config firewall policy
  edit 5
    set name "fsw_to_fol3_wan"
    set uuid 98af1592-354d-51eb-e09e-8d8000c0663a
    set srcintf "wan"
    set dstintf "wan"
    set srcaddr "fsw"
    set dstaddr "fol3_wan_IP"
    set action accept
    set schedule "always"
    set service "CAPWAP" "ALL_ICMP"
  next
end
FGT_Switch_Controller (5) # set dstintf fol3_wan
FGT_Switch_Controller (5) # end

```

The firewall policy is listed in the GUI.



Name	From	To	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
Fabric_to_Internet	Security Fabric mgmt (port3)	Mgmt & Internet (port1)	all	all	always	ALL	ACCEPT	Enabled	no-inspection	All	1.55 GB
DMZ_to_Internet	DMZ (port2)	Mgmt & Internet (port1)	all	all	always	ALL	ACCEPT	Enabled	no-inspection	All	0 B
fol3	fortilink	fol3	all	all	always	ALL	ACCEPT	Disabled	no-inspection	UTM	336 B
to_Internet	via_fgt	Mgmt & Internet (port1)	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
fsw_to_fol3_wan	wan	fol3_wan	fsw	fol3_wan_IP	always	CAPWAP ALL_ICMP	ACCEPT	Disabled	no-inspection	UTM	0 B
Implicit Deny	any	any	all	all	always	ALL	DENY			Enabled	21.93 kB

Configure the WAN router

Configure an untagged interface or VLAN on the LAG connected to the FortiSwitch units. Assign the IP address and DHCP service, including NTP and option 138 (the switch controller IP address).

For the purpose of this procedure, the WAN router is a FortiSwitch unit in standalone mode. The DHCP server is using vendor class identifier (VCI) matching to restrict the IP assignment to FortiSwitch units only.

```
config router static
  edit 2
    set device "to_fgt"
    set dst 172.17.1.0 255.255.255.0
    set gateway 10.40.88.254
  next
end

config system interface
  edit "to_fgt"
    set ip 10.40.88.253 255.255.255.0
    set allowaccess ping https ssh
    set snmp-index 16
    set vlanid 4088
    set interface "internal"
  next
end

config switch interface
  edit "to_fgt"
    set native-vlan 4088
    set snmp-index 14
  next
end

config switch trunk
  edit "to_fgt"
    set mode lacp-active
    set members "port7" "port8"
  next
end

config system interface
  edit "fo13"
    set ip 10.33.33.254 255.255.255.0
    set allowaccess ping https ssh
    set snmp-index 17
    set vlanid 4094
    set interface "internal"
  next
end

config switch interface
  edit "fo13"
    set native-vlan 4094
    set allowed-vlans 1001
    set edge-port disabled
    set snmp-index 15
  next
end

config switch trunk
  edit "fo13"
    set mode lacp-active
```

```
        set members "port5" "port6"
    next
end

config system dhcp server
    edit 1
        set default-gateway 10.33.33.254
        set dns-service local
        set interface "fo13"
        config ip-range
            edit 1
                set end-ip 10.33.33.99
                set start-ip 10.33.33.1
            next
        end
        set lease-time 300
        set netmask 255.255.255.0
        set ntp-service local
        set vci-match enable
        set vci-string "FortiSwitch"
        set wifi-acl 172.17.1.254
    next
end
```

Configure the site1_mclag1 switch

Follow these steps on the site1_mclag1 FortiSwitch unit in the MCLAG peer group:

1. Enable FortiLink mode.

```
config system global
    set switch-mgmt-mode fortilink
end
```

2. Set the switch-controller discovery type to DHCP.

```
config switch-controller global
    set ac-discovery-type dhcp
end
```

3. Enable FortiLink over layer 3 on the switch interface connected to the WAN router and enable LACP on the newly formed `__FoRtILnk0L3__` trunk, which is automatically created by the system.

```
config switch interface
    edit port8
        set fortilink-l3-mode enable
    end

config switch trunk
    edit "__FoRtILnk0L3__"
        set mode lacp-active
        set members "port8"
    next
```

```

end

config switch interface
    edit "__FoRtILnk0L3__"
        set native-vlan 4094
        set allowed-vlans 1
        set dhcp-snooping trusted
        set igmp-snooping-flood-reports enable
        set igmp-snooping-flood-traffic enable
        set snmp-index 12
    next
end

```

```

Connected (encrypted) to: QEMU (FSW_MCLAG1)
name: mgmt    mode: static    ip: 0.0.0.0 0.0.0.0    status: up    type: physical
    mtu-override: disable
== [ internal ]
name: internal    mode: dhcp    ip: 0.0.0.0 0.0.0.0    status: up    type: physical
    mtu-override: disable

S108DUHFUKEFGG54 # get system interface
== [ mgmt ]
name: mgmt    mode: static    ip: 0.0.0.0 0.0.0.0    status: up    type: physical
    mtu-override: disable
== [ internal ]
name: internal    mode: dhcp    ip: 10.33.33.1 255.255.255.0    status: up    type: physical
    mtu-override: disable

S108DUHFUKEFGG54 # execute ping 172.17.1.254
PING 172.17.1.254 (172.17.1.254): 56 data bytes
64 bytes from 172.17.1.254: icmp_seq=0 ttl=254 time=11.9 ms
64 bytes from 172.17.1.254: icmp_seq=1 ttl=254 time=10.7 ms
64 bytes from 172.17.1.254: icmp_seq=2 ttl=254 time=10.2 ms
^C
--- 172.17.1.254 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 10.2/10.9/11.9 ms

S108DUHFUKEFGG54 # _

```

Authorize the site1_mclag1 switch

On the FortiGate device, authorize and name the site1_mclag1 FortiSwitch unit.

FortiGate VM64-KVM FGT_Switch_Controller

Dashboard

Security Fabric

Network

System

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

Managed FortiAPs

WiFi Clients

WiFi Maps

SSIDs

FortiAP Profiles

WIDS Profiles

FortiLink Interface

Managed FortiSwitch

FortiSwitch VLANs

FortiSwitch Ports

FortiSwitch NAC Policies

FortiSwitch Security Policies

Log & Report

Status: Unauthorized

Model: S108DV

+ Create New Edit Delete Authorize Upgrade Connect to CLI Search

Name	Switch Group	Status	Model	Firmware Version	Connecting From	Join Time
S108DVHFUKEGG54		Unauthorized	S108DV			

List FortiLink fol3_wan

FortiGate VM64-KVM FGT_Switch_Controller

Dashboard

Security Fabric

Network

System

Policy & Objects

Security Profiles

VPN

User & Authentication

WiFi & Switch Controller

Managed FortiAPs

WiFi Clients

WiFi Maps

SSIDs

FortiAP Profiles

WIDS Profiles

FortiLink Interface

Managed FortiSwitch

FortiSwitch VLANs

FortiSwitch Ports

FortiSwitch NAC Policies

FortiSwitch Security Policies

Log & Report

Status: Online

Model: S108DV

+ Create New Edit Delete Upgrade Connect to CLI Search

Name	Switch Group	Status	Model	Firmware Version	Connecting From	Join Time
site1_mclag1 (S108DVHFUKEGG54)		Online	S108DV	S108DV-v6.6.0-build5756.201009 (Interim)	10.33.33.1	2020/12/03 11:11:37

List FortiLink fol3_wan

The first screenshot shows the FortiGate VM64-KVM GUI with the 'FortiLink Stack: fol3_wan' configuration. It displays a 'site1_mclag1 (S108DVHFUKEFGG54)' unit connected to 'port8'. A detailed view of the unit shows its serial number, name, status (Online), and FortiLink interface (fol3_wan).

The second screenshot shows the 'Diagnostics and Tools - site1_mclag1' page. It provides general information about the unit and a table of ports.

Port	Trunk	Access Mode	Native VLAN	Allowed VLANs	Device Information	LLD
port1		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)		SL00P d
port2		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)		SL00P d
port3		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)		SL00P d
port4		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)		SL00P d
port5		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)		SL00P d
port6		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)		SL00P d
port7		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)		SL00P d
port8		Normal	FGVM04TM20006534		fe:09:0f:d3:1f:01	SL00P d

Configure the site1_mclag2 switch

Follow these steps on the site1_mclag2 FortiSwitch unit in the MCLAG peer group:

1. Enable FortiLink mode.

```
config system global
    set switch-mgmt-mode fortilink
end
```

2. Set the switch-controller discovery type to DHCP.

```
config switch-controller global
    set ac-discovery-type dhcp
end
```

3. FortiLink over layer 3 is not enabled on the switch interface connected to the WAN router. **NOTE:** The FortiGate device can already be reached using the inter-switch link (ISL) formed with the site1_mclag1 FortiSwitch unit.

```
config switch interface
    edit "8DVHFUKEFGG54-0"
        set native-vlan 4094
        set allowed-vlans 1
        set dhcp-snooping trusted
        set edge-port disabled
        set snmp-index 12
    next
end
```

```

Connected (encrypted) to: QEMU (FSW_MCLAG2)
    set dhcp-snooping trusted
    set edge-port disabled
    set snmp-index 12
next
end

S108DUSPUKEFGG54 # get system interface
== [ mgmt ]
name: mgmt    mode: static    ip: 0.0.0.0 0.0.0.0    status: up    type: physical
    mtu-override: disable
== [ internal ]
name: internal    mode: dhcp    ip: 10.33.33.2 255.255.255.0    status: up    type: physical
    mtu-override: disable

S108DUSPUKEFGG54 # execute ping 172.17.1.254
PING 172.17.1.254 (172.17.1.254): 56 data bytes
64 bytes from 172.17.1.254: icmp_seq=0 ttl=254 time=18.9 ms
64 bytes from 172.17.1.254: icmp_seq=1 ttl=254 time=14.4 ms
64 bytes from 172.17.1.254: icmp_seq=2 ttl=254 time=11.2 ms
^C
--- 172.17.1.254 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 11.2/14.8/18.9 ms

S108DUSPUKEFGG54 #
```

Configure the FortiGate device

1. Authorize and name the site1_mclag2 FortiSwitch unit.

The screenshot shows the FortiGate VM64-KVM FortiSwitch_Controller interface. The left sidebar contains the navigation menu with 'Managed FortiSwitch' selected. The main area displays two donut charts: 'Status' (showing 1 Online and 1 Unauthorized) and 'Model' (showing 1 S108DV). Below the charts is a table with the following data:

Name	Switch Group	Status	Model	Firmware Version	Connecting From	Join Time
site1_mclag1 (S108DVHFUKEFGG54)		Online	S108DV	S108DV-v6.6.0-build5756.201009 (Interim)	10.33.33.1	2020/12/03 11:11:37
S108DVSPUKEFGG54		Unauthorized	S108DV			

The screenshot shows the FortiGate VM64-KVM FortiSwitch_Controller interface after the configuration changes. The 'Status' donut chart now shows 2 Online units. The table below shows the updated state:

Name	Switch Group	Status	Model	Firmware Version	Connecting From	Join Time
site1_mclag1 (S108DVHFUKEFGG54)		Online	S108DV	S108DV-v6.6.0-build5756.201009 (Interim)	10.33.33.1	2020/12/03 11:11:37
site1_mclag2 (S108DVSPUKEFGG54)		Online	S108DV	S108DV-v6.6.0-build5756.201009 (Interim)	10.33.33.2	2020/12/03 11:32:06

The top screenshot shows the FortiGate VM64-KVM interface with the FortiLink Stack configuration. The stack is named 'fol3_wan' and contains two peers: 'site1_mclag1 (S108DVHFUKEFGG...)' and 'site1_mclag2 (S108DVSPUKEFGG...)'. Both peers are connected via their 'port7' interfaces. The bottom screenshot shows the 'Diagnostics and Tools - site1_mclag2' window, displaying general information and a table of ports and their configurations.

Port	Trunk	Access Mode	Native VLAN	Allowed VLANs	Device Information	LLD
port1		Normal	default:fol3_wan (default:22)	quarantine:fol3_wan (quarantine:22)	fe:09:0f:d3:00:11	LLDP d
port2		Normal	default:fol3_wan (default:22)	quarantine:fol3_wan (quarantine:22)	fe:09:0f:d3:00:12	LLDP d
port3		Normal	default:fol3_wan (default:22)	quarantine:fol3_wan (quarantine:22)	fe:09:0f:d3:00:13	LLDP d
port4		Normal	default:fol3_wan (default:22)	quarantine:fol3_wan (quarantine:22)	fe:09:0f:d3:00:14	LLDP d
port5		Normal	default:fol3_wan (default:22)	quarantine:fol3_wan (quarantine:22)	fe:09:0f:d3:0b:02	LLDP d
port6		Normal	default:fol3_wan (default:22)	quarantine:fol3_wan (quarantine:22)	fe:09:0f:d3:23:01	LLDP d
port7		Normal	S108DVHFUKEFGG54	quarantine:fol3_wan (quarantine:22)	02:09:0f:d3:07:02	LLDP d
port8		Normal	default:fol3_wan (default:22)	quarantine:fol3_wan (quarantine:22)	fe:09:0f:d3:1e:02	LLDP d

- To enable the MCLAG peer group from the FortiGate device, use the `switch-recommendations` command, specifying the FortiLink interface and the serial numbers of the MCLAG peers. (Alternatively, on the FortiGate device, set the LLDP profile to `default-auto-mclag-icl` in the ports used for the MCLAG ICL on both peers.)

```
FGT_Switch_Controller # execute switch-controller switch-recommendations set-
tier1-mclag-icl fol3_wan S108DVHFUKEFGG54 S108DVSPUKEFGG54
```

```
CLI Console (1)

FGT_Switch_Controller # exec ssh admin@10.33.33.1
admin@10.33.33.1's password:
site1_mclag1 # show switch trunk
config switch trunk
    edit "__FoRtILnk0L3__"
        set mode lacp-active
        set members "port8"
    next
    edit "_FlInK1_ICL0_"
        set mode lacp-active
        set auto-is1 1
        set mclag-icl enable
        set members "port7"
    next
end

site1_mclag1 # diagnose switch mclag icl
_FlInK1_ICL0_
    icl-ports          7
    egress-block-ports none
    interface-mac      c6:e0:d9:7f:00:01
    local-serial-number S108DVHFUKEFGG54
    peer-mac           06:37:6d:72:2f:77
    peer-serial-number  S108DVSPUKEFGG54
    Local uptime       0 days 3h:36m:40s
    Peer uptime        0 days 0h: 8m:41s
    MCLAG-STP-mac      02:09:0f:d3:00:0b
    keepalive interval 1
    keepalive timeout  60

Counters
    received keepalive packets 10979
    transmitted keepalive packets 11443
    received keepalive drop packets 4
    receive keepalive miss 6

site1_mclag1 #
```

```

CLI Console (4)

FGT_Switch_Controller # exec ssh admin@10.33.33.2
admin@10.33.33.2's password:
site1_mclag2 # show switch trunk
config switch trunk
    edit "_FlInK1_ICL0_"
        set mode lacp-active
        set auto-is1 1
        set mclag-icl enable
        set members "port7"
    next
end

site1_mclag2 # diagnose switch mclag icl
_FlInK1_ICL0_
    icl-ports          7
    egress-block-ports none
    interface-mac      06:37:6d:72:2f:77
    local-serial-number S108DVSPUKEFGG54
    peer-mac           c6:e0:d9:7f:00:01
    peer-serial-number S108DVHFUKEFGG54
    Local uptime       0 days 0h:10m:0s
    Peer uptime        0 days 3h:37m:56s
    MCLAG-STP-mac      02:09:0f:d3:00:0b
    keepalive interval 1
    keepalive timeout  60

Counters
    received keepalive packets 460
    transmitted keepalive packets 460
    received keepalive drop packets 4

site1_mclag2 #

```

3. Connect to the CLI of the site1_mclag2 FortiSwitch unit and enable FortiLink over layer 3 on the switch interface connected to the WAN router. Enable LACP on the newly formed trunk. **NOTE:** The automatically created trunk has the same name as in the site1_mclag1 FortiSwitch unit, so it will form the MCLAG trunk (the trunk name must be the same in both FortiSwitch units to form the MCLAG trunk).

```

config switch interface
    edit port8
        set fortilink-l3-mode enable
    end

config switch trunk
    edit "_FlInK1_ICL0_"
        set mode lacp-active
        set auto-is1 1
        set mclag-icl enable
        set members "port7"
    next
    edit "__FoRtILnk0L3__"
        set mclag enable
        set members "port8"
    next
end

config switch trunk

```

```
edit "__FoRtILnk0L3__"
    set mode lacp-active
end
```

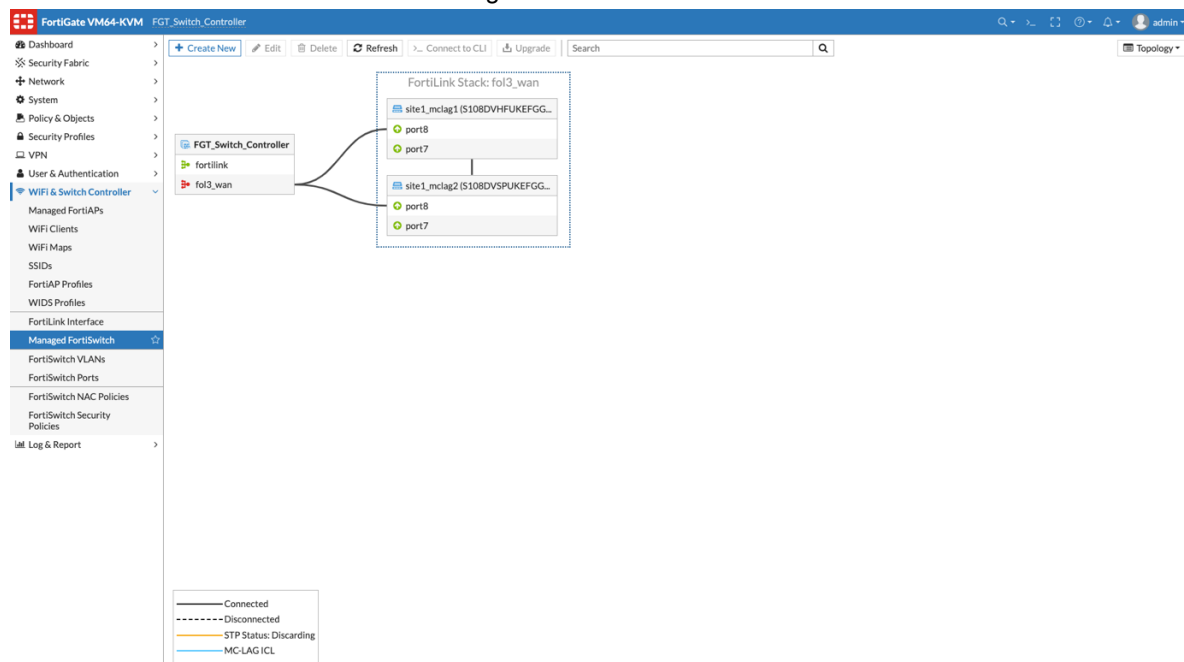
The switch interface is configured automatically.

```
site1_mclag2 # show switch interface __FoRtILnk0L3__
config switch interface
    edit "__FoRtILnk0L3__"
        set native-vlan 4094
        set allowed-vlans 1,4089-4093
        set dhcp-snooping trusted
        set igmp-snooping-flood-reports enable
        set igmp-snooping-flood-traffic enable
        set snmp-index 13
    next
end
```

4. Connect to the CLI of the site1_mclag1 FortiSwitch unit and enable MCLAG on the trunk connected to the WAN router.

```
site1_mclag1 # config switch trunk
site1_mclag1 (trunk) # edit "__FoRtILnk0L3__"
site1_mclag1 (__FoRtILnk0L3__) # set mclag enable
site1_mclag1 (__FoRtILnk0L3__) # end
```

5. Check that both FortiSwitch units are managed.



Configure the access switches

1. Enable FortiLink mode.

```
config system global
    set switch-mgmt-mode fortilink
end
```

2. Set the switch-controller discovery type to DHCP. The ISL is automatically formed with the MCLAG peer group (you do not need to enable FortiLink over layer 3).

```
config switch-controller global
    set ac-discovery-type dhcp
end
```

The screenshot shows a terminal window titled "Connected (encrypted) to: QEMU (FSW_ACCESS1)". The user is in a shell with prompt "S108DVUBYKEFGG54 #". They run "get system interface", which displays details for "mgmt" and "internal" interfaces. The "mgmt" interface is static with IP 0.0.0.0. The "internal" interface is DHCP with IP 10.33.33.3. Then, they run "execute ping 172.17.1.254", which shows two successful ping attempts with times of 35.6 ms and 11.6 ms. Finally, they run "ping statistics", showing 2 packets transmitted and received with 0% loss and round-trip times of 11.6/23.6/35.6 ms.

```
Connected (encrypted) to: QEMU (FSW_ACCESS1)

S108DVUBYKEFGG54 #
S108DVUBYKEFGG54 #
S108DVUBYKEFGG54 #
S108DVUBYKEFGG54 #
S108DVUBYKEFGG54 #
S108DVUBYKEFGG54 #
S108DVUBYKEFGG54 # get system interface
== [ mgmt ]
name: mgmt      mode: static      ip: 0.0.0.0 0.0.0.0      status: up      type: physical
      mtu-override: disable
== [ internal ]
name: internal  mode: dhcp      ip: 10.33.33.3 255.255.255.0  status: up      typ
e: physical    mtu-override: disable

S108DVUBYKEFGG54 # execute ping 172.17.1.254
PING 172.17.1.254 (172.17.1.254): 56 data bytes
64 bytes from 172.17.1.254: icmp_seq=0 ttl=254 time=35.6 ms
64 bytes from 172.17.1.254: icmp_seq=1 ttl=254 time=11.6 ms
^C
--- 172.17.1.254 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 11.6/23.6/35.6 ms

S108DVUBYKEFGG54 # _
```

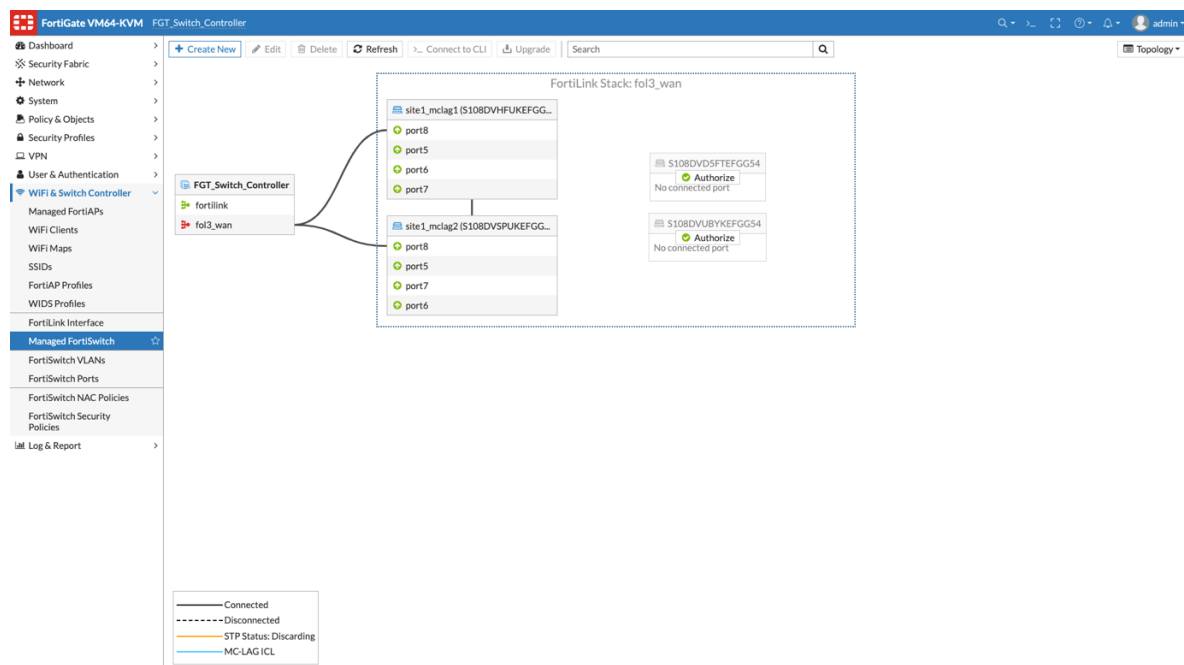
```

Connected (encrypted) to: QEMU (FSW_ACCESS2)
S108DUD5FTEFGG54 #
S108DUD5FTEFGG54 #
S108DUD5FTEFGG54 #
S108DUD5FTEFGG54 #
S108DUD5FTEFGG54 #
S108DUD5FTEFGG54 #
S108DUD5FTEFGG54 #
S108DUD5FTEFGG54 #
S108DUD5FTEFGG54 #
S108DUD5FTEFGG54 # show switch trunk
config switch trunk
    edit "_FlInK1_MLAG_"
        set mode lacp-active
        set auto-isl 1
        set mclag enable
        set members "port8" "port7"
    next
end
S108DUD5FTEFGG54 # get system interface
== [ mgmt ]
name: mgmt      mode: static      ip: 0.0.0.0 0.0.0.0      status: up      type: physical
    mtu-override: disable
== [ internal ]
name: internal  mode: dhcp      ip: 10.33.33.4 255.255.255.0      status: up      typ

```

Finish the FortiSwitch configuration from the FortiGate device

1. Authorize and name the access FortiSwitch units.



MCLAG peer group managed with FortiLink over layer 3

The screenshot displays the FortiGate VM64-KVM interface, specifically the FGT_Switch_Controller section. The left sidebar shows the navigation menu with 'WIFI & Switch Controller' selected. The main area shows a topology diagram for the FortiLink Stack: fol3_wan. The diagram illustrates the connection between the FGT_Switch_Controller and the FortiLink Stack, which includes two MCLAG peer groups (site1_mclag1 and site1_mclag2) and two access interfaces (site1_access1 and site1_access2). The connections are shown as solid lines, indicating they are connected. A legend at the bottom left explains the line types: solid line for Connected, dashed line for Disconnected, orange line for STP Status: Discarding, and blue line for MC-LAG ICL.

The bottom section shows the 'Diagnostics and Tools - site1_access1' window. The 'General' tab is selected, displaying the following information:

- Name: site1_access1
- Serial Number: S108DVUBYKEFGG54
- Version: S108DV-v6.6.0-build5756.201009 (Interim)
- Model: S108DV
- FortiLink Interface: fol3_wan
- IP Address: 10.33.33.3
- Join Time: Minute ago
- Status: Connected
- Registration: Not Registered

The 'Ports' tab is also visible, showing a table of ports and their configurations:

Port	Trunk	Access Mode	Native VLAN	Allowed VLANs	Device Information	LLD
port1		Normal	default:fol3_wan (default.22)	quarantine:fol3_wan (quarantine.22)	02:09:0f:d3:13:01	LLDP d
port2		Normal	default:fol3_wan (default.22)	quarantine:fol3_wan (quarantine.22)	02:09:0f:d3:2d:02	LLDP d
port3		Normal	default:fol3_wan (default.22)	quarantine:fol3_wan (quarantine.22)		LLDP d
port4		Normal	default:fol3_wan (default.22)	quarantine:fol3_wan (quarantine.22)		LLDP d
port5		Normal	default:fol3_wan (default.22)	quarantine:fol3_wan (quarantine.22)		LLDP d
port6		Normal	default:fol3_wan (default.22)	quarantine:fol3_wan (quarantine.22)		LLDP d
port7		Normal	S108DVHFUKEFGG54	quarantine:fol3_wan (quarantine.22)		LLDP d
port8		Normal	S108DVSPUKEFGG54			

Port	Trunk	Access Mode	Native VLAN	Allowed VLANs	Device Information	LLD
port1		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	02:09:0f:d3:2c:02 fe:09:0f:d3:0d:01	UP d
port2		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	02:09:0f:d3:11:01 fe:09:0f:d3:11:02	UP d
port3		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	02:09:0f:d3:00:1a fe:09:0f:d3:00:1b	UP d
port4		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	02:09:0f:d3:00:1b fe:09:0f:d3:00:1c	UP d
port5		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	02:09:0f:d3:00:1c fe:09:0f:d3:00:1d	UP d
port6		Normal	S108DVHUFKEFGG54	quarantine.fol3_wan (quarantine.22)		UP d
port7		Normal	S108DVHUFKEFGG54			
port8		Normal	S108DVSPUKEFGG54			

```

CLI Console (1)

FGT_Switch_Controller # execute switch-controller get-conn-status
Managed-devices in current vdom root:

FortiLink interface : fol3_wan
SWITCH-ID      VERSION      STATUS      FLAG  ADDRESS      JOIN-TIME      NAME
S108DVD5FTEFGG54 v6.6.0 (5756) Authorized/Up 3 10.33.33.4   Thu Dec 3 18:36:35 2020 site1_access2
S108DVHUFKEFGG54 v6.6.0 (5756) Authorized/Up 3 10.33.33.1   Thu Dec 3 14:40:13 2020 site1_mclag1
S108DVSPUKEFGG54 v6.6.0 (5756) Authorized/Up 3 10.33.33.2   Thu Dec 3 14:42:05 2020 site1_mclag2
S108DVUBYKEFGG54 v6.6.0 (5756) Authorized/Up 3 10.33.33.3   Thu Dec 3 18:36:44 2020 site1_access1

Flags: C=config sync, U=upgrading, S=staged, D=delayed reboot pending, E=config sync error, 3=L3
Managed-Switches: 4 (UP: 4 DOWN: 0)

FGT_Switch_Controller # execute switch-controller get-physical-conn standard fol3_wan
This will display connectivity graph information for FortiLink from FortiGate's perspective
NOTE : If FortiSwitch is not authorized, no connectivity information will be shown
NOTE : If FortiSwitch is in idle state, no connectivity information will be shown
NOTE : If FortiSwitch ISL peer has inconsistent info, no connectivity information will be shown

FortiLink interface : fol3_wan

FortiGate(s)
FGVM04TM20006534(fol3_wan) <-----> S108DVHUFKEFGG54(port8)
FGVM04TM20006534(fol3_wan) <-----> S108DVSPUKEFGG54(port8)

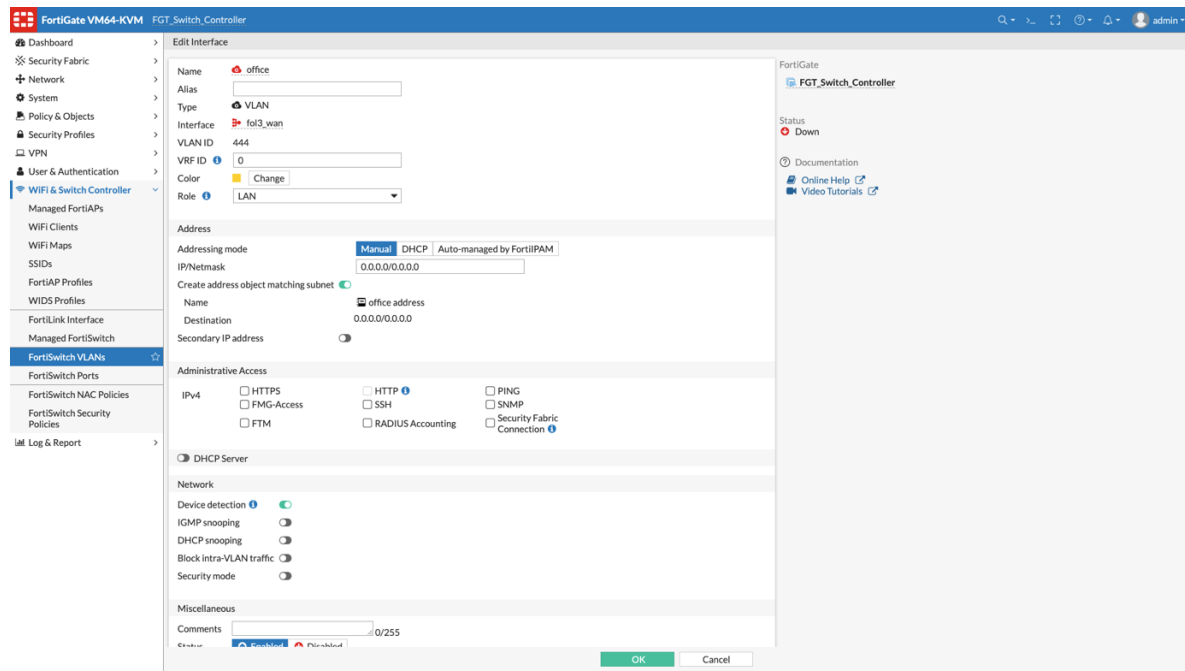
Tier 1
S108DVHUFKEFGG54(port8) <-----> FGVM04TM20006534(fol3_wan)
S108DVSPUKEFGG54(port8) <-----> FGVM04TM20006534(fol3_wan)

Tier 2+
S108DVHUFKEFGG54(port5/8DVD5FTEFGG54-0) <-----> S108DVD5FTEFGG54(port7/_F1InK1_MLAG0_)
S108DVSPUKEFGG54(port5/8DVD5FTEFGG54-0) <-----> S108DVD5FTEFGG54(port8/_F1InK1_MLAG0_)
S108DVSPUKEFGG54(port7/_F1InK1_ICL0_) <-----> S108DVHUFKEFGG54(port7/_F1InK1_ICL0_)
S108DVUBYKEFGG54(port7/_F1InK1_MLAG0_) <-----> S108DVHUFKEFGG54(port6/8DVUBYKEFGG54-0)
S108DVUBYKEFGG54(port8/_F1InK1_MLAG0_) <-----> S108DVSPUKEFGG54(port6/8DVUBYKEFGG54-0)

FGT_Switch_Controller #

```

2. Create FortiSwitch VLANs and assign them to FortiSwitch ports. You do not need to specify the IP address because the FortiGate device will not receive any of the data traffic (it will be switched locally or routed by the WAN router). Therefore, the DHCP service must be provided by the WAN router or other system located at the site.



FortiGate VM64-KVM FortiSwitch_Controller

Dashboard > Security Fabric > Network > System > Policy & Objects > Security Profiles > VPN > User & Authentication > **WiFi & Switch Controller** > Managed FortiSwitches > FortiSwitch VLANs

Edit Interface

Name: office
Alias:
Type: VLAN
Interface: foi3_wan
VLAN ID: 444
VRF ID: 0
Color: Change
Role: LAN

Address

Addressing mode: Manual DHCP Auto-managed by FortiIPAM
IP/Netmask: 0.0.0.0/0.0.0.0
Create address object matching subnet: ☒
Name: office address
Destination: 0.0.0.0/0.0.0.0
Secondary IP address: ☐

Administrative Access

IPv4: ☐ HTTPS ☐ HTTP ☐ PING ☐ SNMP
☐ FMG-Access ☐ SSH ☐ Security Fabric Connection
☐ FTM ☐ RADIUS Accounting

DHCP Server

Network

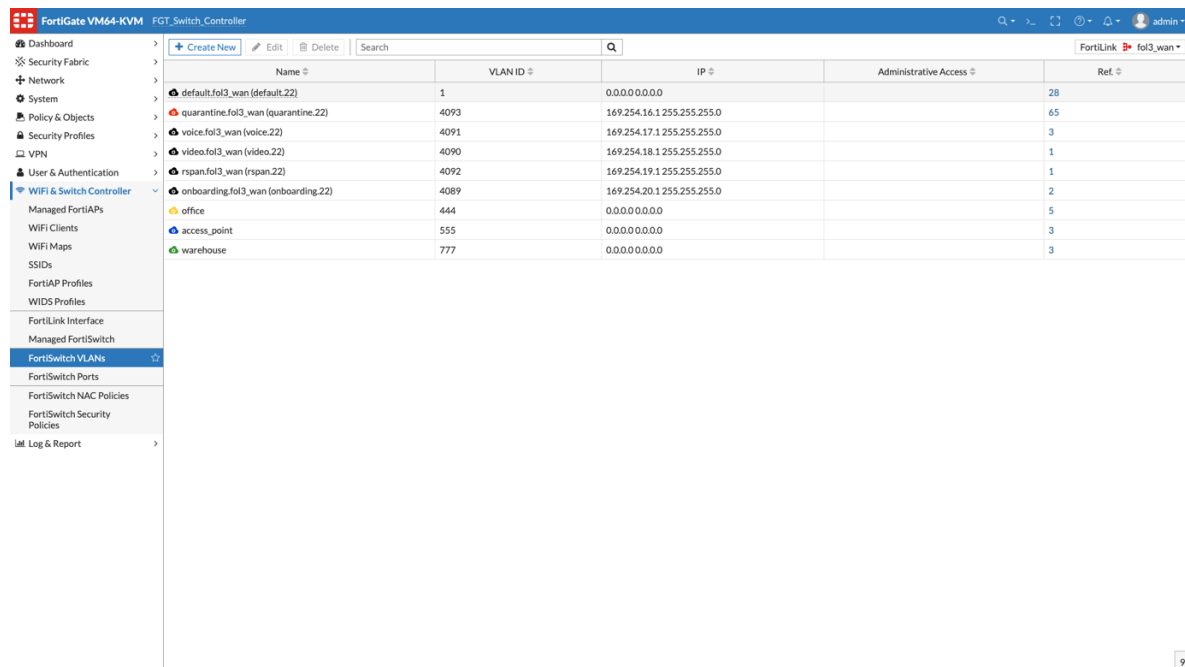
Device detection: ☒
IGMP snooping: ☐
DHCP snooping: ☐
Block intra-VLAN traffic: ☐
Security mode: ☐

Miscellaneous

Comments: 0/255

OK Cancel

FortiGate
FGT_Switch_Controller
Status: Down
Documentation
Online Help
Video Tutorials



FortiGate VM64-KVM FortiSwitch_Controller

Dashboard > Security Fabric > Network > System > Policy & Objects > Security Profiles > VPN > User & Authentication > **WiFi & Switch Controller** > Managed FortiSwitches > FortiSwitch VLANs

Create New Edit Delete Search

Name	VLAN ID	IP	Administrative Access	Ref
default.foi3_wan (default.22)	1	0.0.0.0/0.0.0.0		28
quarantine.foi3_wan (quarantine.22)	4093	169.254.16.1 255.255.255.0		65
voice.foi3_wan (voice.22)	4091	169.254.17.1 255.255.255.0		3
video.foi3_wan (video.22)	4090	169.254.18.1 255.255.255.0		1
rspan.foi3_wan (rspan.22)	4092	169.254.19.1 255.255.255.0		1
onboarding.foi3_wan (onboarding.22)	4089	169.254.20.1 255.255.255.0		2
office	444	0.0.0.0/0.0.0.0		5
access_point	555	0.0.0.0/0.0.0.0		3
warehouse	777	0.0.0.0/0.0.0.0		3

FortiGate VM64-KVM FGT_Switch_Controller							
Port	Trunk	Access Mode	Native VLAN	Allowed VLANs	Device Information	LLDP Profile	Security Policy
site1_access1 - S108DVUBYKEFGG54							
port1		Normal	office	quarantine.fol3_wan (quarantine.22)	02:09:0f:d3:13:01 fe:09:0f:d3:29:01 fe:ff:ff:00:00:29	default-auto-isl	
port2		Normal	access_point	office quarantine.fol3_wan (quarantine.22) warehouse	02:09:0f:d3:26:02 fe:09:0f:d3:2d:01	default-auto-isl	
port3		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	fe:09:0f:d3:00:07	default-auto-isl	
port4		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	fe:09:0f:d3:00:08	default-auto-isl	
port5		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	fe:09:0f:d3:00:09	default-auto-isl	
port6		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	fe:09:0f:d3:00:0a	default-auto-isl	
port7		Normal	S108DVHFUKEFGG54				
port8		Normal	S108DVSPUKEFGG54				
site1_access2 - S108DVDSFTEFGG54							
port1		Normal	office	quarantine.fol3_wan (quarantine.22)	02:09:0f:d3:2c:02 fe:09:0f:d3:0d:01 fe:ff:ff:00:00:2b	default-auto-isl	
port2		Normal	access_point	office quarantine.fol3_wan (quarantine.22) warehouse	02:09:0f:d3:11:01 fe:09:0f:d3:11:02 fe:ff:ff:00:00:27	default-auto-isl	
port3		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	fe:09:0f:d3:00:1a	default-auto-isl	
port4		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	fe:09:0f:d3:00:1b	default-auto-isl	
port5		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	fe:09:0f:d3:00:1c	default-auto-isl	
port6		Normal	default.fol3_wan (default.22)	quarantine.fol3_wan (quarantine.22)	fe:09:0f:d3:00:1d	default-auto-isl	
port7		Normal	S108DVHFUKEFGG54				
port8		Normal	S108DVSPUKEFGG54				
site1_mclag1 - S108DVHFUKEFGG54							
site1_mclag2 - S108DVSPUKEFGG54							

Check the configuration

The following is the relevant FortiGate configuration:

```
FGT_Switch_Controller # show system interface wan
config system interface
    edit "wan"
        set vdom "root"
        set ip 10.40.88.254 255.255.255.0
        set allowaccess ping https ssh http
        set type aggregate
        set member "port9" "port10"
        set lldp-reception enable
        set role wan
        set snmp-index 21
    next
end
FGT_Switch_Controller # show router static 2
config router static
    edit 2
        set dst 10.33.33.0 255.255.255.0
        set gateway 10.40.88.253
        set device "wan"
    next
end
FGT_Switch_Controller # show system interface fol3_wan
config system interface
    edit "fol3_wan"
        set vdom "root"
        set fortilink enable
```

```
        set switch-controller-source-ip fixed
        set ip 172.17.1.254 255.255.255.0
        set allowaccess ping fabric
        set type aggregate
        set device-identification enable
        set lldp-reception enable
        set lldp-transmission enable
        set snmp-index 22
        set switch-controller-nac "fol3_wan"
        set swc-first-create 127
        set lacp-mode static
    next
end

FGT_Switch_Controller # show firewall policy 5
config firewall policy
    edit 5
        set name "fsw_to_fol3_wan"
        set uuid 98af1592-354d-51eb-e09e-8d8000c0663a
        set srcintf "wan"
        set dstintf "fol3_wan"
        set srcaddr "fsw"
        set dstaddr "fol3_wan_IP"
        set action accept
        set schedule "always"
        set service "CAPWAP" "ALL_ICMP"
    next
end

FGT_Switch_Controller # show firewall service custom CAPWAP
config firewall service custom
    edit "CAPWAP"
        set udp-portrange 5246
    next
end

FGT_Switch_Controller # show firewall address fsw
config firewall address
    edit "fsw"
        set uuid 77e968bc-354d-51eb-f618-e3e145d6a172
        set subnet 10.33.33.0 255.255.255.0
    next
end

FGT_Switch_Controller # show firewall address fol3_wan_IP
config firewall address
    edit "fol3_wan_IP"
        set uuid 84cf157c-354d-51eb-ab4f-6518749b4bd9
        set subnet 172.17.1.254 255.255.255.255
    next
end

FGT_Switch_Controller # show switch-controller managed-switch
config switch-controller managed-switch
    edit "S108DVHFUKEFGG54"
        set name "site1_mclag1"
        set fsw-wan1-peer "fol3_wan"
```

```
set fsw-wan1-admin enable
set poe-detection-type 3
set version 1
set max-allowed-trunk-members 8
set pre-provisioned 1
set dynamic-capability 0x000000000000000000000000751c51f9f7
config ports
  edit "port1"
    set vlan "default.22"
    set allowed-vlans "quarantine.22"
    set untagged-vlans "quarantine.22"
    set export-to "root"
    set mac-addr 02:09:0f:d3:00:0c
  next
  edit "port2"
    set vlan "default.22"
    set allowed-vlans "quarantine.22"
    set untagged-vlans "quarantine.22"
    set export-to "root"
    set mac-addr 02:09:0f:d3:00:0d
  next
  edit "port3"
    set vlan "default.22"
    set allowed-vlans "quarantine.22"
    set untagged-vlans "quarantine.22"
    set export-to "root"
    set mac-addr 02:09:0f:d3:00:0e
  next
  edit "port4"
    set vlan "default.22"
    set allowed-vlans "quarantine.22"
    set untagged-vlans "quarantine.22"
    set export-to "root"
    set mac-addr 02:09:0f:d3:00:0f
  next
  edit "port5"
    set vlan "default.22"
    set allowed-vlans "quarantine.22"
    set untagged-vlans "quarantine.22"
    set export-to "root"
    set mac-addr 02:09:0f:d3:0a:01
  next
  edit "port6"
    set vlan "default.22"
    set allowed-vlans "quarantine.22"
    set untagged-vlans "quarantine.22"
    set export-to "root"
    set mac-addr 02:09:0f:d3:22:01
  next
  edit "port7"
    set vlan "default.22"
    set allowed-vlans "quarantine.22"
    set untagged-vlans "quarantine.22"
    set lldp-profile "default-auto-mclag-icl"
    set export-to "root"
    set mac-addr 02:09:0f:d3:1f:01
  next
```



```
edit "port8"
    set vlan "default.22"
    set allowed-vlans "quarantine.22"
    set untagged-vlans "quarantine.22"
    set export-to "root"
    set mac-addr 02:09:0f:d3:1d:02
next
end
next
edit "S108DVSPUKEFGG54"
    set name "site1_mclag2"
    set fsw-wan1-peer "fol3_wan"
    set fsw-wan1-admin enable
    set poe-detection-type 3
    set version 1
    set max-allowed-trunk-members 8
    set pre-provisioned 1
    set dynamic-capability 0x000000000000000000000000751c51f9f7
config ports
    edit "port1"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:11
    next
    edit "port2"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:12
    next
    edit "port3"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:13
    next
    edit "port4"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:14
    next
    edit "port5"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:0b:02
    next
    edit "port6"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
```

```
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:23:01
    next
    edit "port7"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set lldp-profile "default-auto-mclag-icl"
        set export-to "root"
        set mac-addr 02:09:0f:d3:1f:02
    next
    edit "port8"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:1e:02
    next
end
next
edit "S108DVUBYKEFGG54"
    set name "site1_access1"
    set fsw-wan1-peer "fol3_wan"
    set fsw-wan1-admin enable
    set poe-detection-type 3
    set version 1
    set max-allowed-trunk-members 8
    set pre-provisioned 1
    set dynamic-capability 0x000000000000000000000000751c51f9f7
config ports
    edit "port1"
        set vlan "office"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:29:01
    next
    edit "port2"
        set vlan "access_point"
        set allowed-vlans "office" "quarantine.22" "warehouse"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:2d:01
    next
    edit "port3"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:07
    next
    edit "port4"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
```

```
        set mac-addr 02:09:0f:d3:00:08
    next
    edit "port5"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:09
    next
    edit "port6"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:0a
    next
    edit "port7"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:20:02
    next
    edit "port8"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:20:02
    next
end
next
edit "S108DVD5FTEFGG54"
    set name "site1_access2"
    set fsw-wan1-peer "fol3_wan"
    set fsw-wan1-admin enable
    set poe-detection-type 3
    set version 1
    set max-allowed-trunk-members 8
    set pre-provisioned 1
    set dynamic-capability 0x000000000000000000000000751c51f9f7
config ports
    edit "port1"
        set vlan "office"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:0d:01
    next
    edit "port2"
        set vlan "access_point"
        set allowed-vlans "office" "quarantine.22" "warehouse"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:11:02
    next
    edit "port3"
```

```
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:1a
    next
    edit "port4"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:1b
    next
    edit "port5"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:1c
    next
    edit "port6"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:00:1d
    next
    edit "port7"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:0b:01
    next
    edit "port8"
        set vlan "default.22"
        set allowed-vlans "quarantine.22"
        set untagged-vlans "quarantine.22"
        set export-to "root"
        set mac-addr 02:09:0f:d3:0b:01
    next
end
next
end
```

The following is the relevant configuration of the WAN router:

```
WAN_ROUTER # show system interface to_fgt
config system interface
    edit "to_fgt"
        set ip 10.40.88.253 255.255.255.0
        set allowaccess ping https ssh
        set snmp-index 16
        set vlanid 4088
        set interface "internal"
    next
end
```

```
WAN_ROUTER # show switch interface to_fgt
config switch interface
  edit "to_fgt"
    set native-vlan 4088
    set snmp-index 14
  next
end
```

```
WAN_ROUTER # show switch trunk to_fgt
config switch trunk
  edit "to_fgt"
    set mode lacp-active
    set members "port7" "port8"
  next
end
```

```
WAN_ROUTER # show system interface fol3
config system interface
  edit "fol3"
    set ip 10.33.33.254 255.255.255.0
    set allowaccess ping https ssh
    set snmp-index 17
    set vlanid 4094
    set interface "internal"
  next
end
```

```
WAN_ROUTER # show system dhcp server
config system dhcp server
  edit 1
    set default-gateway 10.33.33.254
    set dns-service local
    set interface "fol3"
    config ip-range
      edit 1
        set end-ip 10.33.33.99
        set start-ip 10.33.33.1
      next
    end
    set lease-time 300
    set netmask 255.255.255.0
    set ntp-service local
    set vci-match enable
    set vci-string "FortiSwitch"
    set wifi-acl 172.17.1.254
  next
end
```

```
WAN_ROUTER # show switch interface fol3
config switch interface
  edit "fol3"
    set native-vlan 4094
    set allowed-vlans 1001
    set edge-port disabled
    set snmp-index 15
  next
```

```
end

WAN_ROUTER # show switch trunk fol3
config switch trunk
    edit "fol3"
        set mode lacp-active
        set members "port5" "port6"
    next
end

WAN_ROUTER # show router static 2
config router static
    edit 2
        set device "to_fgt"
        set dst 172.17.1.0 255.255.255.0
        set gateway 10.40.88.254
    next
end
```

The following is the relevant configuration of the FortiSwitch MCLAG 1:

```
site1_mclag1 # show switch-controller global
config switch-controller global
    set ac-discovery-type dhcp
end

site1_mclag1 # show switch trunk
config switch trunk
    edit "__FoRtILnk0L3__"
        set mode lacp-active
        set mclag enable
        set members "port8"
    next
    edit "_FlInK1_ICL0_"
        set mode lacp-active
        set auto-is1 1
        set mclag-icl enable
        set members "port7"
    next
    edit "8DVUBYKEFGG54-0"
        set mode lacp-active
        set auto-is1 1
        set mclag enable
        set members "port6"
    next
    edit "8DVD5FTEFGG54-0"
        set mode lacp-active
        set auto-is1 1
        set mclag enable
        set members "port5"
    next
end

site1_mclag1 # show switch interface __FoRtILnk0L3__
config switch interface
    edit "__FoRtILnk0L3__"
        set native-vlan 4094
```

```
        set allowed-vlans 1,444,555,777,4089-4093
        set dhcp-snooping trusted
        set snmp-index 12
    next
end

site1_mclag1 # show switch interface _FlInK1_ICL0_
config switch interface
    edit "_FlInK1_ICL0_"
        set native-vlan 4094
        set allowed-vlans 1,444,555,777,4089-4093
        set dhcp-snooping trusted
        set edge-port disabled
        set snmp-index 13
    next
end

site1_mclag1 # show switch physical-port port8
config switch physical-port
    edit "port8"
        set lldp-profile "default-auto-isl"
        set speed auto
        set storm-control-mode disabled
    next
end

site1_mclag1 # show switch physical-port port7
config switch physical-port
    edit "port7"
        set l2-learning disabled
        set lldp-profile "default-auto-mclag-icl"
        set speed auto
        set storm-control-mode disabled
        set l2-sa-unknown forward
    next
end

site1_mclag1 # show switch physical-port port6
config switch physical-port
    edit "port6"
        set lldp-profile "default-auto-isl"
        set speed auto
    next
end

site1_mclag1 # show switch physical-port port5
config switch physical-port
    edit "port5"
        set lldp-profile "default-auto-isl"
        set speed auto
    next
end
```

The following is the relevant configuration of the FortiSwitch MCLAG 2:

```
site1_mclag2 # show switch-controller global
config switch-controller global
```

```
    set ac-discovery-type dhcp
end

sitel_mclag2 # show switch trunk
config switch trunk
    edit "_FlInK1_ICL0_"
        set mode lacp-active
        set auto-isl 1
        set mclag-icl enable
        set members "port7"
    next
    edit "__FoRtILnk0L3__"
        set mode lacp-active
        set mclag enable
        set members "port8"
    next
    edit "8DVUBYKEFGG54-0"
        set mode lacp-active
        set auto-isl 1
        set mclag enable
        set members "port6"
    next
    edit "8DVD5FTEFGG54-0"
        set mode lacp-active
        set auto-isl 1
        set mclag enable
        set members "port5"
    next
end

sitel_mclag2 # show switch interface __FoRtILnk0L3__
config switch interface
    edit "__FoRtILnk0L3__"
        set native-vlan 4094
        set allowed-vlans 1,444,555,777,4089-4093
        set dhcp-snooping trusted
        set snmp-index 13
    next
end

sitel_mclag2 # show switch interface _FlInK1_ICL0_
config switch interface
    edit "_FlInK1_ICL0_"
        set native-vlan 4094
        set allowed-vlans 1,444,555,777,4089-4093
        set dhcp-snooping trusted
        set edge-port disabled
        set snmp-index 12
    next
end

sitel_mclag2 # show switch physical-port port8
config switch physical-port
    edit "port8"
        set lldp-profile "default-auto-isl"
        set speed auto
        set storm-control-mode disabled
```



```
    next
end

site1_mclag2 # show switch physical-port port7
config switch physical-port
    edit "port7"
        set l2-learning disabled
        set lldp-profile "default-auto-mclag-icl"
        set speed auto
        set storm-control-mode disabled
        set l2-sa-unknown forward
    next
end

site1_mclag2 # show switch physical-port port6
config switch physical-port
    edit "port6"
        set lldp-profile "default-auto-isl"
        set speed auto
    next
end

site1_mclag2 # show switch physical-port port5
config switch physical-port
    edit "port5"
        set lldp-profile "default-auto-isl"
        set speed auto
    next
end
```

The following is the relevant configuration of the FortiSwitch access switch 1:

```
site1_access1 # show switch-controller global
config switch-controller global
    set ac-discovery-type dhcp
end

site1_access1 # show switch trunk
config switch trunk
    edit "_FlInK1_MLAG0_"
        set mode lacp-active
        set auto-isl 1
        set mclag enable
        set members "port7" "port8"
    next
end

site1_access1 # show switch interface _FlInK1_MLAG0_
config switch interface
    edit "_FlInK1_MLAG0_"
        set native-vlan 4094
        set allowed-vlans 1,444,555,777,4089-4093
        set dhcp-snooping trusted
        set edge-port disabled
        set snmp-index 13
    next
end
```

```
sitel_access1 # show switch physical-port port7
config switch physical-port
    edit "port7"
        set lldp-profile "default-auto-isl"
        set speed auto
        set storm-control-mode disabled
    next
end
```

```
sitel_access1 # show switch physical-port port8
config switch physical-port
    edit "port8"
        set lldp-profile "default-auto-isl"
        set speed auto
        set storm-control-mode disabled
    next
end
```

```
sitel_access1 # show switch interface port1
config switch interface
    edit "port1"
        set native-vlan 444
        set allowed-vlans 4093
        set untagged-vlans 4093
        set snmp-index 1
    next
end
```

```
sitel_access1 # show switch interface port2
config switch interface
    edit "port2"
        set native-vlan 555
        set allowed-vlans 444,777,4093
        set untagged-vlans 4093
        set snmp-index 2
    next
end
```

The following is the relevant configuration of the FortiSwitch access switch 2:

```
sitel_access2 # show switch-controller global
config switch-controller global
    set ac-discovery-type dhcp
end

sitel_access2 # show switch trunk
config switch trunk
    edit "_FlInK1_MLAG0_"
        set mode lacp-active
        set auto-isl 1
        set mclag enable
        set members "port8" "port7"
    next
end

sitel_access2 # show switch interface _FlInK1_MLAG0_
```

```
config switch interface
  edit "_FlInKl_MLAG0_"
    set native-vlan 4094
    set allowed-vlans 1,444,555,777,4089-4093
    set dhcp-snooping trusted
    set edge-port disabled
    set snmp-index 13
  next
end

sitel_access2 # show switch physical-port port7
config switch physical-port
  edit "port7"
    set lldp-profile "default-auto-isl"
    set speed auto
    set storm-control-mode disabled
  next
end

sitel_access2 # show switch physical-port port8
config switch physical-port
  edit "port8"
    set lldp-profile "default-auto-isl"
    set speed auto
    set storm-control-mode disabled
  next
end

sitel_access2 # show switch interface port1
config switch interface
  edit "port1"
    set native-vlan 444
    set allowed-vlans 4093
    set untagged-vlans 4093
    set snmp-index 1
  next
end

sitel_access2 # show switch interface port2
config switch interface
  edit "port2"
    set native-vlan 555
    set allowed-vlans 444,777,4093
    set untagged-vlans 4093
    set snmp-index 2
  next
end
```



FORTINET®



Copyright© 2022 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.