FortiAuthenticator 产品实施一本通

版本	1.2
时间	2024 年 3 月
设备版本	v6.4.4, build1028 (GA)
作者	夏苗青
状态	已审核
反馈	support_cn@fortinet.com

目录

简介.....4
一. FAC 初始安装.....5
1. FAC License.....5
2. FAC 初始配置.....6
2.1 接口相关配置.....6
2.2 配置 FAC 其它管理信息.....7
2.3 SMTP 设置.....8
2.4 FAC SNMP 相关设置.....9
3. 用户管理.....10
3.1 本地用户.....10
3.2 Remote 用户.....13
3.3 MAC 地址认证用户.....14
3.4 用户组.....14
3.5 Remote 用户同步规则.....18
3.6 关于 Radius Realm 设置.....22
3.7 FortiToken 的使用.....24
4. LDAP Server 配置.....27
5. 证书相关配置.....28
5.1 FAC https 证书.....28
5.2 SMTP 通讯用证书.....30
5.3 使用 FAC 给别的设备下发证书.....31
5.4 FAC 给防火墙下发 SAML 认证证书.....36
6. HA 部署.....38
6.1 HA A-P 模式介绍.....38
6.2 HA A-P 模式的配置.....39
6.3 HA A-P 模式状态查看.....41
6.4 HA A-P 模式的 HA 心跳和切换.....42
6.5 HA A-P HA 日志查看.....44
6.6 HA LB 模式介绍.....44
6.7 HA LB 模式的配置.....45
6.8 HA LB 模式状态查看.....46
6.9 HA LB 模式的心跳.....47
6.10 HA LB 模式日志查看.....47
二. FAC 常用部署案例介绍.....49
1. 无线 WPA2 企业认证.....49
1.1 测试组网.....49
1.2 防火墙相关配置.....49
1.3 FAC 侧相关配置.....51
1.4 相关测试日志.....55
2. 无线 MAC+Portal 认证.....57

2.1 测试组网 57
2.2 防火墙相关配置 57
2.3 FAC 侧相关配置 61
2.4 相关测试日志 64
3. FortiClient 基于 SAML 的 VPN 认证 68
3.1 测试组网 68
3.2 FAC 侧相关配置 69
3.3 防火墙侧相关配置 72
3.4 PC 侧相关配置 83
3.5 相关测试日志 83
4. TACACS+ 认证 86
4.1 测试组网 86
4.2 防火墙侧相关配置 86
4.3 FAC 侧配置 89
4.4 相关测试日志 92
三. 日常维护 96
1. 管理员操作 96
1.1 admin 管理员操作 96
1.2 其它管理员操作 96
1.3 REST API 管理员 98
2. 系统配置文件备份和恢复 99
3. 设备重启 99
4. 设备关机 100
5. 设备升级 100
6. FAC 日志相关 101
6.1 日志查看 101
6.2 日志下载 102
6.3 日志设置 102
6.4 用户审计 103
四. 常见问题及 debug 方法 104
1. FAC 的 debug 方法 104
1.1 Log 日志 104
1.2 Debug 日志 104
1.3 Debug 报告 106
1.4 报文抓取 106
2. 常见问题的处理方法 107

简介

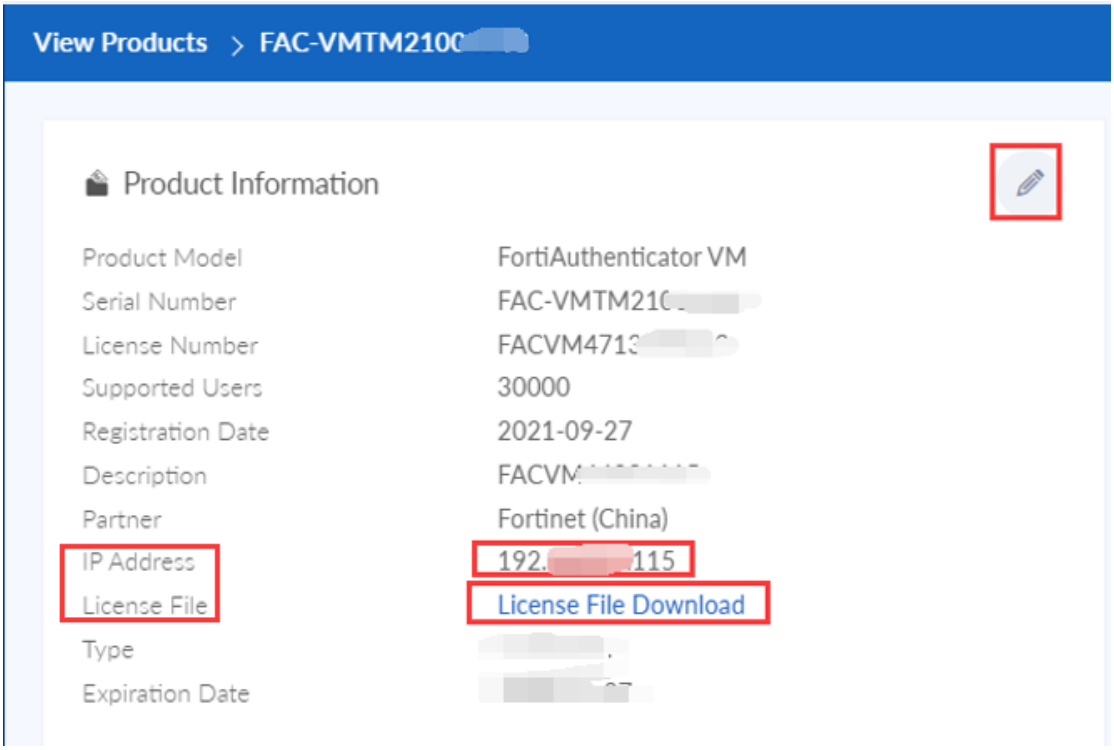
FAC(FortiAuthenticator) 作为专业认证服务器支持 Radius/Portal/Saml/OAuth 等认证, 本文描述了 FAC 设备在部署时的配置指导以及一些售后经常遇到的一些问题的解决和分析方法.

一. FAC 初始安装

1. FAC License

1.1 对于 FAC VM 设备的 License，可以在 support 帐号上下载，注册这个设备时会提示设置设备的 ip 地址，FAC 的 VM license 之后会绑定这个 ip 地址，这个 ip 地址可以是 FAC 任何一个接口的 ip 地址；

1.2 如果 FAC 需要修改这个 ip 地址，那么需要先在 support 网站修改这个 ip 地址，然后重新下载 license，然后在 FAC 上修改 ip 地址后，导入这个新的 license.

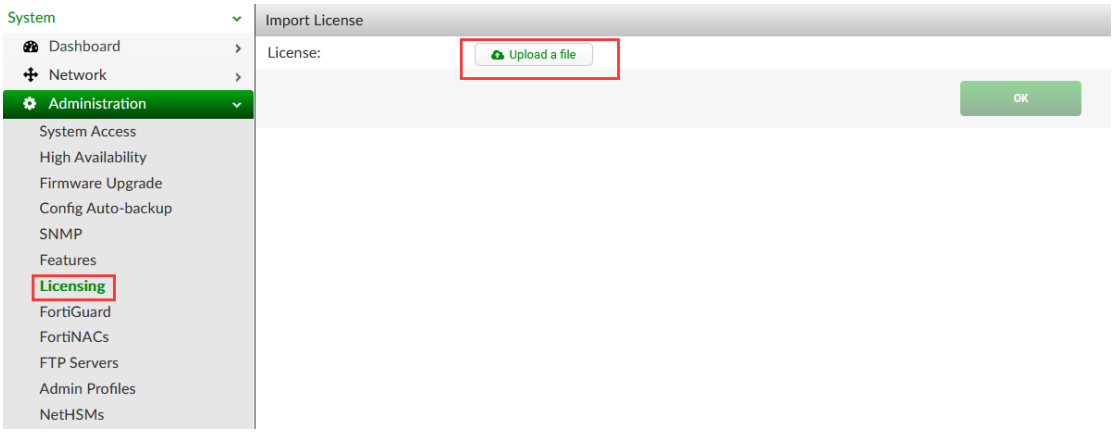


1.3 购买的 FAC 使用的 token 的 license 是永久的.

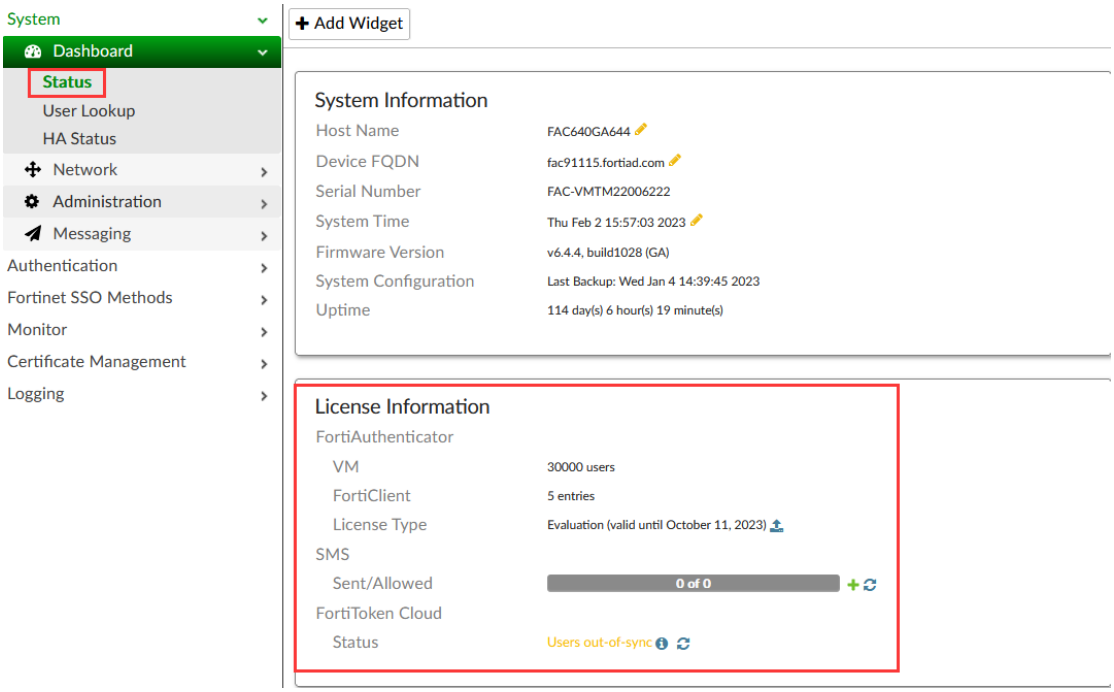
1.4 HA 设备之间的 token license 可以有限共享，具体可参考 HA 部署的章节.

1.5 FAC 的 token license 与 FAC 的序列号绑定，如需转移 token license 请联系售后 CS team 做此操作.

1.6 可在 FAC 的下面管理页面上传 FAC 的 License



1.7 可在 FAC 的 status 页面查看 License 的相关信息



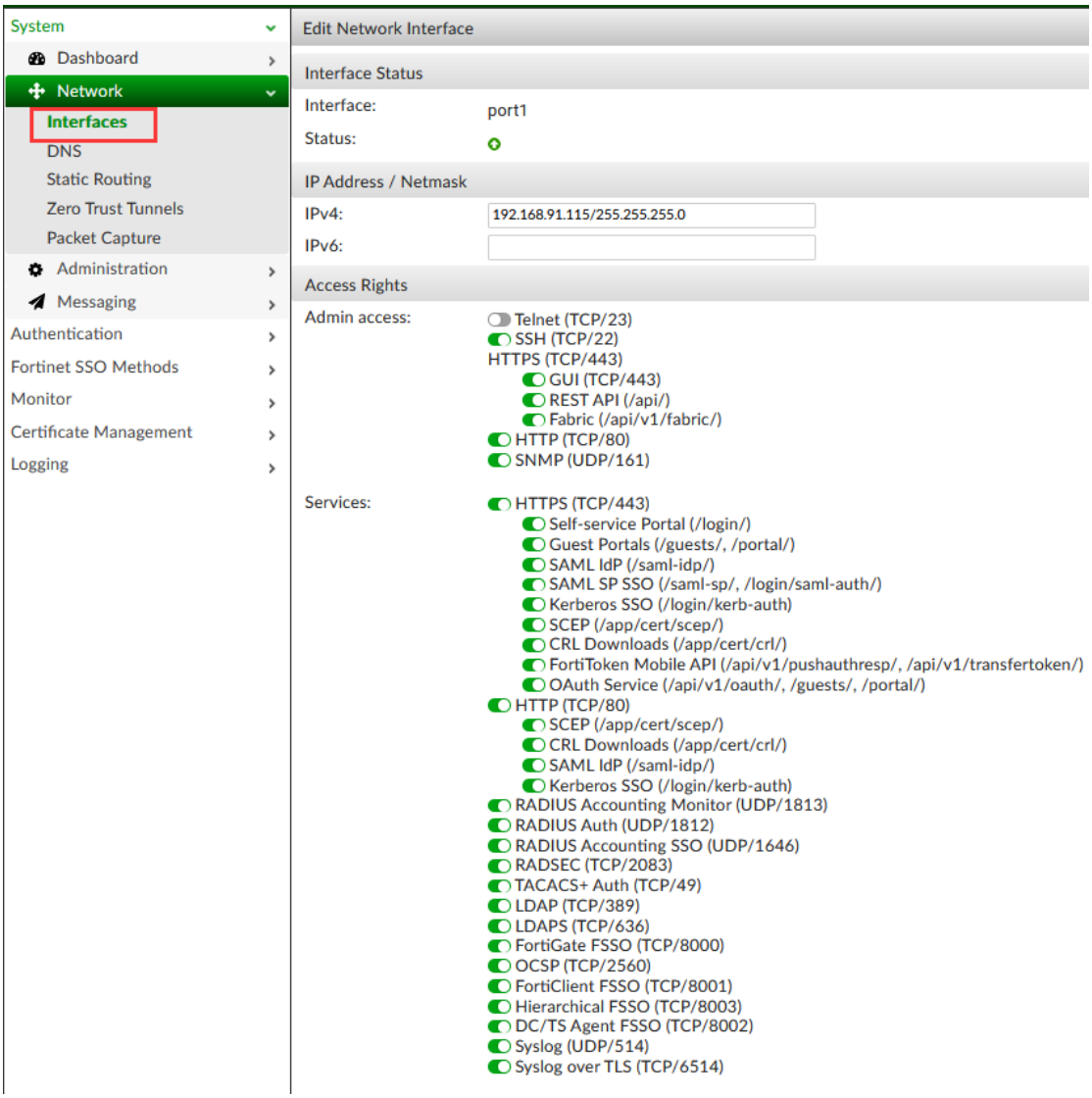
2. FAC 初始配置

2.1 接口相关配置

登录 FAC 的命令行下，配置 FAC 的接口地址，比如:

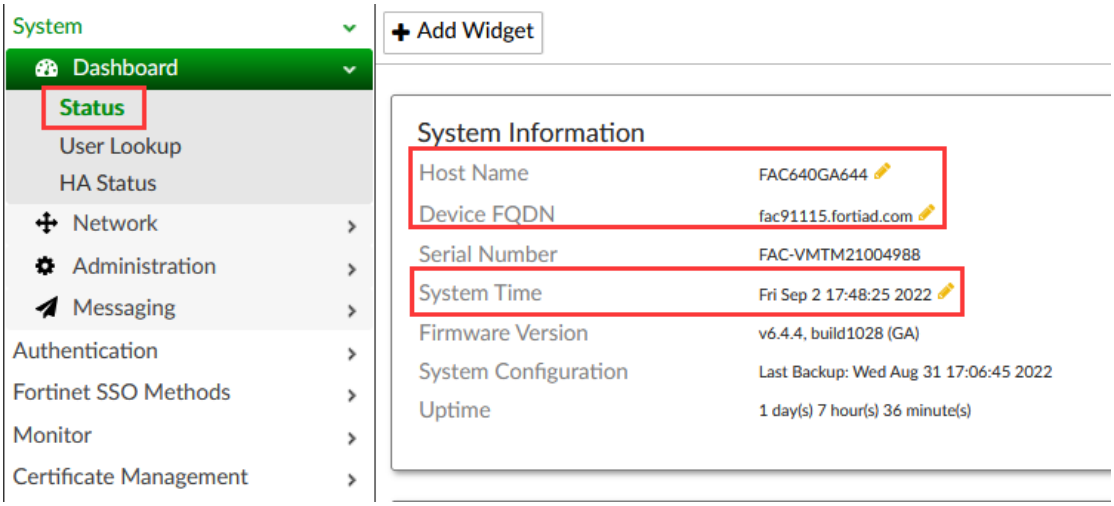
```
config system interface
        edit port1
                set ip 192.168.91.115/255.255.255.0
                set mtu 1500
                set allowaccess snmp ssh http-gui https-api https-fabric https-gui
        next
end

config system interface
        edit port1
                set ip 192.168.91.115/255.255.255.0
                set mtu 1500
                set allowaccess snmp ssh http-gui https-api https-fabric https-gui
        next
end
```

注意:配置完成后，能够登录到 FAC 的 GUI 页面后，需要在下面的接口下根据业务需要开启相应的接口访问权限.



2.2 配置 FAC 其它管理信息

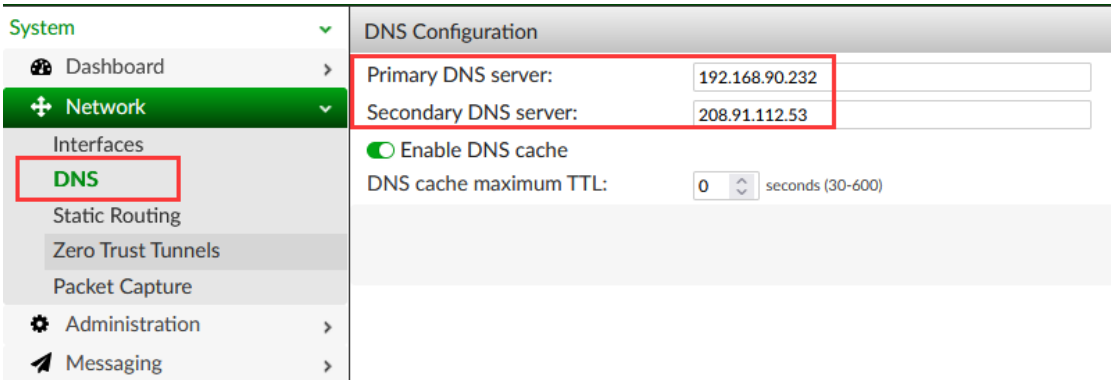
登录 FAC 的管理页面后，可以配置 FAC 的 Hostname/时间等信息



注意, FAC 的时间必须正确，否则可能会导致有些认证失败.

DNS 设置:

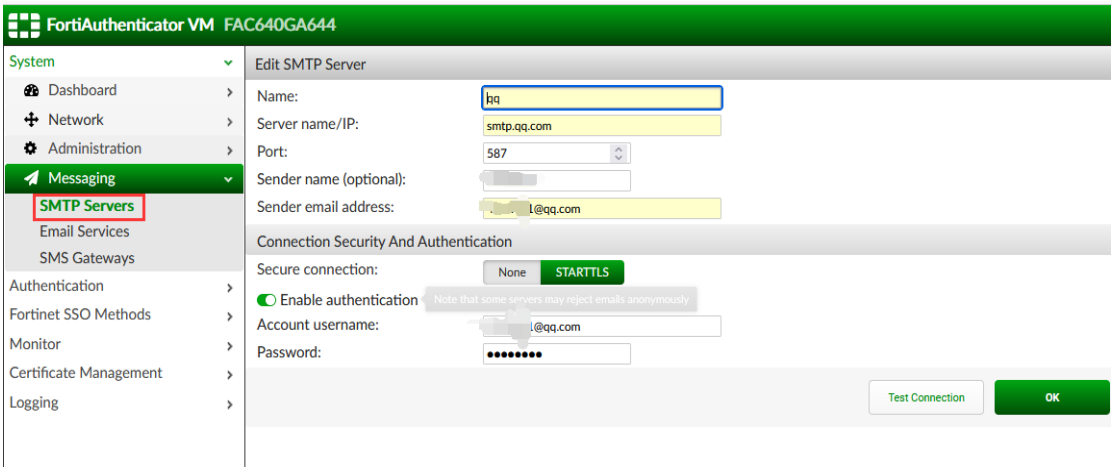
有些认证比如 wpa2 认证，需要 FAC 要加入到域，那 DNS Server 必须能做 AD 域名解析，所以如果 AD 域也是 DNS Server 的话,可以把 FAC DNS 域指向 AD 域的 DNS Server.



2.3 SMTP 设置

有些场景需要 FAC 通过 SMTP 发送邮件给用户，比如发送 email token 或是发送 FTM token 激活邮件.

如果可能，最好是使用跟用户一个邮件域的邮箱地址:

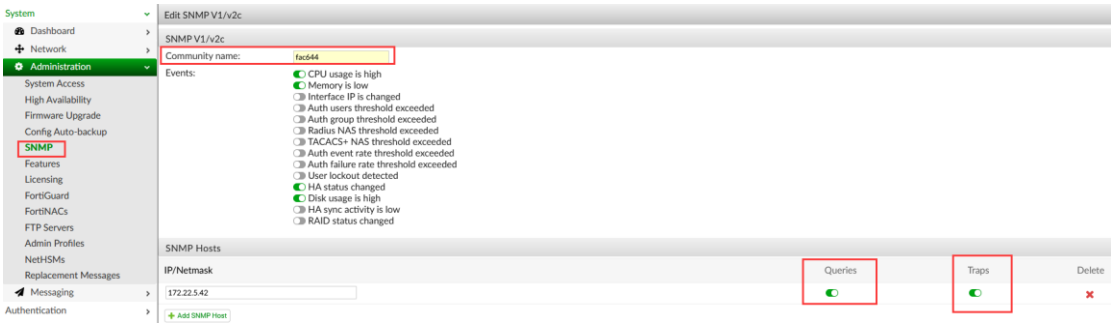


注意: SMTP 配置完成后可以点击上面的”Test Connection” 来测试一下, SMTP 是否能正常工作;

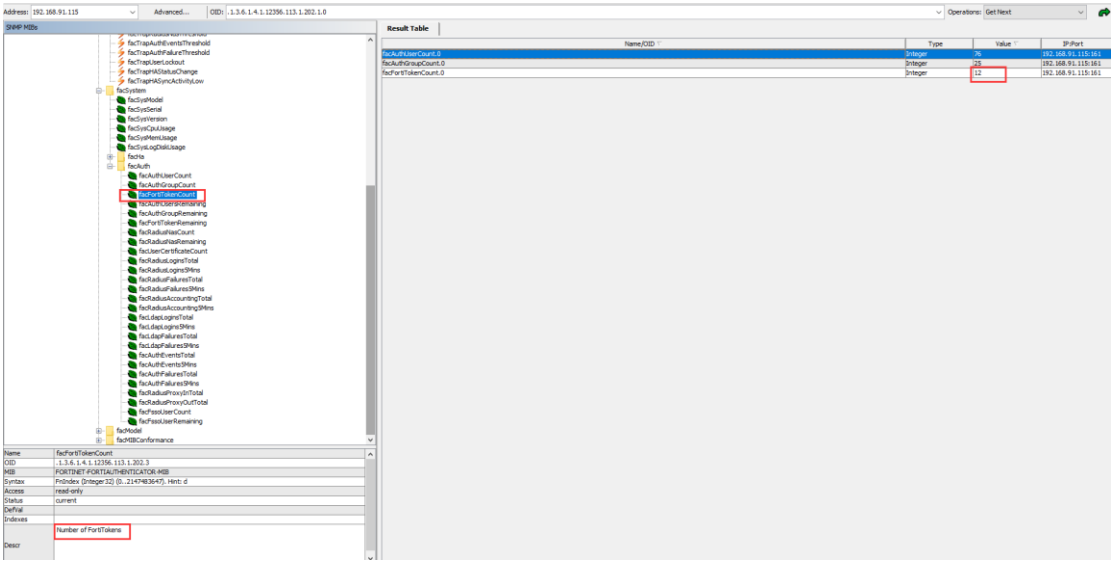
然后设置邮箱为默认使用邮箱.

2.4 FAC SNMP 相关设置

可以配置 FAC 的 snmp 查询和 TRAP:

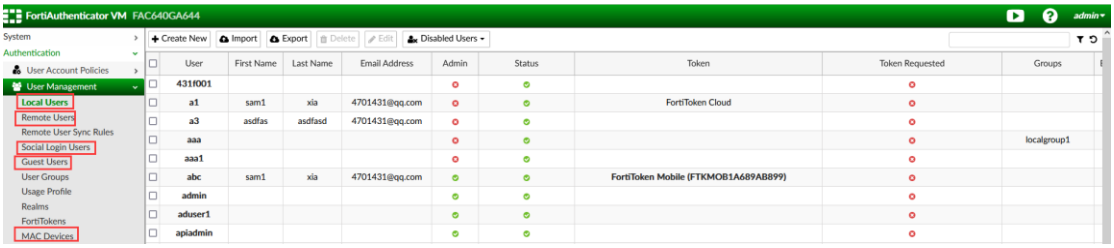


注意:FAC 的 snmp 查询都是 read-only, 下图示例为读取 FAC 的 token 数量:



3. 用户管理

FAC 上的用户根据认证场景的不同，包括本地用户/远端用户/Social 认证用户/访客用户以及 MAC 地址认证用户.

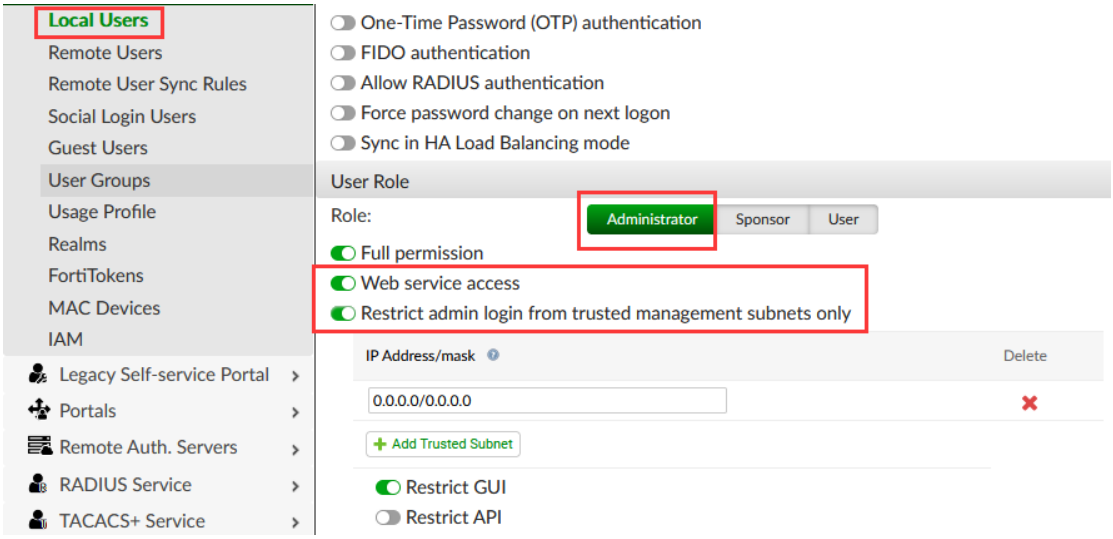


3.1 本地用户

本地用户即创建在 FAC 本地数据库的用户，管理员可以在创建好本地用户，配置正确的用户邮箱等信息后，选择给用户是否配置 token;

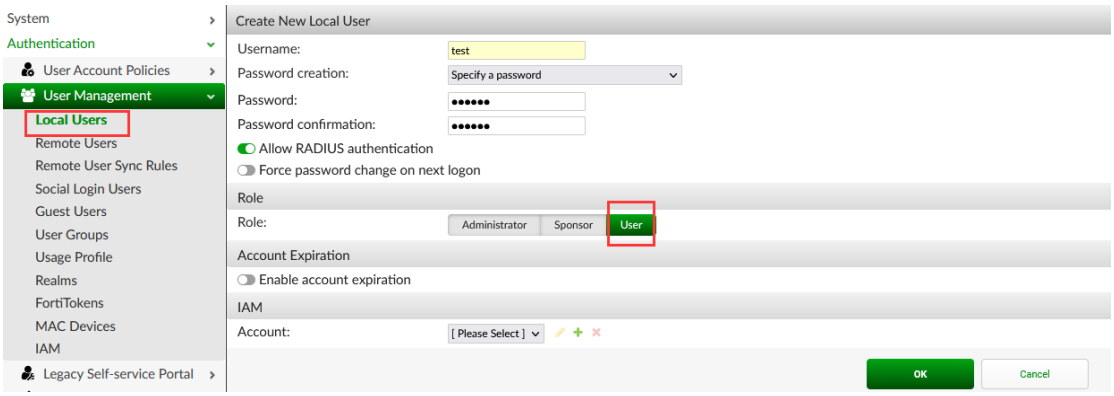
管理员用户:

创建管理员用户时,可以选择是否开启用户的 REST API 访问权限或是登录的网络限制:

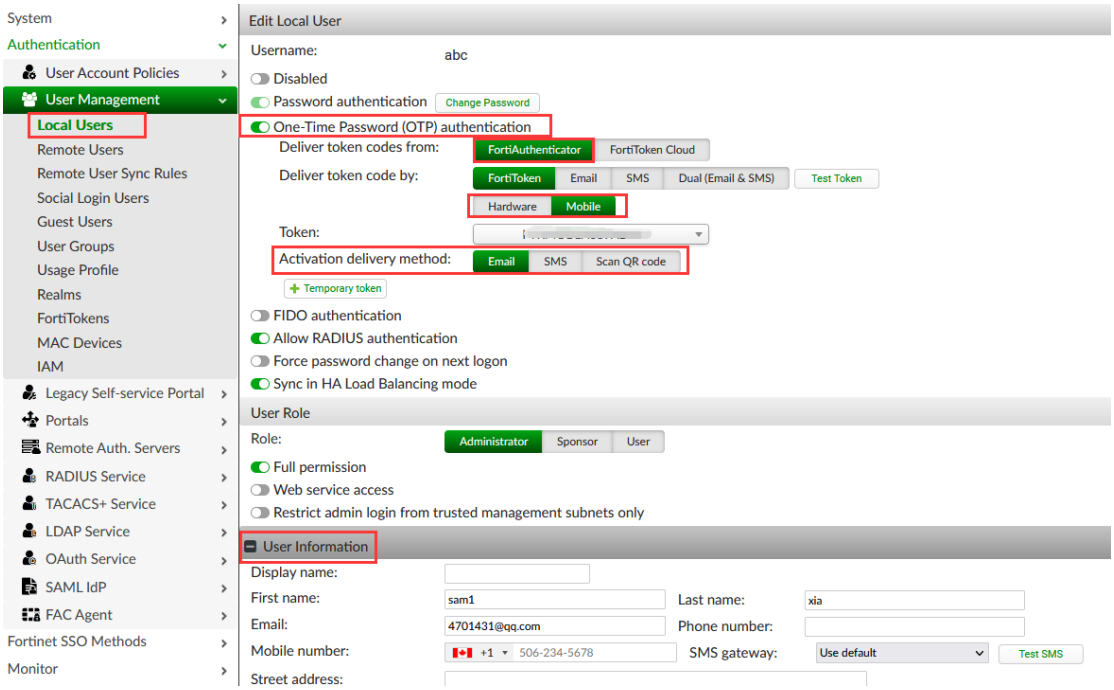


本地用户:

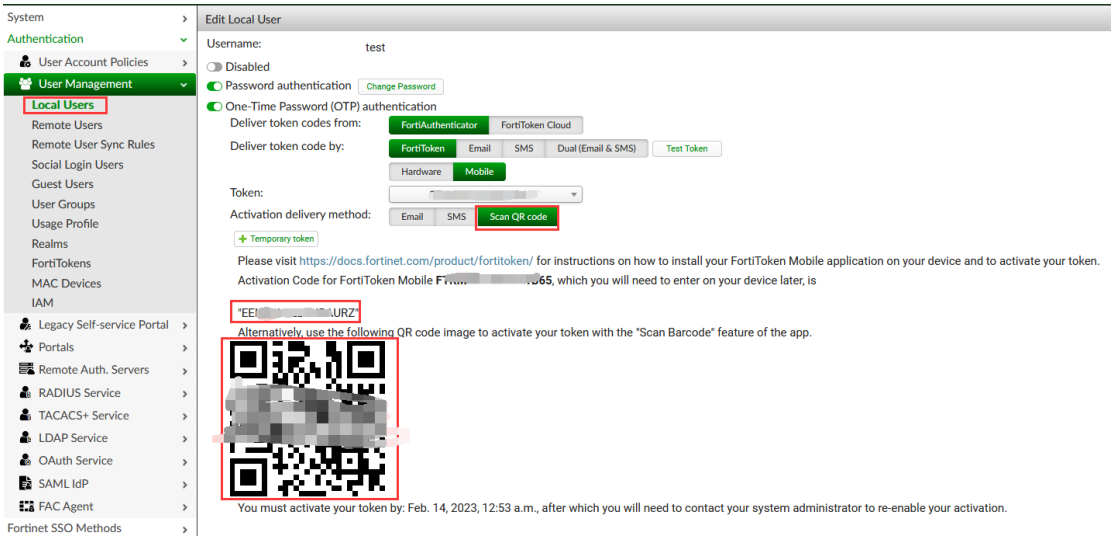
本地用户创建后，才能添加用户的更多个人信息:



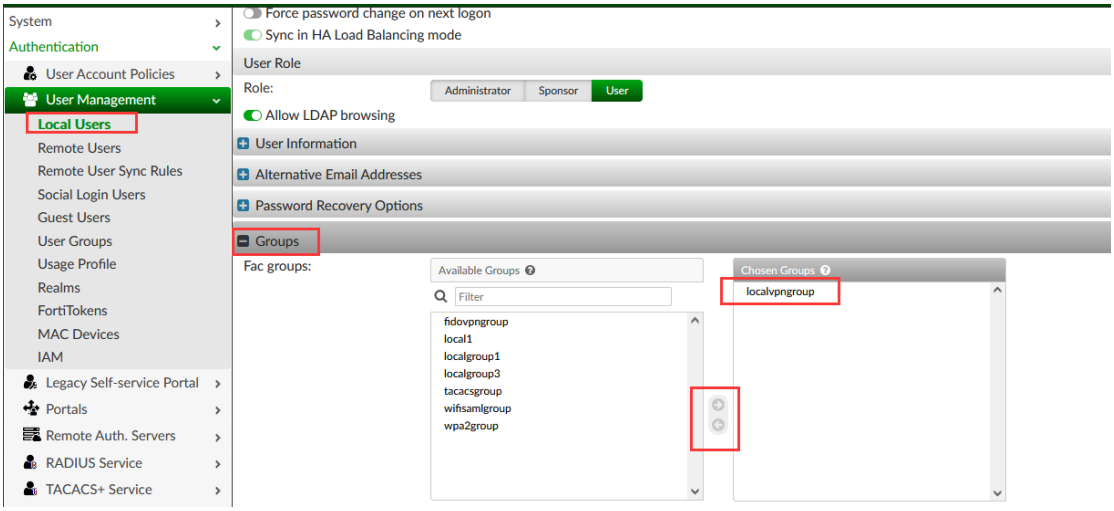
配置了用户的一些基本信息后，就可以给本地用户分 token:



给用户分配 token 时，可以选择是用 Email/短信的方式发功 token 信息给用户，提示用户激活 token，另外还可以选择直接显示 QR 码，然后选择以别的方式把这个 QR 码发送给用户(比如用户邮箱暂时不能收取邮件):



创建用户的同时，还可以选择配置用户的组信息:



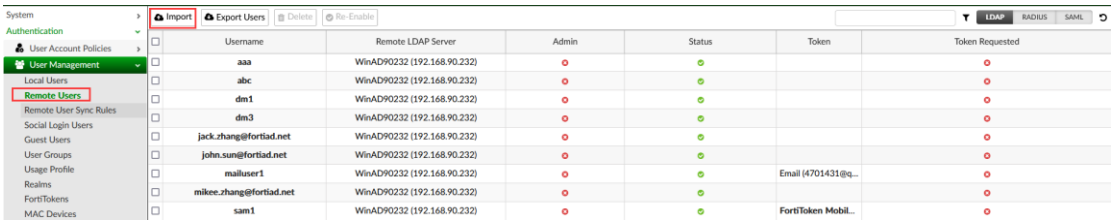
用户的组信息可以在上面页面配置，也可以在用户组的配置页面进行配置;

3.2 Remote 用户

Remote 用户是指用户 base 在远端服务器上的用户，Remote 用户有 LDAP/Radius/SAML，常用的 remote 用户是 LDAP 用户;

需要注意的是:FAC 导入 Remote 用户只是为了对用户认证做更多的控制，比如用户 group 控制，用户是否开启 token 认证等，FAC 没有用户的密码信息，所以每次认证时 FAC 通过把用户的信息发送给远端的 server 去校验，所以理论上来说，即使 FAC 上没有这个 Remote 用户的信息，Remote 用户也可以通过 FAC 去做认证;

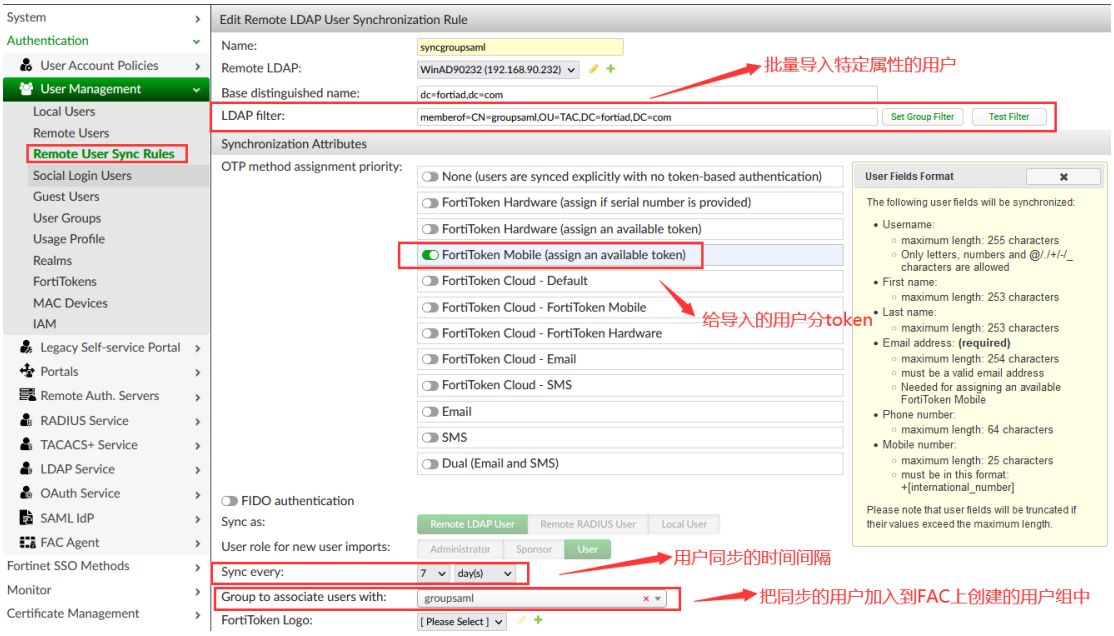
Remote 用户可以手动导入，并且手动给 Remote 用户分 token:



也可以基于同步规则批量导入特定用户，并且可以选择在导入用户的同时是否给用户自动分配 token:

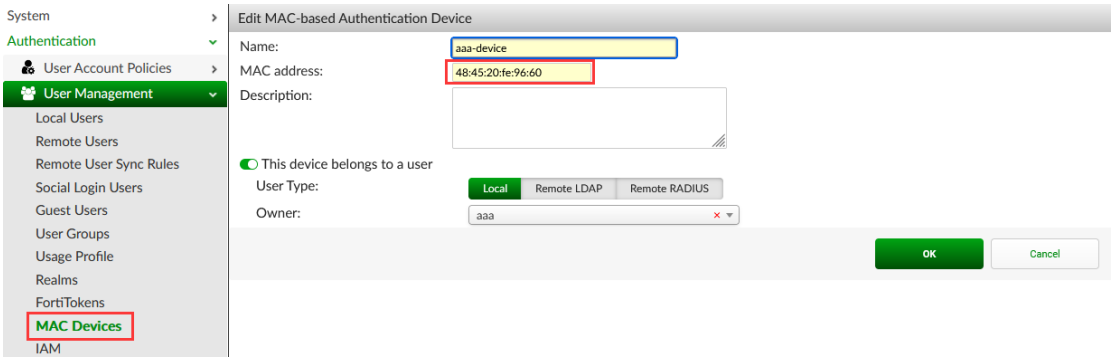
比如下面示例中，把 LDAP Server 上所有的 groupsaml 组中的用户导入

到 FAC 上，同时把这些用户加入到 FAC 上创建的 groupsaml 这个组中:



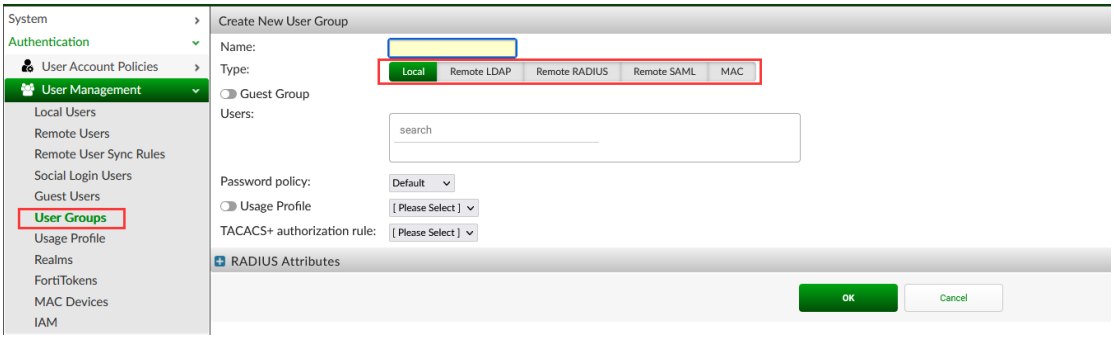
3.3 MAC 地址认证用户

FAC 支持 MAC 地址认证，以及 Portal 认证的 MAB Bypass 认证，可以在 FAC 上手动或自动添加 MAC 地址设备（Portal + MAB Bypass);



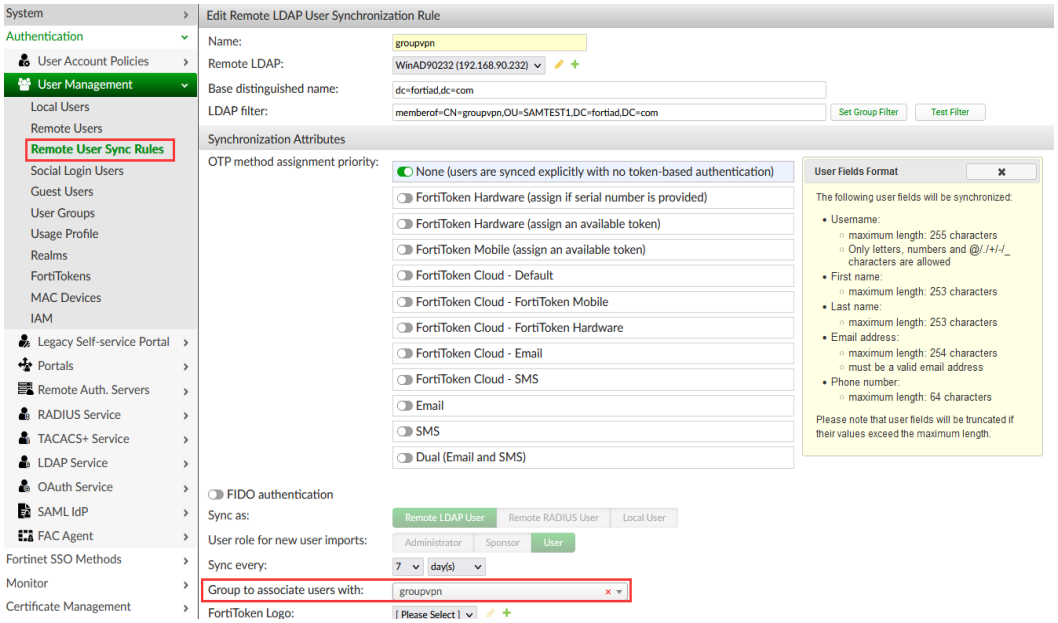
3.4 用户组

FAC 上可以配置不同用户属于不同的组:

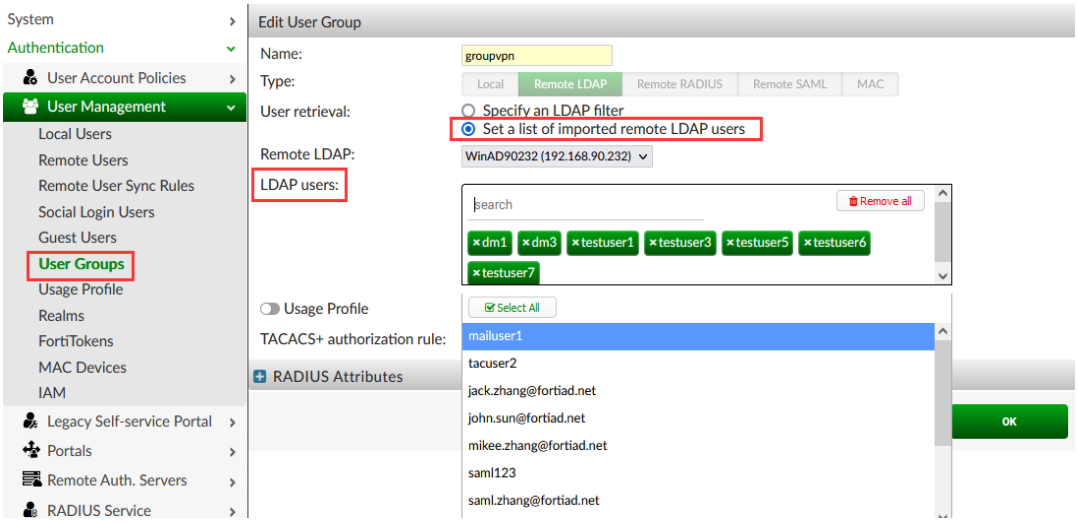


对于 Remote LDAP 用户，加入用户组有三种方式:

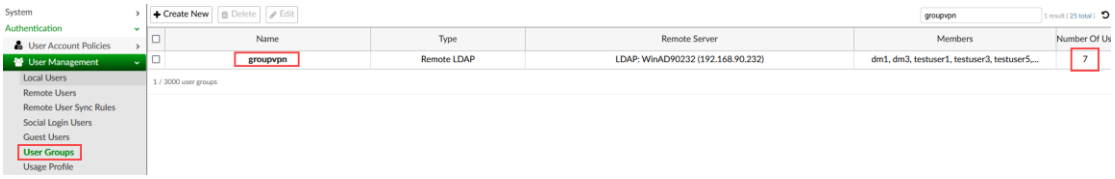
i. 基于自动同步规则，导入用户时自动把用户导入到配置的组中



ii. 手动把导入的用户加入到配置的 group

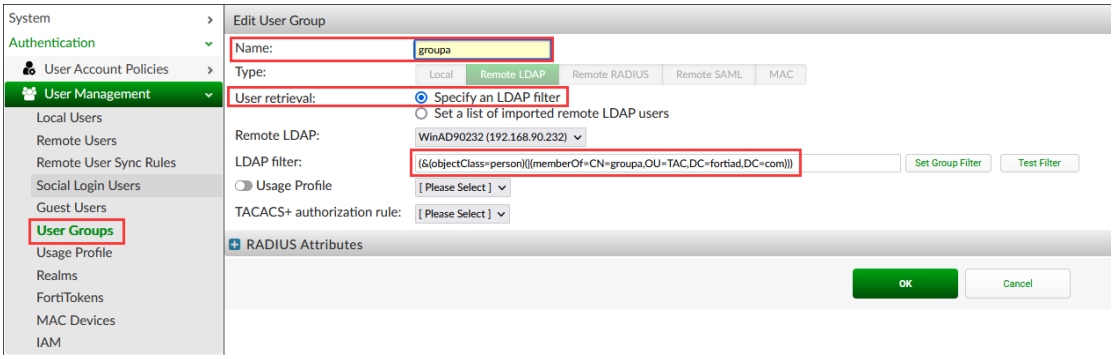


对于上面两种方式的用户组，可以显示组里面的用户数量，比如:



iii. 在用户认证时检查用户的组属性

这种方式一般适用于 Remote LDAP 用户在 AD 服务器上频繁变更组信息:



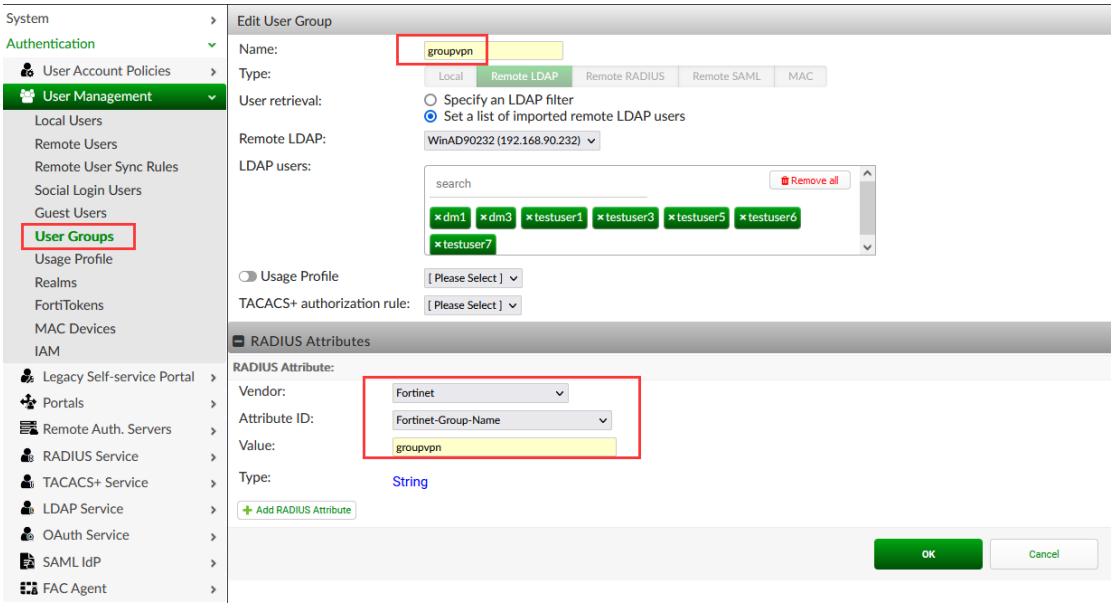
当选择" User retrieval"的方式为" Specify an LDAP filter"时,每次认证时,FAC 都会使用配置的"LDAP filter"去从 LDAP server 上重新读取一下用户的组信息.

使用这中方式建立的 group 不会显示用户组里面的数量,因为都是每次认证时才检查用户组信息:

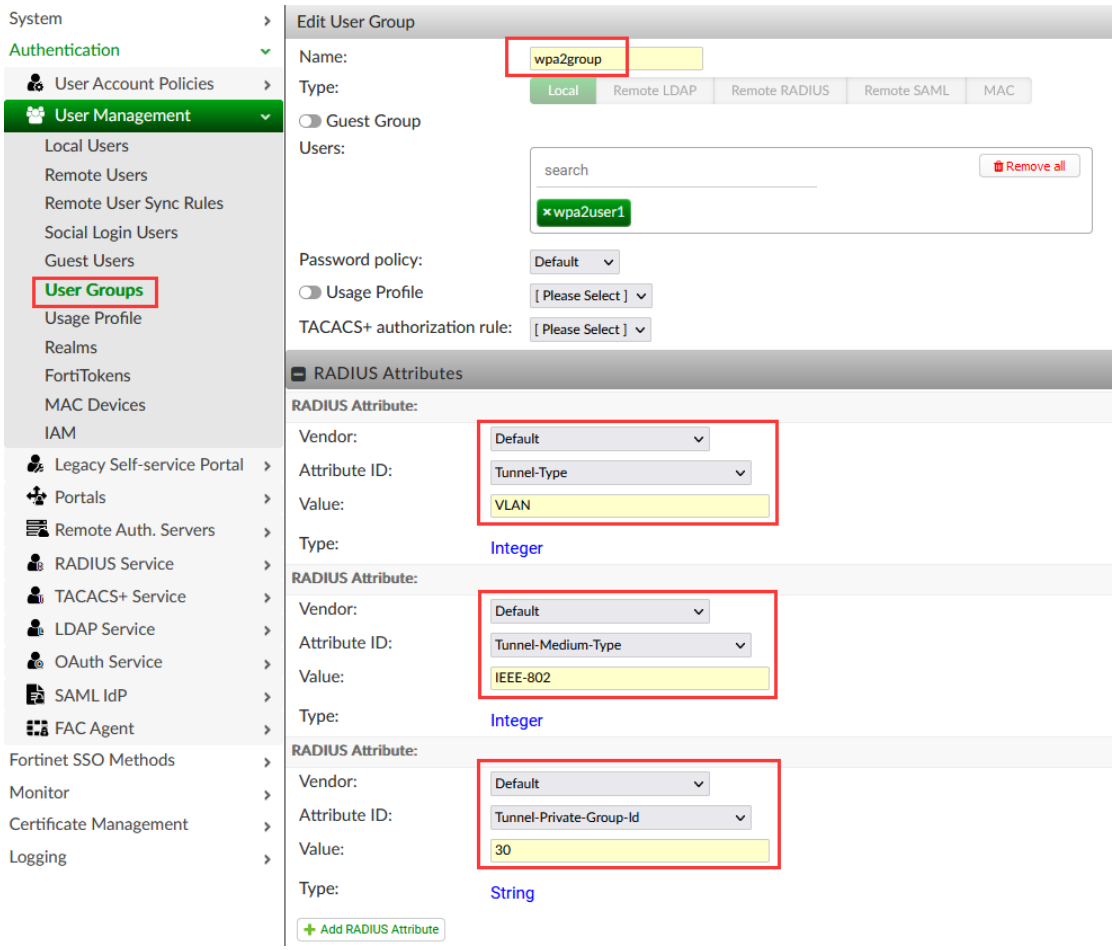
iv. 返回用户属性给 radius 认证客户端

比如常用的返回用户的 group 属性或是 vlan 信息给 radius 认证客户端

返回 group 属性:

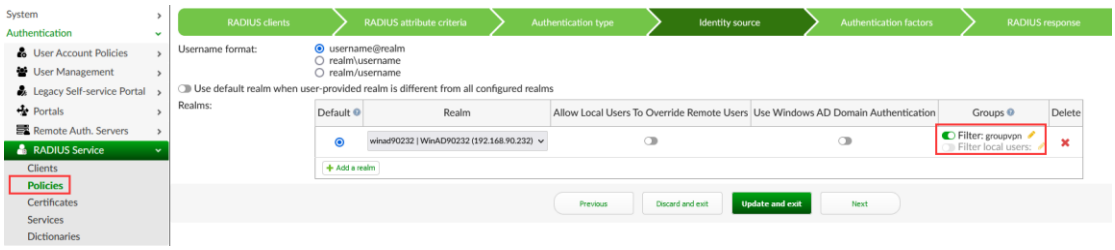


返回用户 vlan 信息:



请注意，需要在 radius policy 中开启用户组校验后, FAC 才会返回认

证用户的 group 中设置的 radius 属性:

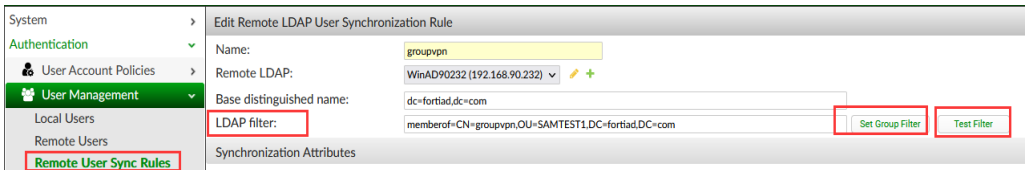


3.5 Remote 用户同步规则

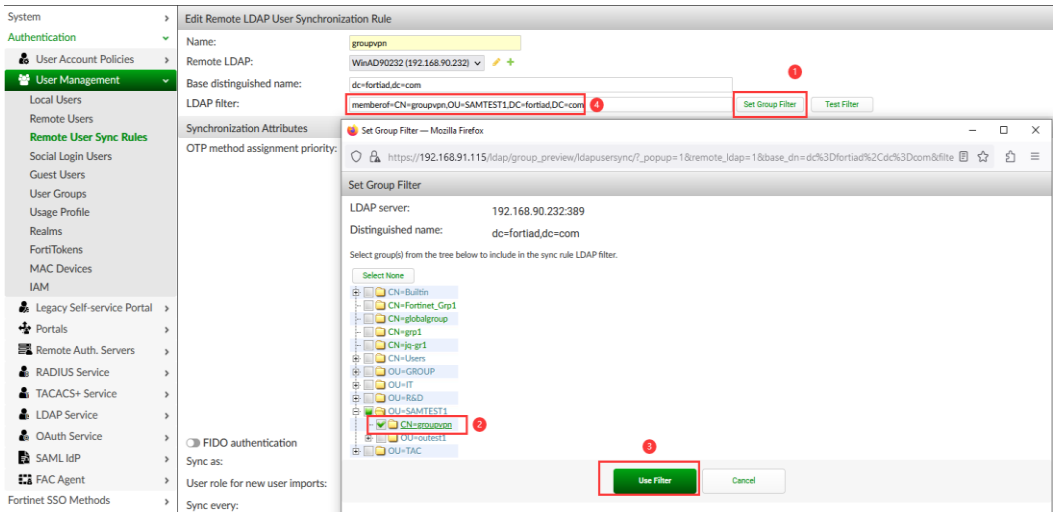
当 FAC 从远端服务器上同步用户时，可以基于同步规则批量同步不同属性的用户.

i. 用户匹配规则(LDAP filter)

用户匹配规则是同步用户时重要的一个设置:

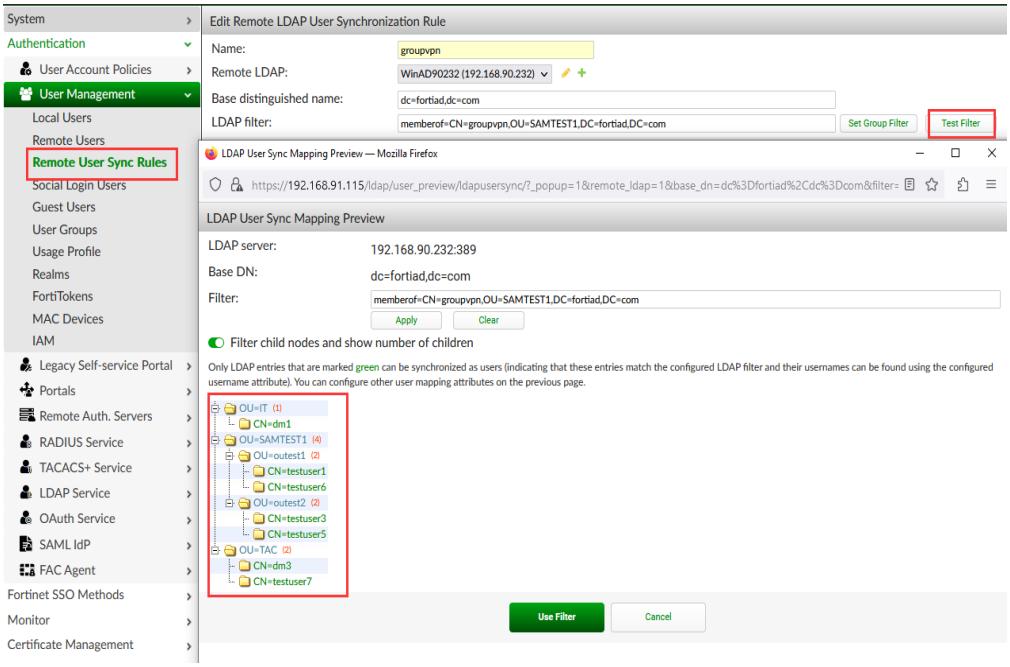


如果是同步 LDAP Server 上某一个组的用户，那直接使用”Set Group Filter”，就可以得到匹配规则:



设置好用户匹配规则后，可以使用”Test Filter”来验证一下配置

的匹配规则是否正确，点击”Test Filter”后显示基于当前匹配规则下远端 LDAP Server 上的用户，也就是可以同步过来的用户:



FAC 的同步规则配置比较灵活，可参考下面的链接:

https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-LDAP-filter-syntax/ta-p/197063

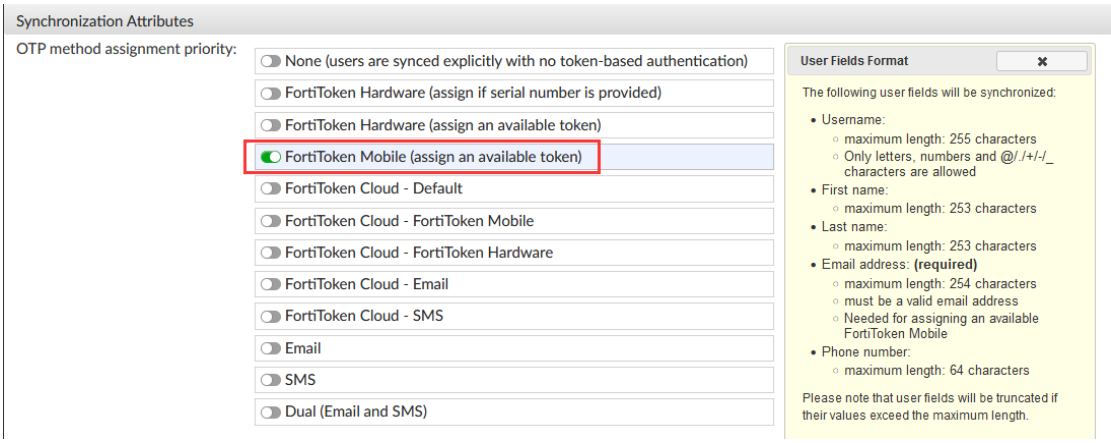
有的部署场景不是基于用户 group 的属性来同步用户，

比如所有有 vpn 权限的用户在 ldap server 上的属性为 accessTitle=vpn,

则 ldap filter 就可以设置为: (accessTitle=vpn);

另外还可以基于用户在 ldap server 上的字段值来导入，比如用户在 ldap server 都有一个属性值 vpnAccessLevel，不同用户值不同，比如有的是 1，有的是 2，那就可以设置下面的 filter 来导入用户特定用户: (vpnAccessLevel=1);

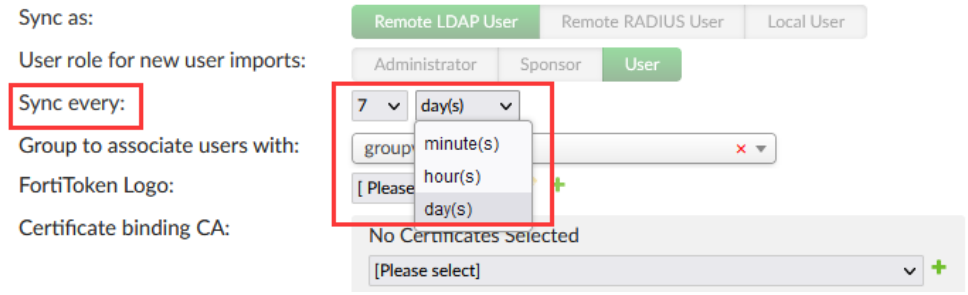
ii. 同步用户的同时给用户分 token



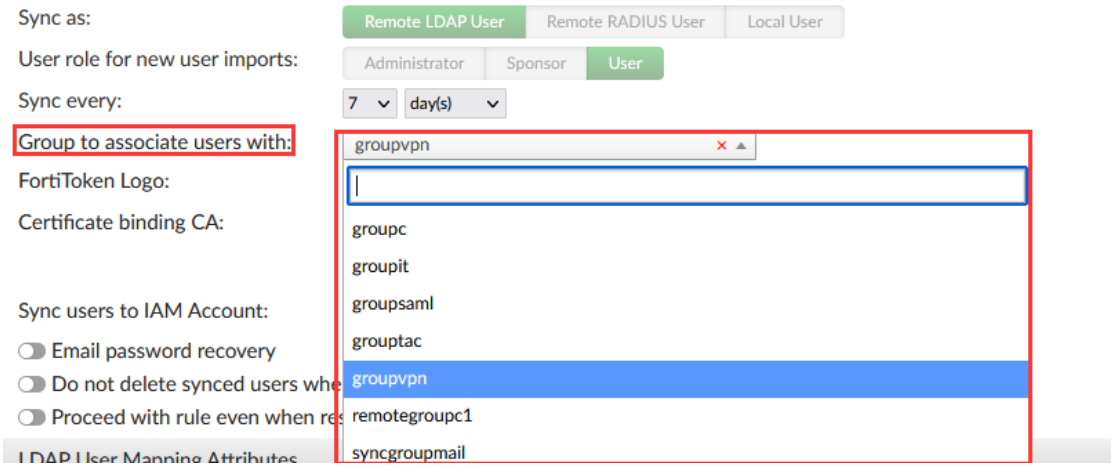
注意：如果同步的用户开启分配 FTM token,但是又没有有效的 email 信息或是给用户邮箱发送 token 激活邮件失败，那么此用户也会同步失败;

iii. 用户同步规则的同步周期

如果 LDAP Server 上的用户不是很频繁的添加，建议设置同步周期至少大于 30 分钟



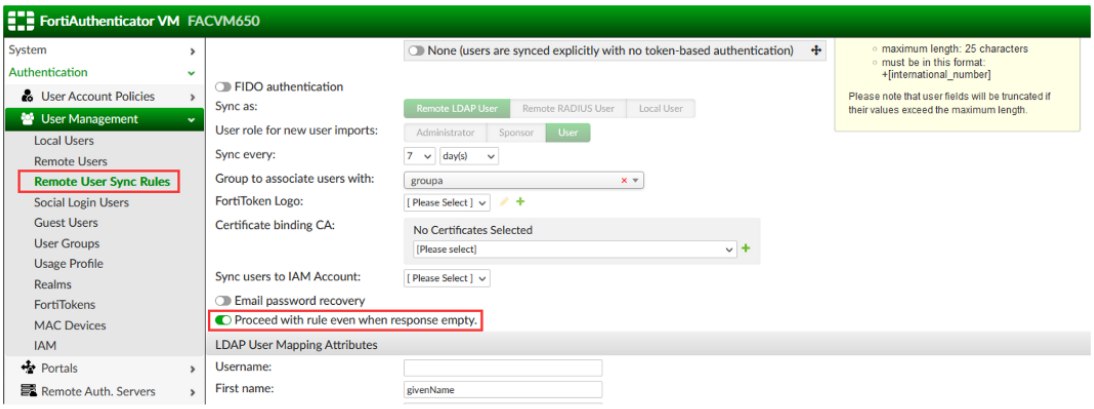
iv. 设置用户同步时自动加入设置的用户组



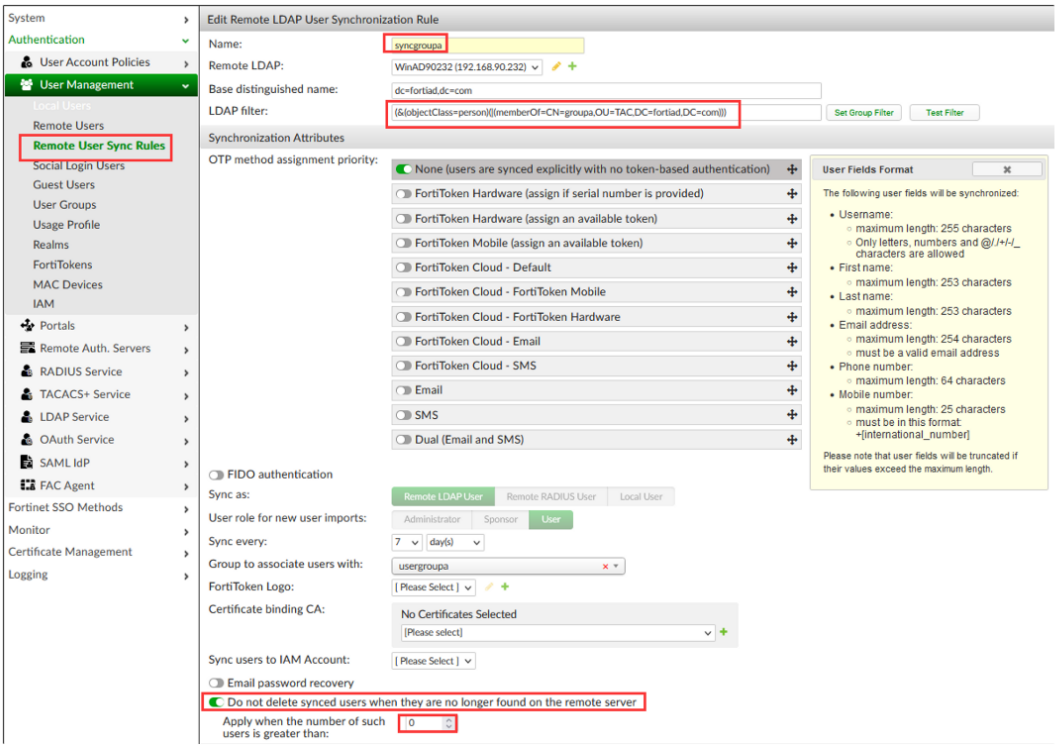
v. 关于自动同步的用户的删除

FAC 基于同步规则同步用户时，比如基于 group 来同步用户，如果此用户在远端 ldap server 上已经从这个 group 删除时，那么手动或自动执行这个同步规则时，FAC 基于下面的规则判断是否在 FAC 上删除这个用户，同时满足下面两个条件就会从 FAC 上删除这个用户：

- 这个用户已经从 ldap server 上这个 group 删除了，并且执行这个同步规则后，ldap server 返回不为空，即 ldap server 上有用户还属于这个 group，并且这个用户没有被 FAC 别的同步规则匹配导入过
- 如果执行这个同步规则后，ldap server 返回为空，并且同步规则开启了"Proceed with rule even when response empty”即下图中的开关：



另外还可以开启下面配置,即同步用户时不删除 FAC 已经同步过的用户：



请注意：为了防止因为 FAC 上配置的 ldap server 管理员的帐号问题,或是在 ldap server 上因为管理员误操作导致用户被错误从 ldap server 上的某些组中删除，这样导致 FAC 在同步 ldap 用户时也相应地从 FAC 上删除这些 ldap 用户，建议在配置用户同步规则时开启上面的配置” Do not delete synced users when they are no longer found on the remote server”;

这样可以避免误删除用户，开启这个配置后，如果确定 FAC 上已经同步的某些用户不需要了而且也不在 ldap server 上了，可以手动从 FAC 上删除这些用户。

3.6 关于 Radius Realm 设置

i. Realm 一般是指 FAC 跟多一个域对接时，用于区分用户的认证源.

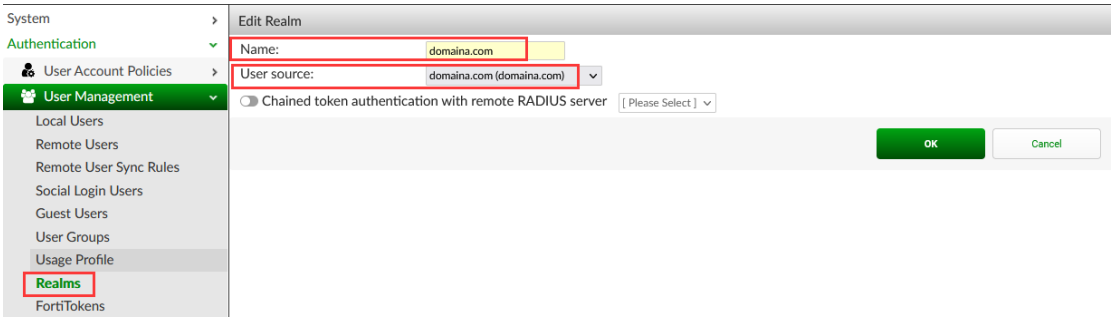
Realm 有三种形式:

username@realm

realm\username

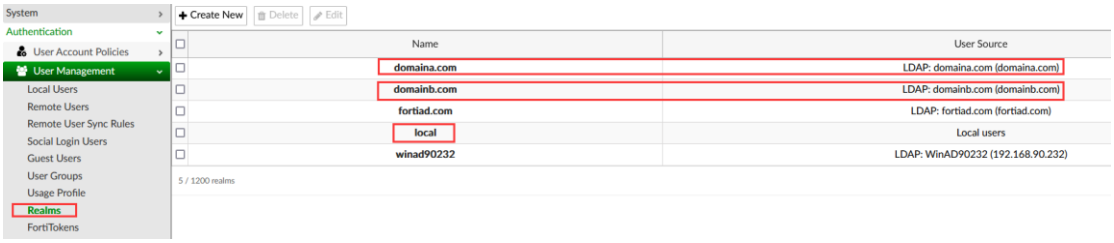
realm/username

ii. Realm 配置时需要配置一个 realm 名和认证源:

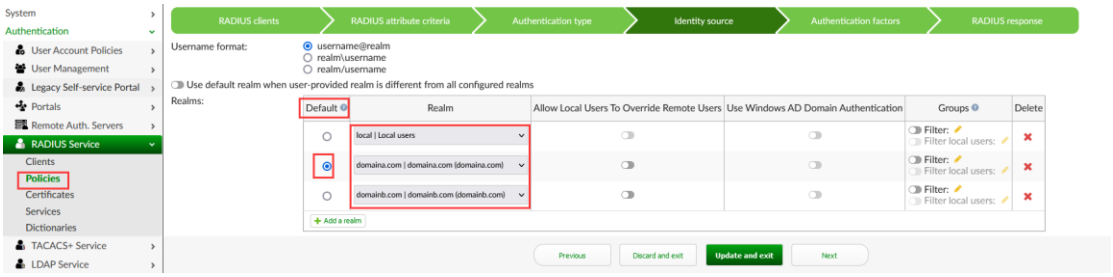


认证时通过匹配 Name 来确定通过哪个认证源来认证用户.

比如下面的 realm 设置, domaina.com 和 domainb.com 以及 local:



在 Radius 服务的 policy 下做下面的配置时:



- 当用户认证时输入的用户名为 username 或 username@domaina.com 时, FAC 会跟 domaina.com 发起认证
- 当用户认证时输入的用户名为 username@domainb.com 时, FAC 会跟 domainb.com 发起认证
- 当用户认证时输入的用户名为 username@local 时, FAC 会使用 FAC 本地 local 用户帐号来对用户进行认证

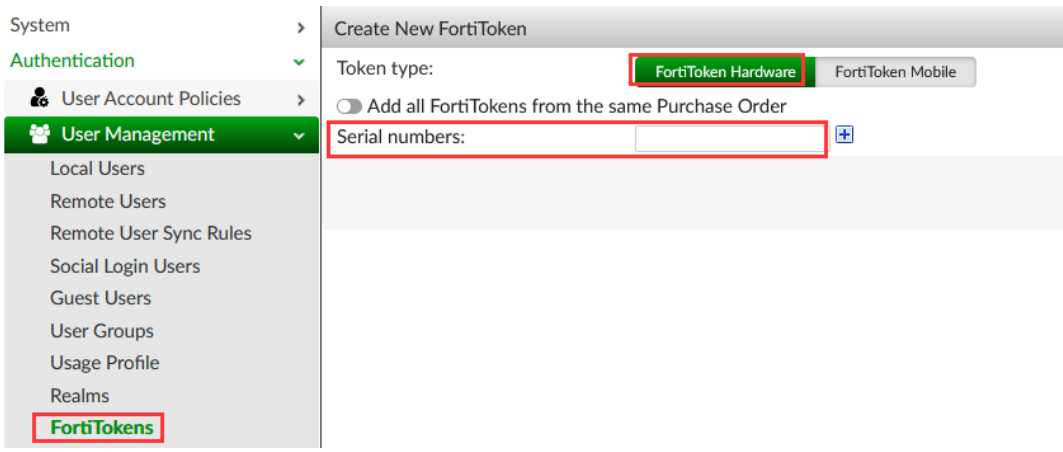
3.7 FortiToken 的使用

FAC 常用的 token 有 Fortitoken 硬件设备(FTK), Fortitoken mobile(FTM), email token, SMS token.

- FTK: 用户随身携带 FTK 设备，不需用户做 token 激活的操作
- FTM: 用户需要在终端设备上安装 Fortitoken Mobile app，用户需要在收到 token 激活邮件后，使用 Fortitoken Mobile app 扫码激活 token
- Email token: 用户认证时，如果开启 email token 认证，则 FAC 会给用户的邮箱发送 token，以便用户做 token 认证;
- SMS token: FAC 需要跟短信网关对接，用户认证时，如果开启短信认证，则 FAC 会给用户的手机号发送 token，以便用户做 token 认证

i. Token 导入

对于硬件 FTK token，需要输入 token 的序列号:



对于 FTM token,用户购买 FTM token license 后，会收到一个包含 token 激活码的 pdf 文件,需要输入 token 的激活码.

License 文件示例:

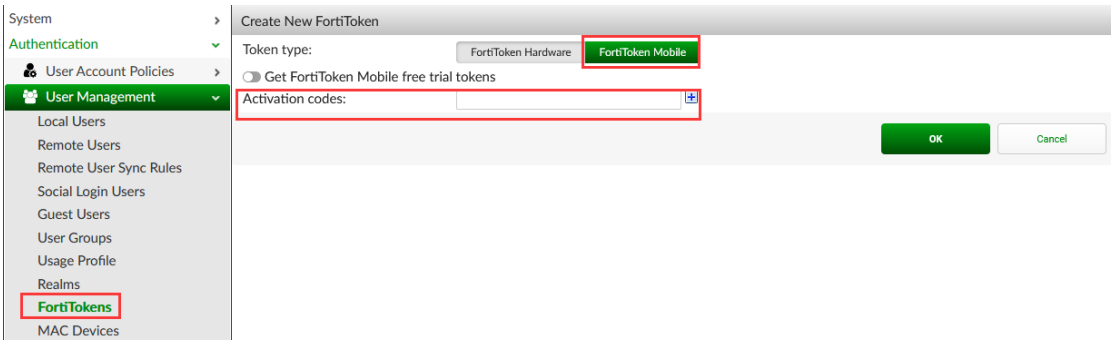
FortiToken™
Mobile Redemption Certificate

5

Tokens

Activation Code	EA4C
Certificate Valid Until	JUL 14, 2022
Serial Number	EFTM

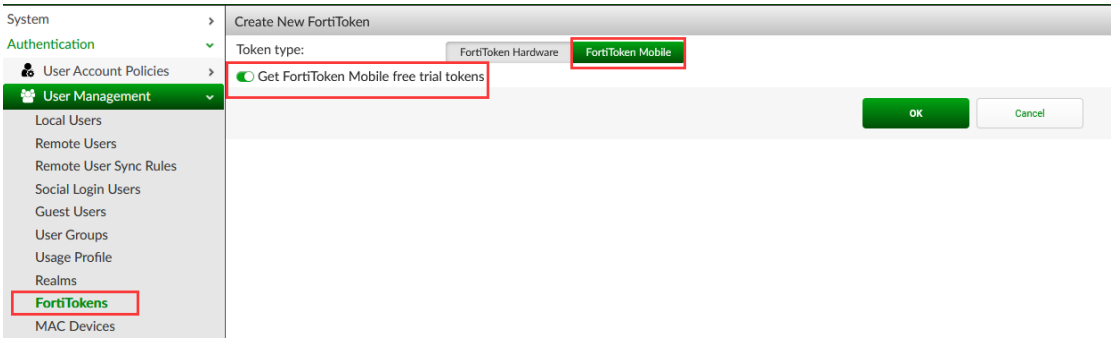
在下面界面输入激活码:



注意: token 的 license 是永久的，但是从上面的 license 文件中可以看到,token 有激活的截止期，必须在截止期前激活 token;

另外:

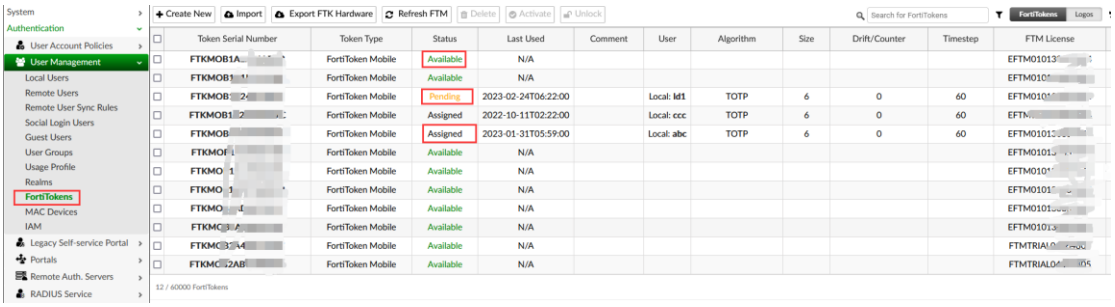
FAC 自带两个免费的 FTM token，可在下面界面获取:



在 FAC 的 HA 部署时，免费的 token 会被删掉，不能使用.

ii. Token 管理

在 token 管理界面可以看到 token 的使用情况:

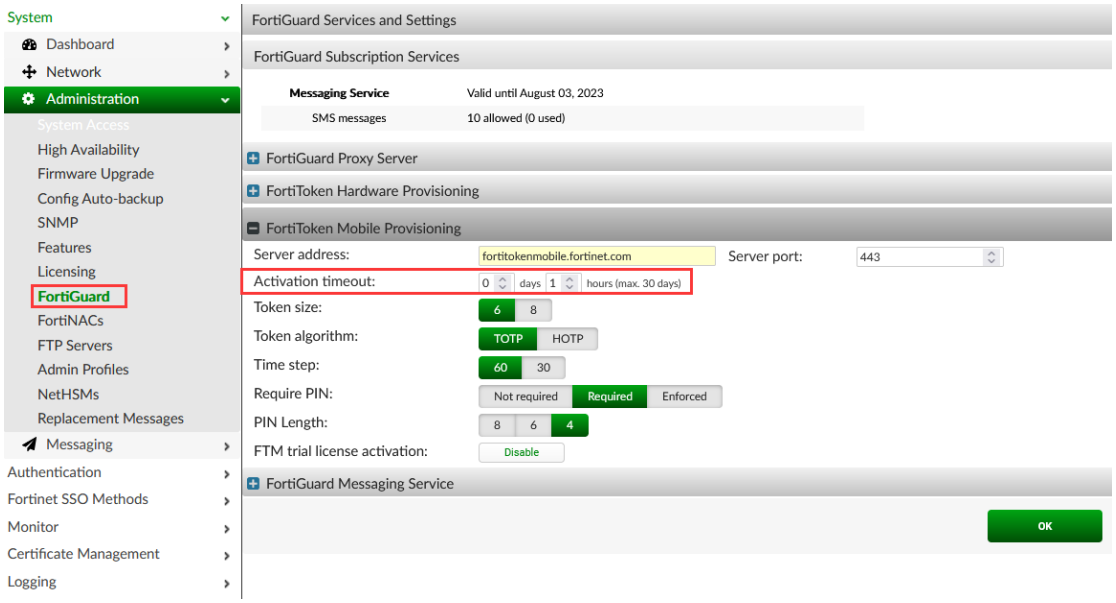


Token 有四种状态:

Available: 表示当前 token 未被分配，是可分配状态

Pending: 表示当前已发送此 token 的激活邮件给用户，用户还没有扫码激活 token

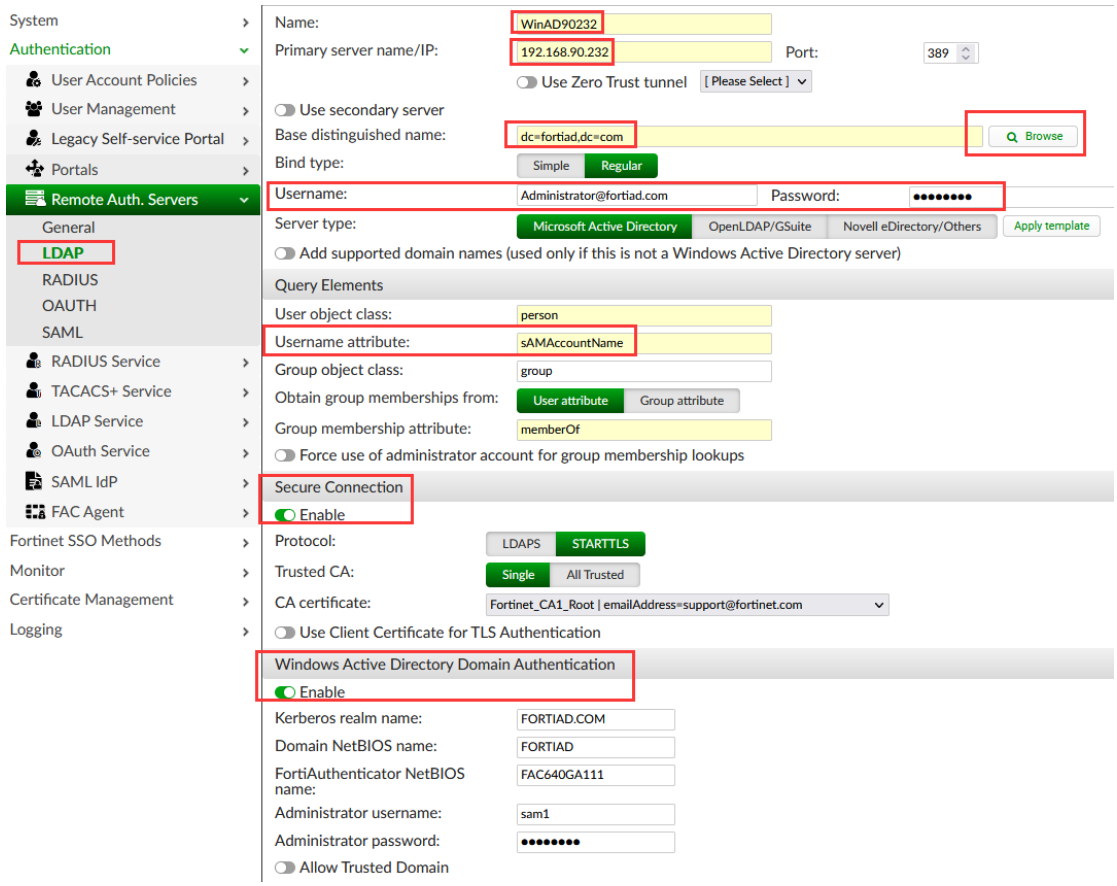
Lock: 当用户在设置的时间内没有扫码激活 token，则 token 变为 Lock 状态，下面的界面可以设置这个 token 激活超时时间.



Assigned：表示此 token 当前已分配给用户，处于正常使用状态

4. LDAP Server 配置

当 FAC 与远端 LDAP Server 对接时，需要在 FAC 上配置对接的 LDAP Server:



请注意：在配置 FAC 跟 LDAP Server 对接时，请配置一个单独的 LDAP

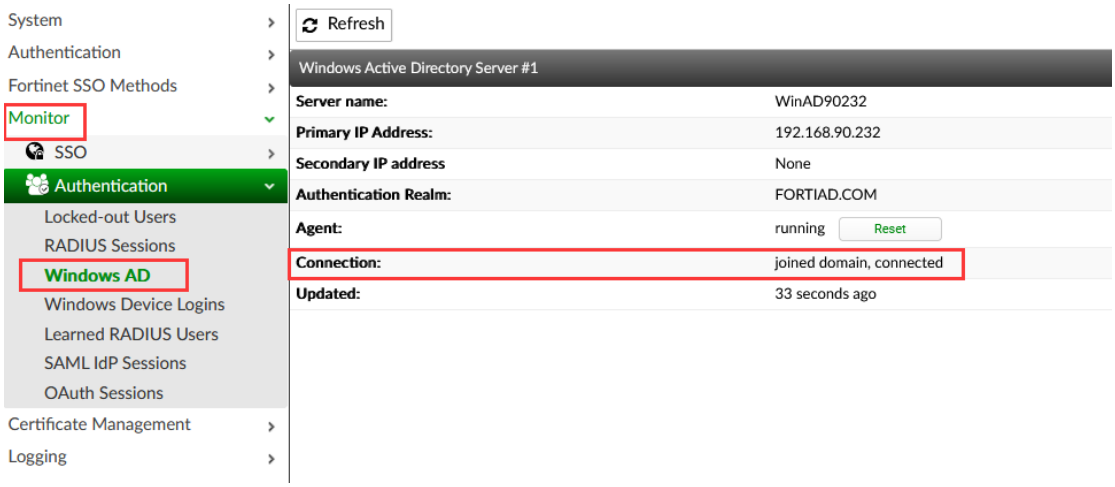
Server 的 administrator 权限的帐号来给 FAC 专门使用，否则可能会因为这个帐号的权限问题导致 FAC 同步 ldap server 上的用户异常，从而导致 FAC 上误删除已经同步导入到 FAC 上的 ldap server 上的用户。

i. 配置完成后可点击”Browser”来测试与 FAC 的连通性

ii. 默认情况下 FAC 与 LDAP Server 的通讯没有加密,这样用户的认证密码有泄露的危险，所以建议开启 LDAP 的”Secure Connection”

iii. 如果 LDAP 用户使用不是 pap 认证，那么需要开启” Windows Active Directory Domain Authentication”，让 FAC 加入到 AD 域.

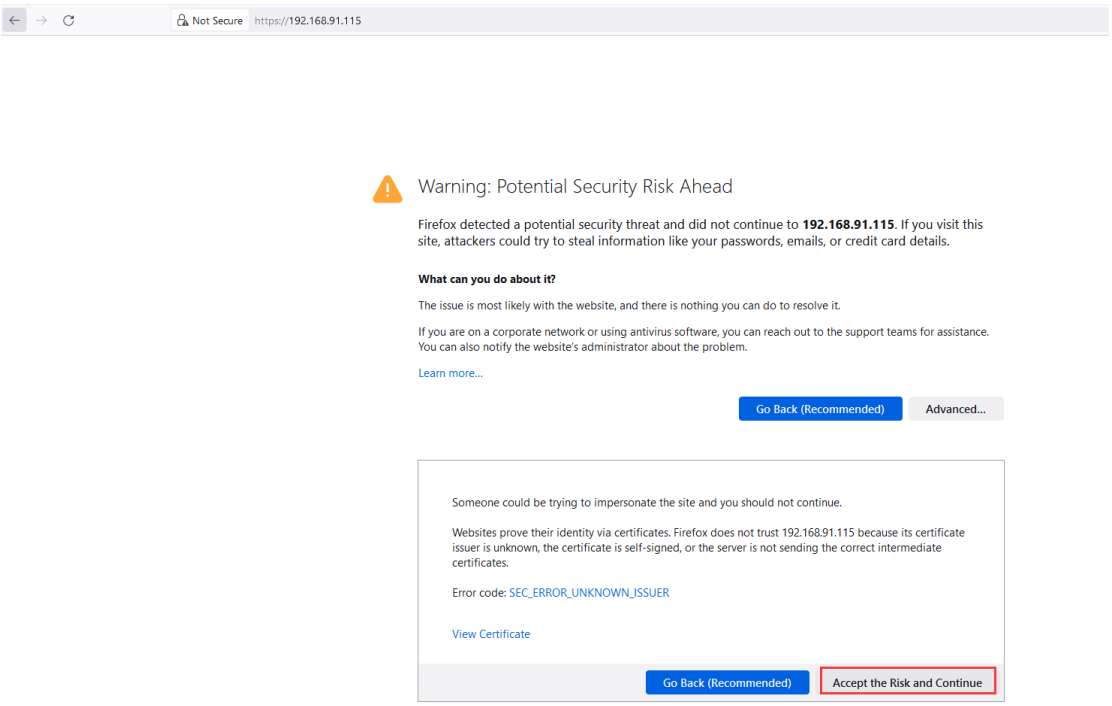
在下面页面可以查看 FAC 加入到 AD 域的状态:



5. 证书相关配置

5.1 FAC https 证书

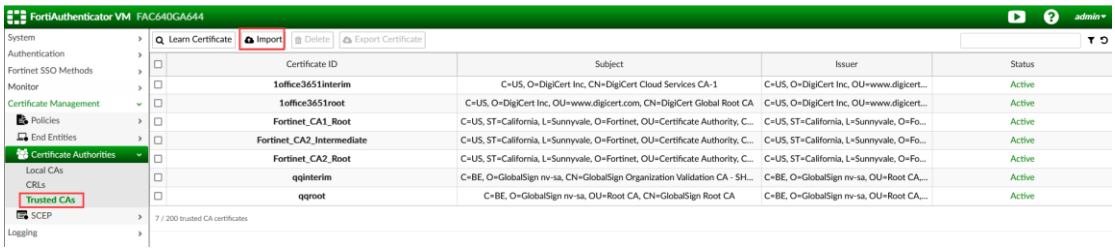
当我们登录 FAC 或是 FAC 作为 portal server，登录 portal 认证页面时，浏览器会弹出证书告警:



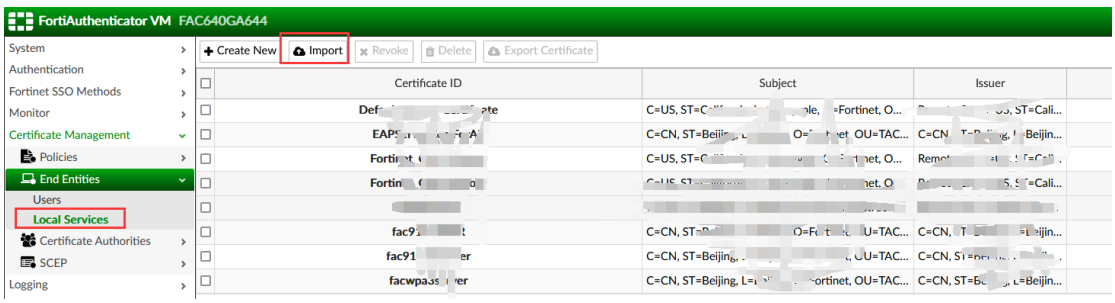
这是因为 FAC 使用的是自带的 https server 证书，不是公有 CA 发布的,可以点击接收以便继续访问 FAC,如果要导入第三方的 https 证书，

通过以下方法可以导入第三方 https server 证书:

i. 导入第三方 CA 证书:

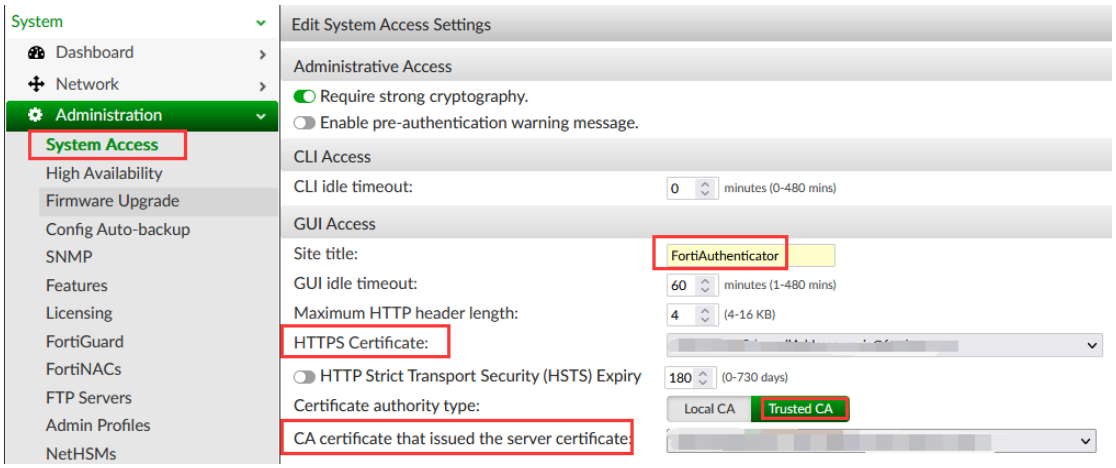


ii. 导入第三方 SSL 证书:

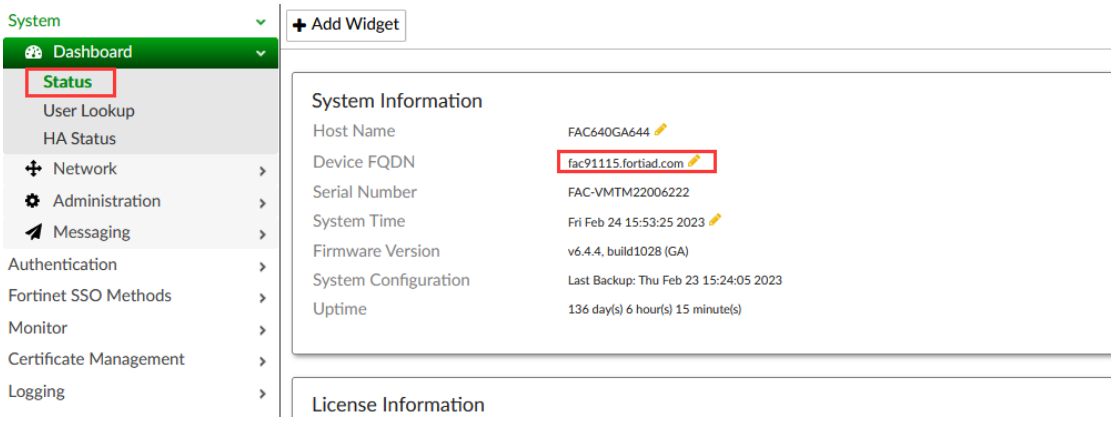


iii. 启用导入的 https server 证书

在下面的配置页面调用前面导入的 CA 证书和 Server 证书:

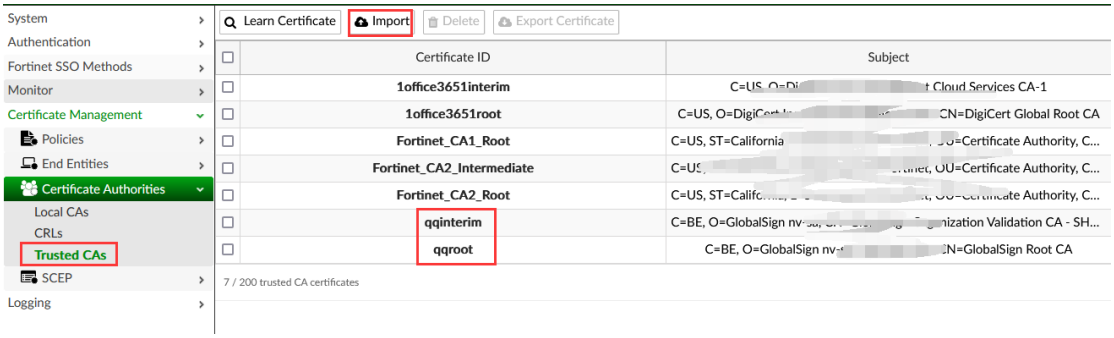


注意: 证书都是跟域名相关的, 所以在导入 server 证书到 FAC 时, 需要明确证书中的域名设置, 然后在 FAC 上要配置匹配的域名:



5.2 SMTP 通讯用证书

在做 FAC 的 SMTP 配置时, 如果 SMTP 使用的是 STARTTLS 模式的话, 需要在下面页面导入 SMTP mail server 侧的 CA 证书:



注意:有的邮箱服务器需要导入 CA 证书和中间证书.

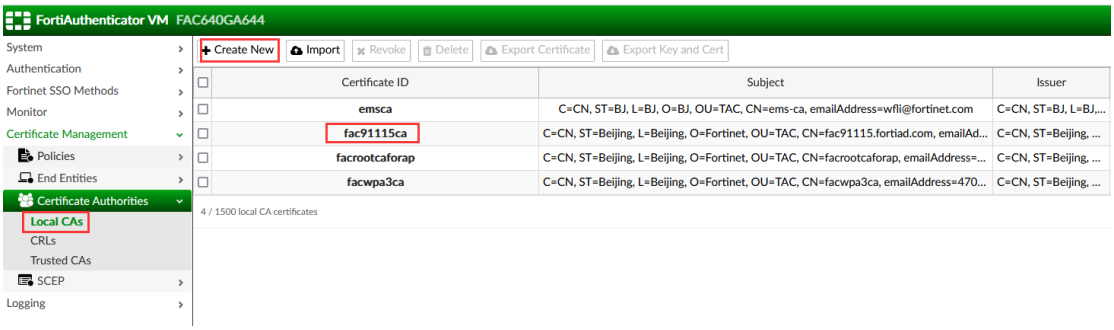
可参考下面 KB 来下载 SMTP server 证书:

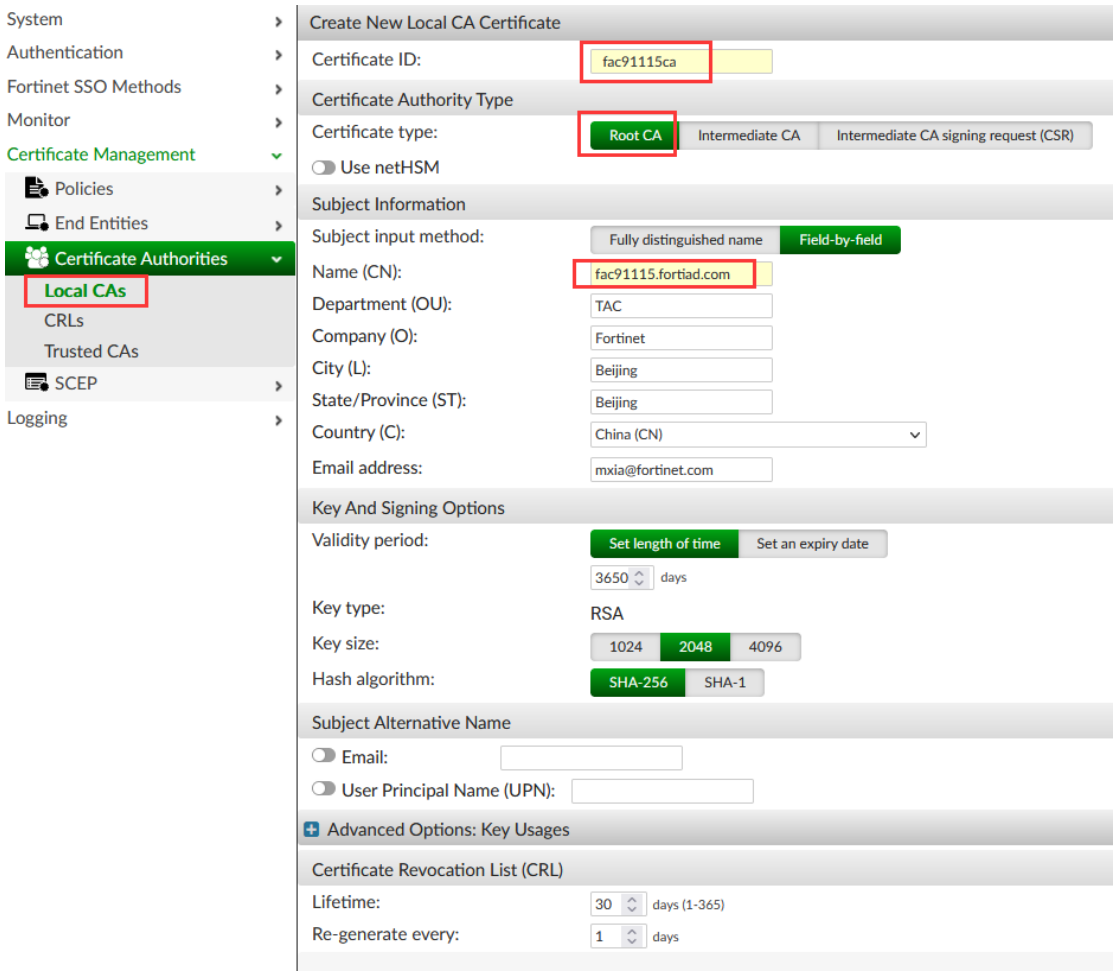
https://community.fortinet.com/t5/FortiAuthenticator/Technical-Tip-Configure-Microsoft-Office-365-SMTP-as-Mail-server/ta-p/214959

5.3 使用 FAC 给别的设备下发证书

可以使用 FAC 给别的设备下发域名证书, 比如使用 FAC 给防火墙设备下发 https server 证书.

i. 创建 CA 证书

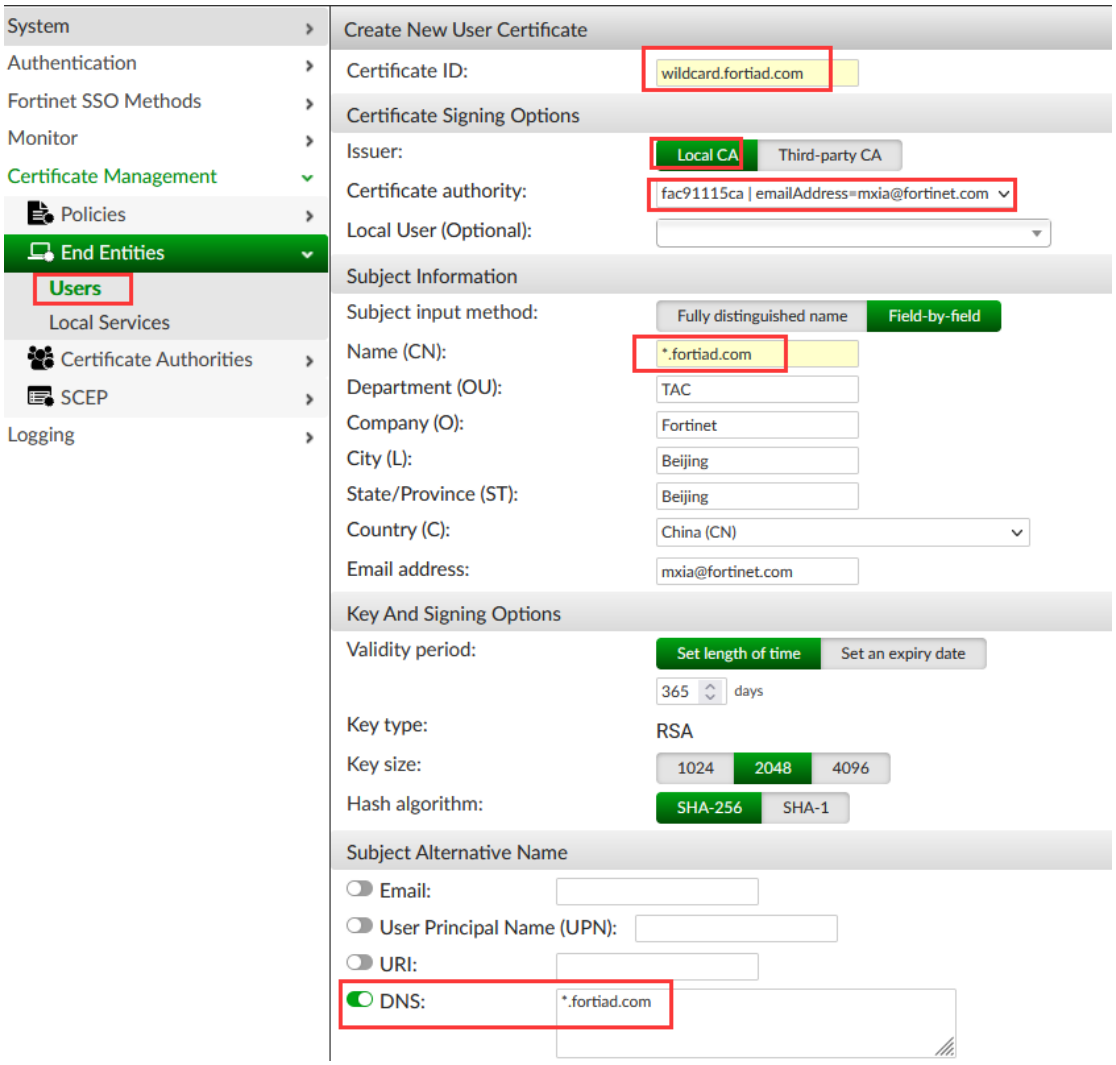




创建完成后，导入这个 CA 证书.

ii. 基于 CA 证书创建服务器域名证书

创建一个基于域名的通配符 Server 证书:

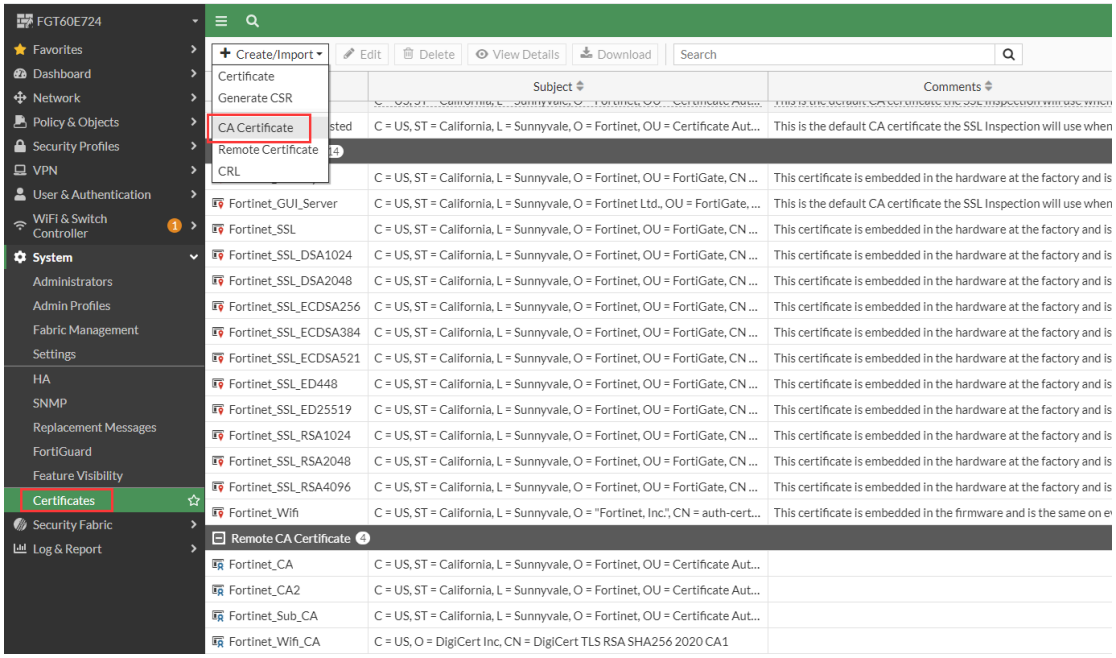


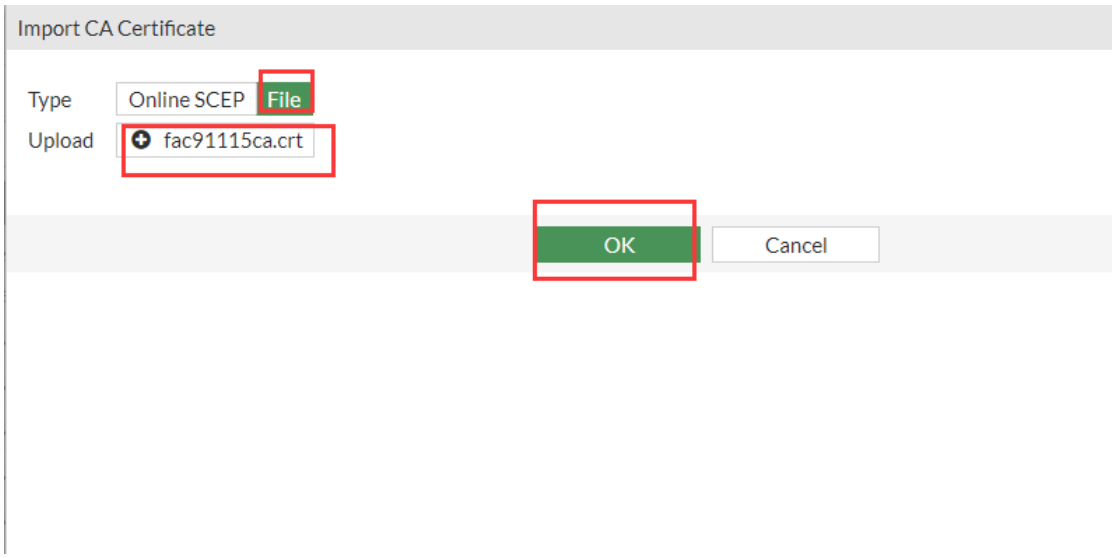
上面的 CN 和 DNS 必须一致,

创建完成后，导入这个域名证书.

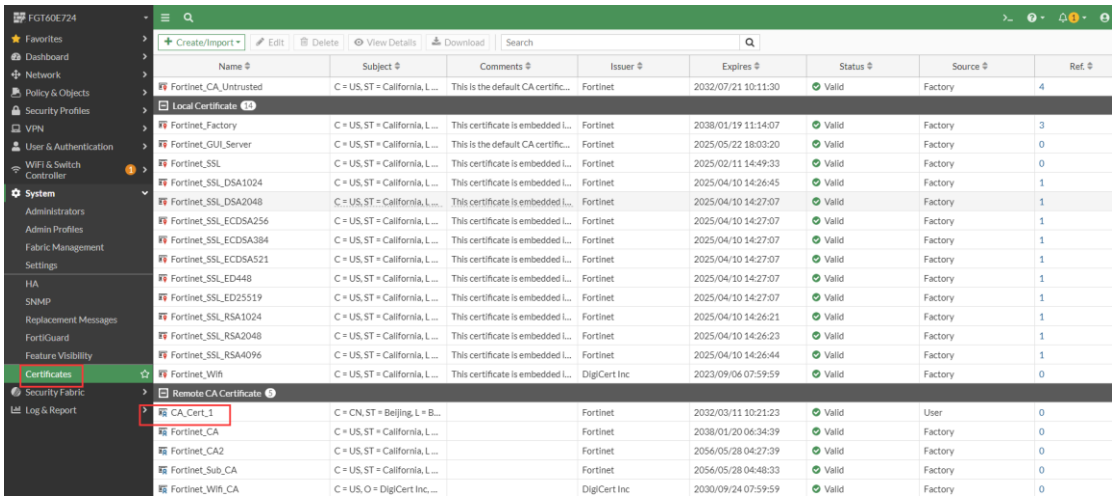
iii. 防火墙导入 CA 证书

收到导入 CA 证书

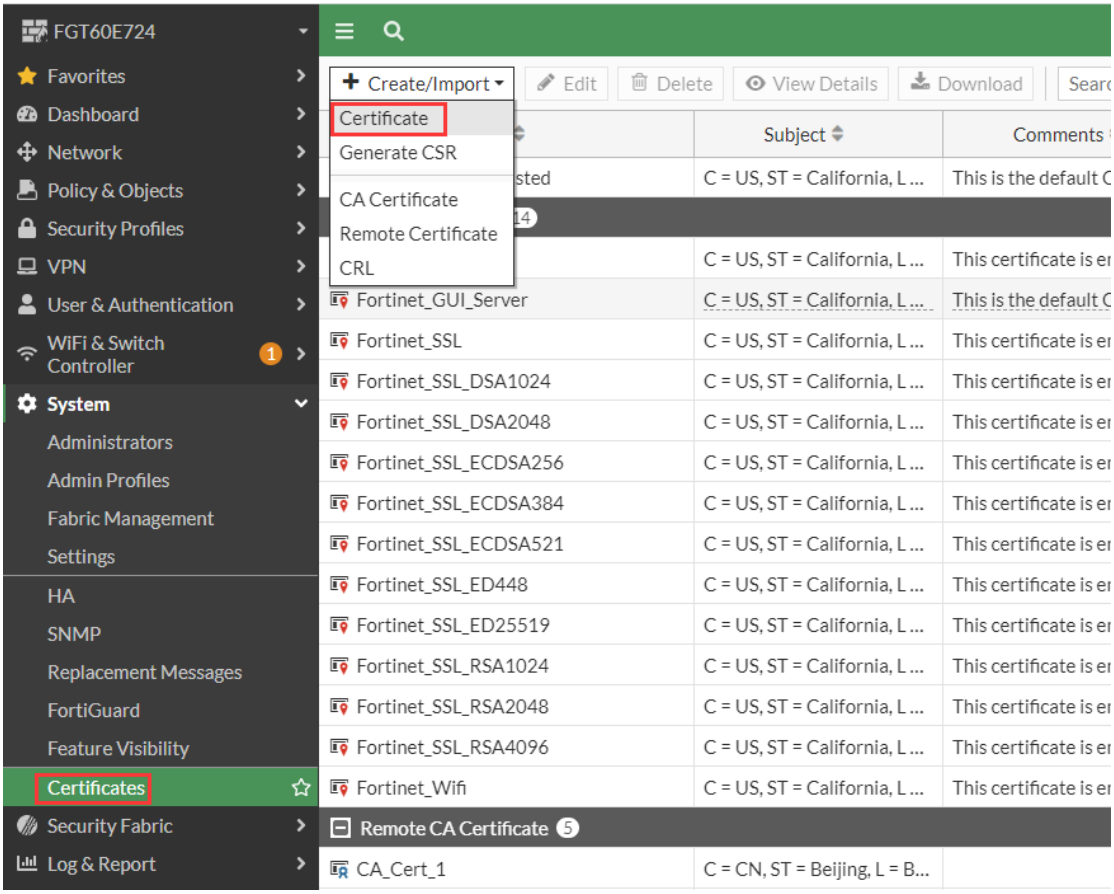

FGT60E724
Favorites
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Administrators
Admin Profiles
Fabric Management
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Security Fabric
Log & Report
Create/Import
Certificate
Generate CSR
CA Certificate
Remote Certificate
CRL
Edit
Delete
View Details
Download
Search
Subject
Comments
Fortinet_GUI_Server
Fortinet_SSL
Fortinet_SSL_DSA1024
Fortinet_SSL_DSA2048
Fortinet_SSL_ECDSA256
Fortinet_SSL_ECDSA384
Fortinet_SSL_ECDSA521
Fortinet_SSL_ED448
Fortinet_SSL_ED25519
Fortinet_SSL_RSA1024
Fortinet_SSL_RSA2048
Fortinet_SSL_RSA4096
Fortinet_Wifi
Remote CA Certificate 4
Fortinet_CA
Fortinet_CA2
Fortinet_Sub_CA
Fortinet_Wifi_CA
C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN ...
This certificate is embedded in the hardware at the factory and is
C = US, ST = California, L = Sunnyvale, O = Fortinet Ltd., OU = FortiGate, ...
This is the default CA certificate the SSL Inspection will use when
C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...
C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1

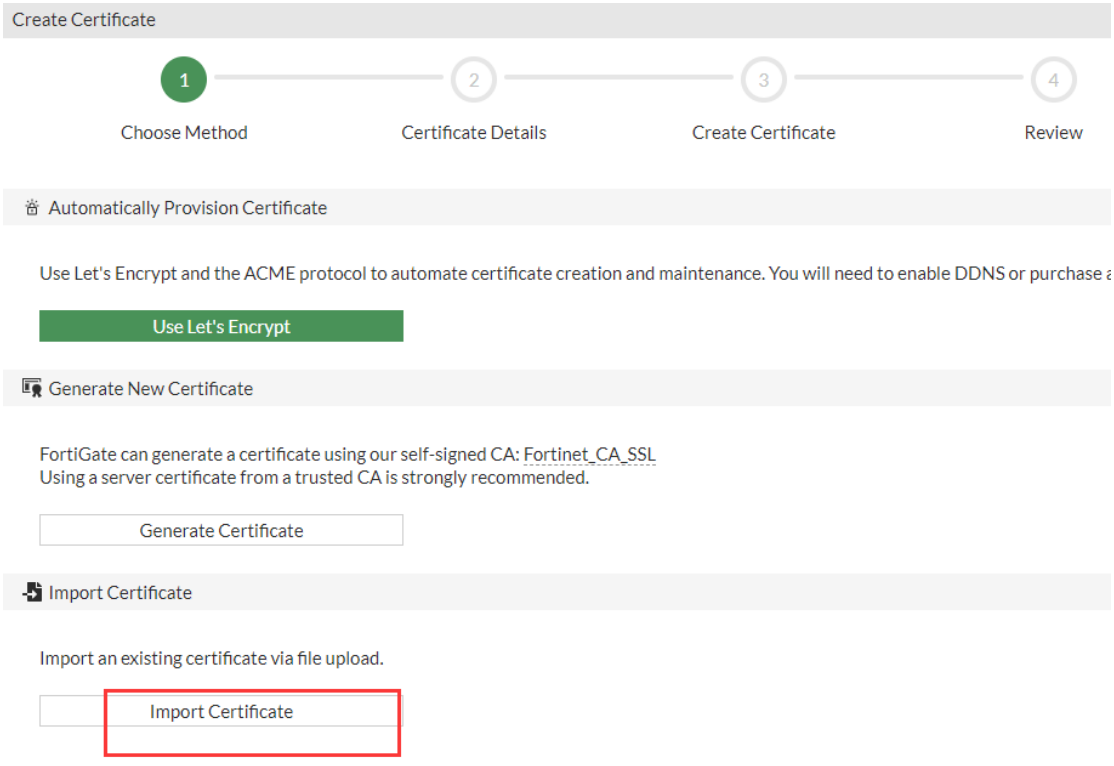

Import CA Certificate
Type
Online SCEP
File
Upload
fac91115ca.crt
OK
Cancel

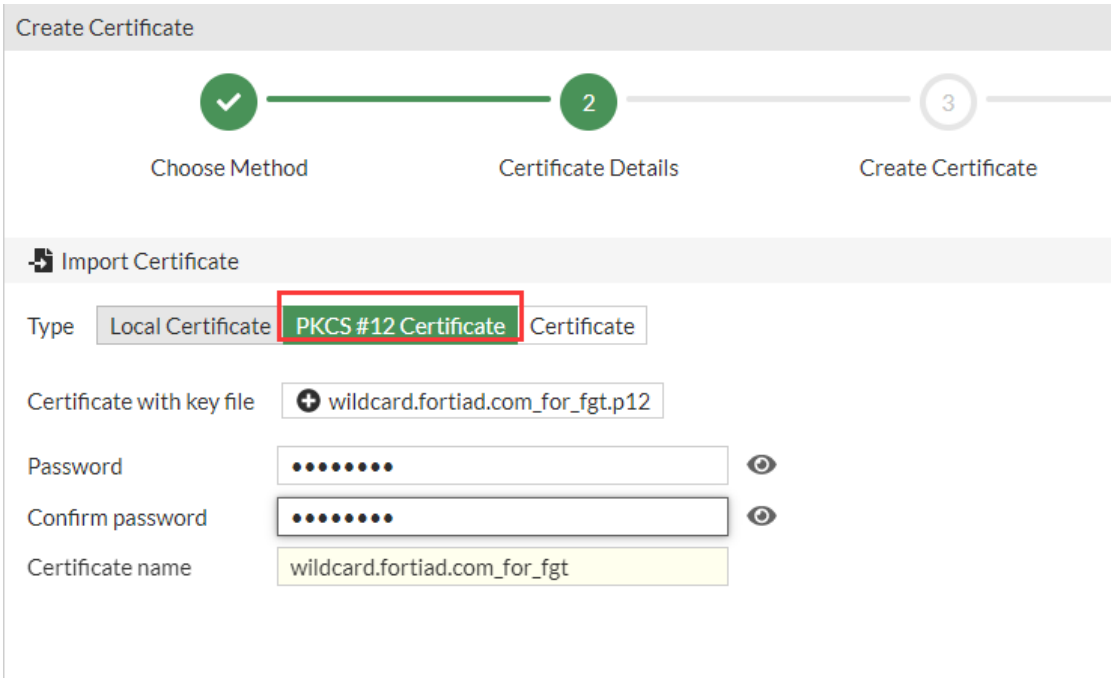
证书导入完成后:

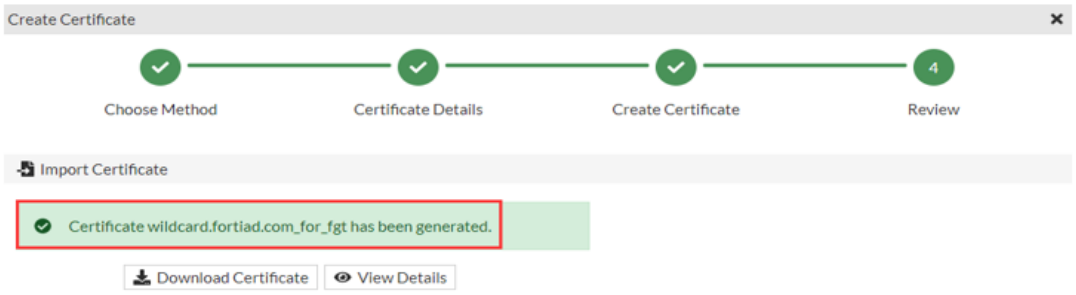

FGT60E724
Create/Import
Edit
Delete
View Details
Download
Search
Name
Subject
Comments
Issuer
Expires
Status
Source
Ref.
Fortinet_CA_Untrusted
Local Certificate 16
Fortinet_Factory
Fortinet_GUI_Server
Fortinet_SSL
Fortinet_SSL_DSA1024
Fortinet_SSL_DSA2048
Fortinet_SSL_ECDSA256
Fortinet_SSL_ECDSA384
Fortinet_SSL_ECDSA521
Fortinet_SSL_ED448
Fortinet_SSL_ED25519
Fortinet_SSL_RSA1024
Fortinet_SSL_RSA2048
Fortinet_SSL_RSA4096
Fortinet_Wifi
Remote CA Certificate 5
CA_Cert_1
Fortinet_CA
Fortinet_CA2
Fortinet_Sub_CA
Fortinet_Wifi_CA

iv. 防火墙导入域名证书:

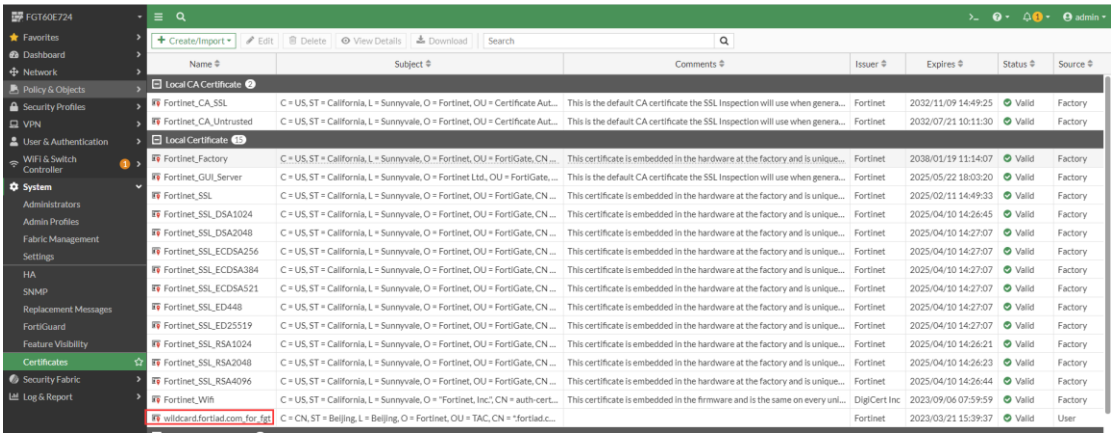








证书导入成功后:

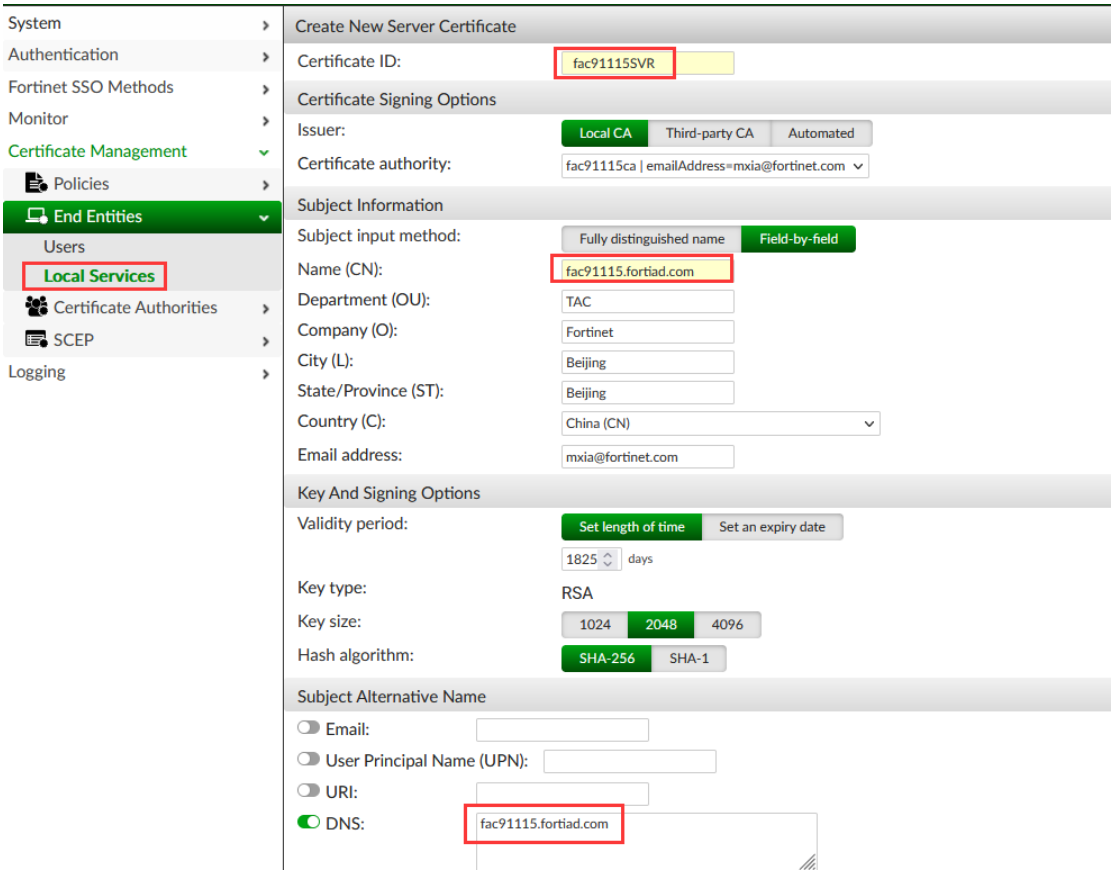


5.4 FAC 给防火墙下发 SAML 认证证书

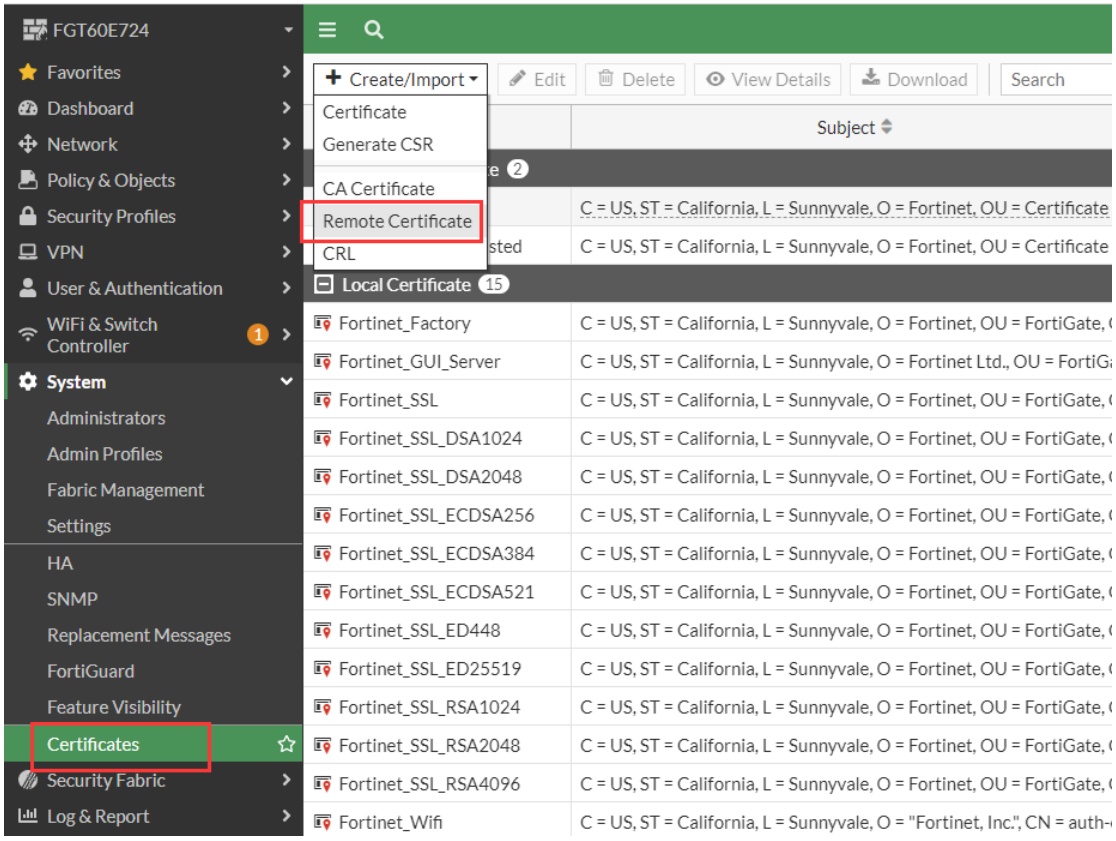
当防火墙与 FAC 对接做 SAML 认证的时候,比如防火墙做 SAML SP, FAC 做 SAML IdP, 此时需要从 FAC 下发 SAML 认证的证书给防火墙;

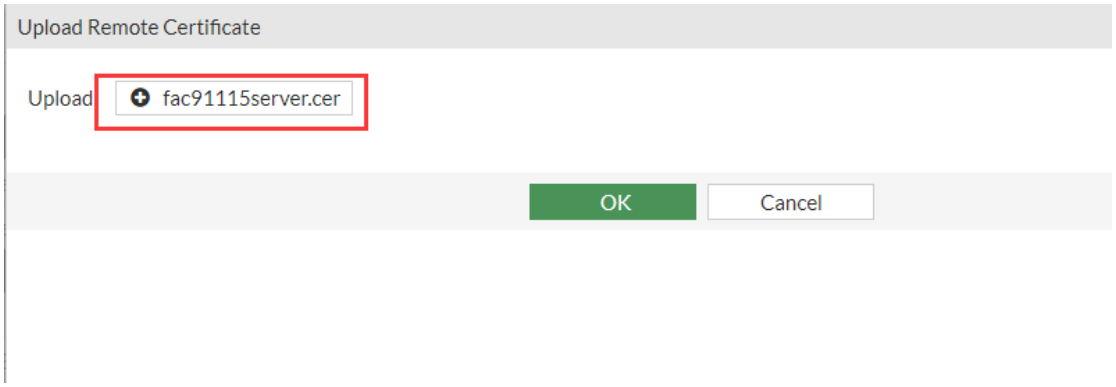
i. 与上面 5.3 章节配置一样，下载 CA 证书到防火墙上.

ii. 在 FAC 上创建 Server 证书并下载下来.



iii. 防火墙导入 Server 证书





导入成功后:

6. HA 部署

FAC 有两种 HA 部署方式, 即 HA A-P 模式和 HA –LB 模式

6.1 HA A-P 模式介绍

HA A-P: 即主备模式，一般是两个 FAC 之间二层相连, FAC 的角色为 Primary 或是 Secondary;

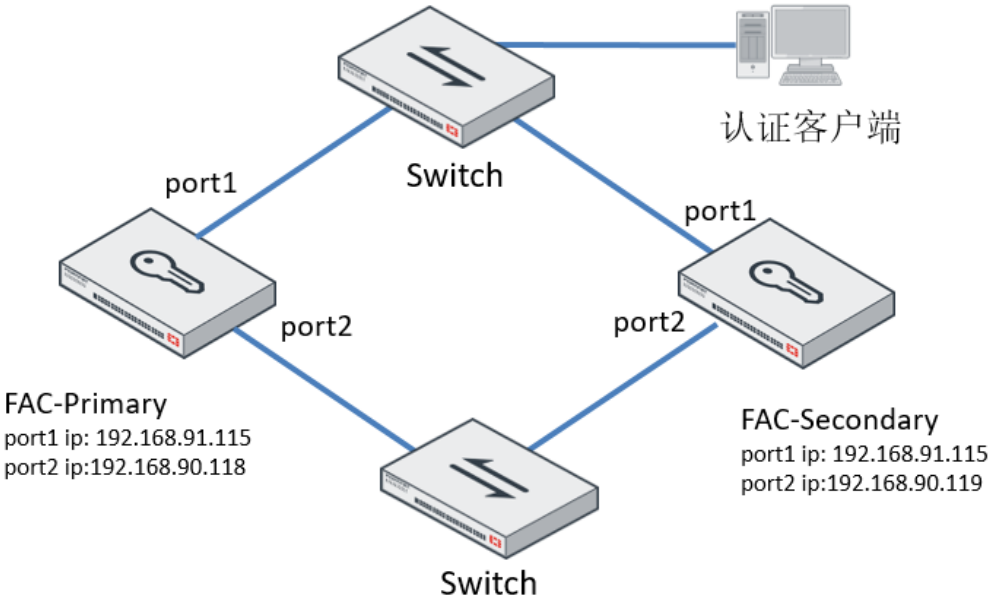
A-P 模式的要求两个 FAC 之间:

- 设备型号一样
- 软件版本一样
- 用户 license 一样
- A-P Cluster 只需要一份 Token license

在主备模式下，两个 FAC 可以设置不同的管理地址，然后通过管理地址登录主备设备；但是整个 Cluster 只有一个业务 ip 地址，即相当于 radius client 侧配置的 radius server 的 ip 地址.

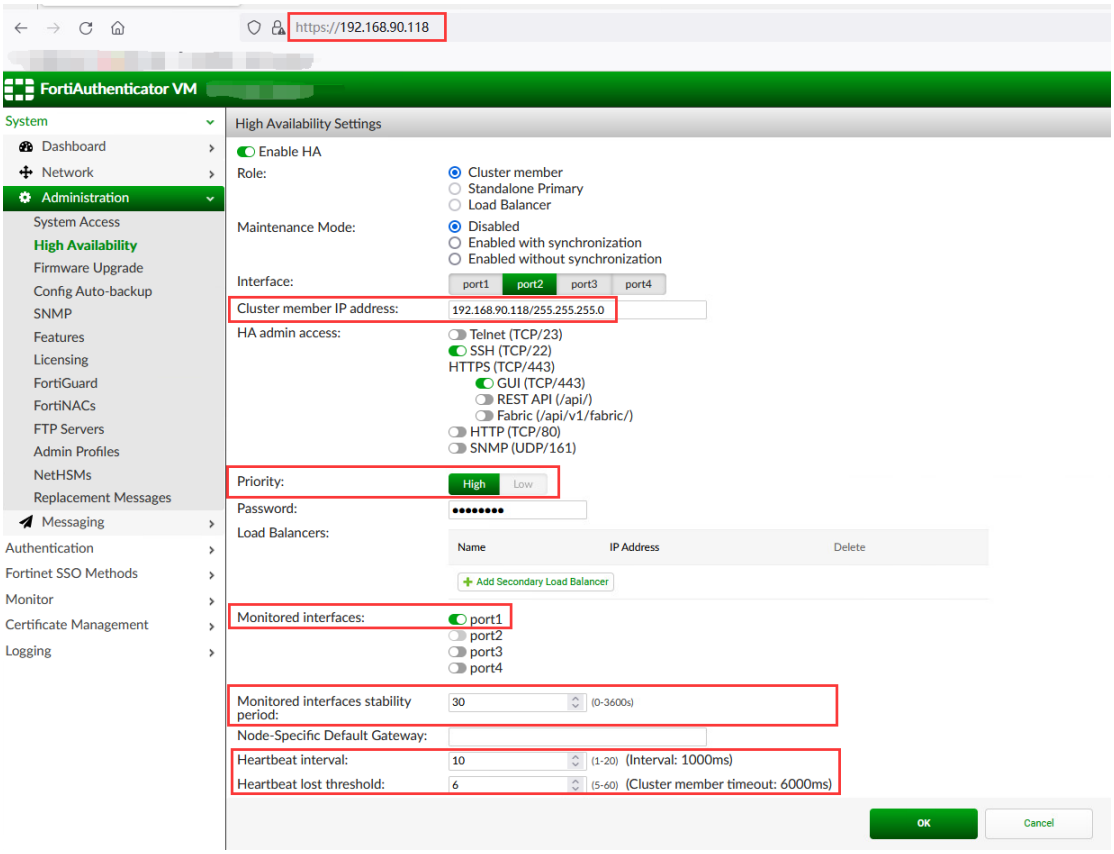
6.2 HA A-P 模式的配置

测试拓扑:



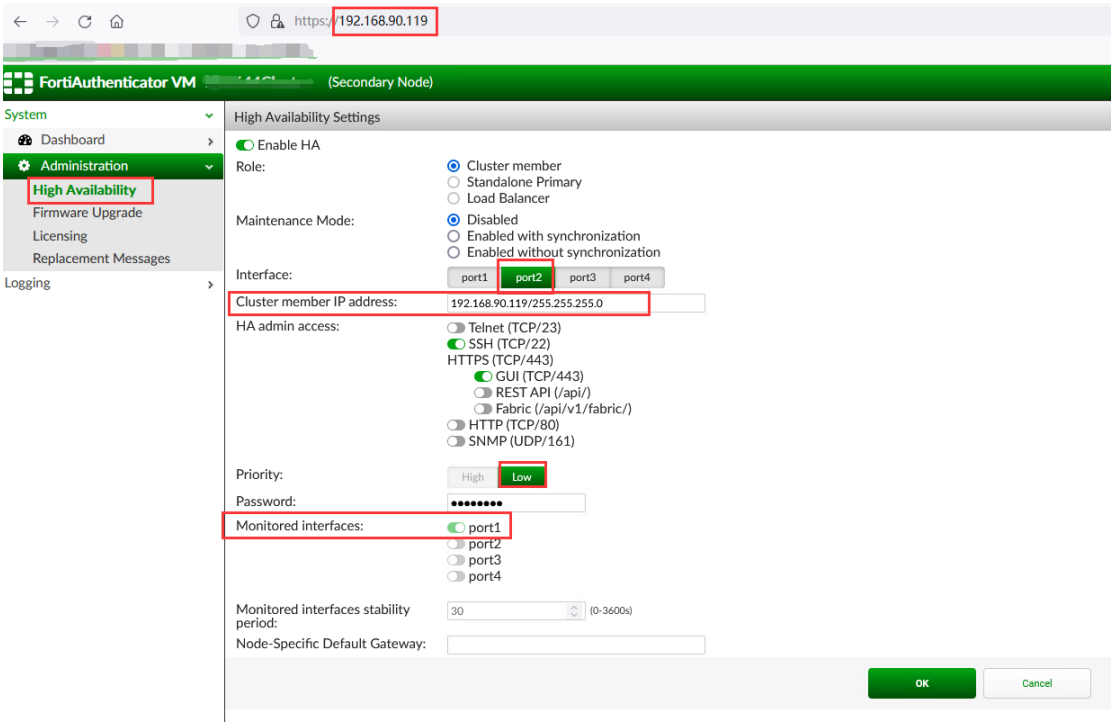
FAC port1 为业务口, FAC port2 为心跳口，也可以作为管理口;

Cluster Primary 侧的配置:



Cluster Secondary 侧的配置:

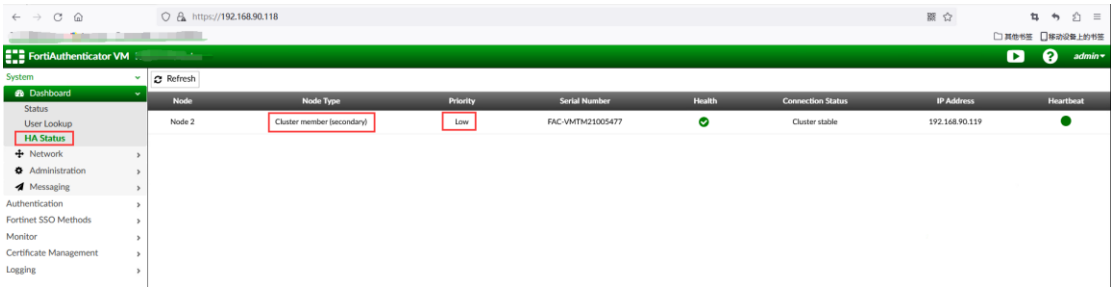
注:Secondary FAC 的 GUI 页面只有少部分管理菜单;

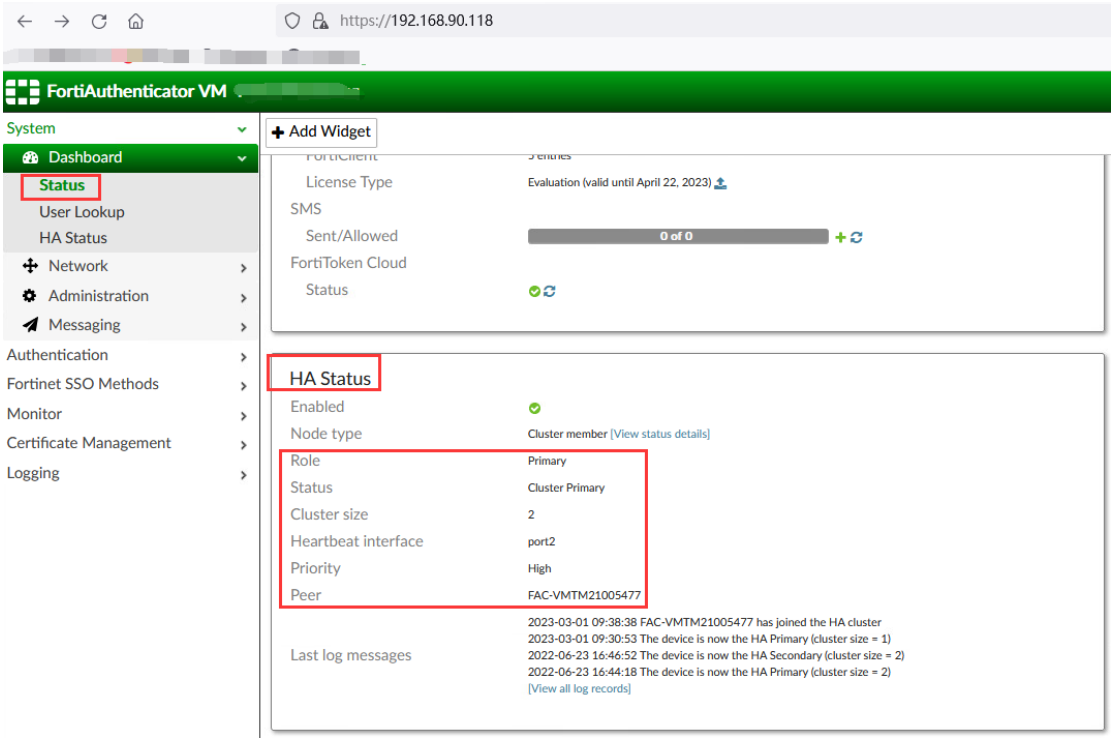


建议如无必要,不要配置” Node-Specific Default Gateway”, 因为可能引起 FAC 的路由变化.

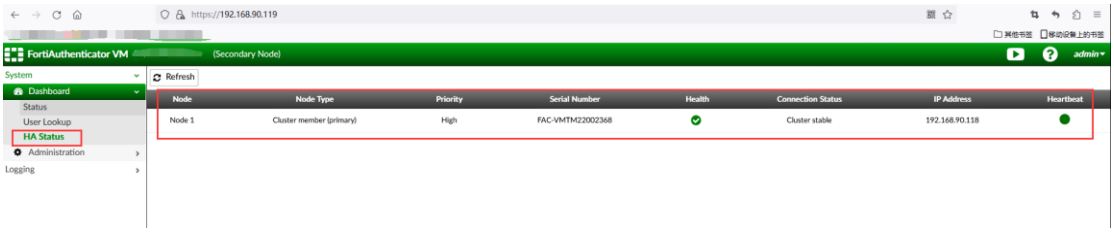
6.3 HA A-P 模式状态查看

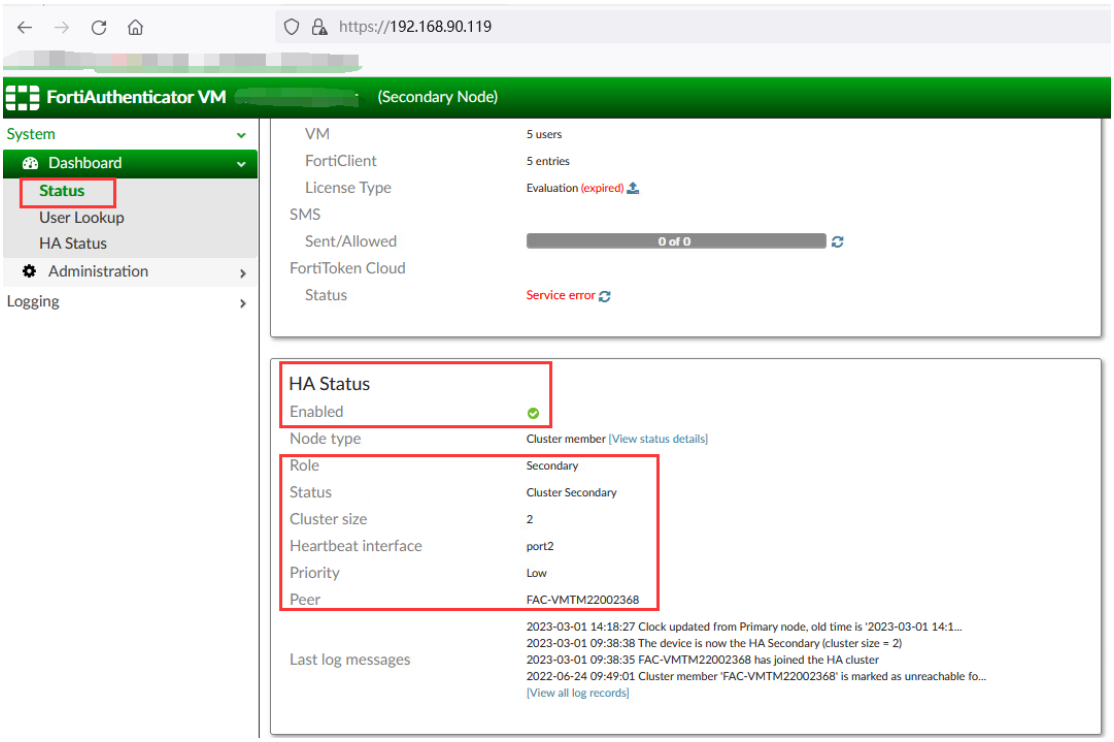
Cluster Primary 侧的 HA 状态:



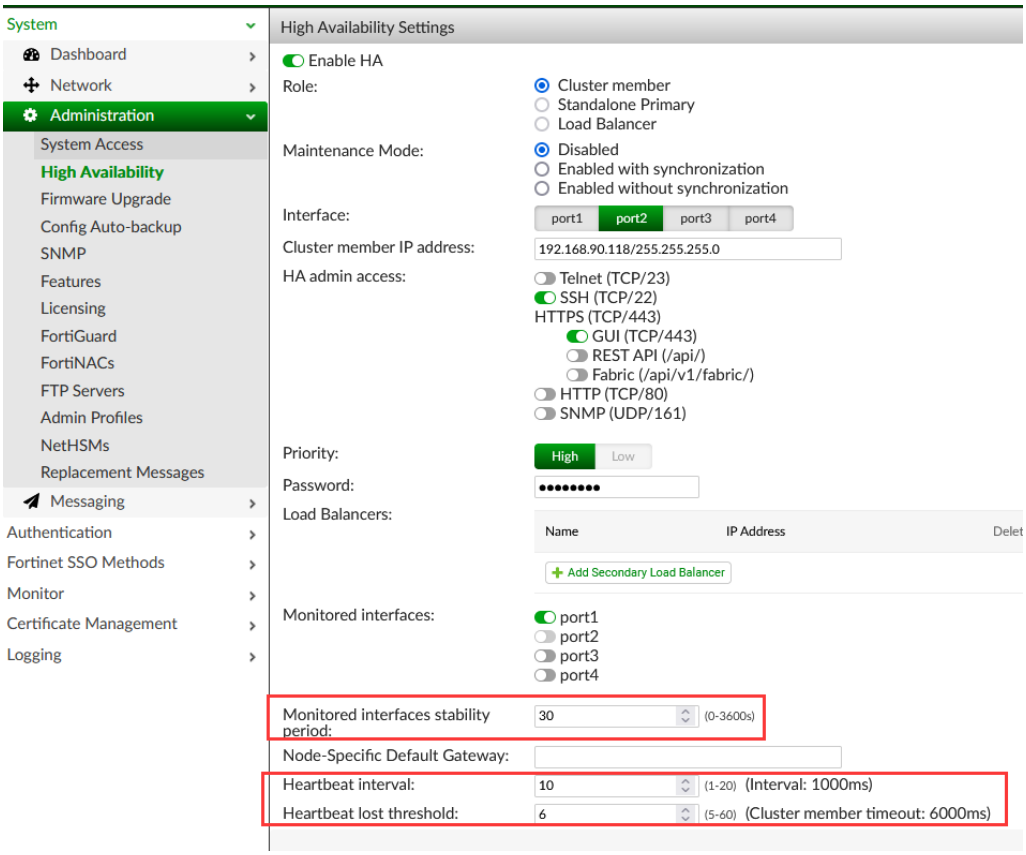


Cluster Secondary 侧的 HA 状态:





6.4 HA A-P 模式的 HA 心跳和切换



A-P 模式的切换有两个判断条件，一个是心跳接口，一个是监控接口；

Heartbeat interval:

心跳报文间隔:单位 0.1 秒，建议配置间隔为秒级，比如设置为 10 即 1 秒

Heartbeat lost threshold:

心跳报文丢失阈值

如果在(心跳报文间隔 X 心跳报文丢失阈值)时间内没有心跳报文，则触发 HA 切换计算;

如果主机重启或断电，则备机会切换到 Active 状态;

如果是拔掉正常工作的 HA 部署的心跳线，则可能会造成双主状态

Monitored interfaces stability period:

监控接口的稳定周期:

监控口插拔也一样会触发 HA 的计算;

如果 Active FAC 拔掉监控线，经过此时间后,Active FAC 变为 Slave 状态,Slave FAC 变为 Active 状态

A-P 模式是**主机强占**模式，即只要网络正常，高优先级的主机永远都是 Active 状态.

i.

在正常工作状态下，主机工作在 Active，备机工作在 Slave，如果重启主机,备机会工作在 Active 状态,如果主机启动后，主机会先变为 Slave 状态从备机同步配置，这种状态稳定 5 分钟后，主机会再次变为 Active 状态;

ii.

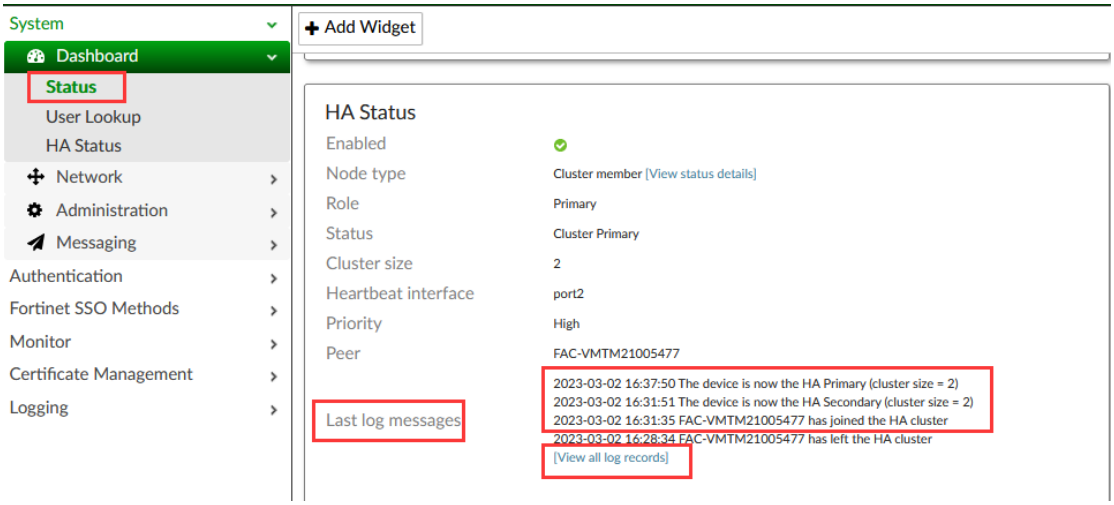
在正常工作状态下,如果拔掉主机的监控线，默认 30 秒后,会重新计算 HA,备机会工作在 Active 状态，如果再次插入主机监控线，默认 30 秒后,会重新计算 HA,主机会立即切换到 Active 状态,不需要稳定状态 5 分

钟后再开始强占.

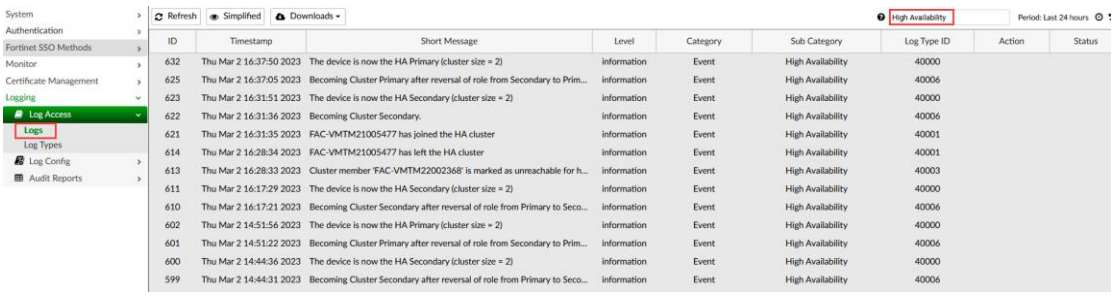
另外，需要注意的 HA 切换完成后，FAC 主机不会立即处于工作状态，FAC 内部需要几十秒钟做一些内部的数据操作,等这些操作完成后 FAC 才处于正常工作状态.

6.5 HA A-P HA 日志查看

从 FAC 的 status 日志可以看到 HA 的相关日志:



更多的 HA 日志可以在日志中查询:



6.6 HA LB 模式介绍

HA LB: 即主主模式，一般是 FAC 之间不在同一个地方，通过三层相连；LB 模式可以理解为是两个独立工作的 FAC，但是 LB Slave 会从 LB Master 同步一些认证相关的配置;

FAC 的角色为 Standalone Master 或 Load Balancing Slave

A-A LB 模式部署时, FAC 之间:

- 设备型号可以不一样
- 软件版本必须一样
- 根据部署需求, 用户 license 可以不一样
- A-A LB 之间的 token, 如果用户在 Standalone Master 上分的 token, 可以同步到 LB 上使用, 用户在 LB 上分的 token 不能在 Standalone Master 上使用

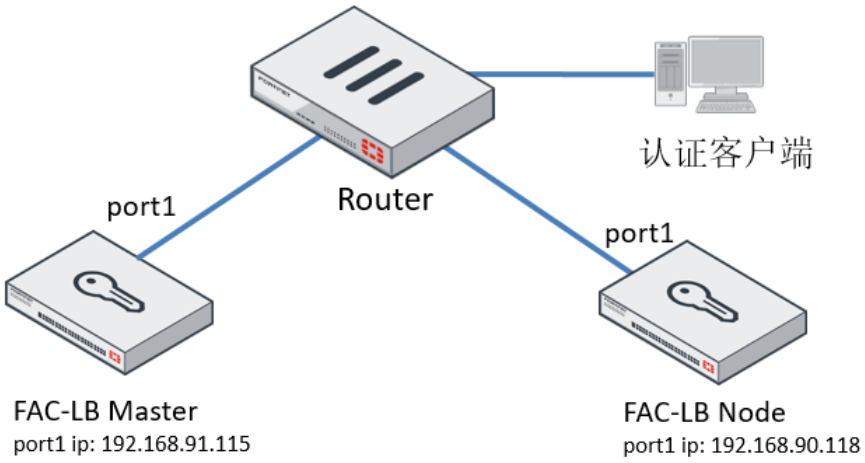
  关于 LB 模式的配置同步:

  Standalone Master 不会从 LB node 同步配置, 只有 LB node 从 Master 同步配置, 同步的配置有:
- Token 和种子
- Local 用户信息
- Remote 用户信息
- Group 映射关系
- 用户和 token 的映射
- Local Services 和 Local CA 下的相关证书
- 本地用户/远端用户的证书绑定关系
- SAML 相关配置:
  - Authentication > SAML IdP > General 下的 IdP 配置
  - Authentication > SAML IdP > Service Providers 下的 SP 配置
- 可以配置在 LB 之间同步管理员

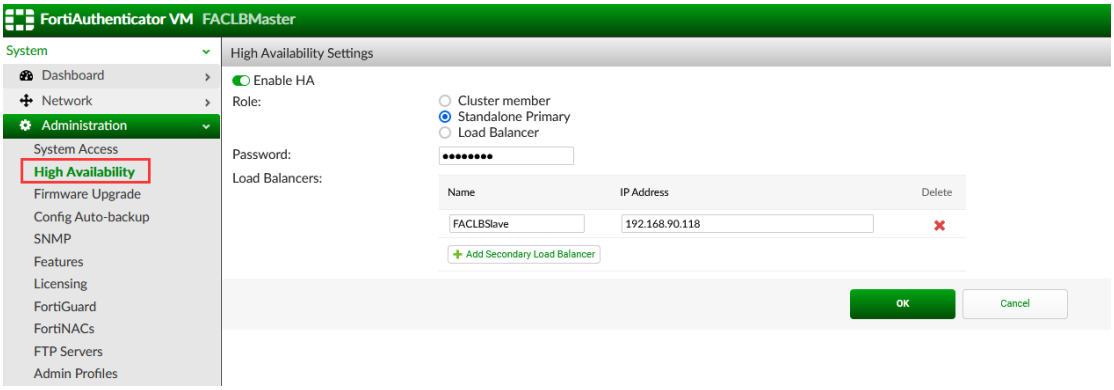
另外, 建议对于不同步的配置, 在配置时两个 FAC 建议配置相同规则/策略/group 名字.

6.7 HA LB 模式的配置

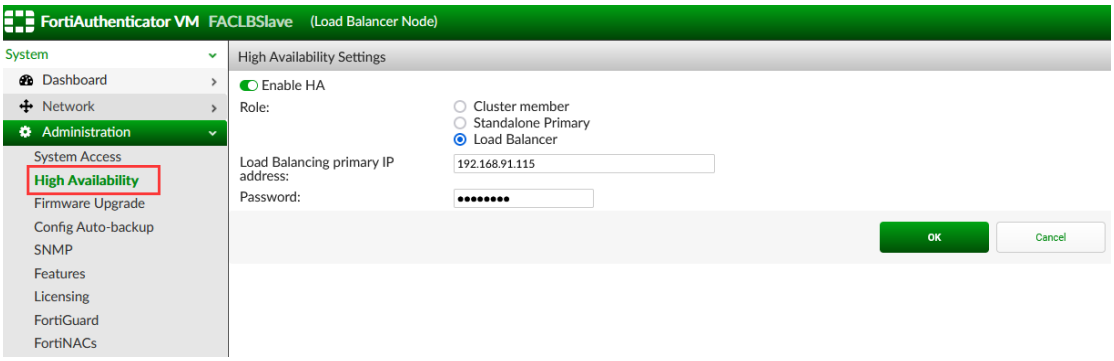
测试拓扑:



LB Primary 侧的配置:

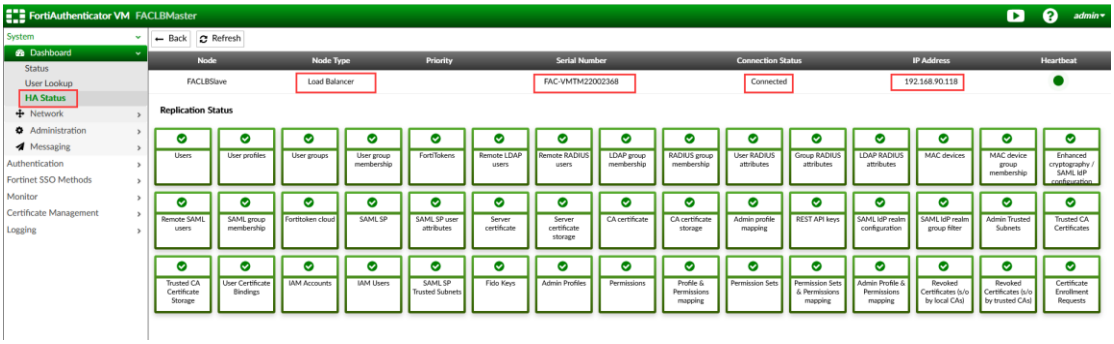


LB Node 侧的配置:

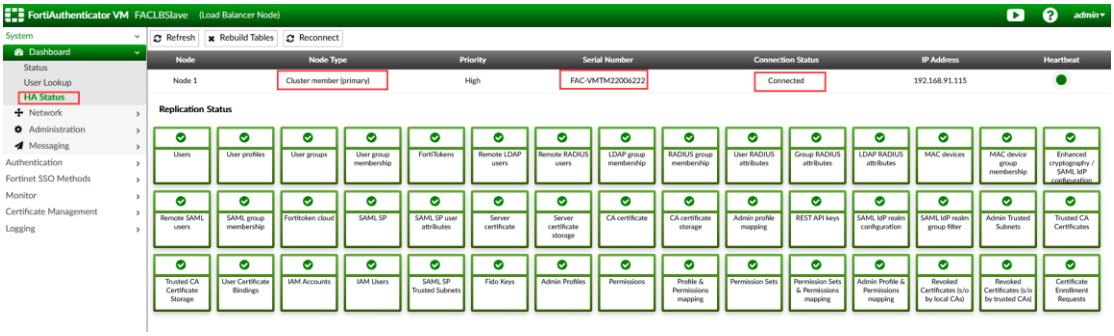


6.8 HA LB 模式状态查看

LB Primary 的 LB 状态:



LB Node 的 LB 状态:



6.9 HA LB 模式的心跳

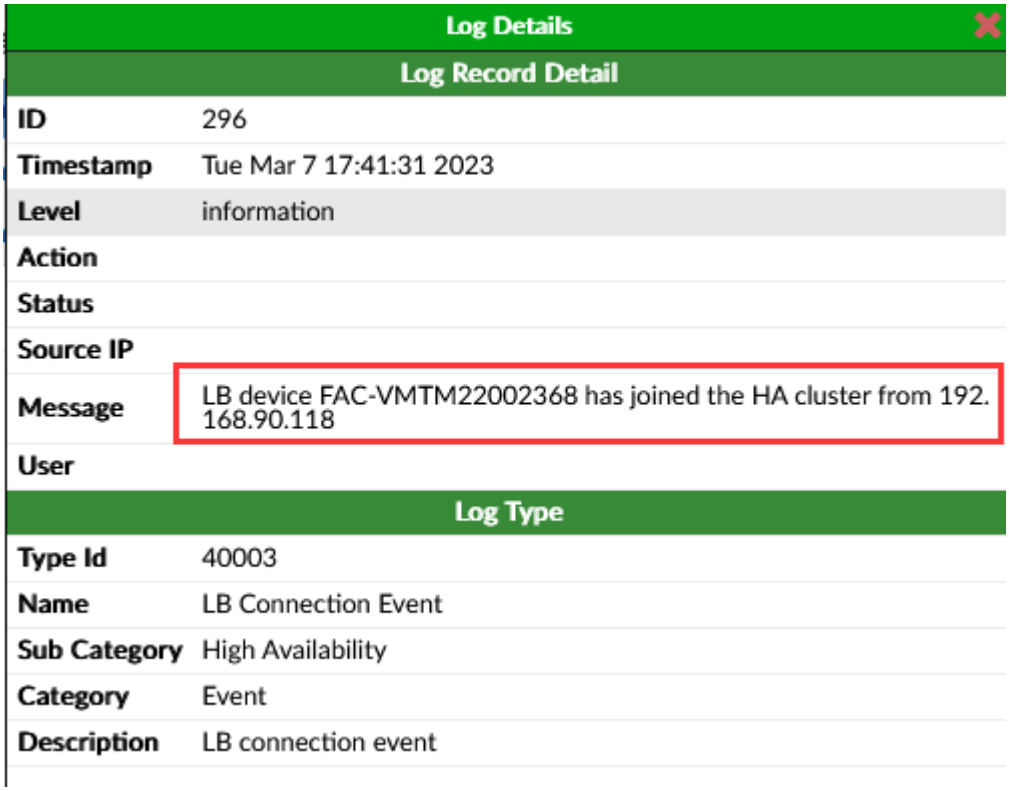
LB Node 配置完成后, LB Node 使用 udp 721 端口向 LB Primary 发起 LB Join request, 每 20 秒发送一次, 如果收到了 LB Primary 的 Join ack, 则建立 vpn 通道, 使用 udp 1194 端口进行通讯;

LB Node 每 5 秒发送一次心跳报文给 LB Primary, LB Primary 收到心跳报文后返回一个 HB-Ack 给 LB Node;

如果超过 210 秒 LB Node 没有收到 HB-Ack, LB Node 会删除 VPN 通道, 重新开始尝试与 LB Primary 建立 HA LB 连接;

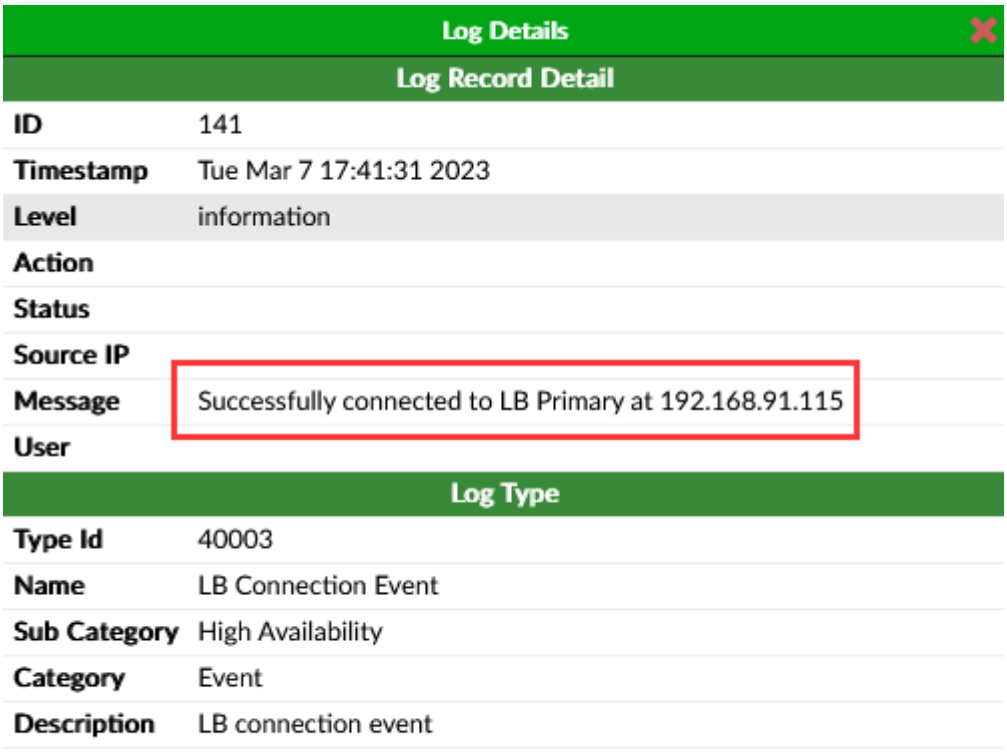
6.10 HA LB 模式日志查看

LB Primary 日志:



Log Details	
Log Record Detail	
ID	296
Timestamp	Tue Mar 7 17:41:31 2023
Level	information
Action	
Status	
Source IP	
Message	LB device FAC-VMTM22002368 has joined the HA cluster from 192.168.90.118
User	
Log Type	
Type Id	40003
Name	LB Connection Event
Sub Category	High Availability
Category	Event
Description	LB connection event

LB Node 日志:



Log Details	
Log Record Detail	
ID	141
Timestamp	Tue Mar 7 17:41:31 2023
Level	information
Action	
Status	
Source IP	
Message	Successfully connected to LB Primary at 192.168.91.115
User	
Log Type	
Type Id	40003
Name	LB Connection Event
Sub Category	High Availability
Category	Event
Description	LB connection event

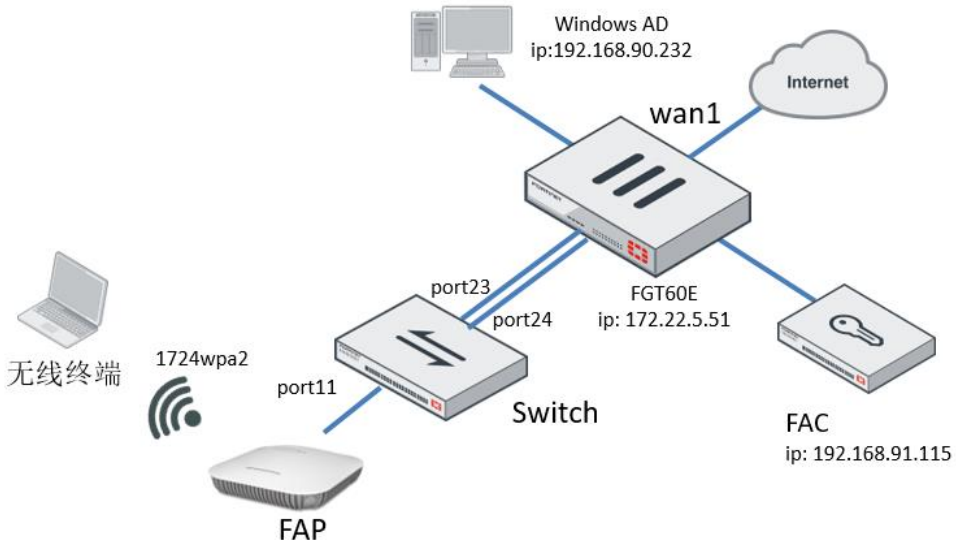
二. FAC 常用部署案例介绍

FAC 作为专业的认证服务器支持 Portal 认证/802.1x 认证/SAML 认证等，本章节介绍相关认证的组网和配置.

1. 无线 WPA2 企业认证

无线终端使用 ldap 帐号连接 wpa2 ssid，并获取 FAC 下发的动态 vlan31;

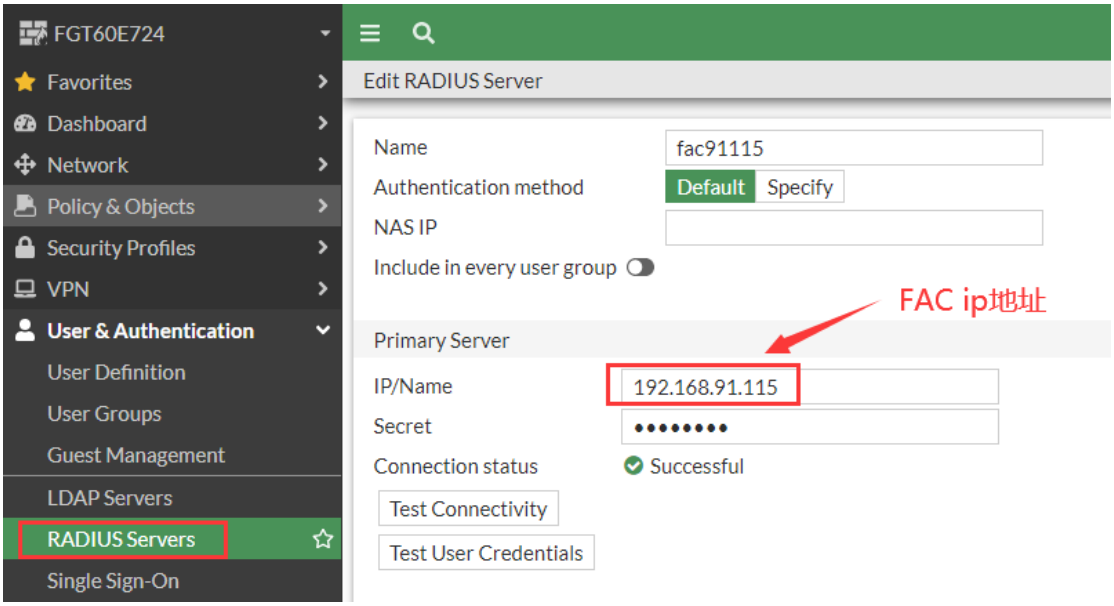
1.1 测试组网



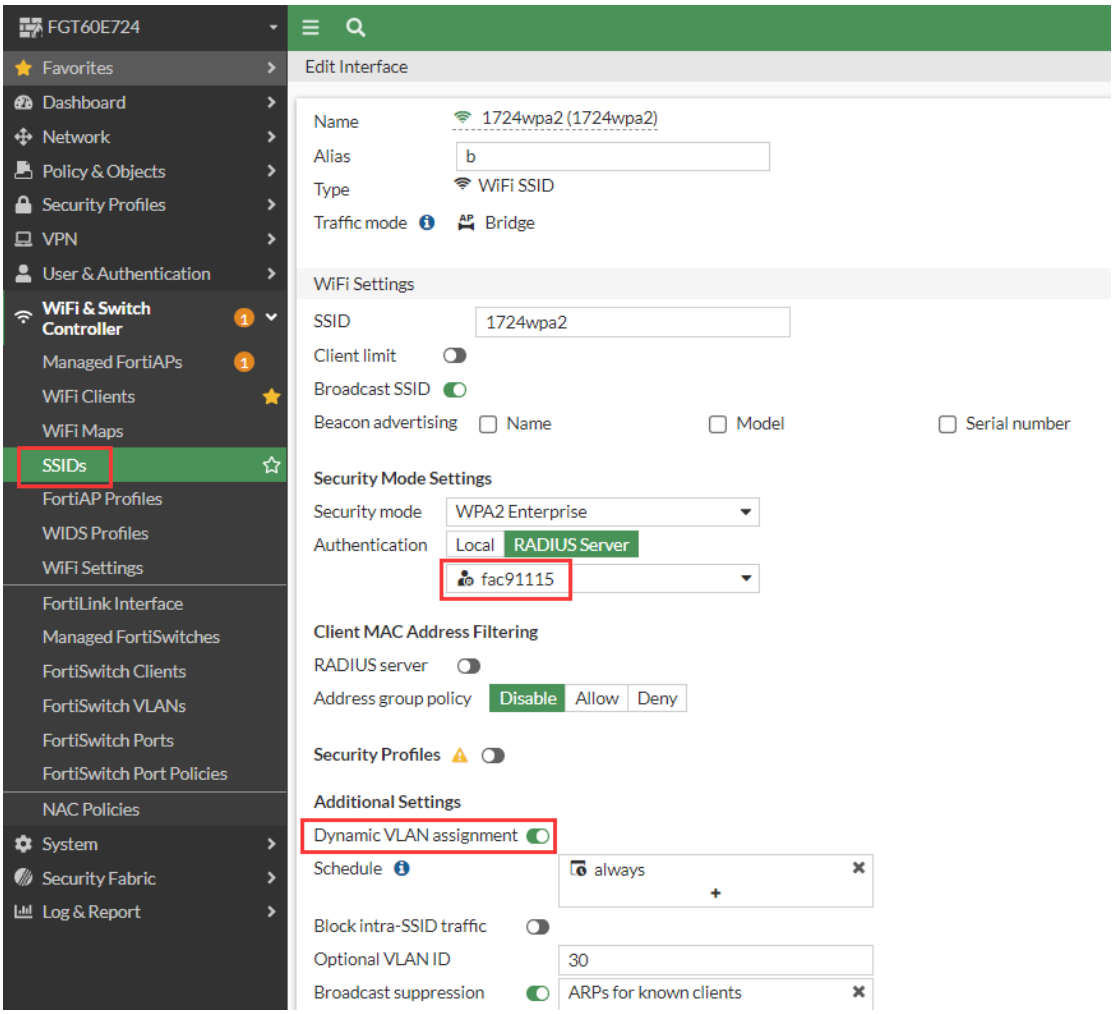
FAC 作为 radius server，跟 ldap server 对接，同步远端 ldap server 用户

1.2 防火墙相关配置

无线 radius 配置:

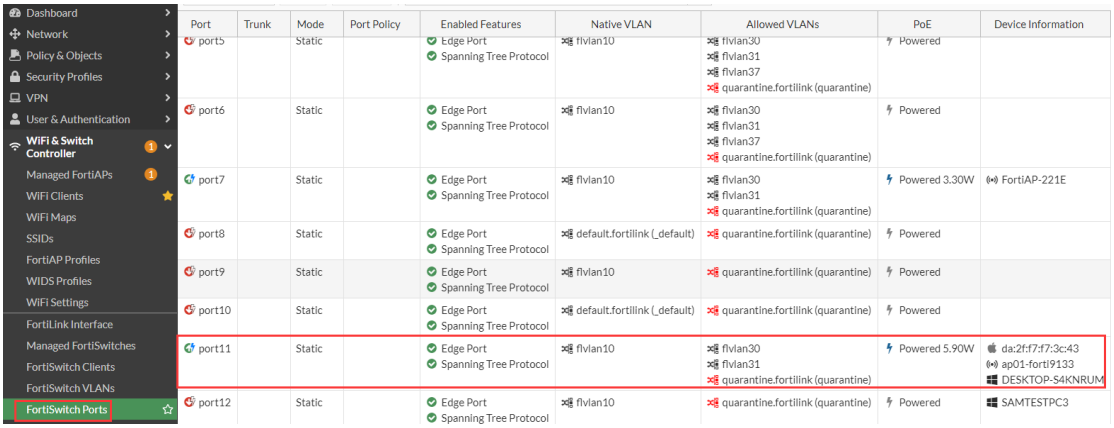


无线 ssid 配置:



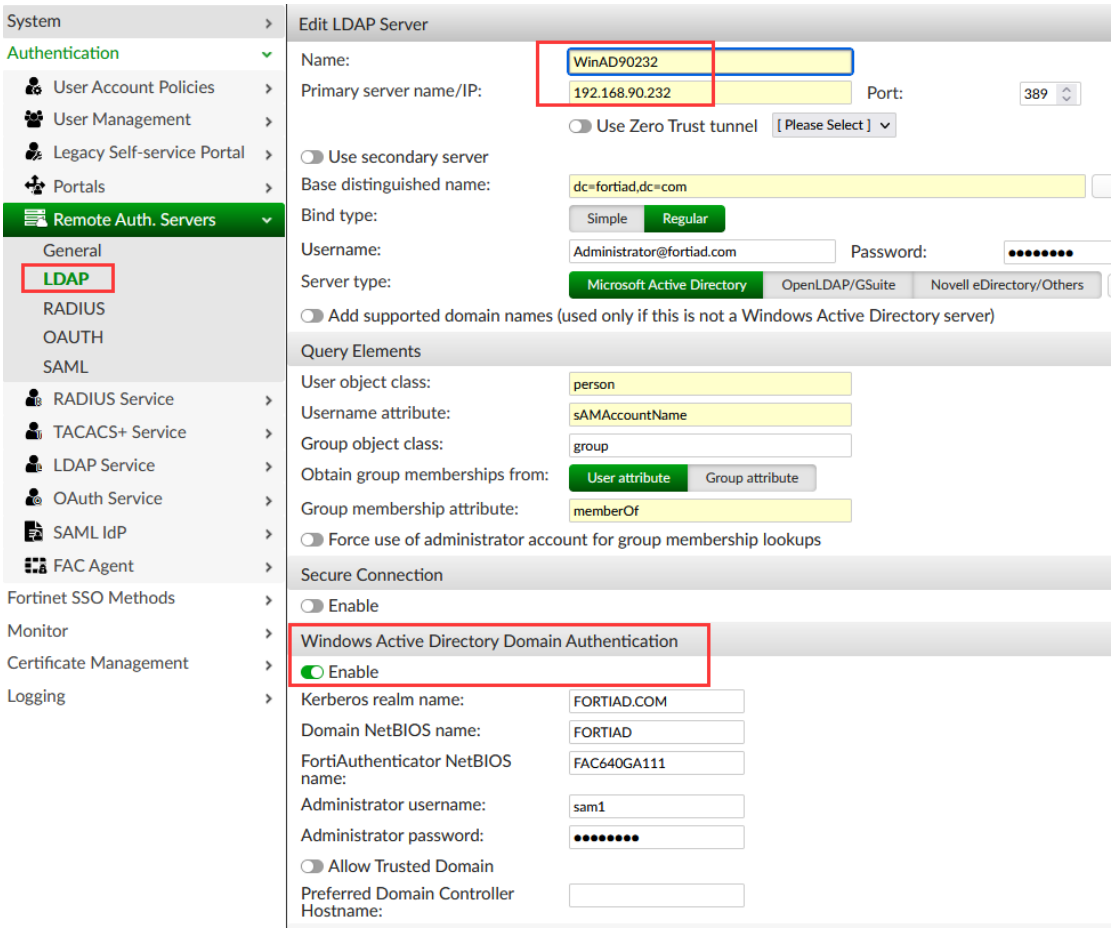
上图中，无线配置的”Optional VLAN ID” 为 vlan 30，又开启了动态 vlan 下发,表示如果 radius server 下发了动态 vlan 那就给终端下发此 vlan，如果没有下发 vlan，那终端无线连上后获取的就是默认的 vlan30.

交换机端口配置:

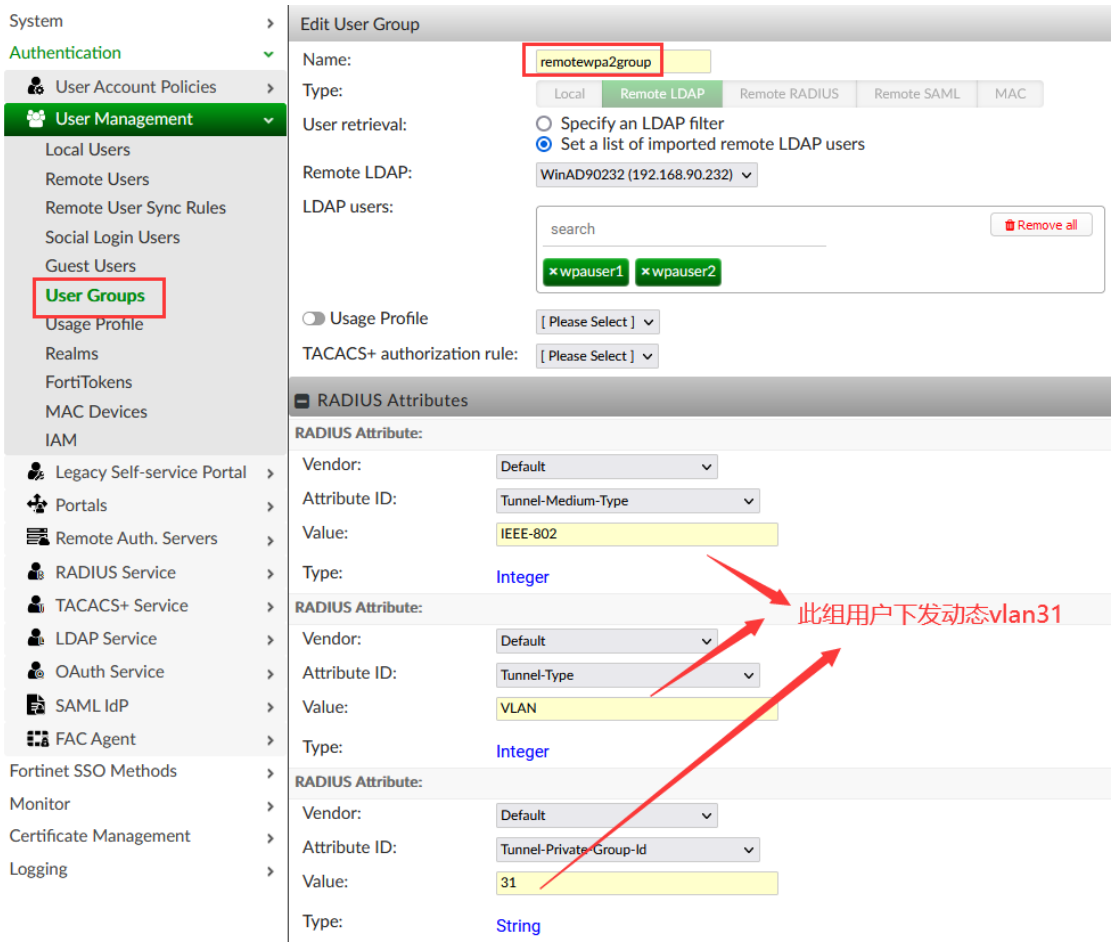


1.3 FAC 侧相关配置

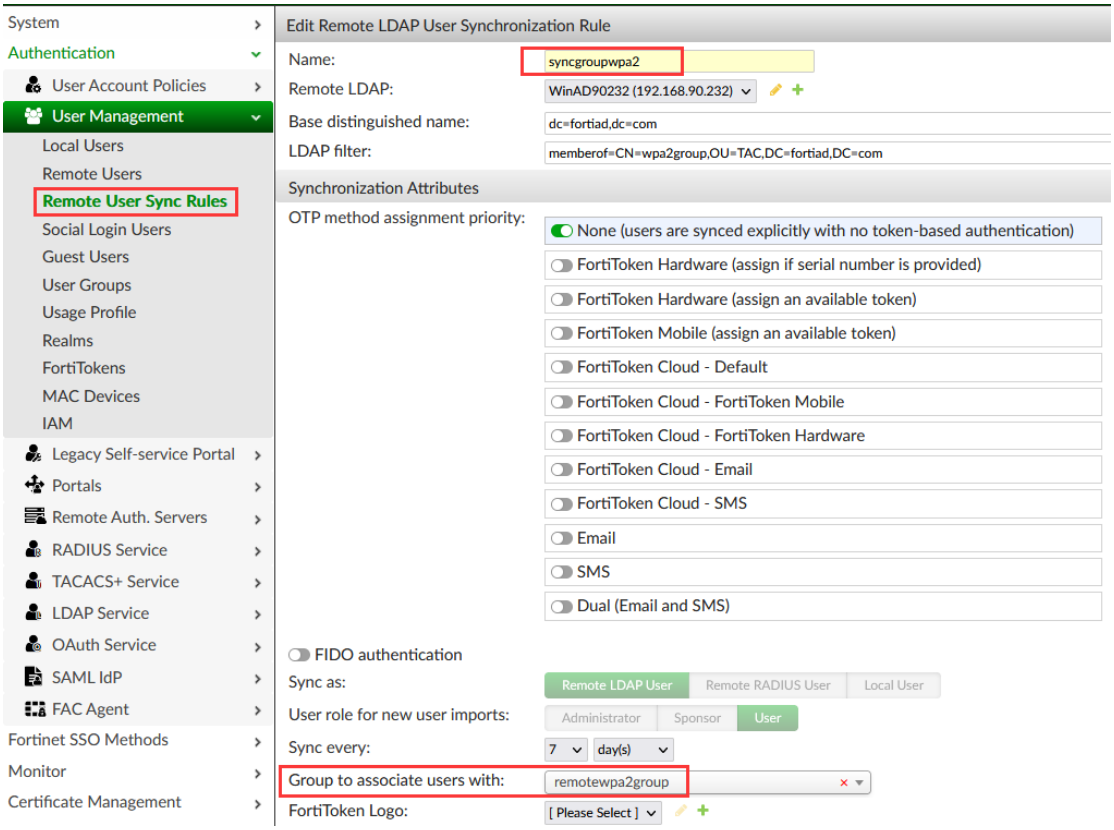
Ldap server 配置:



Radius group 配置，此 group 配置动态 vlan 下发属性:

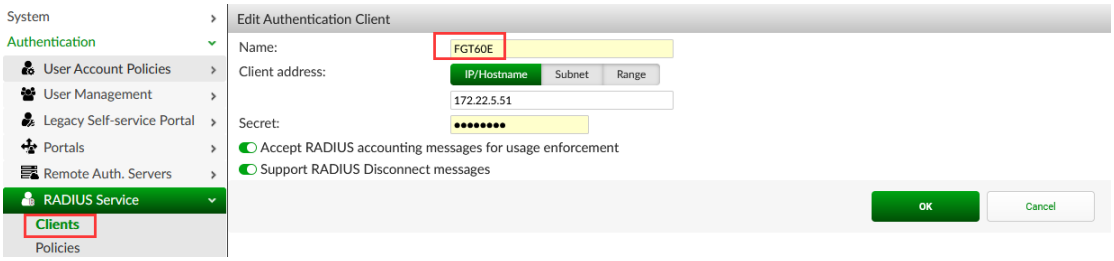


配置自动同步规则,同步 ldap server 上的 wpa2group 的用户到 remotewpa2group:

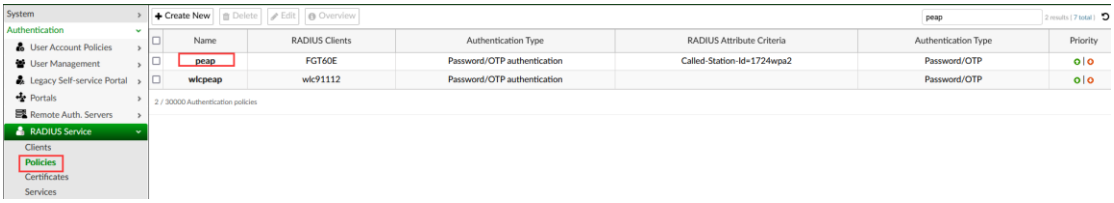


手动或自动同步后:

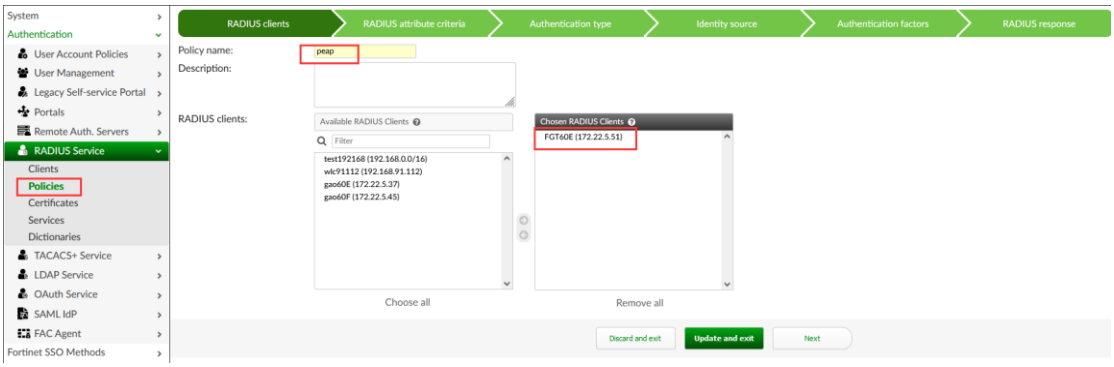
配置 radius 客户端，即配置 FGT60E 作为 radius 客户端

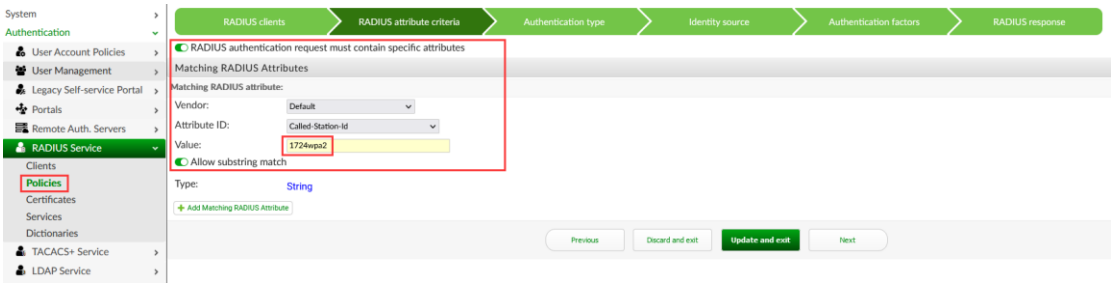


配置 radius 认证策略:



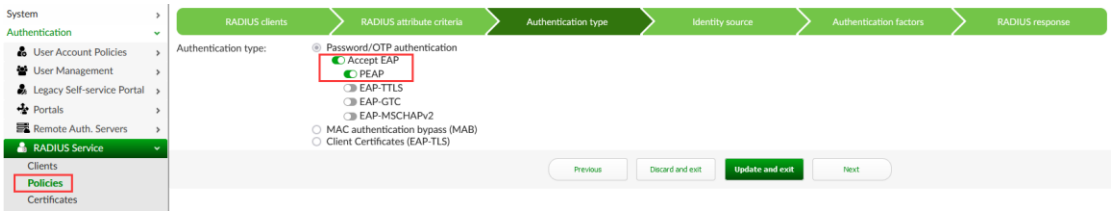
详细的配置信息为:

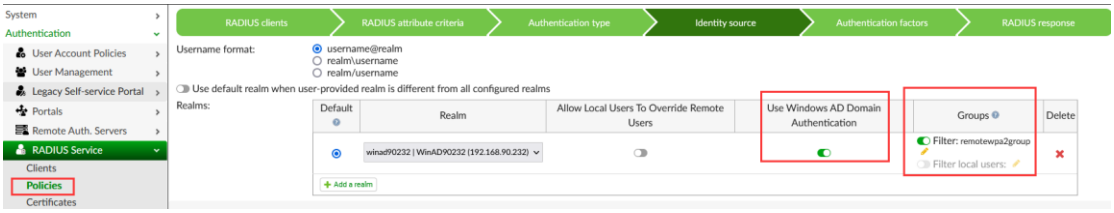




注意：上面配置中,开启了”RADIUS authentication request must contain specific attributes”

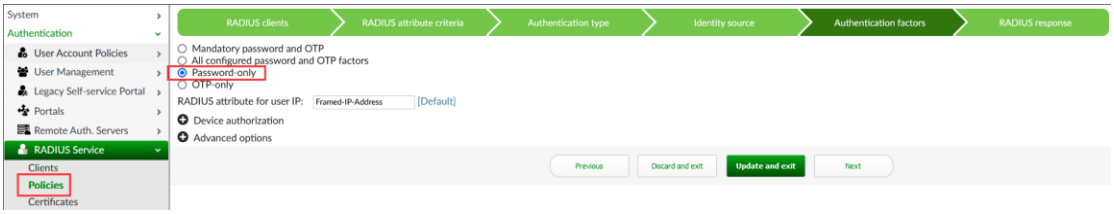
这是为了 radius 访问策略的控制，因为同一个认证请求可能命中了 FAC 上的多个认证策略，虽然 FAC 的认证策略也有的优先级，但是在多个认证策略下，开启此功能可以更好的控制认证请求，比如此例中必须是认证的 ssid 中带有 1724wpa2 的字符串才会命中此认证策略;





上图配置中，因为是 wpa2 认证，必须是 FAC 加入 AD 域，且开启”Use Windows AD domain authentication”.

另外，因为是基于 group 开启了 radius 动态 vlan，所以必须开启 group filter.



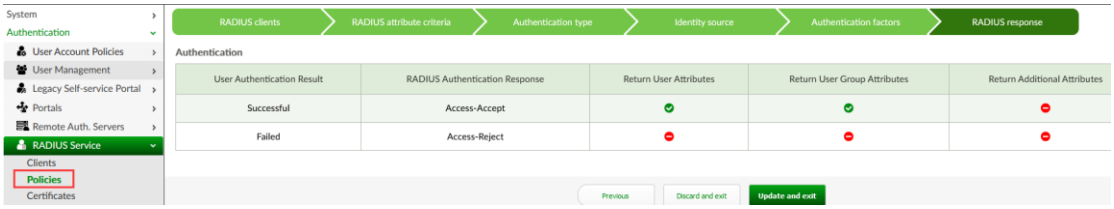
注意上图中的配置，如果用户分配了 token，但是 wpa2 认证又不适合和 token 认证一起用，所以开启的是 Password-only.

Mandatory password and OTP：强制用户必须是双因素认证

All configured password and OTP factors：如果用户开启了 token 认证，则必须做 token 认证，如果用户没有开启 token 认证则不需要 token 认证.

Password-only：不管用户是否开启了 token 认证，对用户只校验密码，不做 token 认证;

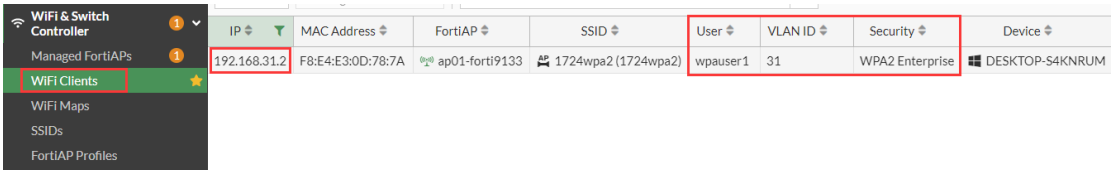
OTP-only： 对用户只做 token 认证，即用户认证时，把 token 当作密码输入;



至此配置完成;

1.4 相关测试日志

防火墙上显示终端接入成功,获取 vlan31 网段的 ip 地址:



FAC 的日志显示用户 802.1x 认证成功:

Log Details	
Log Record Detail	
ID	80198
Timestamp	Tue Feb 28 15:47:01 2023
Level	information
Action	Authentication
Status	Success
Source IP	172.22.5.51
Message	802.1x authentication successful
User	wpauser1
Log Type	
Type Id	20420
Name	802.1x Authentication OK
Sub Category	Authentication
Category	Event
Description	802.1x authentication successful

FAC 的 radius debug 日志显示了更详细的信息，包括命中的认证策略，返回的 radius 属性值:

```
(95) facauth: ===>NAS IP:172.22.5.51
(95) facauth: ===>Username:wpauser1
(95) facauth: ===>Timestamp:1677570421.589112, age:0ms
(95) # Executing group from file /usr/etc/raddb/sites-enabled/default
(95) eap: Expiring EAP session with state 0x2f2f113727c10897
(95) eap: Finished EAP session with state 0x2f2f113727c10897
(95) eap: Previous EAP request found for state 0x2f2f113727c10897, released from the list
(95) # Executing section post-auth from file /usr/etc/raddb/sites-enabled/default
(95)         &User-Name !* ANY
(95)       &reply::TLS-Session-Cipher-Suite += &session-state:TLS-Session-Cipher-Suite[*] -> 'ECDHE-RSA-AES256-GCM-SHA384'
(95)       &reply::TLS-Session-Version += &session-state:TLS-Session-Version[*] -> 'TLS 1.2'
(95)       &reply::User-Name += &session-state:User-Name[*] -> 'wpauser1'
(95) facauth: ===>NAS IP:172.22.5.51
(95) facauth: Found authclient from preloaded authclients list for 172.22.5.51: FGT60E (172.22.5.51)
(95) facauth: Found vendor 0, attr 30 --> "1774wpa2"
(95) facauth: Found authpolicy 'peap' for client '172.22.5.51'
(95) facauth: Client type: external (subtype: radius)
(95) facauth: Input raw_username: (null) Realm: (null) username: wpauser1
(95) facauth: Searching default realm as well
(95) facauth: Realm not specified, default goes to Windows AD, id: 1
(95) facauth: User [enable fido: false, token count: 0, revoked_token_count: 0]
(95) facauth: Policy [fido_auth_opt: disabled, twofactor: password only, no_fido: two factor, revoked: reject]
(95) facauth: Decided on [is_fido: false, two_factor: password only, token_type: none]
(95) facauth: EAP authentication success - add configured radius attributes to response
(95) facauth: Add Radius attribute: attr_id:65 (attr 65, vendor 0) attr:6
(95) facauth: Add Radius attribute: attr_id:64 (attr 64, vendor 0) attr:13
(95) facauth: Add Radius attribute: attr_id:81 (attr 81, vendor 0) attr:31
(95) facauth: Updated auth log 'wpauser1': 802.1x authentication successful
(95) Sent Access-Accept Id 63 from 192.168.91.115:1812 to 172.22.5.51:19502 length 0
(95)   MS-MPPE-Recv-Key = 0x04015fff8b265d204864eb8ce2a5bca7332238d145096d59db6f9ce02e477f84
(95)   MS-MPPE-Send-Key = 0x8c810bf56c91e8a470c71b5ab131e35f12136f4220b8c6477f2d5a6f8f58c974
(95)   EAP-Message = 0x03ee0004
(95)   Message-Authenticator = 0x00000000000000000000000000000000
(95)   User-Name = "wpauser1"
(95)   Tunnel-Medium-Type += IEEE-802
(95)   Tunnel-Type += VLAN
(95)   Tunnel-Private-Group-Id += "31"
```

命中的认证策略

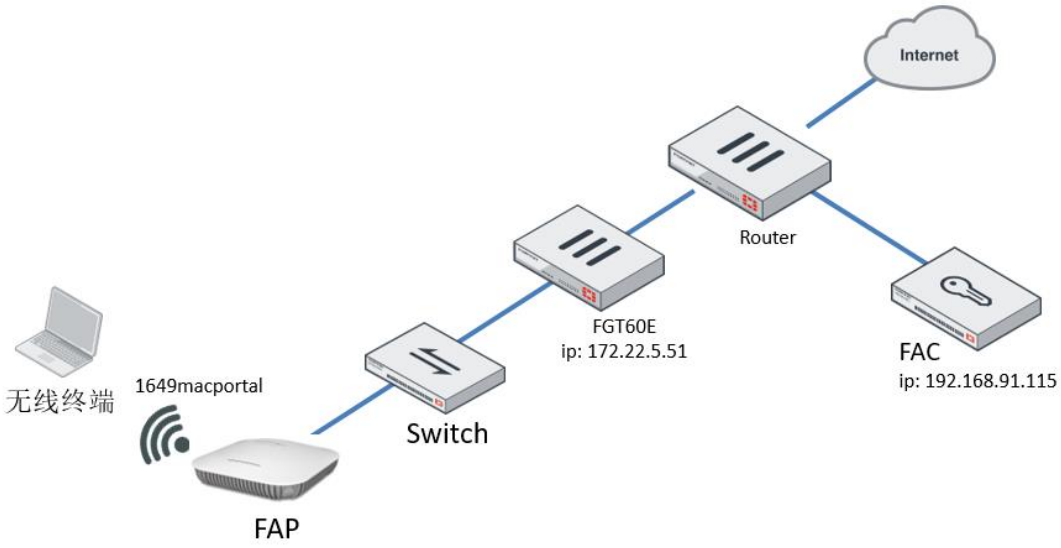
认证成功后返回的radius vlan属性

2. 无线 MAC+Portal 认证

- 用户首次接入无线网络时，首先先做 MAC 认证,因为是新用户，Radius server 后台没有记录此用户的 MAC 地址，所以 MAC 认证失败，引导用户做 Portal 认证; Portal 认证成功后，后台 Radius server 记录用户的 MAC 地址信息,以便后续的 MAC 认证

- 当用户离开无线网络后，再次接入无线网路时，首先还是先对用户做无感知的 MAC 认证，由于用户 MAC 地址已经记录在 Radius server 上,所以用户 MAC 认证成功后，用户就可以直接上网了,无需再做 Portal 认证，提高用户体验.

2.1 测试组网



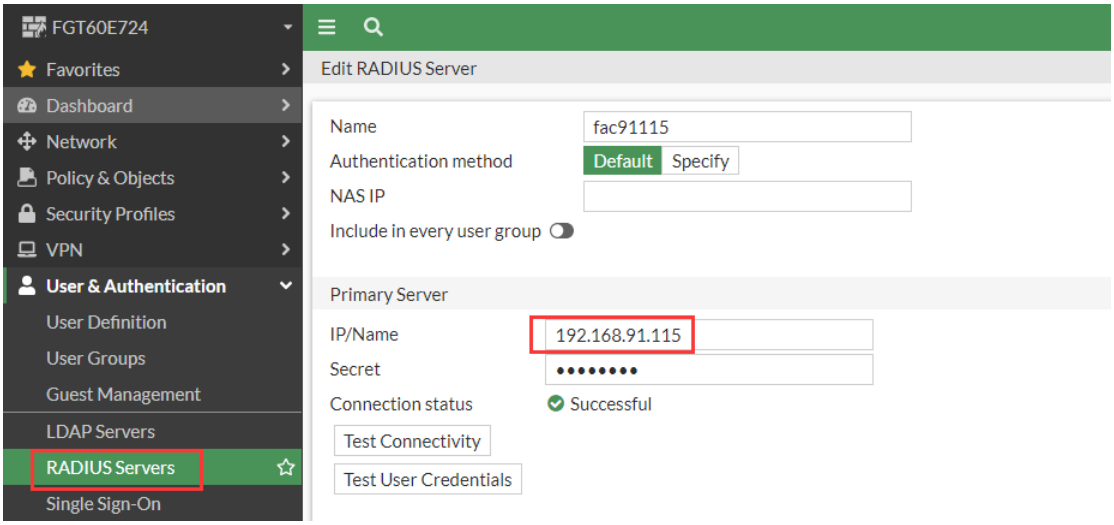
无线 ssid ” 1649macportal”，开启 mac+portal 认证,

FAC 作为 portal server 和 radius server，支持 mac+portal 认证;

2.2 防火墙相关配置

无线 radius 和 radius group 相关配置:

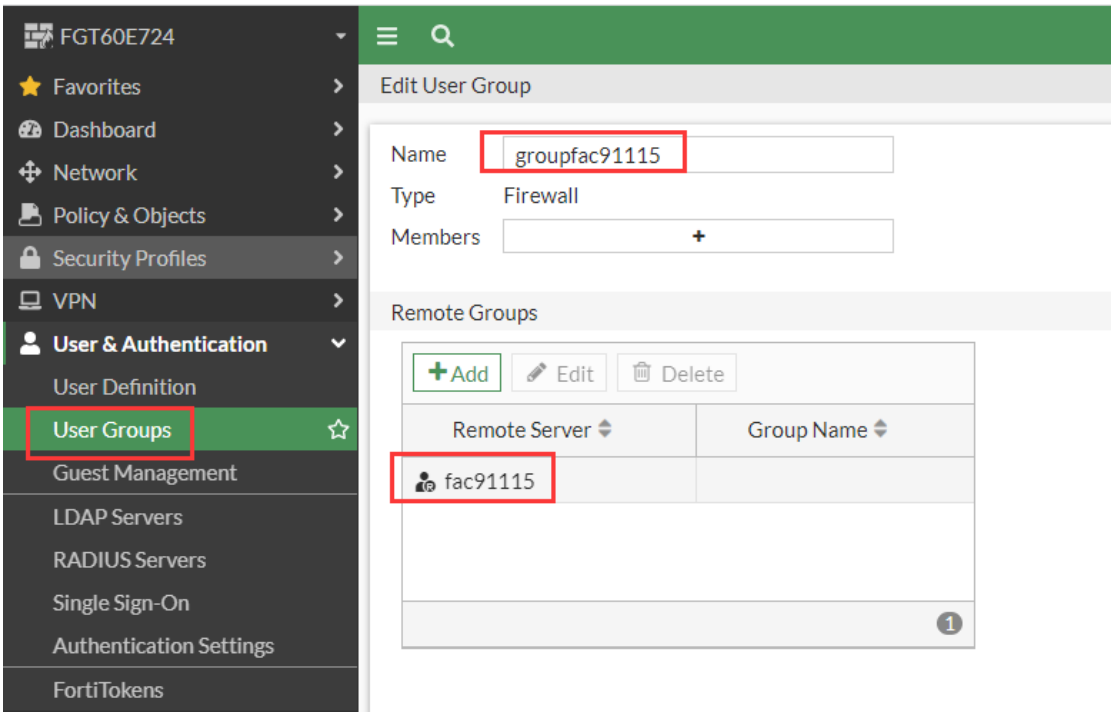
Radius server 配置:



CLI:

```
config user radius
   edit "fac91115"
      set server "192.168.91.115"
      set secret ENC XXX
      set acct-interim-interval 240
      set radius-coa enable
      set source-ip "172.22.5.51"
      config accounting-server
         edit 1
            set status enable
            set server "192.168.91.115"
            set secret ENC XXX
            set port 1813
         next
      end
   next
end
```

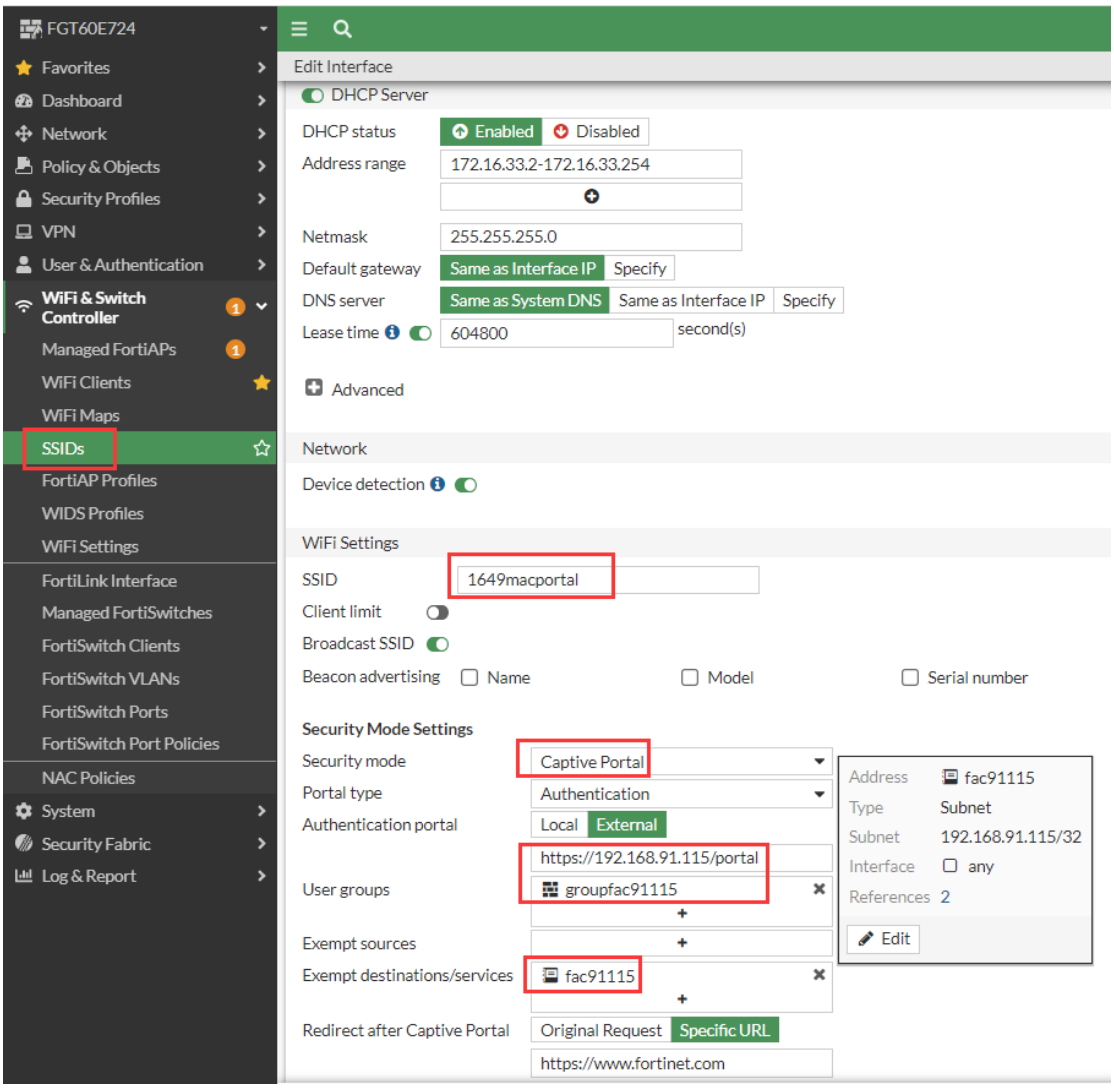
无线 radius group 配置:



CLI:

```
FGT60E724 # show user group groupfac91115
config user group
   edit "groupfac91115"
      set member "fac91115"
   next
end
```

无线 SSID 相关配置:

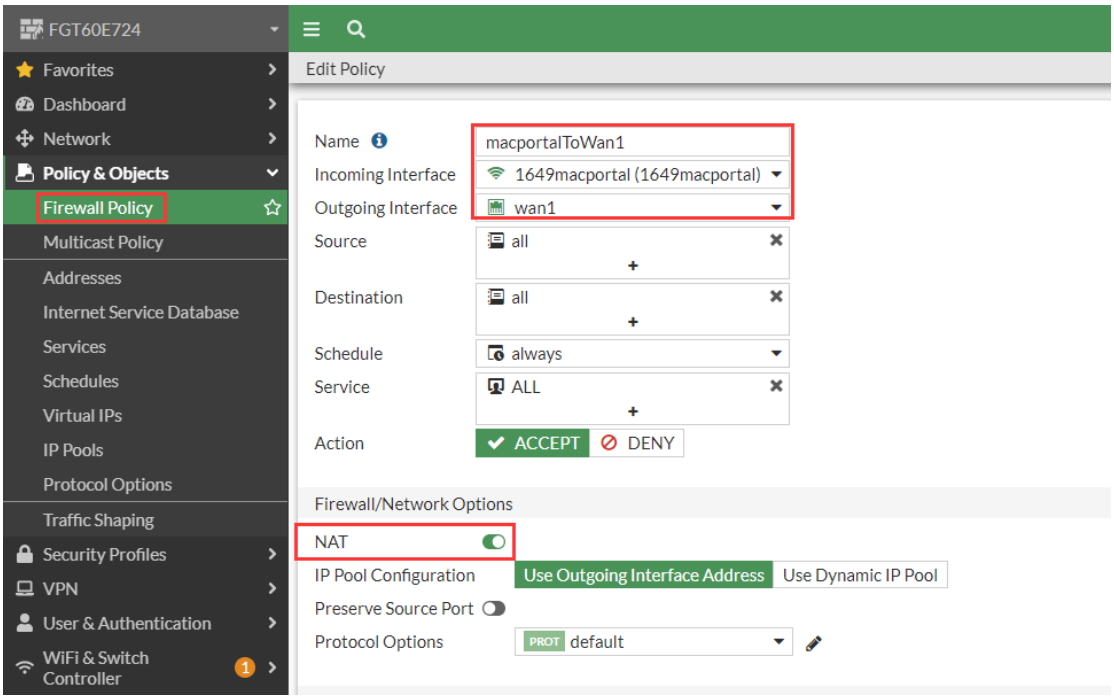


CLI 配置:

```
show wireless-controller vap 1649macportal
config wireless-controller vap
    edit "1649macportal"
        set ssid "1649macportal"
        set security captive-portal
        set external-web "https://192.168.91.115/portal"
        set mac-auth-bypass enable
        set selected-usergroups "groupfac91115"
        set security-exempt-list "1649macportal-exempt-list"
        set security-redirect-url "https://www.fortinet.com"
        set schedule "always"
        set captive-portal-fw-accounting enable
        set quarantine disable
    next
end
```

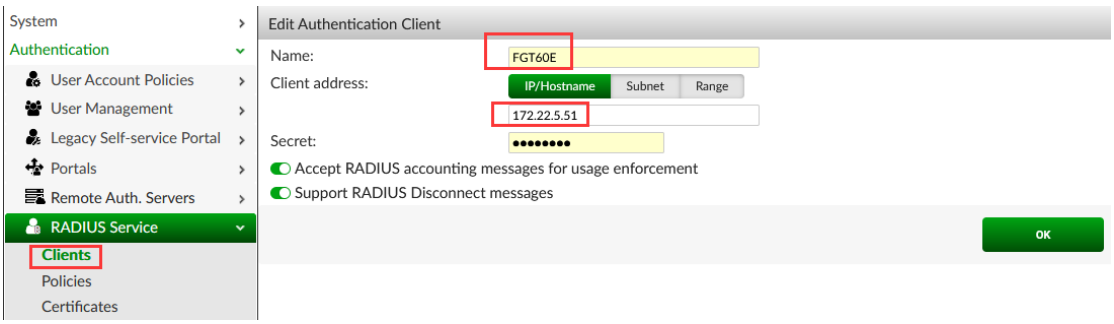
注意:上面 portal 的登录页面是 FAC 上配置的页面，不同的 FAC 的版本上配置的 portal 登录页面可能 url 不一样，具体可检查 FAC 侧的配置.

无线接口上网的防火墙策略，不需要再做 portal 认证的例外等相关配置.

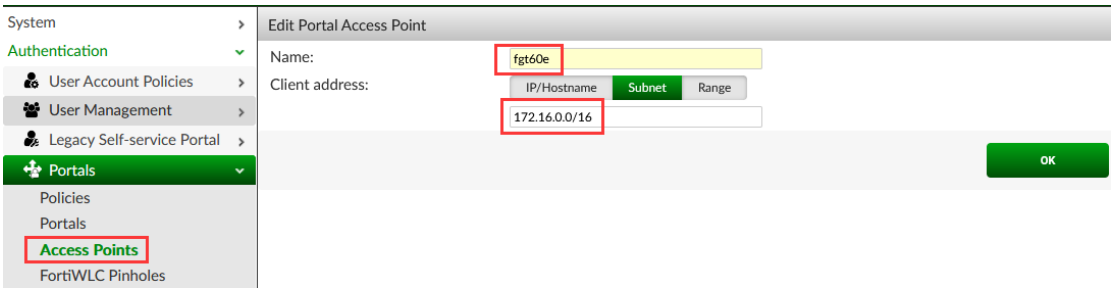


2.3 FAC 侧相关配置

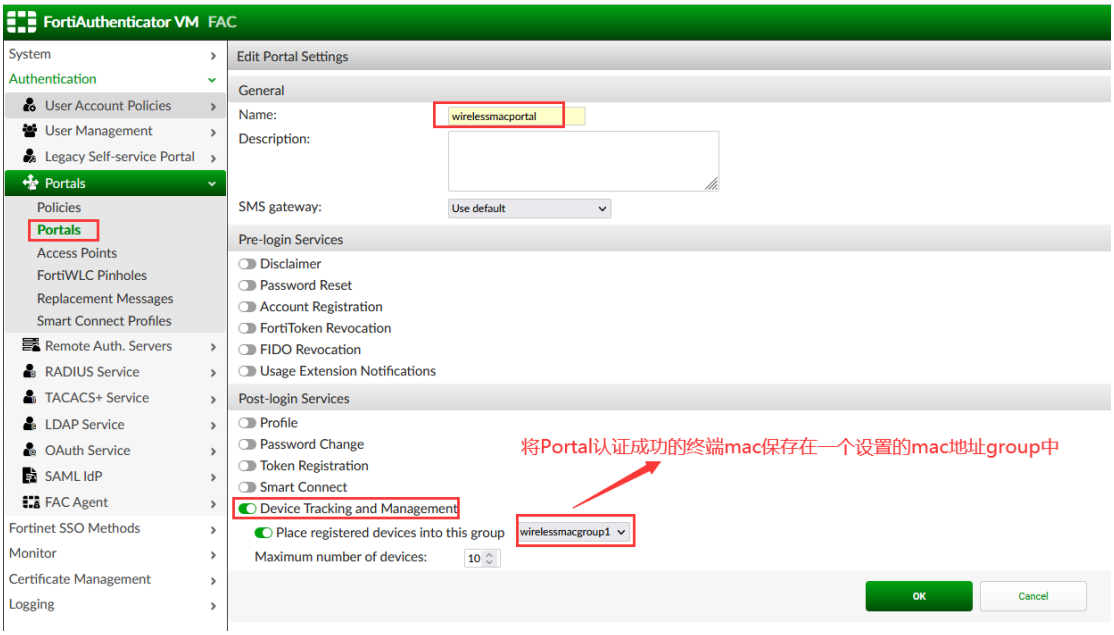
Radius client 配置，把 FGT 作为 radius client 加入到 FAC:



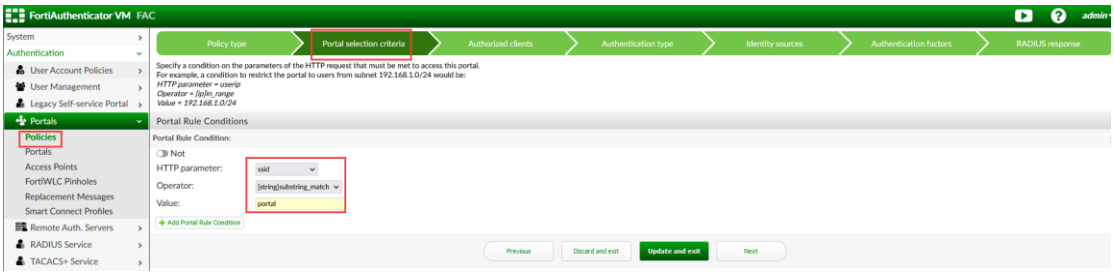
FAC 上的 AP 配置，注意：这里的 AP 配置指的是本例中无线集中转发的接口的 ip 地址信息，实际部署时，如果不好确认，可配置为网段:

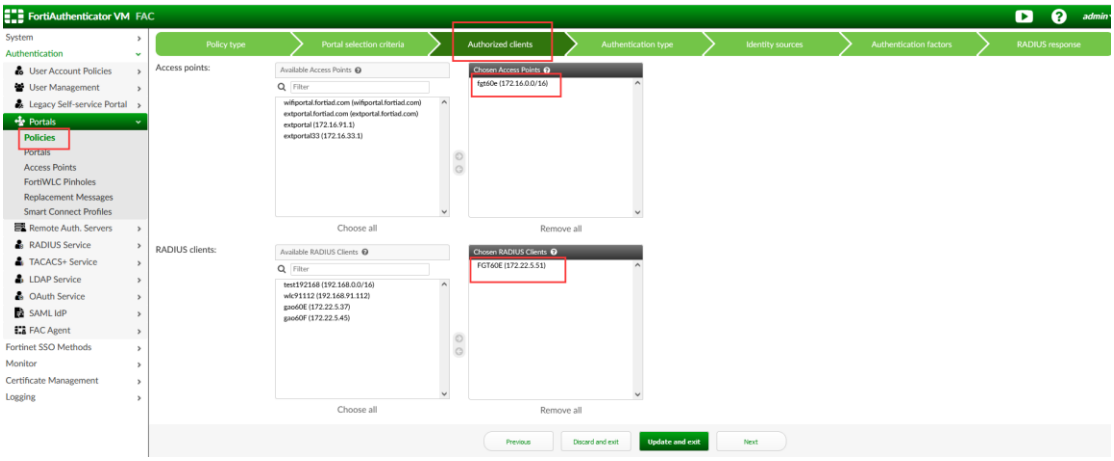


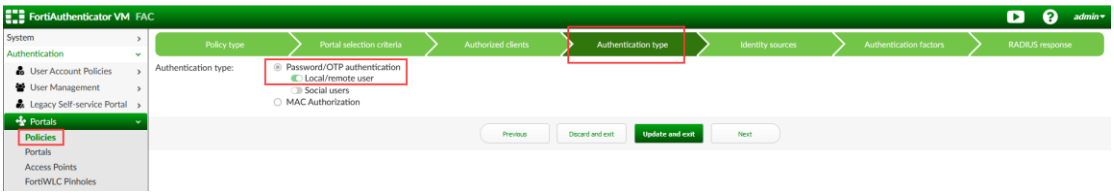
新建 Portal 设置，因为本例中开启了 mac 地址 MAB 认证，所以需要开启记录认证终端的 mac 地址，以便终端再次认证时使用 mac 地址无感知认证:

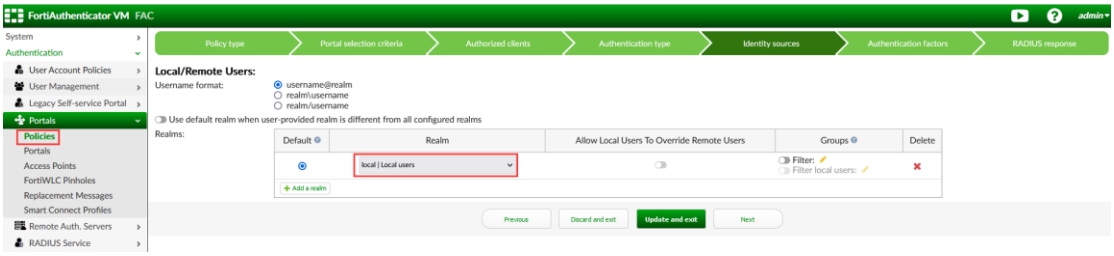


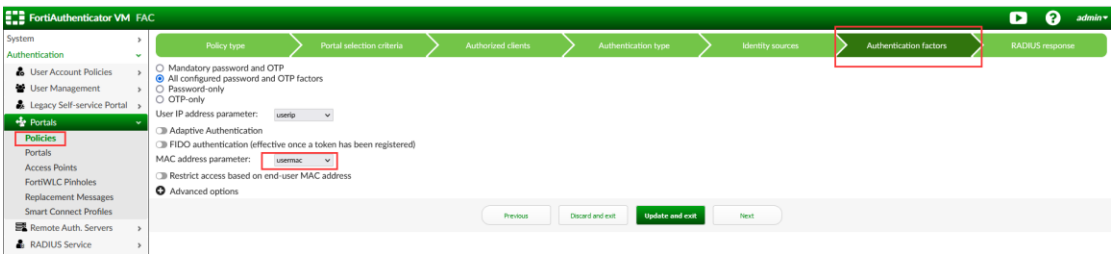
配置 Portal Policy:

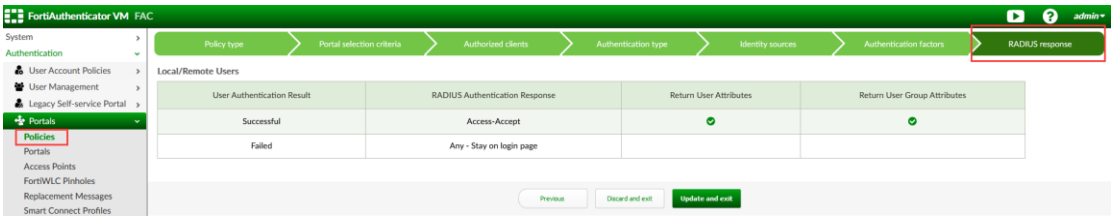

FortiAuthenticator VM FAC
admin
System
Authentication
User Account Policies
User Management
Legacy Self-service Portal
Portals
Policies
Portals
Access Points
FortiWLC Pinholes
Replacement Messages
Smart Connect Profiles
Remote Auth. Servers
RADIUS Service
TACACS+ Service
Policy type
Portal selection criteria
Authorized clients
Authentication type
Identity sources
Authentication factors
RADIUS response
Specify a condition on the parameters of the HTTP request that must be met to access this portal.
For example, a condition to restrict the portal to users from subnet 192.168.1.0/24 would be:
HTTP parameter = userip
Operator = ip/ip_range
Value = 192.168.1.0/24
Portal Rule Conditions
Portal Rule Condition:
Not
HTTP parameter:
ssid
Operator:
[string]substring_match
Value:
portal
Add Portal Rule Condition
Previous
Discard and exit
Update and exit
Next


FortiAuthenticator VM FAC
admin
Policy type
Portal selection criteria
Authorized clients
Authentication type
Identity sources
Authentication factors
RADIUS response
Access points:
Available Access Points
Chosen Access Points
fgt60e (172.16.0.0/16)
wifiportal.fortiad.com (wifiportal.fortiad.com)
extportal.fortiad.com (extportal.fortiad.com)
extportal (172.16.91.1)
extportal33 (172.16.33.1)
Choose all
Remove all
RADIUS clients:
Available RADIUS Clients
Chosen RADIUS Clients
FGT60E (172.22.5.51)
test192168 (192.168.0.0/16)
wlc91112 (192.168.91.112)
gso60E (172.22.5.37)
gso60F (172.22.5.45)
Choose all
Remove all
Previous
Discard and exit
Update and exit
Next

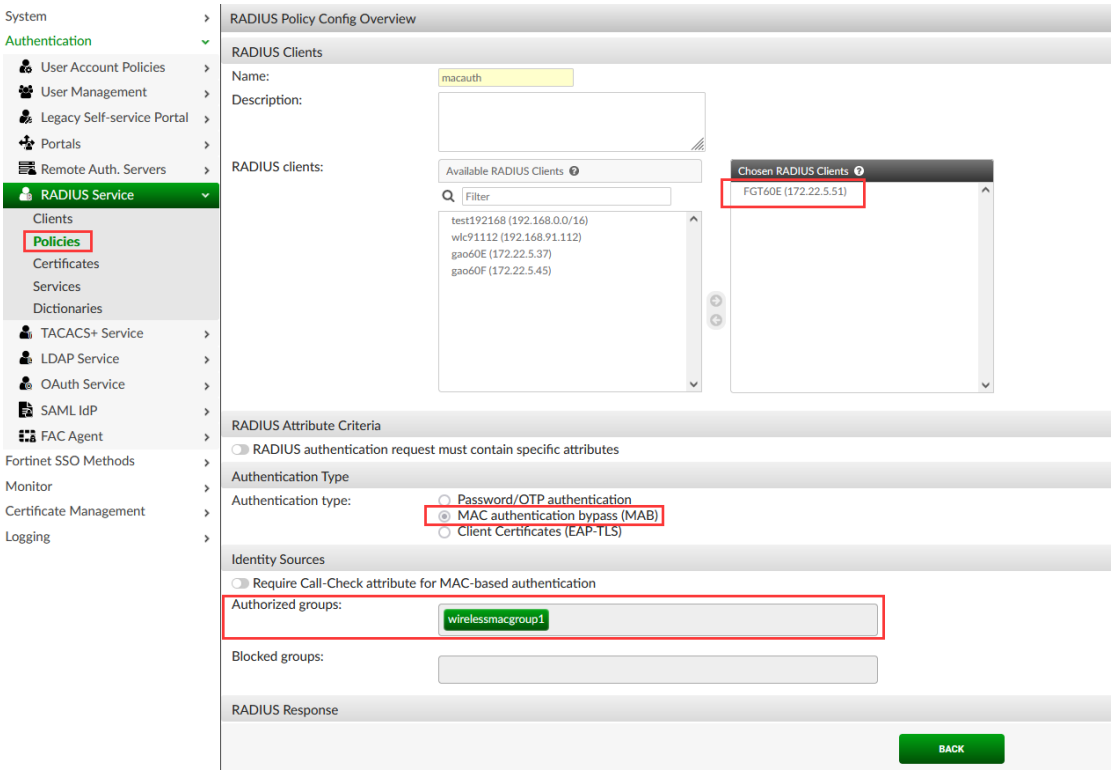

FortiAuthenticator VM FAC
admin
Policy type
Portal selection criteria
Authorized clients
Authentication type
Identity sources
Authentication factors
RADIUS response
Authentication type:
Password/OTP authentication
Local/remote user
Social users
MAC Authorization
Previous
Discard and exit
Update and exit
Next


FortiAuthenticator VM FAC
admin
Policy type
Portal selection criteria
Authorized clients
Authentication type
Identity sources
Authentication factors
RADIUS response
Local/Remote Users:
Username format:
username@realm
realm\username
realm/username
Use default realm when user-provided realm is different from all configured realms
Realms:
Default
Realm
Allow Local Users To Override Remote Users
Groups
Delete
local | Local users
Filter:
Filter local users:
Add a realm
Previous
Discard and exit
Update and exit
Next


FortiAuthenticator VM FAC
admin
Policy type
Portal selection criteria
Authorized clients
Authentication type
Identity sources
Authentication factors
RADIUS response
Mandatory password and OTP
All configured password and OTP factors
Password-only
OTP-only
User IP address parameter:
userip
Adaptive Authentication
FIDO authentication (effective once a token has been registered)
MAC address parameter:
usermac
Restrict access based on end-user MAC address
Advanced options
Previous
Discard and exit
Update and exit
Next



至此 Portal 认证配置完成，再配置一个 mac 地址认证 radius 策略，针对 portal 认证成功后记录的 mac 地址终端:



2.4 相关测试日志

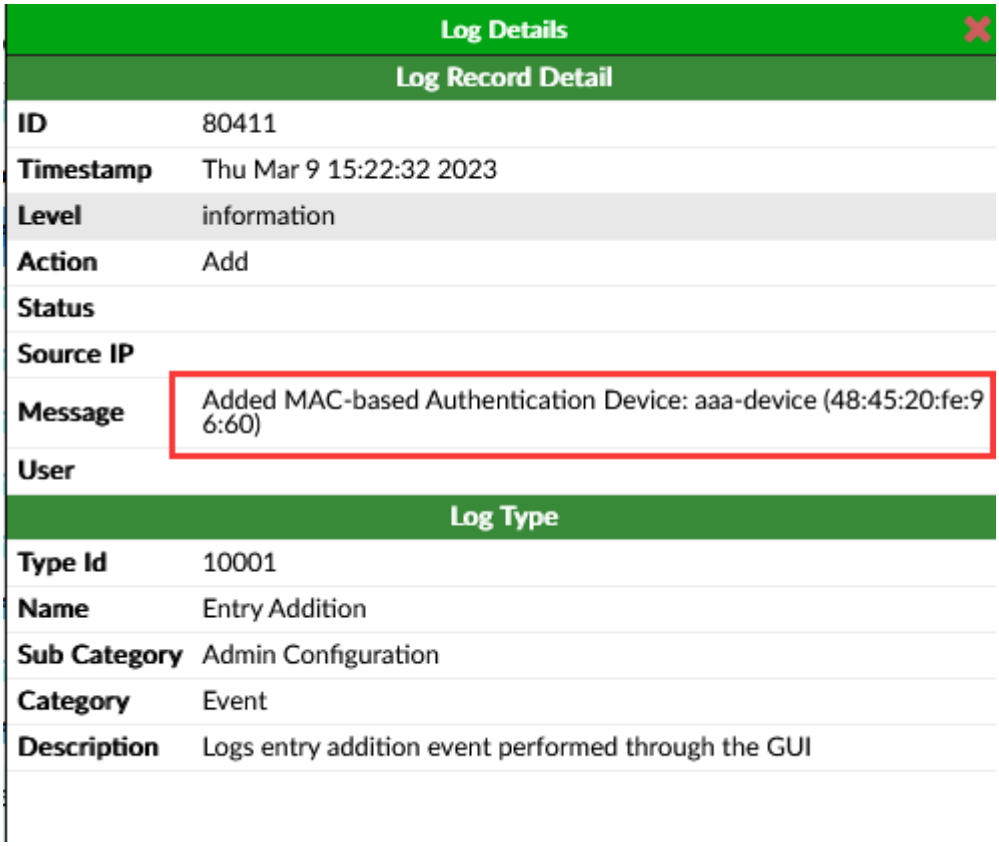
终端第一次接入网络时，会先对终端进行 MAC 地址认证，由于是新用户，mac 地址认证会失败:

Log Details	
Log Record Detail	
ID	80406
Timestamp	Thu Mar 9 15:22:00 2023
Level	information
Action	Authentication
Status	Failed
Source IP	172.22.5.51
Message	MAC-based authentication failed: unknown MAC address
User	484520fe9660
Log Type	
Type Id	20401
Name	MAC Authentication Failed No MAC address
Sub Category	Authentication
Category	Event
Description	Authentication failed, MAC address not found

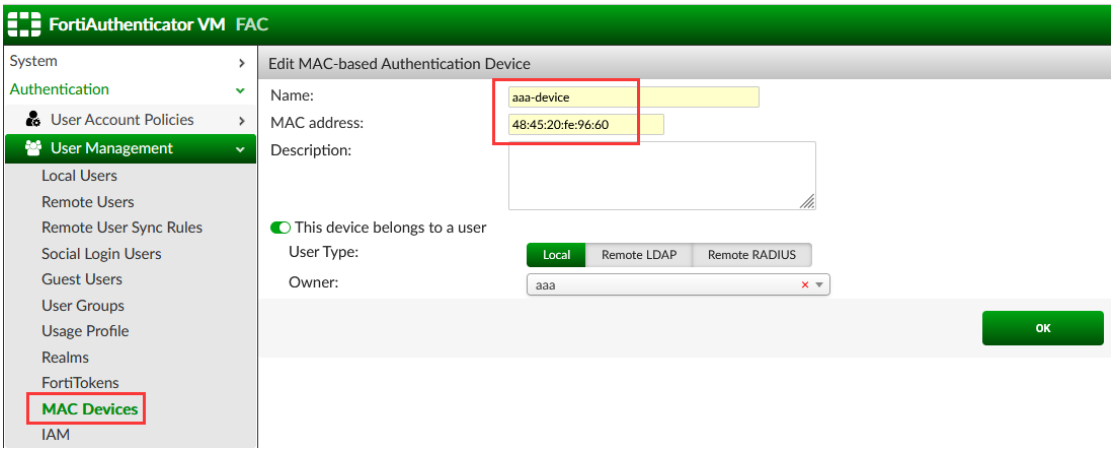
MAC 认证失败后，转 portal 认证，提示用户输入登录信息，用户输入正确登录信息，用户 portal 认证成功:

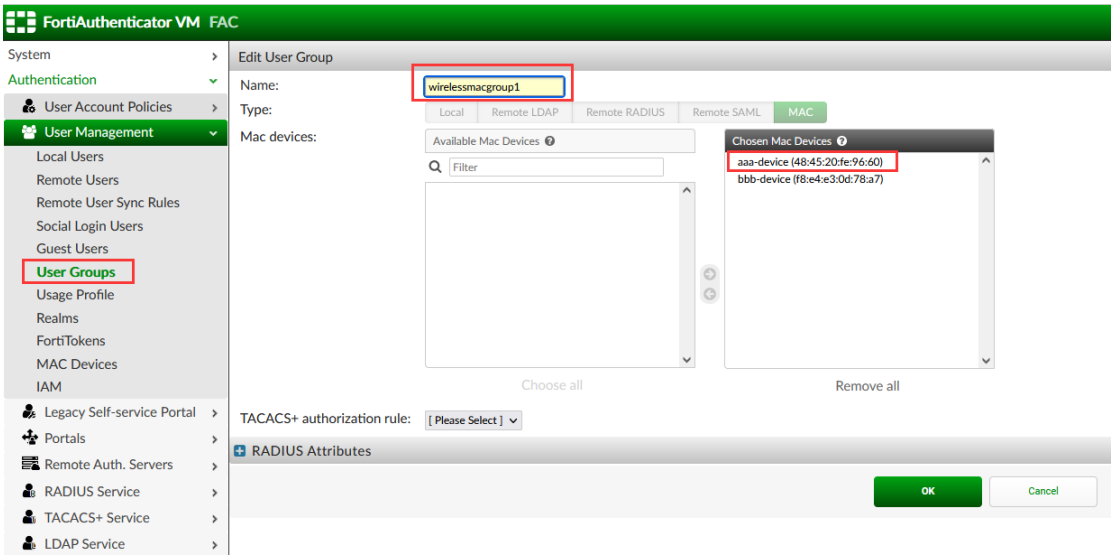
Log Details	
Log Record Detail	
ID	80410
Timestamp	Thu Mar 9 15:22:15 2023
Level	information
Action	Login
Status	Success
Source IP	172.22.5.51
Message	[aaa] has successfully logged in guest portal[wirelessmacportal]
User	aaa
Log Type	
Type Id	20604
Name	Guest Portal Authentication OK
Sub Category	Authentication
Category	Event
Description	Guest portal authentication request succeed

用户 portal 认证成功后, mac 地址被记录在 FAC 上:

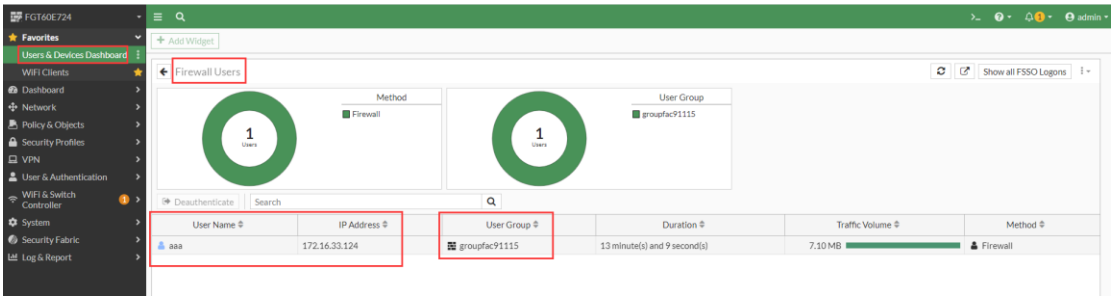


FAC 上此 MAC 地址终端被记录在 mac device 中，并自动加入到设置的 mac 地址组中:

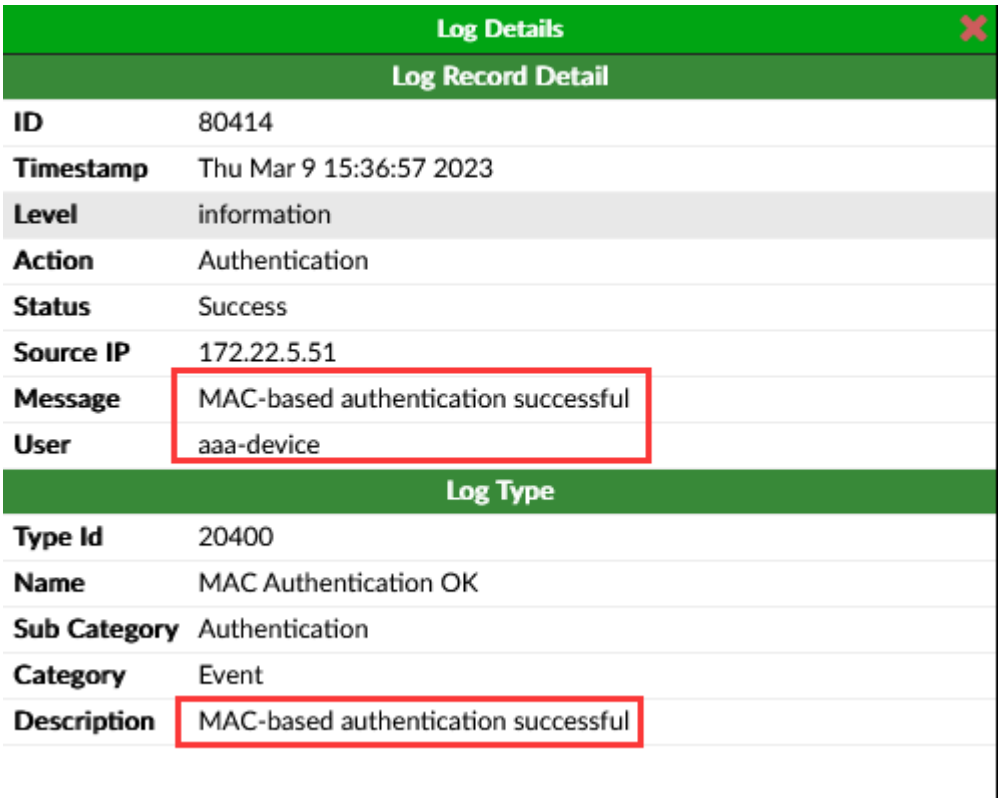




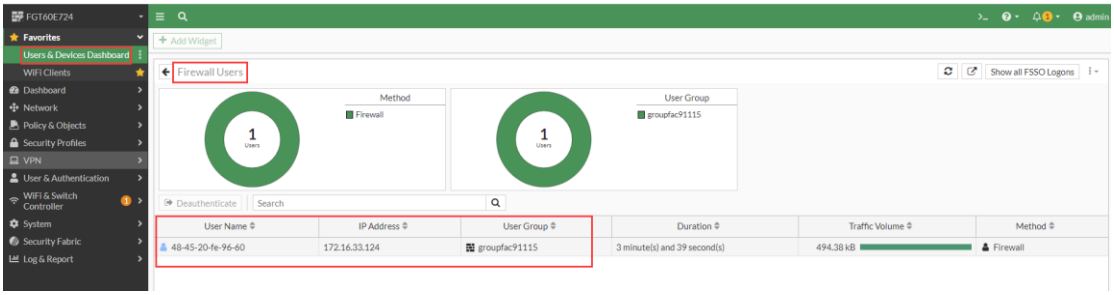
防火墙上显示用户 portal 认证成功:



用户离开，过段时间后再接入无线网络时，先触发 MAC 地址认证，由于终端 MAC 地址已经记录在 FAC 上，此时 MAC 地址认证成功，用户无感知接入无线网络:



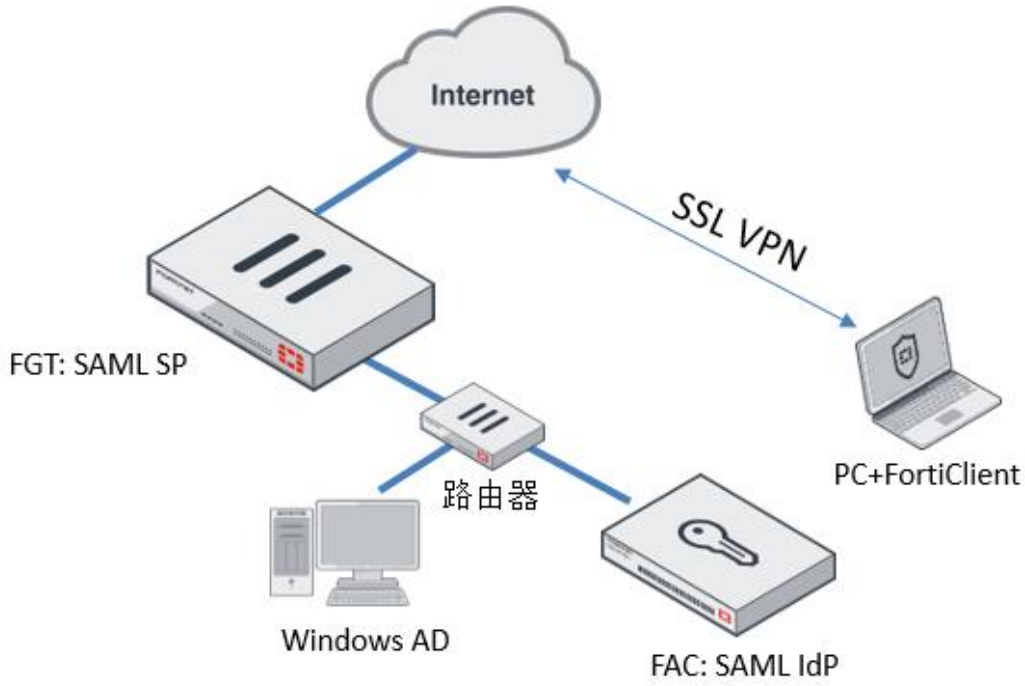
防火墙上也显示用户 mac 地址认证成功:



3. FortiClient 基于 SAML 的 VPN 认证

VPN 认证是远程办公室时常用的认证方式，有很多客户在部署时要求 VPN 是基于 SAML 的认证.

3.1 测试组网



FGT 作为 SAML SP 响应终端发起的基于 SAML 的 vpn 拨号;

FAC 作为 SAML IdP 处理 FGT 发起的 SAML 认证请求;

Windows AD 作为用户认证源与 FAC 对接;

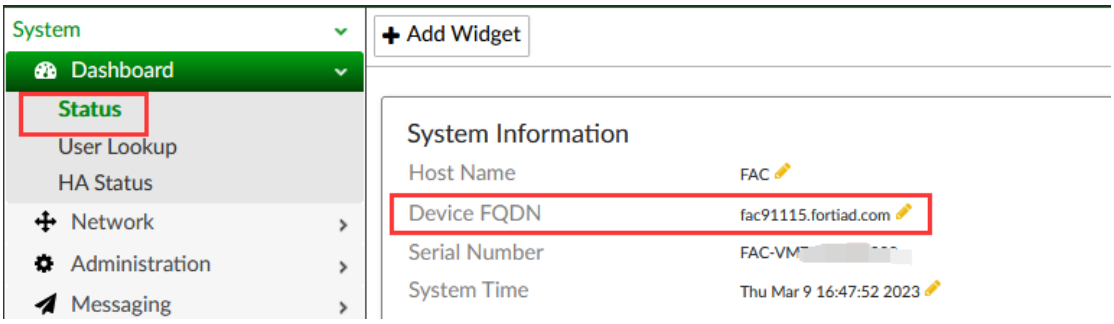
注:

- 本例中使用 FAC 签发相关证书，实际部署可能使用有公信力的证书;
- 实际部署时域名解析跟 DNS Server 侧配置有关,请根据实际部署情况来配置;

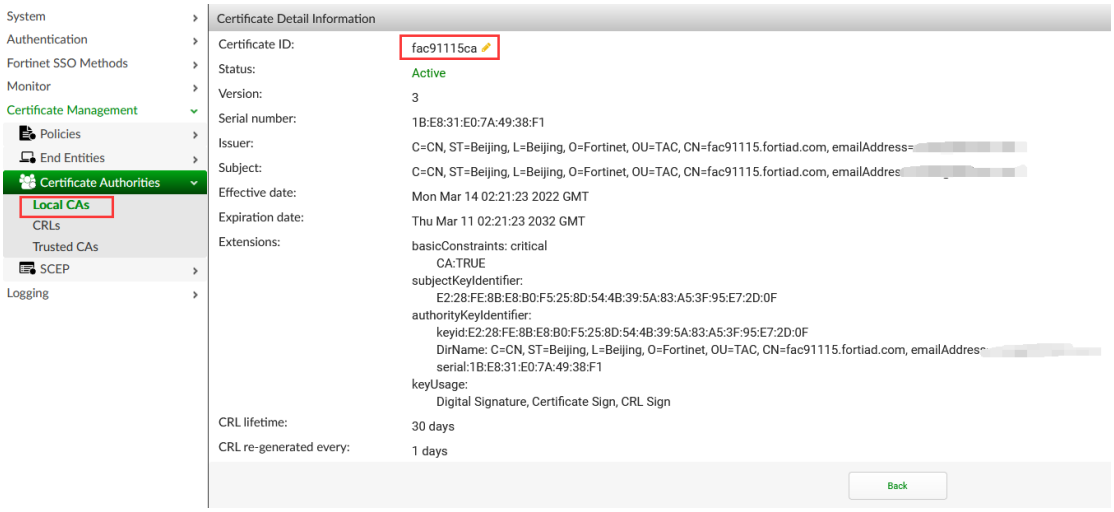
3.2 FAC 侧相关配置

3.2.1 FAC 证书相关操作

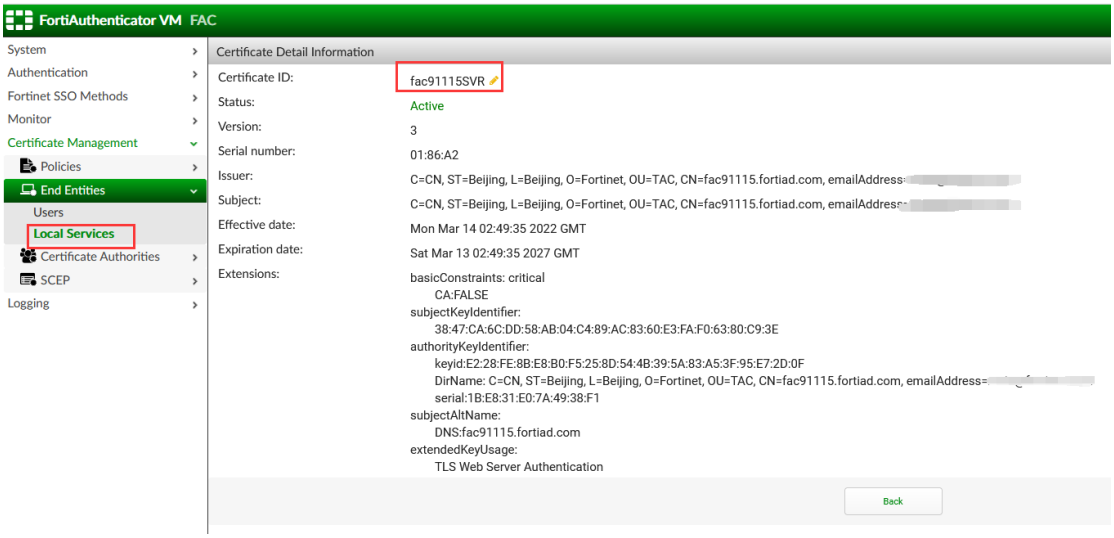
首先需要配置 FAC 的域名:



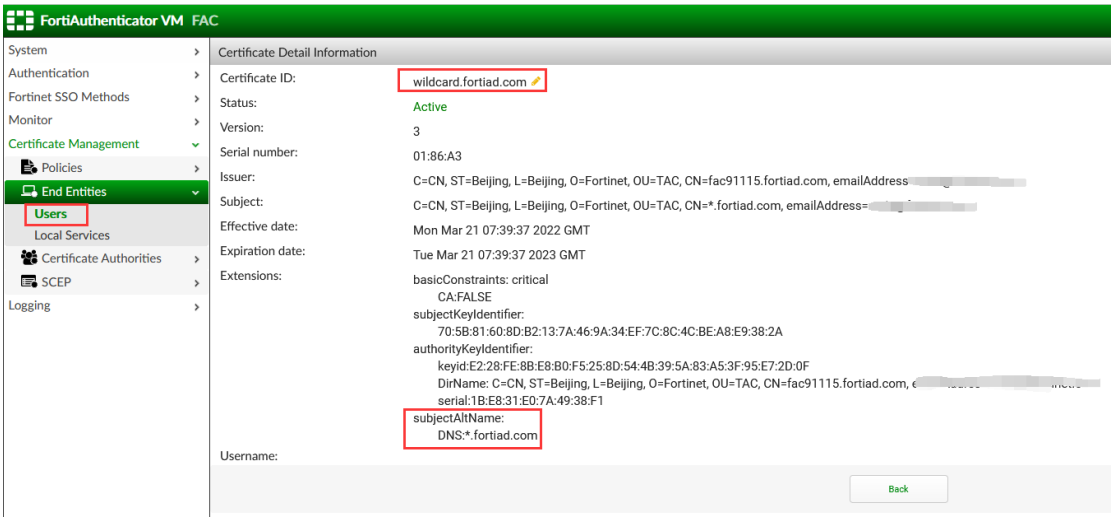
创建私有 CA 证书:



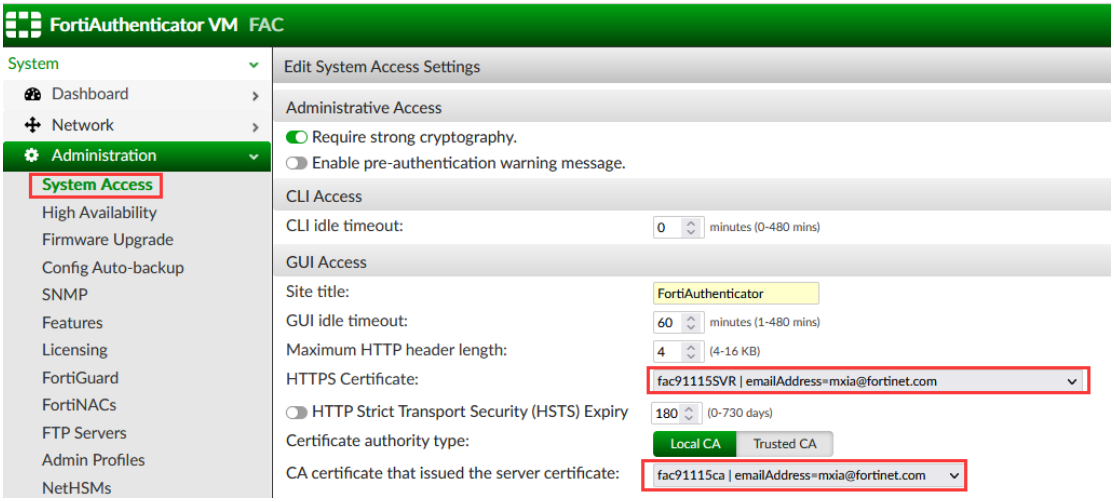
基于 CA 证书创建 Server 证书:



创建一个基于域名的通配符证书:

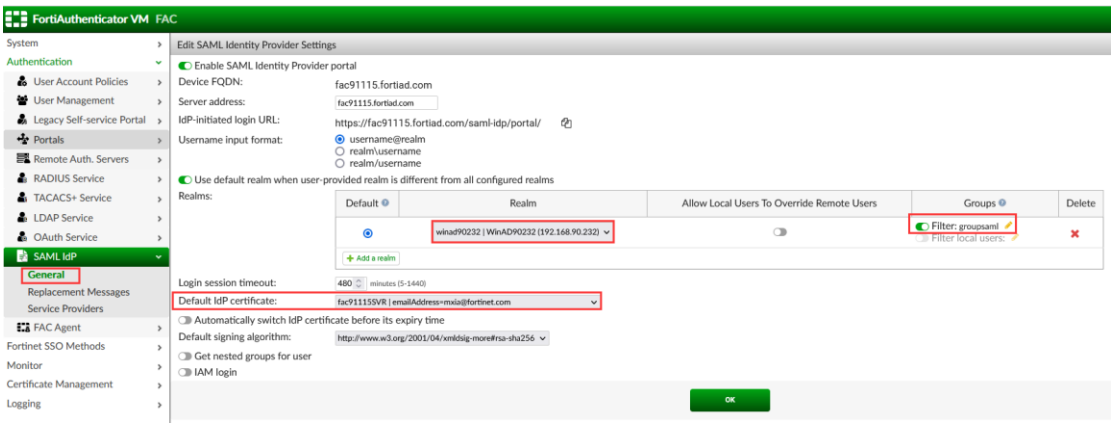


配置 FAC 的 https 访问证书，调用之前配置的证书:

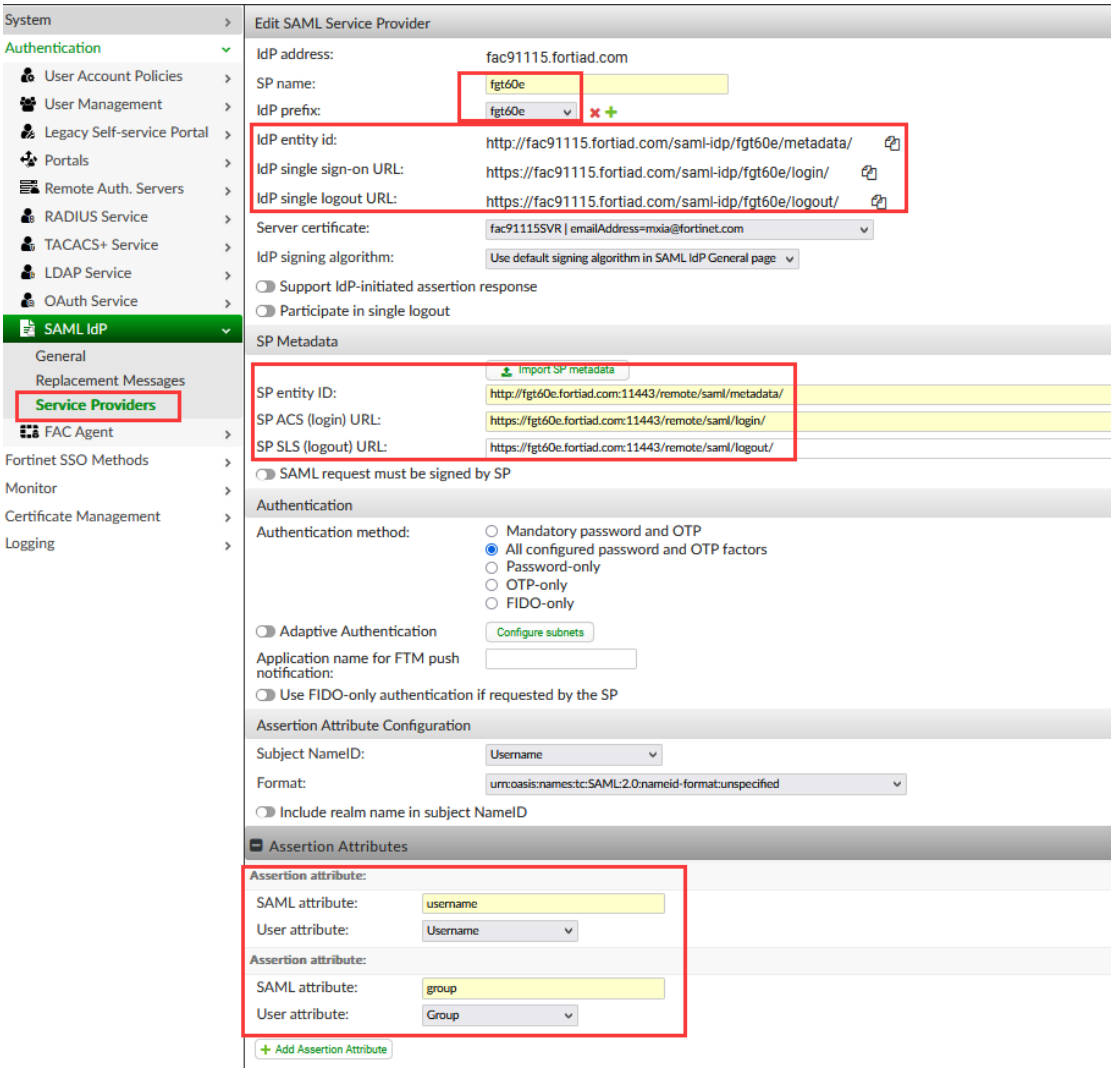


3.2.2 FAC SAML 相关配置

开启 SAML IdP 认证:



配置 SAML SP 相关信息:



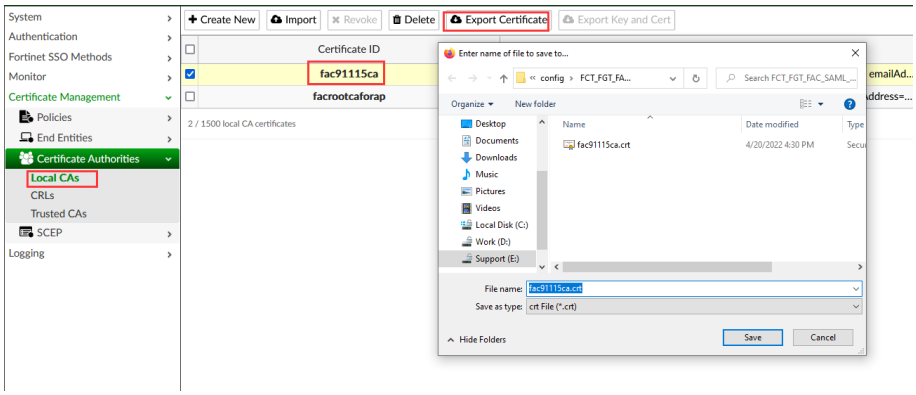
注意: FAC 的相关 SAML 配置必须与 FGT 侧的 SAML 配置一致或对应.

3.3 防火墙侧相关配置

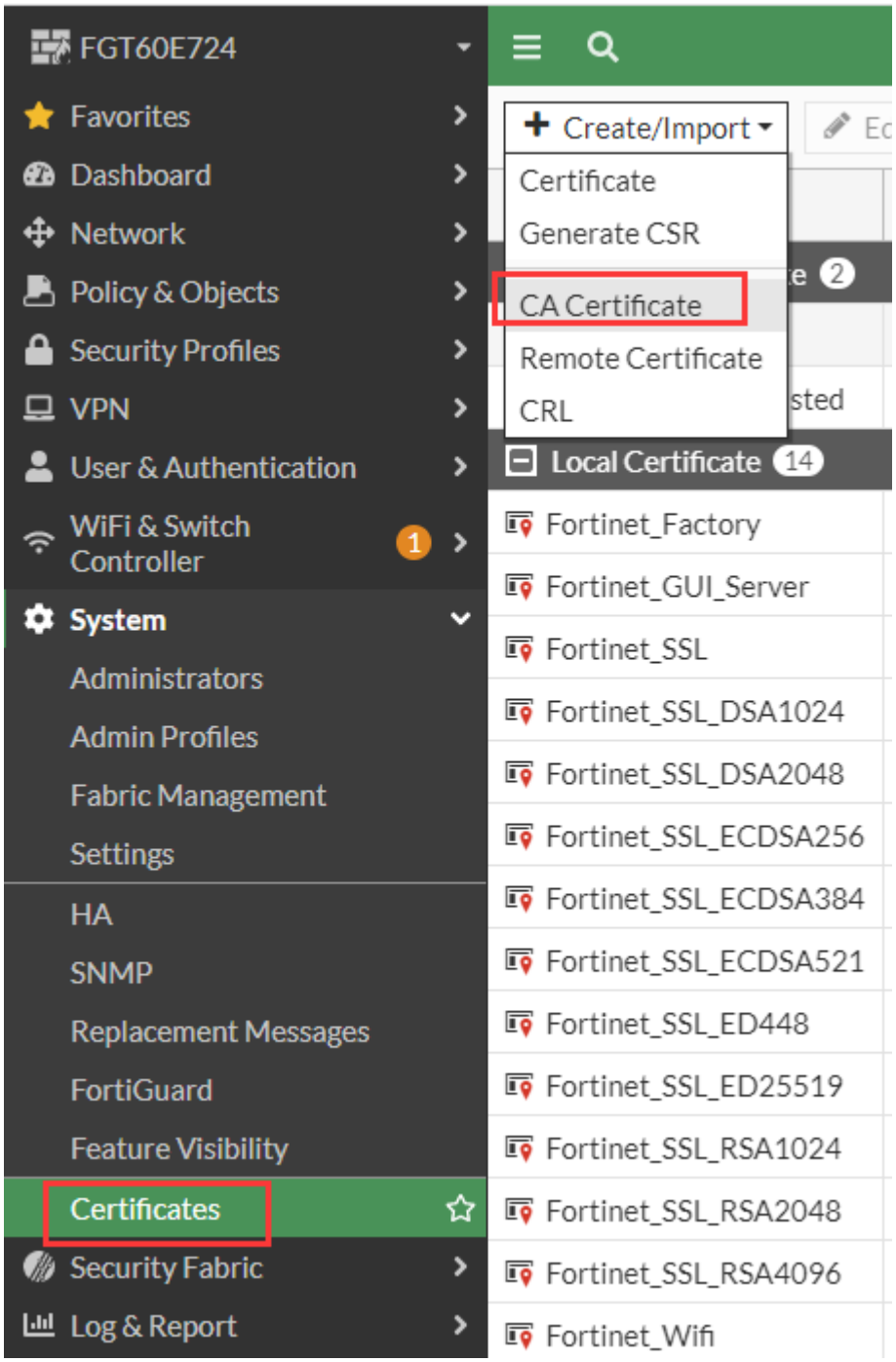
防火墙侧的配置涉及到证书和 SAML SP 以及 VPN 相关的配置:

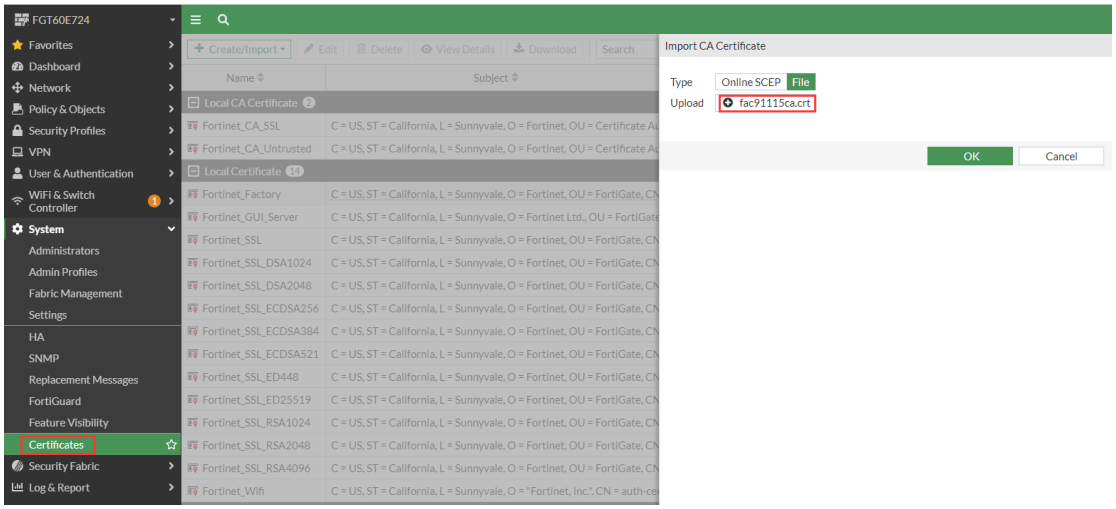
3.3.1 证书相关的配置

从 FAC 上导出私有 CA 证书:

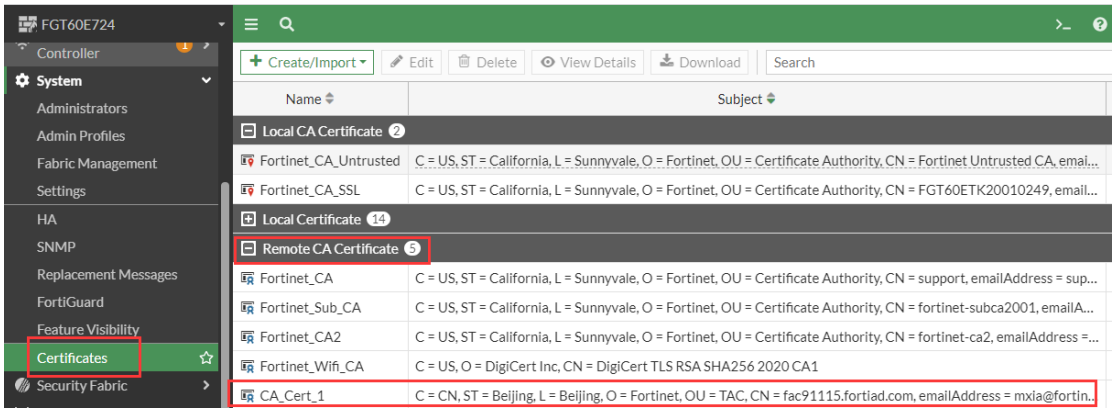


FGT 上导入此 CA 证书:

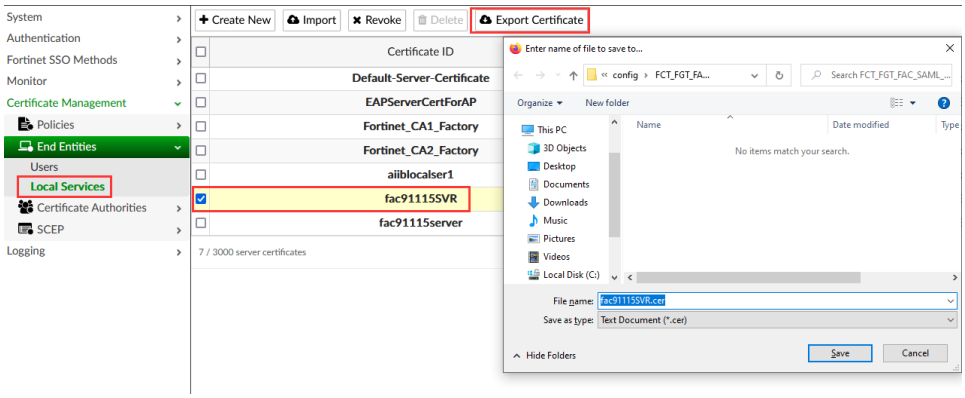

FGT60E724
Favorites
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
1
System
Administrators
Admin Profiles
Fabric Management
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Security Fabric
Log & Report
Create/Import
Certificate
Generate CSR
CA Certificate
Remote Certificate
CRL
Local Certificate 14
Fortinet_Factory
Fortinet_GUI_Server
Fortinet_SSL
Fortinet_SSL_DSA1024
Fortinet_SSL_DSA2048
Fortinet_SSL_ECDSA256
Fortinet_SSL_ECDSA384
Fortinet_SSL_ECDSA521
Fortinet_SSL_ED448
Fortinet_SSL_ED25519
Fortinet_SSL_RSA1024
Fortinet_SSL_RSA2048
Fortinet_SSL_RSA4096
Fortinet_Wifi



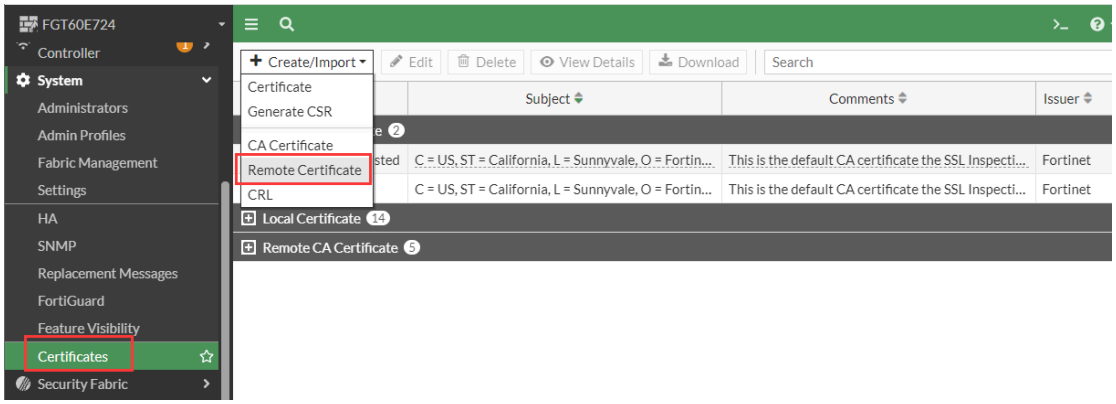
导入成功后:

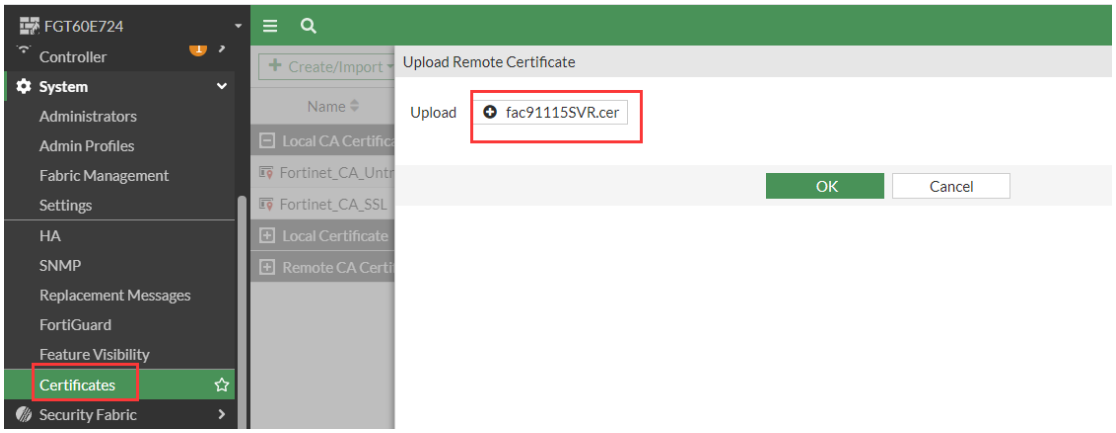


从 FAC 上导出 Server 证书:

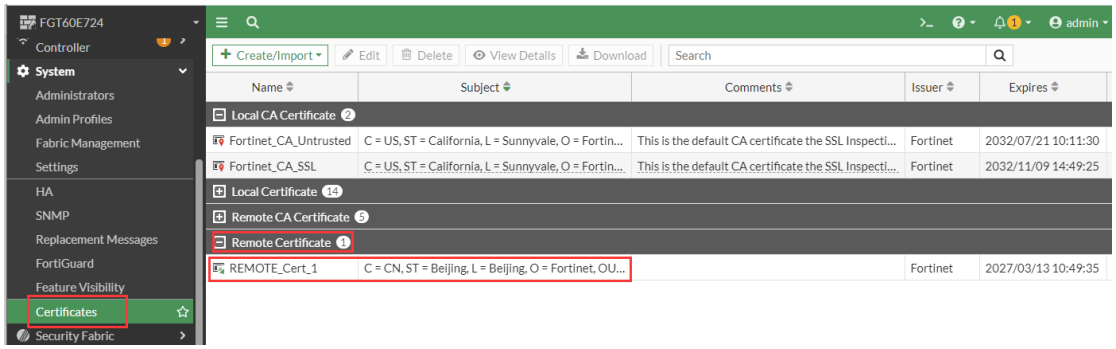


FGT 上导入此证书:

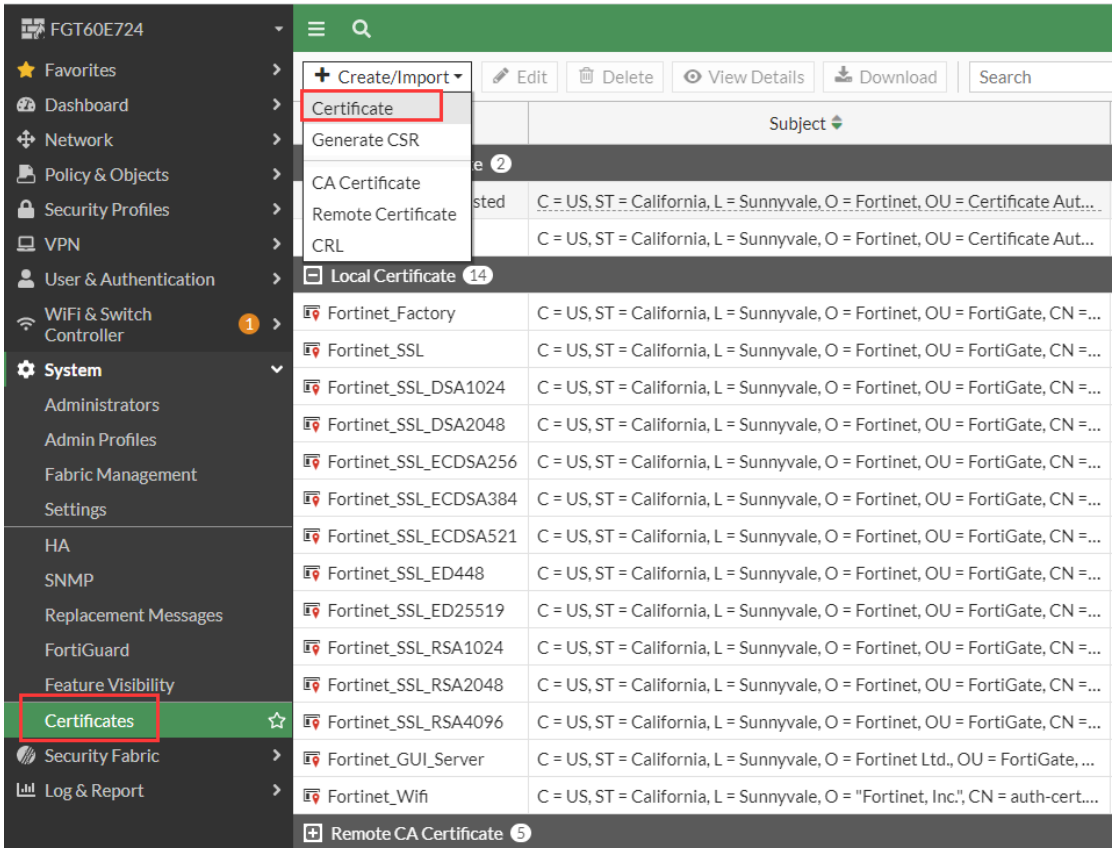


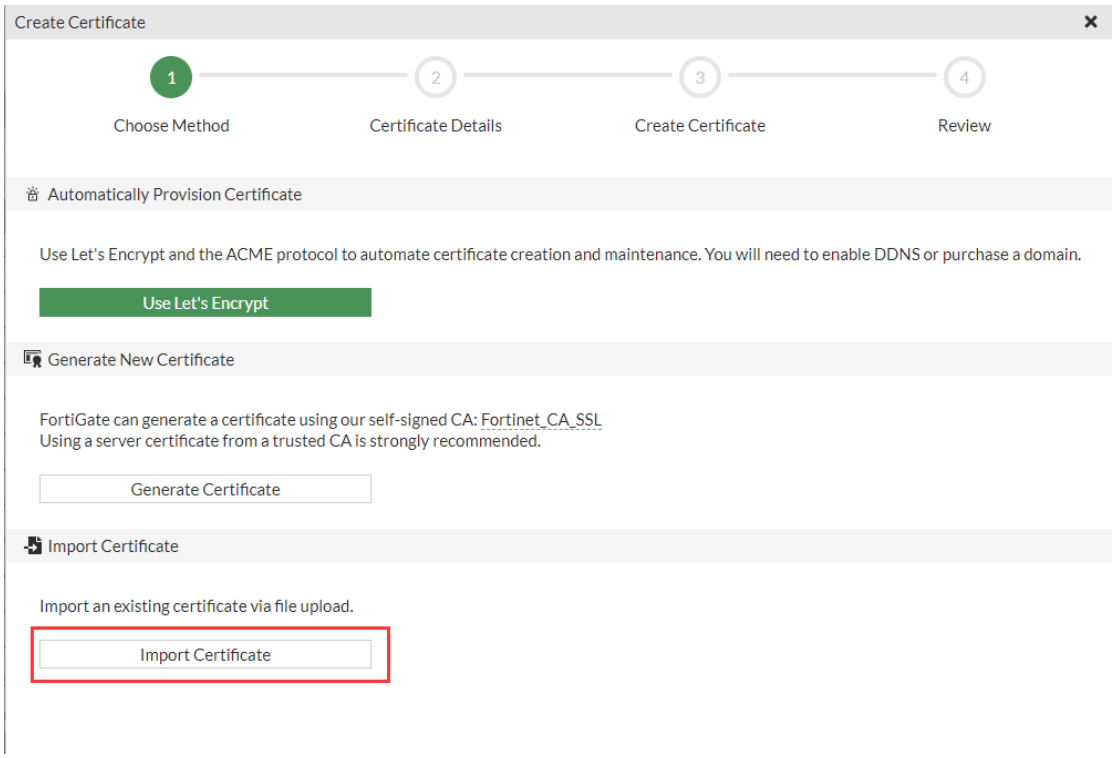


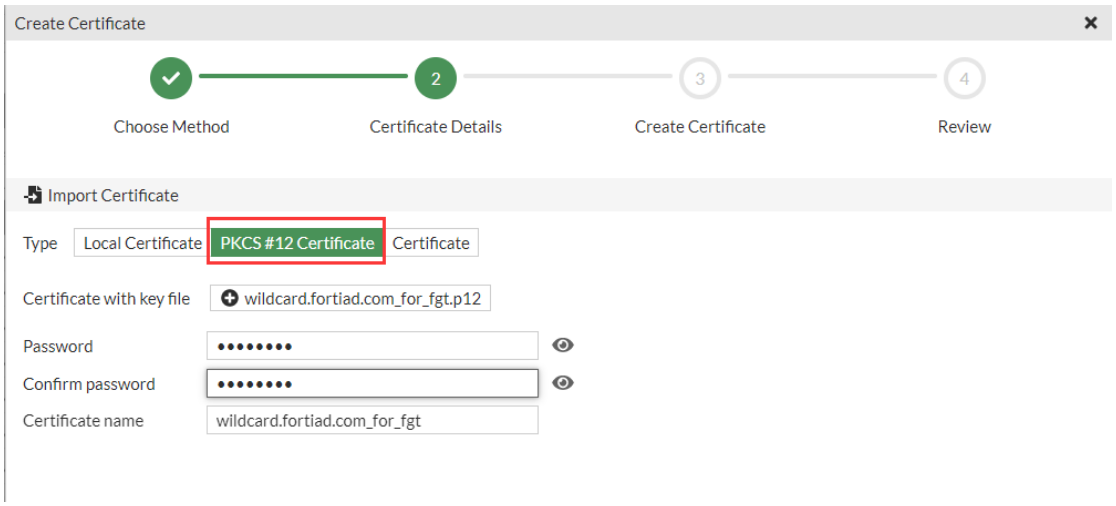
导入成功后:



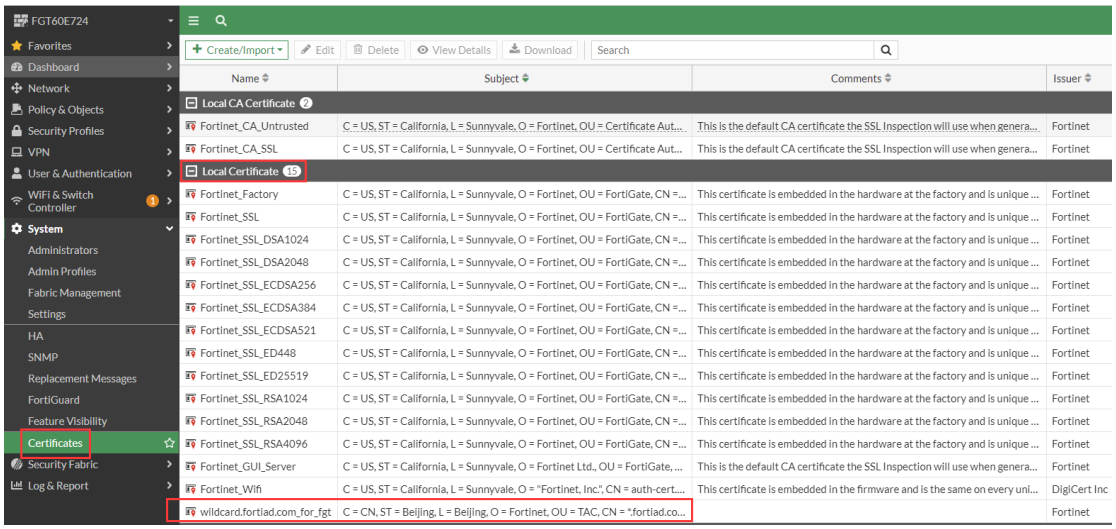
FGT 上导入域名证书:


FGT60E724
Favorites
Dashboard
Network
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi & Switch Controller
System
Administrators
Admin Profiles
Fabric Management
Settings
HA
SNMP
Replacement Messages
FortiGuard
Feature Visibility
Certificates
Security Fabric
Log & Report
Create/Import
Edit
Delete
View Details
Download
Search
Certificate
Generate CSR
CA Certificate
Remote Certificate
CRL
Subject
Local Certificate 14
Fortinet_Factory
Fortinet_SSL
Fortinet_SSL_DSA1024
Fortinet_SSL_DSA2048
Fortinet_SSL_ECDSA256
Fortinet_SSL_ECDSA384
Fortinet_SSL_ECDSA521
Fortinet_SSL_ED448
Fortinet_SSL_ED25519
Fortinet_SSL_RSA1024
Fortinet_SSL_RSA2048
Fortinet_SSL_RSA4096
Fortinet_GUI_Server
Fortinet_Wifi
Remote CA Certificate 5

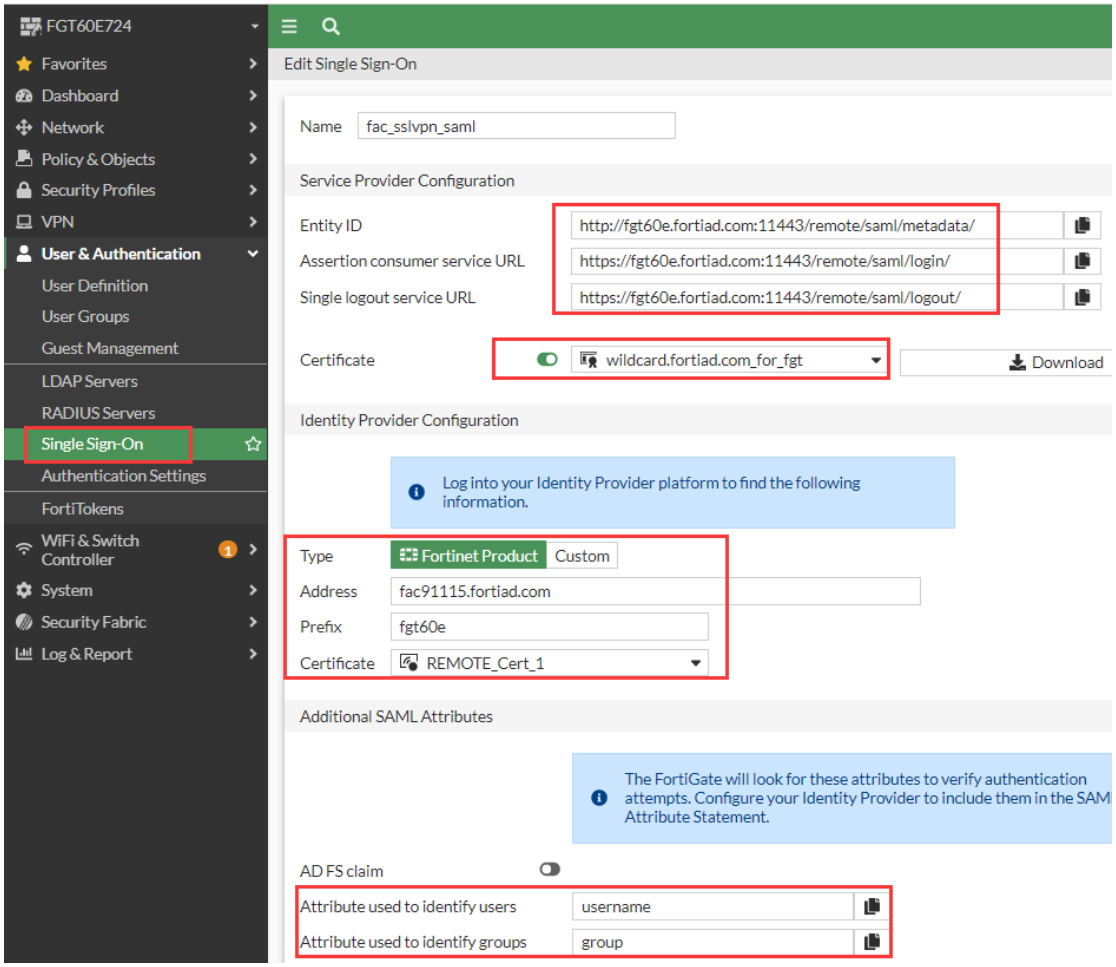

Create Certificate
Choose Method
Certificate Details
Create Certificate
Review
Automatically Provision Certificate
Use Let's Encrypt and the ACME protocol to automate certificate creation and maintenance. You will need to enable DDNS or purchase a domain.
Use Let's Encrypt
Generate New Certificate
FortiGate can generate a certificate using our self-signed CA: Fortinet_CA_SSL
Using a server certificate from a trusted CA is strongly recommended.
Generate Certificate
Import Certificate
Import an existing certificate via file upload.
Import Certificate



导入成功后:



3.3.2 防火墙 SAML 相关配置:

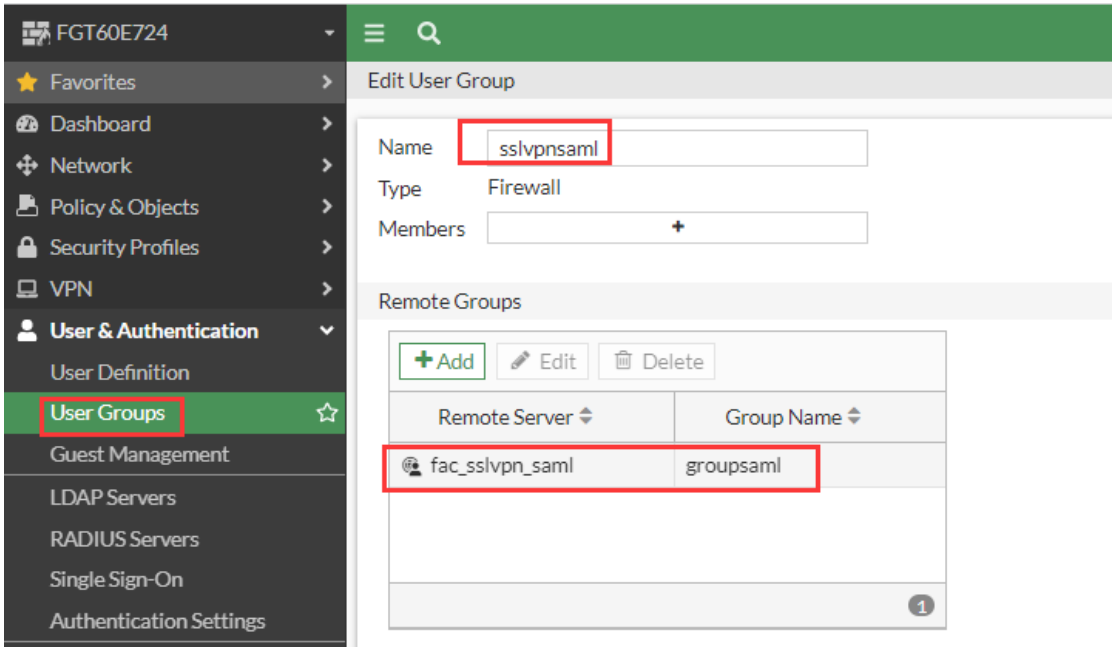


CLI 下的配置:

```
config user saml
    edit "fac_sslvpn_saml"
        set cert "wildcard.fortiad.com_for_fgt"
        set entity-id "http://fgt60e.fortiad.com:11443/remote/saml/metadata/"
        set single-sign-on-url "https://fgt60e.fortiad.com:11443/remote/saml/login/"
        set single-logout-url "https://fgt60e.fortiad.com:11443/remote/saml/logout/"
        set idp-entity-id "http://fac91115.fortiad.com/saml-idp/fgt60e/metadata/"
        set idp-single-sign-on-url "https://fac91115.fortiad.com/saml-idp/fgt60e/login/"
        set idp-single-logout-url "https://fac91115.fortiad.com/saml-idp/fgt60e/logout/"
        set idp-cert "REMOTE_Cert_1"
        set user-name "username"
        set group-name "group"
        set digest-method sha1
    next
end
```

注意: FGT 侧的 SAML 配置必须要与 FAC 侧的 SAML 配置对应一致.

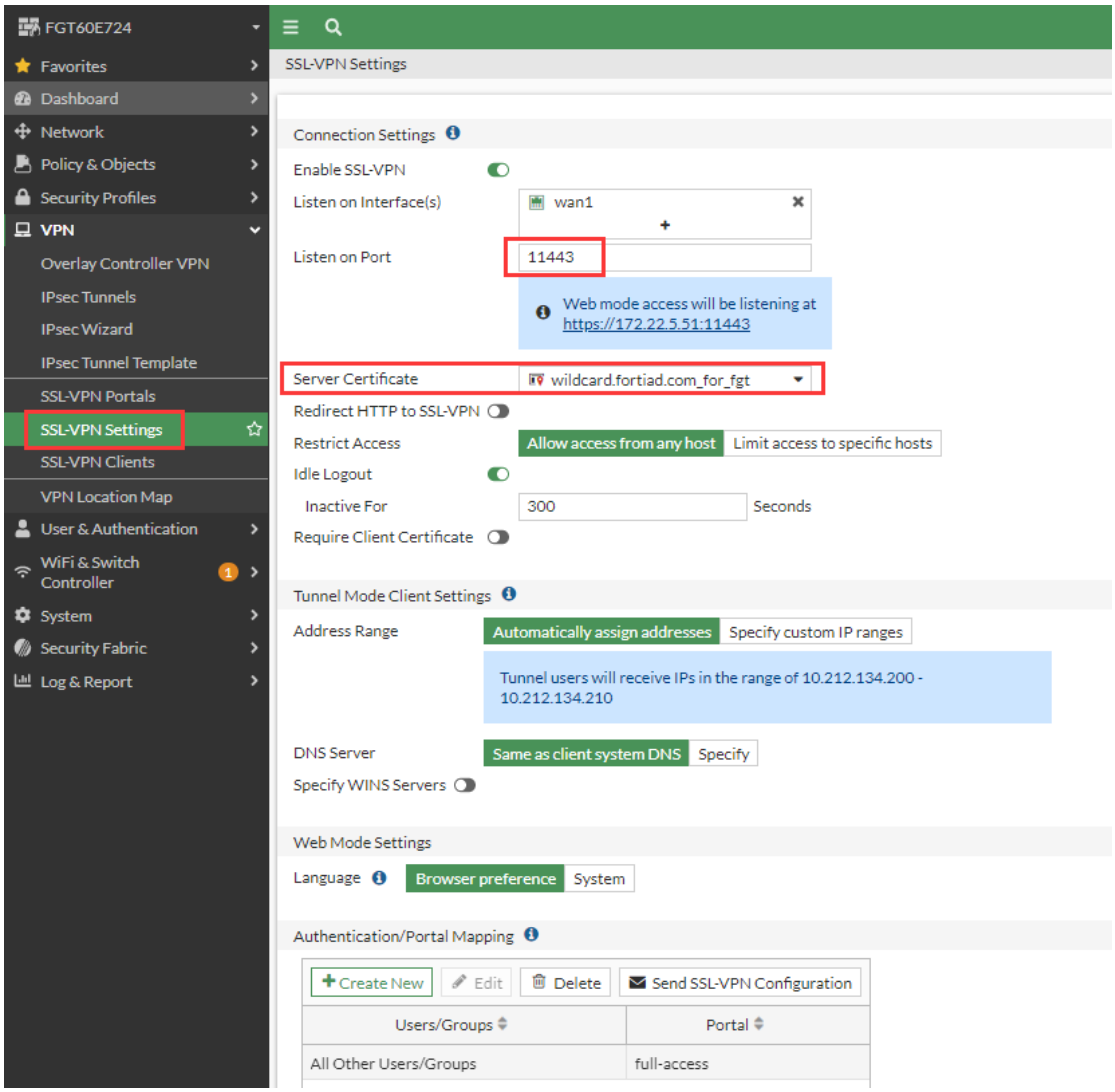
SAML 用户认证组:



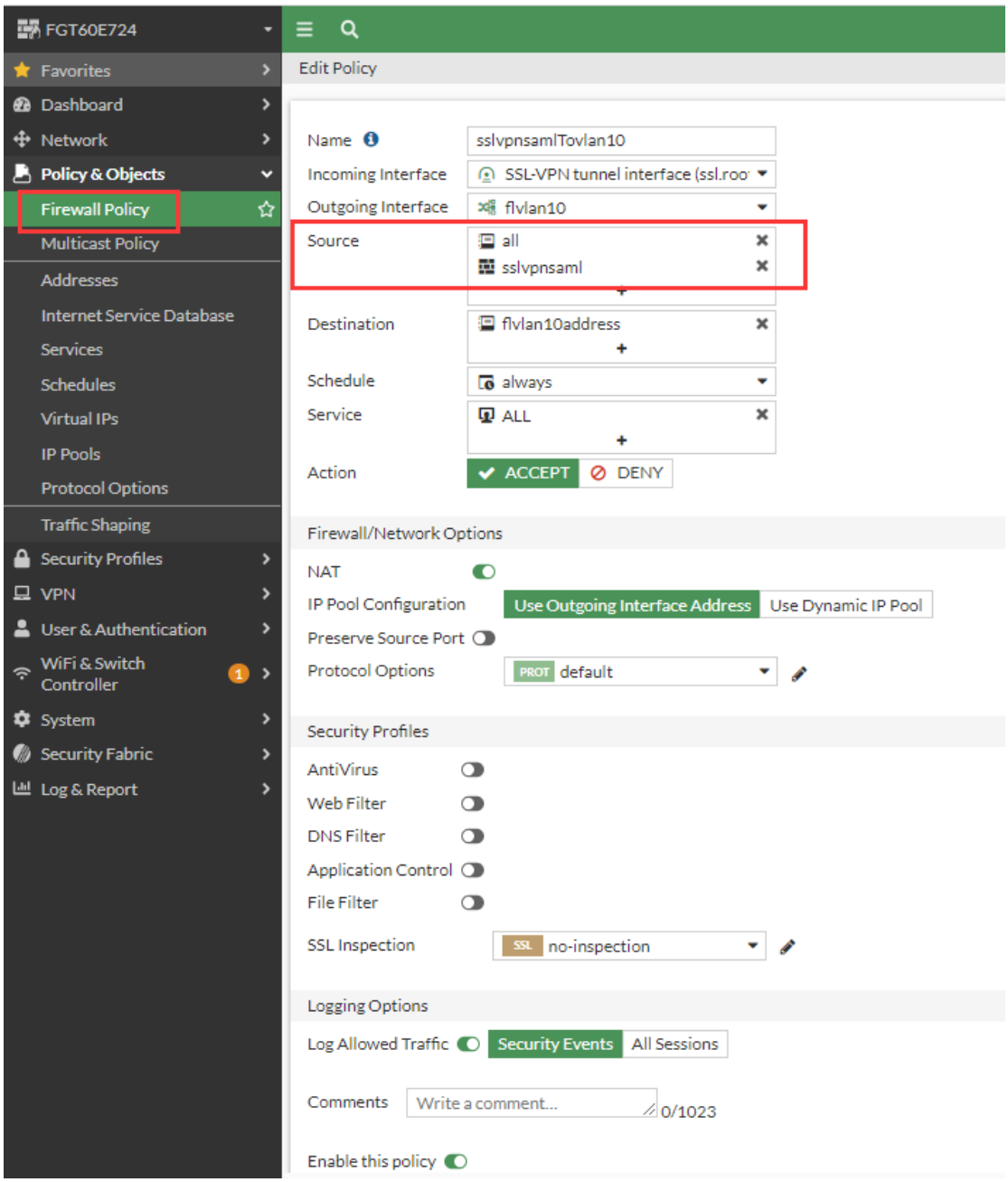
CLI 配置:

```
config user group
    edit "sslvpnsaml"
        set member "fac_sslvpn_saml"
        config match
            edit 1
                set server-name "fac_sslvpn_saml"
                set group-name "groupsaml"
            next
        end
    next
end
```

3.3.3 VPN 相关配置


FGT60E724
Favorites
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
WiFi & Switch Controller
System
Security Fabric
Log & Report
SSL-VPN Settings
Connection Settings
Enable SSL-VPN
Listen on Interface(s)
wan1
Listen on Port
11443
Web mode access will be listening at https://172.22.5.51:11443
Server Certificate
wildcard.fortiad.com_for_fgt
Redirect HTTP to SSL-VPN
Restrict Access
Allow access from any host
Limit access to specific hosts
Idle Logout
Inactive For
300
Seconds
Require Client Certificate
Tunnel Mode Client Settings
Address Range
Automatically assign addresses
Specify custom IP ranges
Tunnel users will receive IPs in the range of 10.212.134.200 - 10.212.134.210
DNS Server
Same as client system DNS
Specify
Specify WINS Servers
Web Mode Settings
Language
Browser preference
System
Authentication/Portal Mapping
Create New
Edit
Delete
Send SSL-VPN Configuration
Users/Groups
Portal
All Other Users/Groups
full-access

VPN 访问策略:

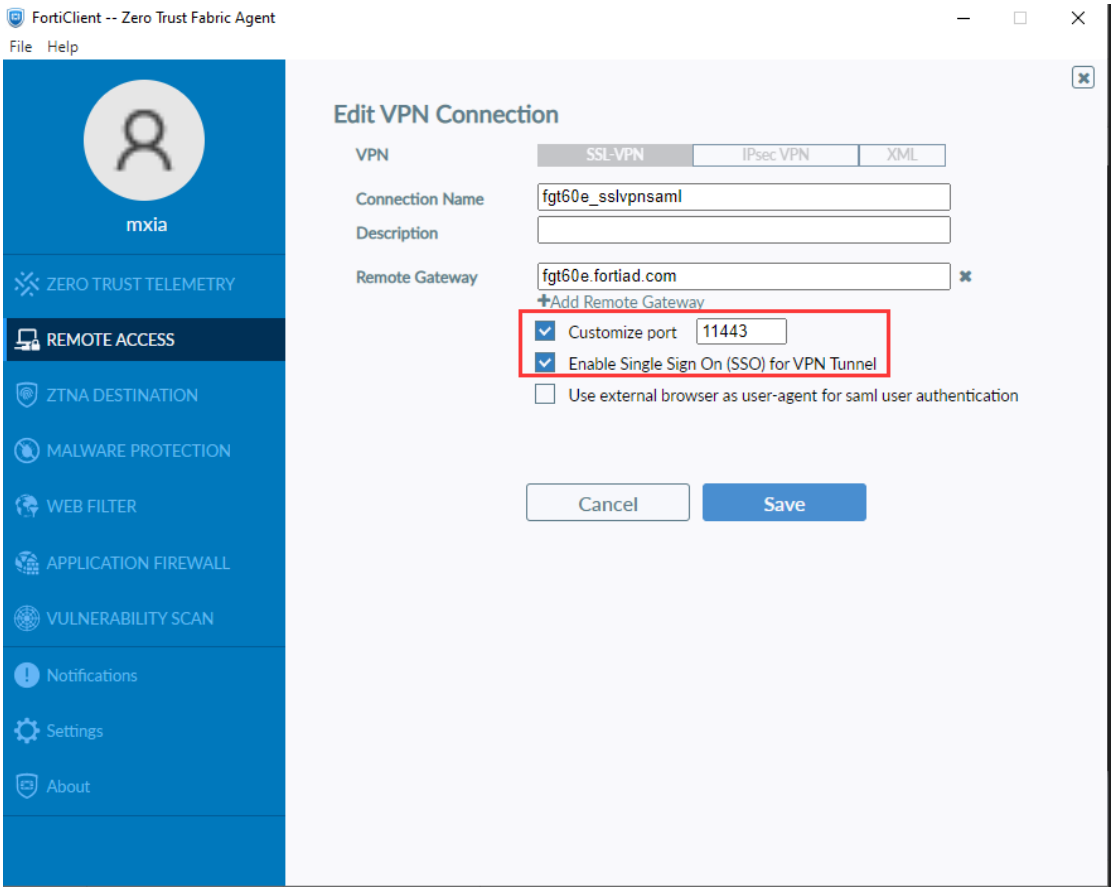


加大 VPN 认证的超时时间:

```
config system global
    set admin-server-cert "wildcard.fortiad.com_for_fgt"
    set admintimeout 360
    set alias "FortiGate-60E"
    set gui-certificates enable
    set hostname "FGT60E724"
    set management-port-use-admin-sport disable
    set remoteauthtimeout 120
    set switch-controller enable
    set timezone 55
end
```

3.4 PC 侧相关配置

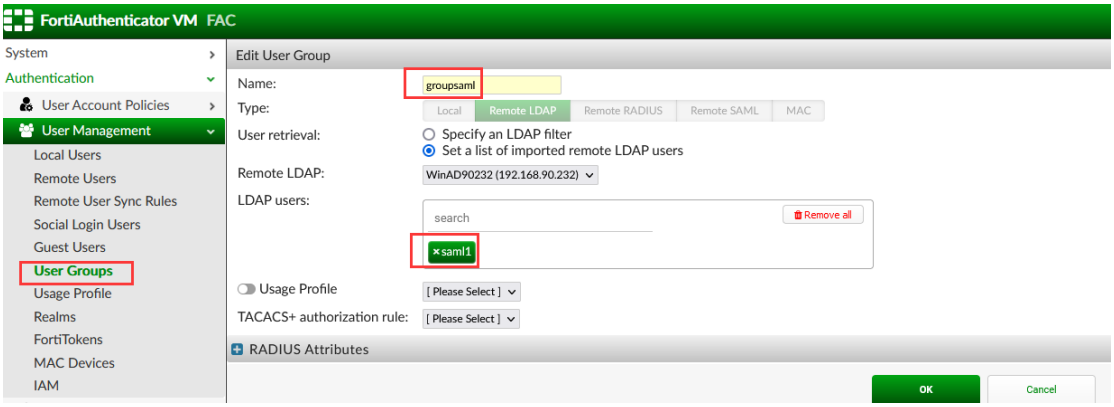
下面是 Forticlient 的配置，需要开启 SAML 认证:



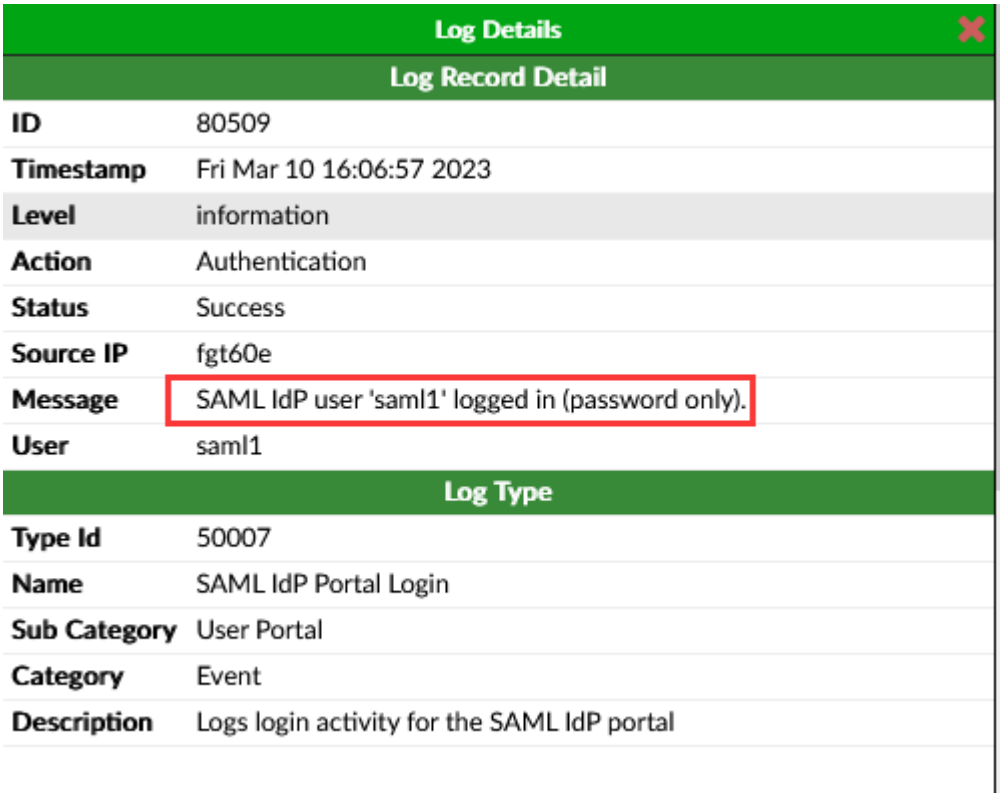
另外需要注意: 如果不是使用的公有 CA 证书，则终端侧需要安装 CA 证书.

3.5 相关测试日志

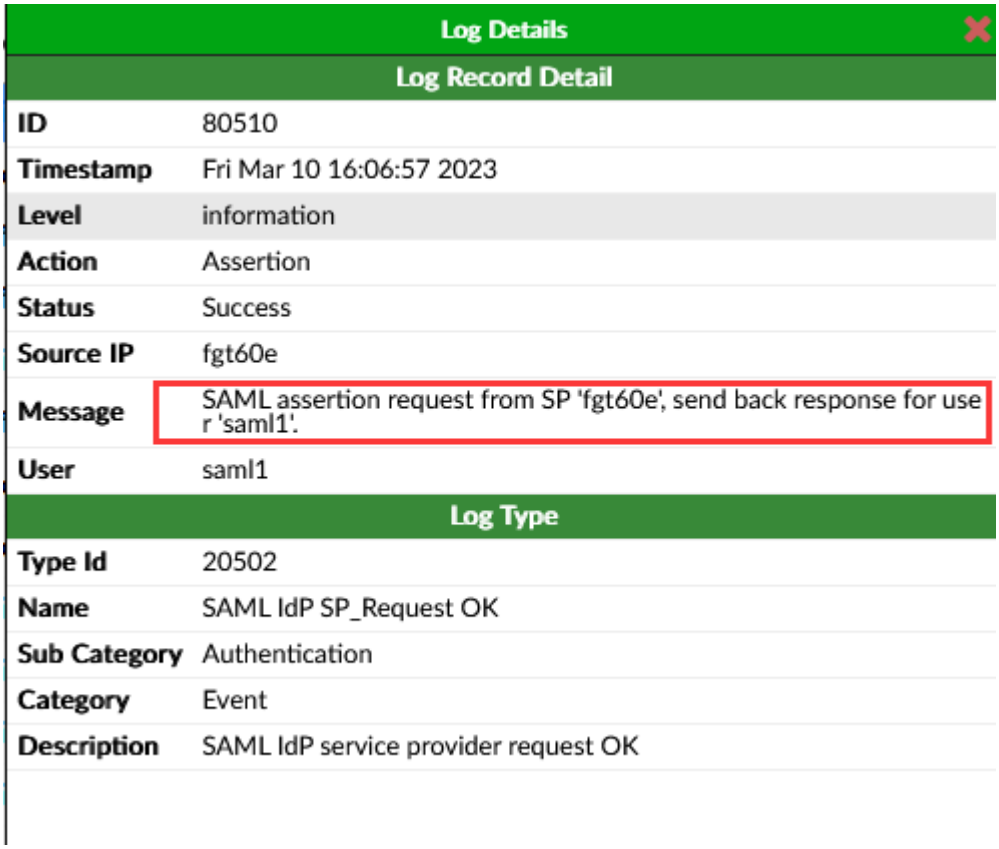
测试时，使用用户 saml1 进行测试，此用户属于 group: groupsaml.



用户认证输入正确的用户名和密码后，FAC 上显示用户 saml 认证成功.

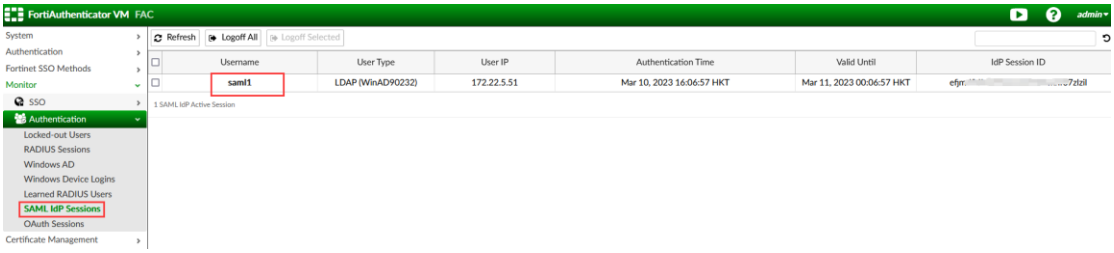


FAC 返回认证成功的断言给 FGT:



Log Details	
Log Record Detail	
ID	80510
Timestamp	Fri Mar 10 16:06:57 2023
Level	information
Action	Assertion
Status	Success
Source IP	fgt60e
Message	SAML assertion request from SP 'fgt60e', send back response for user 'saml1'.
User	saml1
Log Type	
Type Id	20502
Name	SAML IdP SP_Request OK
Sub Category	Authentication
Category	Event
Description	SAML IdP service provider request OK

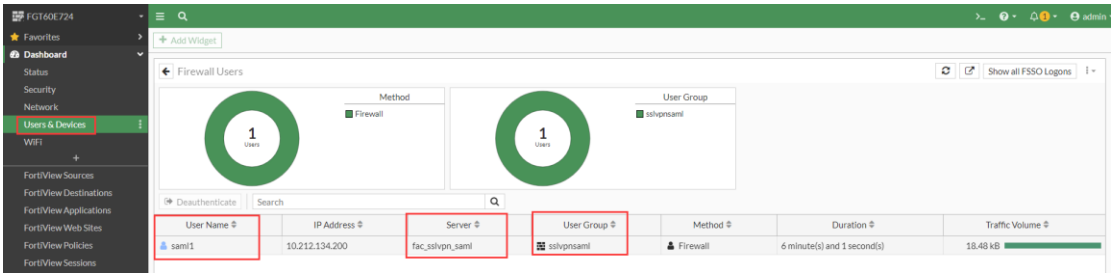
FAC 上添加了此用户的 SAML 认证 IdP Session:



下面是 FGT 上 SAML 的 debug 日志，可以看到在 FAC 返回给 FGT 的断言中包含了用户的 username 和 group 信息:

```
</Session>
samld_send_common_reply [122]:     Attr: 17, 27, magic=453e1fdaa20f91fa
samld_send_common_reply [122]:     Attr: 18, 25, 2023-03-10T08:31:34z
samld_send_common_reply [118]:     Attr: 10, 19, 'username' 'saml1'
samld_send_common_reply [118]:     Attr: 10, 20, 'group' 'groupsaml'
samld_send_common_reply [122]:     Attr: 11, 1069, https://fac91115.fortiad.com/saml-idp/fgt60e/logout/?SAMLRequest=lZJRb4IwFIXf9ytI37UtKNNGSVQkIVHn1Pjgy
1khaCNtkRbnzx%2BFLXF7MNljz73nu%2BfedKSpyAuyUCdVmQ27Vkwb5y5yqUlTGYOqlERRzTWRVDBNTEK2k%2BWCuF1EilIzlagcPFieO6jWrDRcSeDE4Rh89EN%2FigZoGPrzAfYnPTQPw8gdzgaeO5
tGvQg4elbqun8Mantt0rpisdSGSlNLyPU6yOtgtEMDgn3iDQ%2FACesduK5mcZ2NKTSBMKPJEGPc72aqnk%2FTbqIEtHk7PC1gdj1%2BYjBvzgBBMLIV0gwrA4uwhKbn0U8w7vU8WDKhDGtgUDBDU2ooH
MFHRMtb1eeIQydSpaDm%2BZ2swtNO1rSSSuqCJTzjLAX0dmO57xXNrVC2K%2F47HwjsG3%2FHbJO1MQuyZdqePJYpuwevn%2B2wPq55vGQ3l1Xx474vLnux3URC3%2FqbI18dr7u3y1relLi1%2FQG8%2
FKi%2FPInwBQ%3D%3D&RelayState=magic%3D453e1fdaa20f91fa&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09%2Fxmldsig%23rsa-sha1&Signature=KfjTcY037ZTs0Z0qirNlhf1D
p3p5%2BBLr1SgTsiZYHVkGcntUk96tIvT4M1SmaiuXehlwi1He5M75MVTNm%2FqOeB%2FORopBFTKNjDBICwJnD6d8PBQcrt%2BnritwblEmVPrehP59j1pMRPth6c8nqOGmB%2Fley2ZYMQP%2FO4zWz
X5AiDZ%2FiVlLZfdEKZdWOCEcnGrtItq7hAj2uUvc03Xtejze9k2%2BXQ2Is4iO4YKjE49aKfDtiL45TvqT%2FmE8NiV9PPdpZf43WGdLN7y8RRAkRDGPlrCYvJmE8ocNwiGEryZBl6btHKZ5fetlI%2F
RtpL%2BdLMZd%2Bzj%2BdrF2kD2R5MUvYRSOCQ%3D%3D
```

FGT 上也显示了用户 SAML 认证成功的记录:



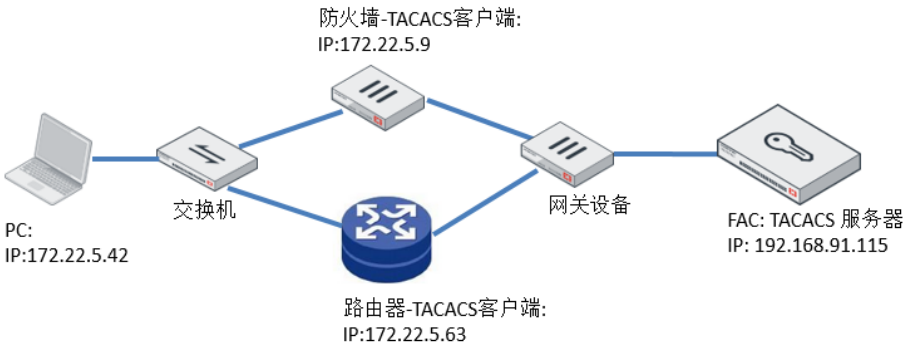
4. TACACS+ 认证

TACACS+ 认证通常用于网络设备的登录管理，本例中 FAC 通过 TACACS+来对防火墙和第三方路由器进行登录管理.

4.1 测试组网

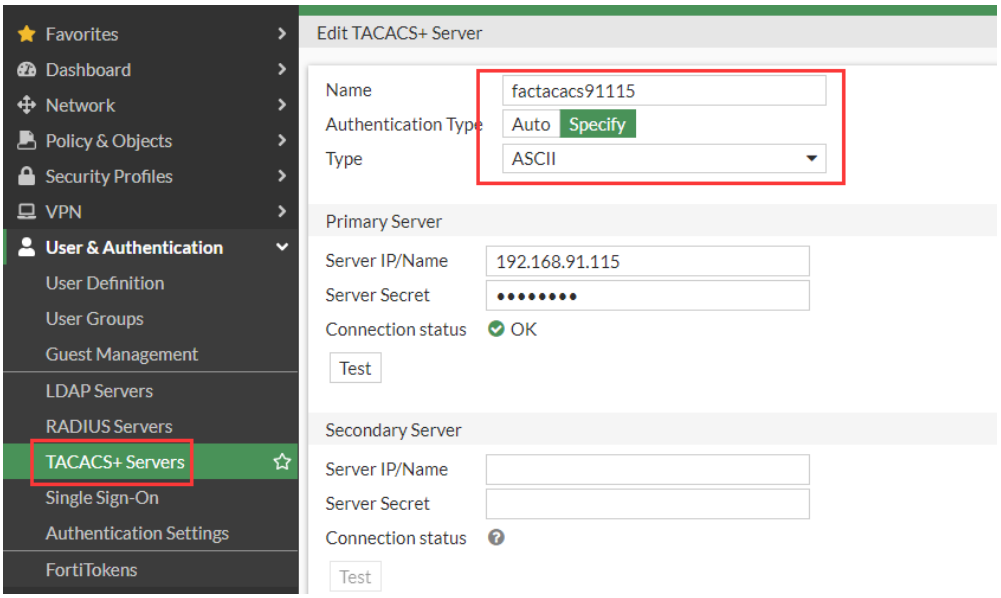
拓扑:

- PC 使用帐号 tactest1 登录防火墙 172.22.5.9 的 GUI 页面，获取从 FAC 返回的只读 admin profile;
- PC 使用帐号 tactest3 通过 SSH 登录路由器 172.22.5.63，登录后，只能在路由器的命令下执行 FAC 上设置的允许执行的 CLI 命令，执行其它 CLI 命令会报错.



4.2 防火墙侧相关配置

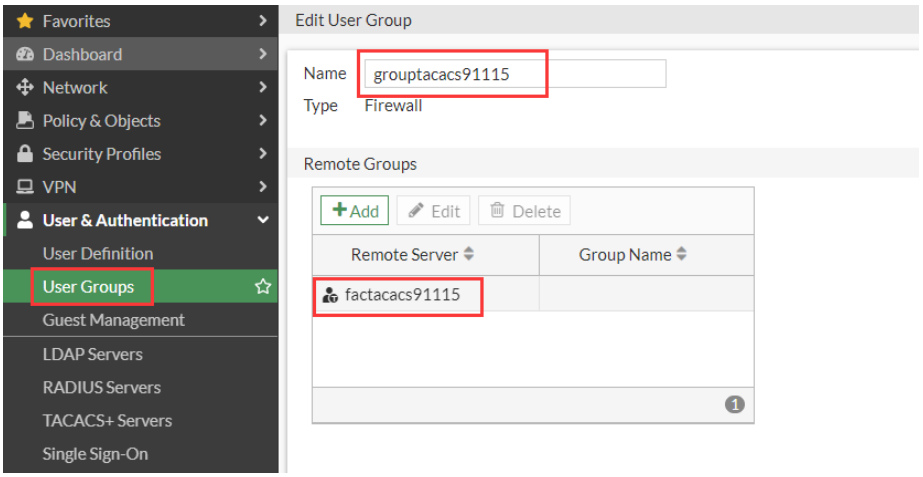
TAACACS 服务器配置:



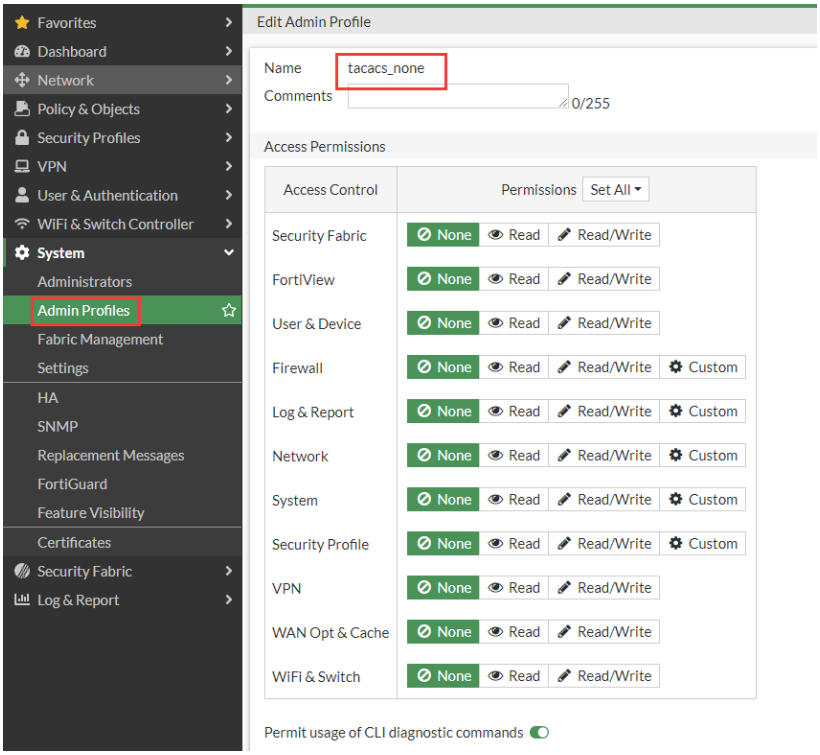
CLI 配置:

```
FWF61E723-1 # show user tacacs+
config user tacacs+
    edit "factacacs91115"
        set server "192.168.91.115"
        set key ENC XXX
        set authen-type ascii
        set authorization enable
    next
end
```

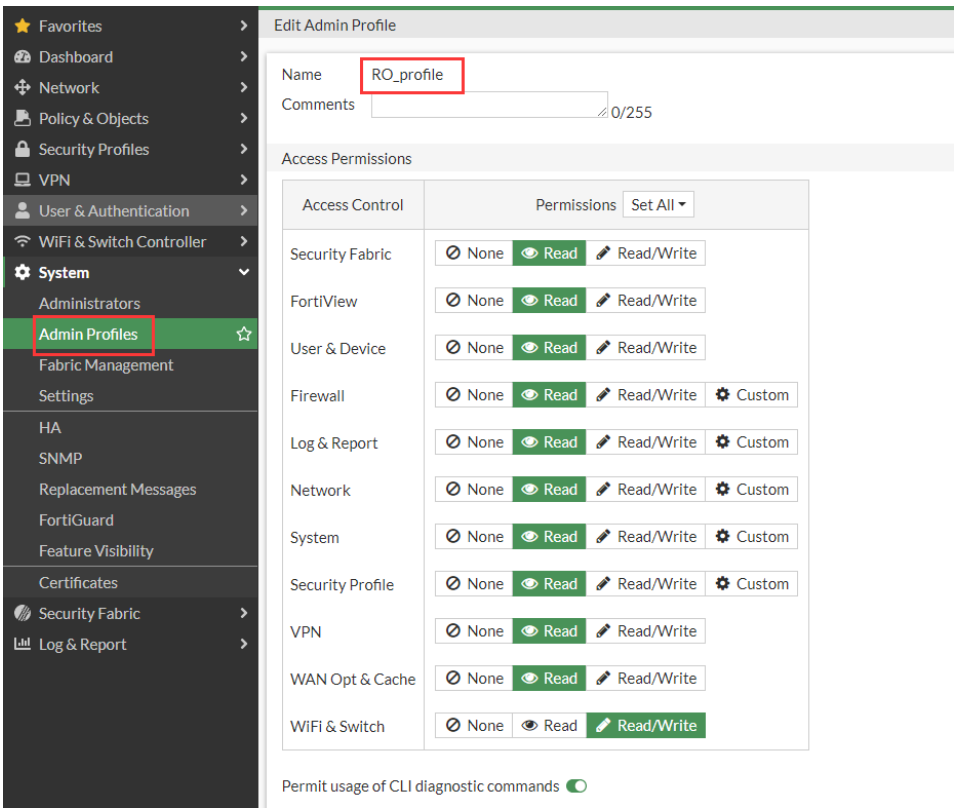
配置 TACACS group:



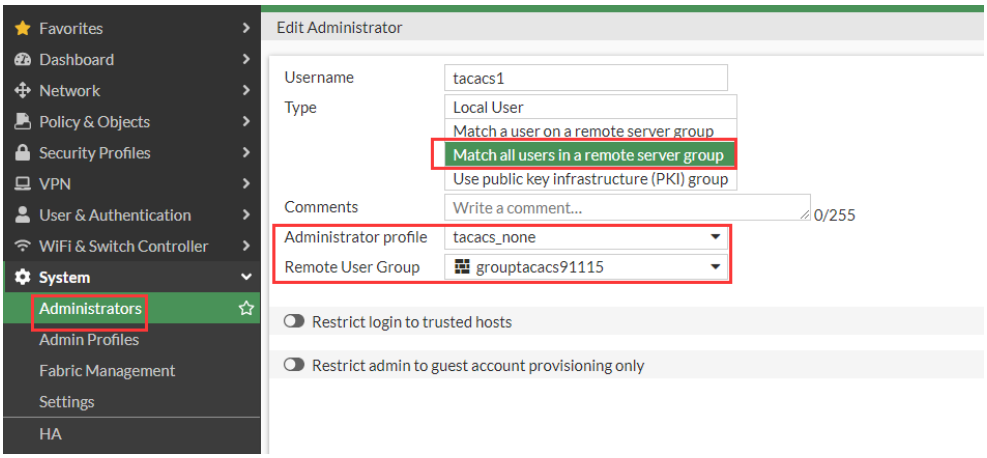
配置一个空的 admin profile:



再配置一个只读的 admin profile，这个是 TACACS 返回的 profile:



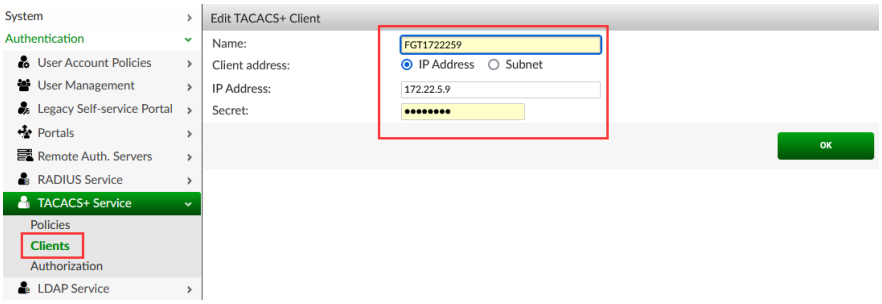
最后配置用户 TACACS 登录:



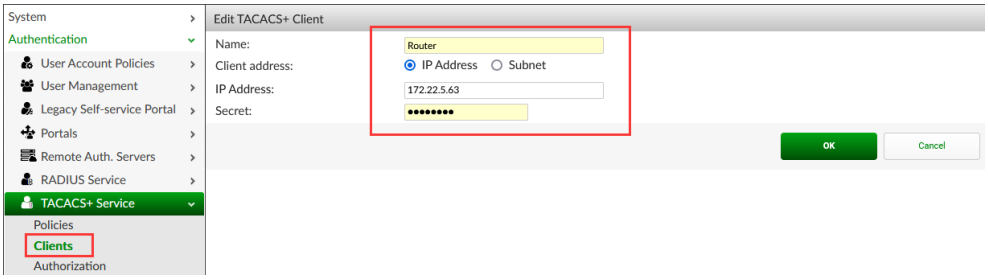
4.3 FAC 侧配置

4.3.1 配置两个 TACACS 客户端

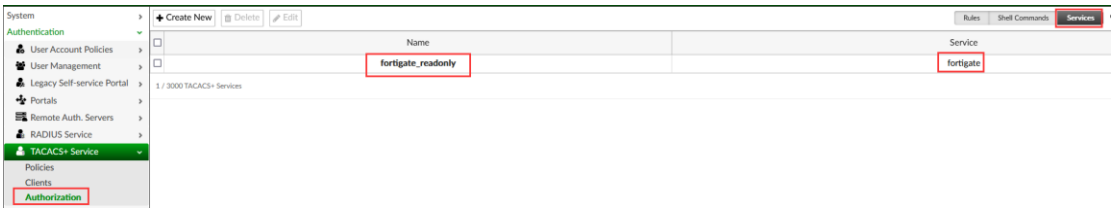
一个是防火墙:

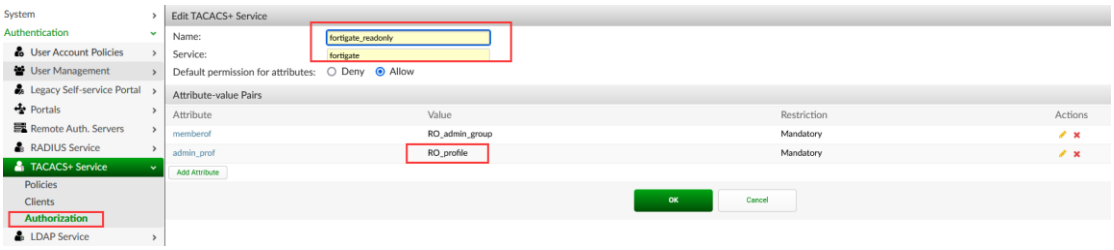


一个是 Router:



4.3.2 配置防火墙的 Service，即返回用户的 admin profile:

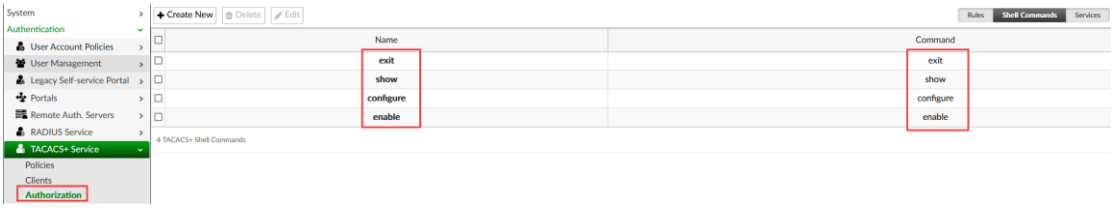


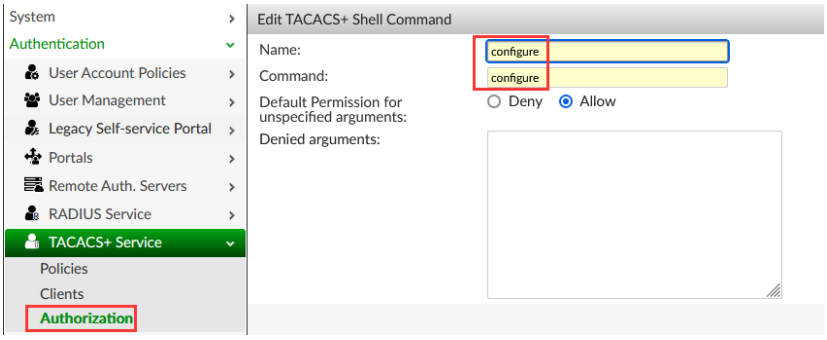


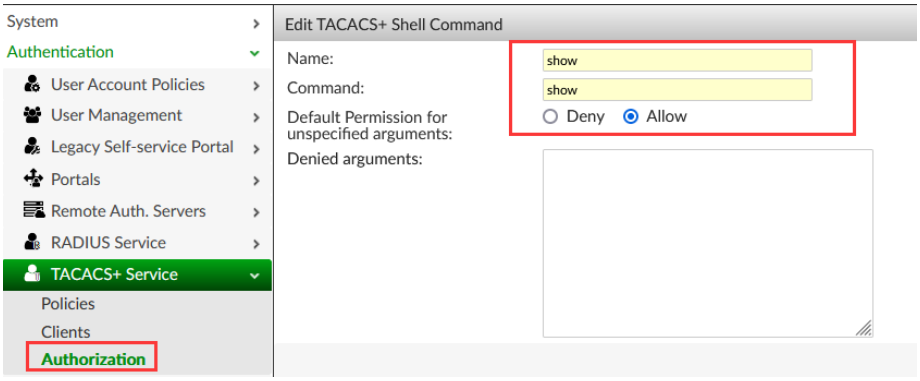
注意:上面配置的 admin profile:RO_profile 要与防火墙侧配置的一致;

4.3.3 配置允许执行的 shell command:

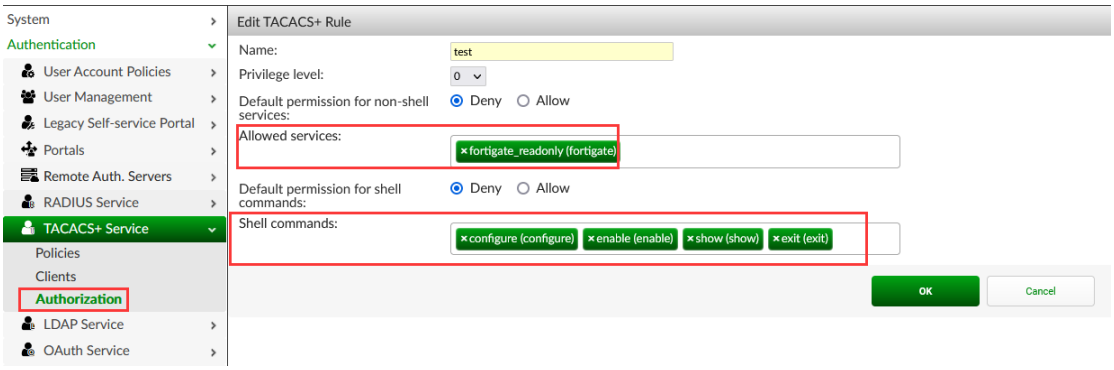
配置只允许在路由器的 CLI 下执行: enable/show/configure/exit 这四个命令关键字开始的命令:



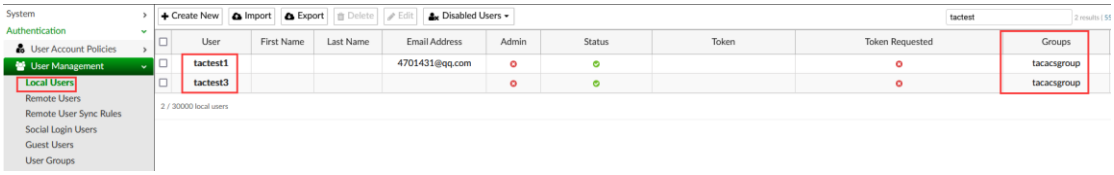


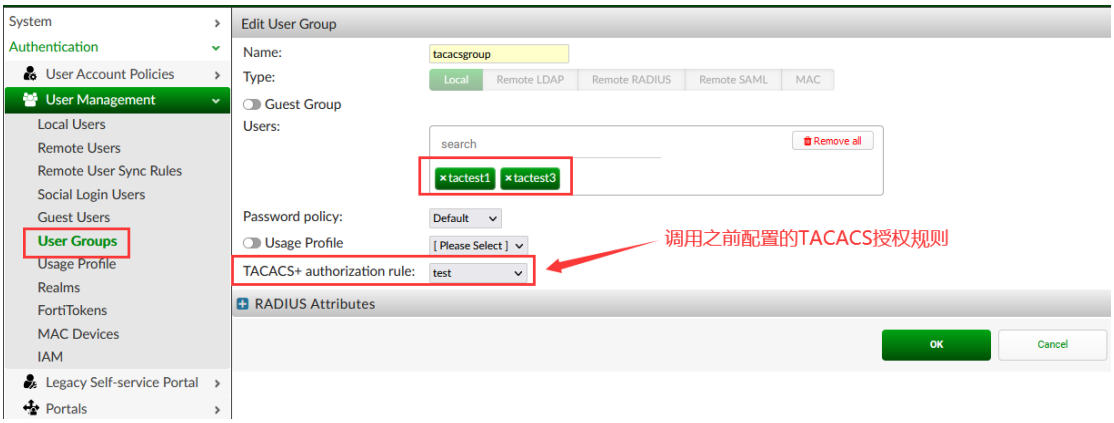


4.3.4 配置授权规则



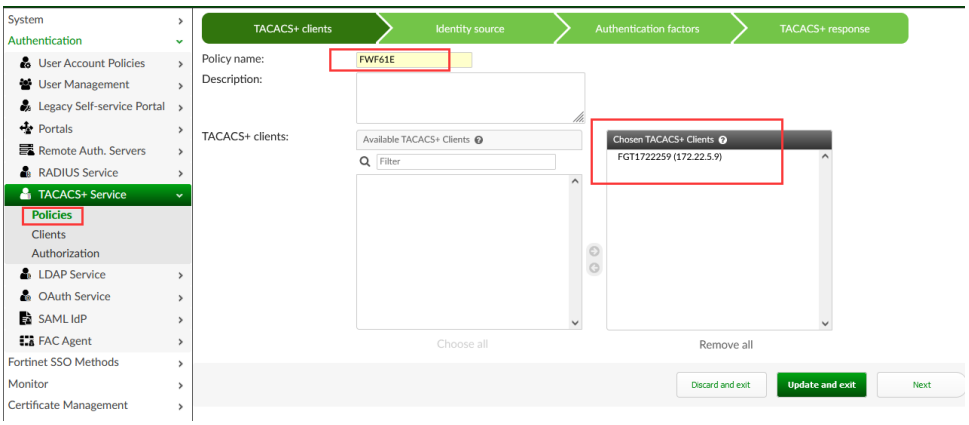
4.3.5 配置 TACACS 认证用户和 group

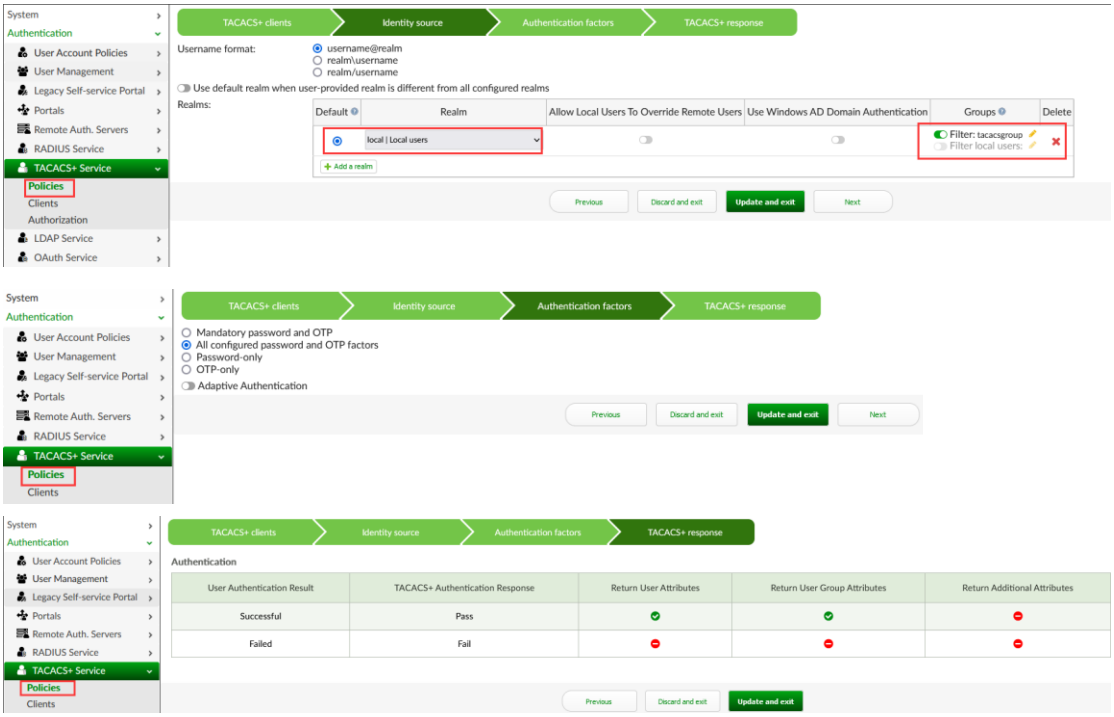




4.3.6 配置 TACACS 认证策略

防火墙和 Router 的认证策略配置类似，以防火墙为例:





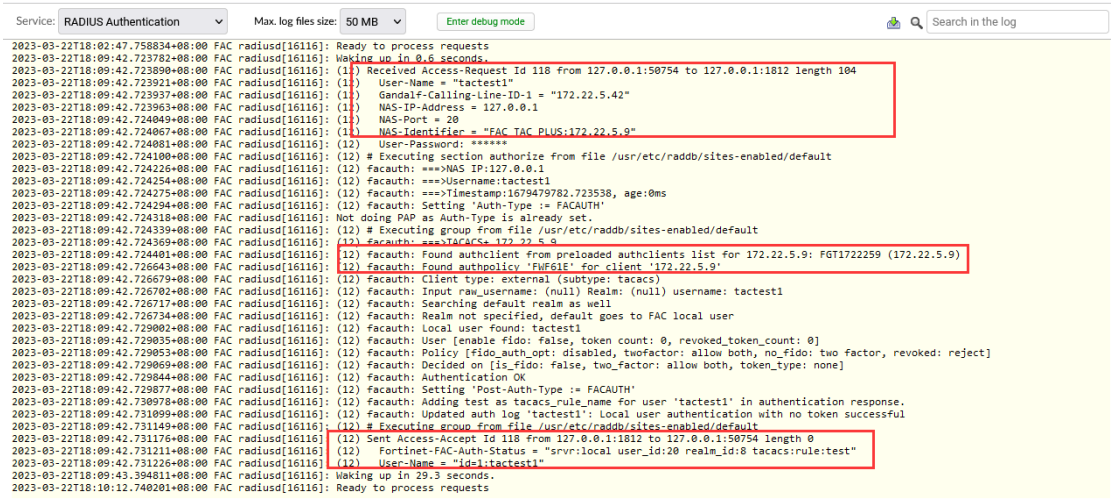
4.4 相关测试日志

4.4.1 防火墙 TACACS 认证日志

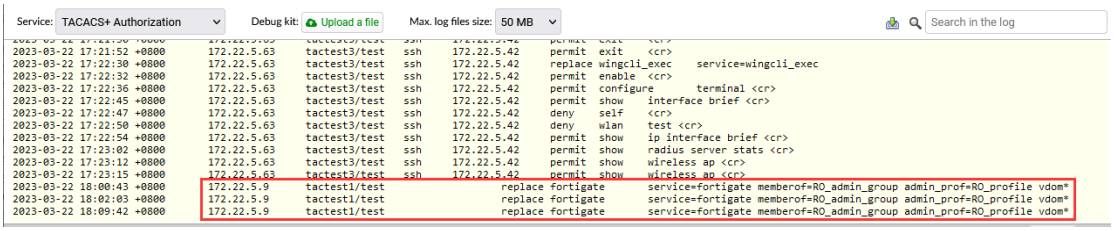
FAC 认证日志:

Log Details	
Log Record Detail	
ID	81027
Timestamp	Wed Mar 22 18:09:42 2023
Level	information
Action	Authentication
Status	Success
Source IP	FAC_TAC_PLUS:172.22.5.9
Message	Local user authentication with no token successful
User	tactest1
Log Type	
Type Id	20001
Name	Authentication OK No FTK
Sub Category	Authentication
Category	Event
Description	Authentication successful without FortiToken

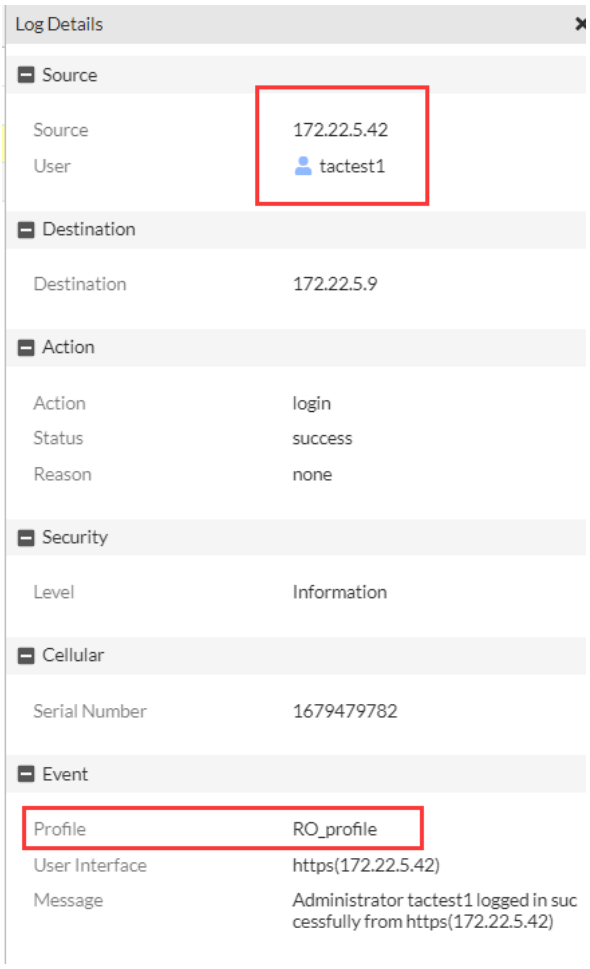
FAC radius 认证日志:



TACACS 授权日志，将 admin profile 信息返回给防火墙:



防火墙系统日志:

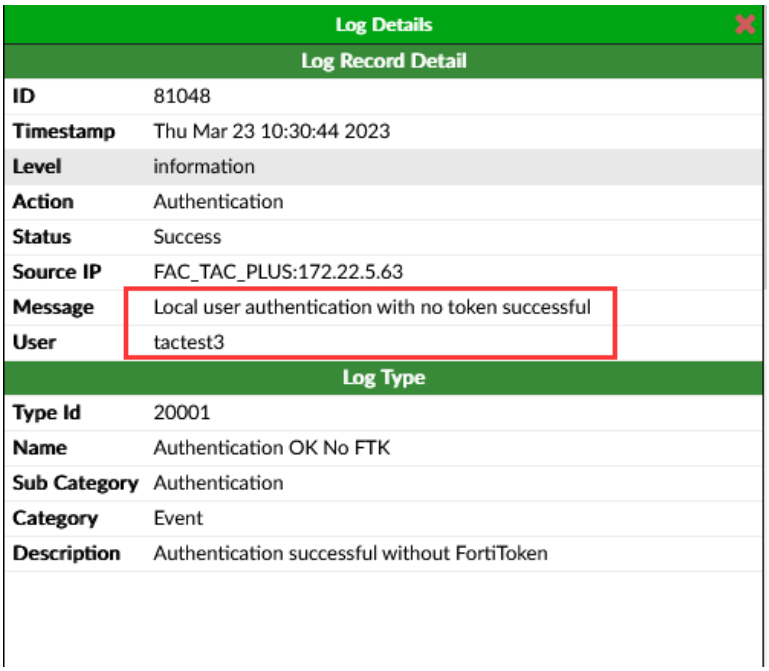


防火墙 fnbamd 进程 debug 日志:

```
[675] parse_author_reply-arg_cnt 4
[725] parse_author_reply-Authorization arg0: service=fortigate
[725] parse_author_reply-Authorization arg1: memberof=RO_admin_group
[725] parse_author_reply-Authorization arg2: admin_prof=RO_profile
[725] parse_author_reply-Authorization arg3: vdom*
[729] parse_author_reply-Authorization result=2
[16607] fnbam_user_auth_group_match-req id: 177934753, server: factacacs91115, local auth: 0, dn match: 0
[277] find_matched_usr_grps-Passed group matching
```

4.4.2 路由器 TACACS 认证日志

FAC 认证日志:



Log Details

Log Record Detail

ID	81048
Timestamp	Thu Mar 23 10:30:44 2023
Level	information
Action	Authentication
Status	Success
Source IP	FAC_TAC_PLUS:172.22.5.63
Message	Local user authentication with no token successful
User	tactest3

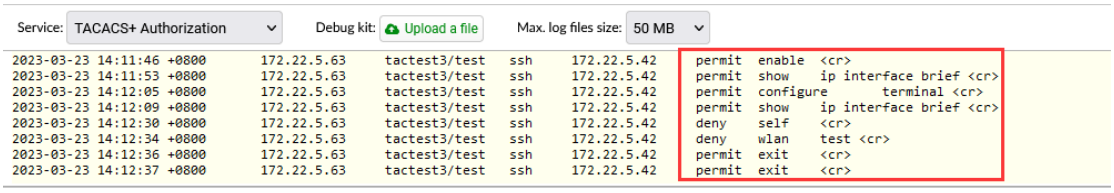
Log Type

Type Id	20001
Name	Authentication OK No FTK
Sub Category	Authentication
Category	Event
Description	Authentication successful without FortiToken

FAC Radius 认证 debug 日志:

```
Service: RADIUS Authentication   Max. log files size: 50 MB   Enter debug mode   Search in the l
2023-03-23T10:30:44.590757+08:00 FAC radiusd[16116]: (33) Received Access-Request Id 44 from 127.0.0.1:58510 to 127.0.0.1:1812 length 105
2023-03-23T10:30:44.590784+08:00 FAC radiusd[16116]: (33)   User-Name = "tactest3"
2023-03-23T10:30:44.590800+08:00 FAC radiusd[16116]: (33)   Gandalf-Calling-Line-ID-1 = "172.22.5.42"
2023-03-23T10:30:44.590815+08:00 FAC radiusd[16116]: (33)   NAS-IP-Address = 127.0.0.1
2023-03-23T10:30:44.590832+08:00 FAC radiusd[16116]: (33)   NAS-Port = 20
2023-03-23T10:30:44.590847+08:00 FAC radiusd[16116]: (33)   NAS-Identifier = "FAC_TAC_PLUS:172.22.5.63"
2023-03-23T10:30:44.590860+08:00 FAC radiusd[16116]: (33)   User-Password: ******
2023-03-23T10:30:44.591039+08:00 FAC radiusd[16116]: (33) # Executing section authorize from file /usr/etc/raddb/sites-enabled/default
2023-03-23T10:30:44.591141+08:00 FAC radiusd[16116]: (33) facauth: ===>NAS IP:127.0.0.1
2023-03-23T10:30:44.591163+08:00 FAC radiusd[16116]: (33) facauth: ===>Username:tactest3
2023-03-23T10:30:44.591182+08:00 FAC radiusd[16116]: (33) facauth: ===>Timestamp:1679538644.590512, age:0ms
2023-03-23T10:30:44.591200+08:00 FAC radiusd[16116]: (33) facauth: Setting 'Auth-Type := FACAUTH'
2023-03-23T10:30:44.591233+08:00 FAC radiusd[16116]: Not doing PAP as Auth-Type is already set.
2023-03-23T10:30:44.591253+08:00 FAC radiusd[16116]: (33) # Executing group from file /usr/etc/raddb/sites-enabled/default
2023-03-23T10:30:44.591292+08:00 FAC radiusd[16116]: (33) facauth: ===>TACACS+ 172.22.5.63
2023-03-23T10:30:44.591327+08:00 FAC radiusd[16116]: (33) facauth: Found authclient from preloaded authclients list for 172.22.5.63: Router (172.22.5.63)
2023-03-23T10:30:44.593523+08:00 FAC radiusd[16116]: (33) facauth: Found authpolicy 'RouterPolicy' for client '172.22.5.63'
2023-03-23T10:30:44.593574+08:00 FAC radiusd[16116]: (33) facauth: Client type: external (subtype: tacacs)
2023-03-23T10:30:44.593590+08:00 FAC radiusd[16116]: (33) facauth: Input raw_username: (null) Realm: (null) username: tactest3
2023-03-23T10:30:44.593604+08:00 FAC radiusd[16116]: (33) facauth: Searching default realm as well
2023-03-23T10:30:44.593630+08:00 FAC radiusd[16116]: (33) facauth: Realm not specified, default goes to FAC local user
2023-03-23T10:30:44.595861+08:00 FAC radiusd[16116]: (33) facauth: Local user found: tactest3
2023-03-23T10:30:44.595894+08:00 FAC radiusd[16116]: (33) facauth: User [enable fido: false, token count: 0, revoked_token_count: 0]
2023-03-23T10:30:44.595911+08:00 FAC radiusd[16116]: (33) facauth: Policy [fido_auth_opt: disabled, twofactor: allow both, no_fido: two factor, revoked: reject]
2023-03-23T10:30:44.595928+08:00 FAC radiusd[16116]: (33) facauth: Decided on [is_fido: false, two_factor: allow both, token_type: none]
2023-03-23T10:30:44.596719+08:00 FAC radiusd[16116]: (33) facauth: Authentication OK
2023-03-23T10:30:44.596748+08:00 FAC radiusd[16116]: (33) facauth: Setting 'Post-Auth-Type := FACAUTH'
2023-03-23T10:30:44.597837+08:00 FAC radiusd[16116]: (33) facauth: Adding test as tacacs_rule_name for user 'tactest3' in authentication response.
2023-03-23T10:30:44.597956+08:00 FAC radiusd[16116]: (33) facauth: Updated auth log 'tactest3': Local user authentication with no token successful
2023-03-23T10:30:44.597994+08:00 FAC radiusd[16116]: (33) # Executing group from file /usr/etc/raddb/sites-enabled/default
2023-03-23T10:30:44.598020+08:00 FAC radiusd[16116]: (33) Sent Access-Accept Id 44 from 127.0.0.1:1812 to 127.0.0.1:58510 length 0
2023-03-23T10:30:44.598047+08:00 FAC radiusd[16116]: (33)   Fortinet-FAC-Auth-Status = "srvr:local user_id:39 realm_id:22 tacacs:rule:test"
2023-03-23T10:30:44.598062+08:00 FAC radiusd[16116]: (33)   User-Name = "id=1:tactest3"
2023-03-23T10:30:45.258816+08:00 FAC radiusd[16116]: Waking up in 29.3 seconds.
2023-03-23T10:31:14.610848+08:00 FAC radiusd[16116]: Ready to process requests
```

由于 FAC 上是配置的路由器的 shell 的 CLI 命令授权，下面的 TACACS 的 debug 日志显示了对用户在登录路由器的命令下，执行命令的授权:



```
Service: TACACS+ Authorization   Debug kit: Upload a file   Max. log files size: 50 MB
2023-03-23 14:11:46 +0800   172.22.5.63   tactest3/test   ssh   172.22.5.42   permit  enable  <cr>
2023-03-23 14:11:53 +0800   172.22.5.63   tactest3/test   ssh   172.22.5.42   permit  show    ip interface brief <cr>
2023-03-23 14:12:05 +0800   172.22.5.63   tactest3/test   ssh   172.22.5.42   permit  configure       terminal <cr>
2023-03-23 14:12:09 +0800   172.22.5.63   tactest3/test   ssh   172.22.5.42   permit  show    ip interface brief <cr>
2023-03-23 14:12:30 +0800   172.22.5.63   tactest3/test   ssh   172.22.5.42   deny    self    <cr>
2023-03-23 14:12:34 +0800   172.22.5.63   tactest3/test   ssh   172.22.5.42   deny    wlan    test <cr>
2023-03-23 14:12:36 +0800   172.22.5.63   tactest3/test   ssh   172.22.5.42   permit  exit    <cr>
2023-03-23 14:12:37 +0800   172.22.5.63   tactest3/test   ssh   172.22.5.42   permit  exit    <cr>
```

从上面的日志可以看到，当用户在路由器的命令行下执行命令时,执行 FAC 上允许执行的命令时，路由器的 CLI 会运行执行改命令,用户执行不在 FAC 上配置的允许执行的命令时, FAC 会返回禁止执行，用户执

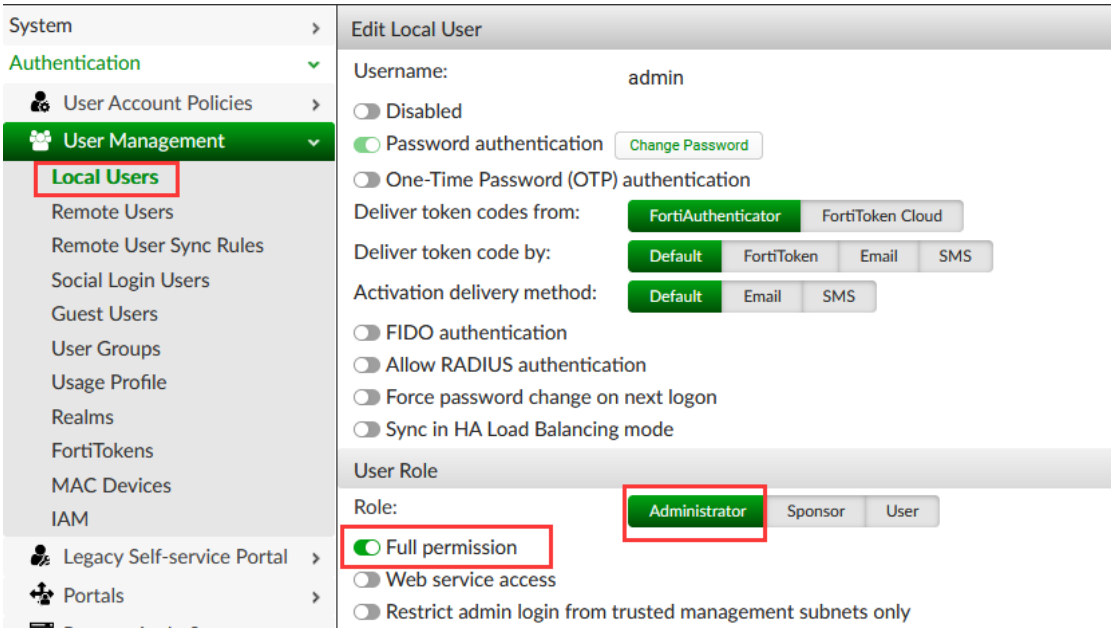
行此命令会提示失败.

三. 日常维护

1. 管理员操作

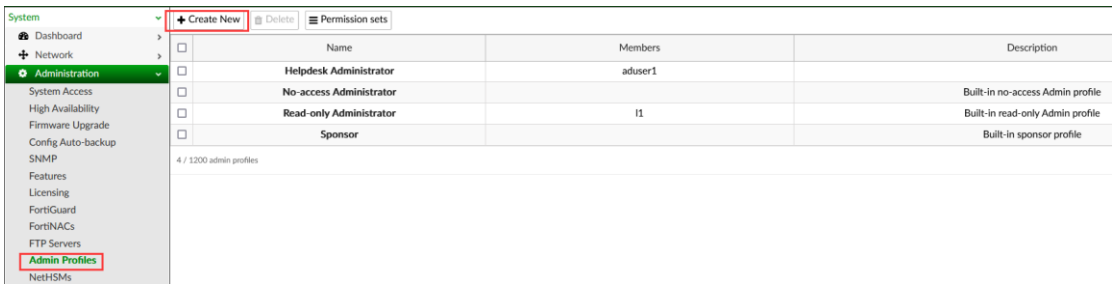
1.1 admin 管理员操作

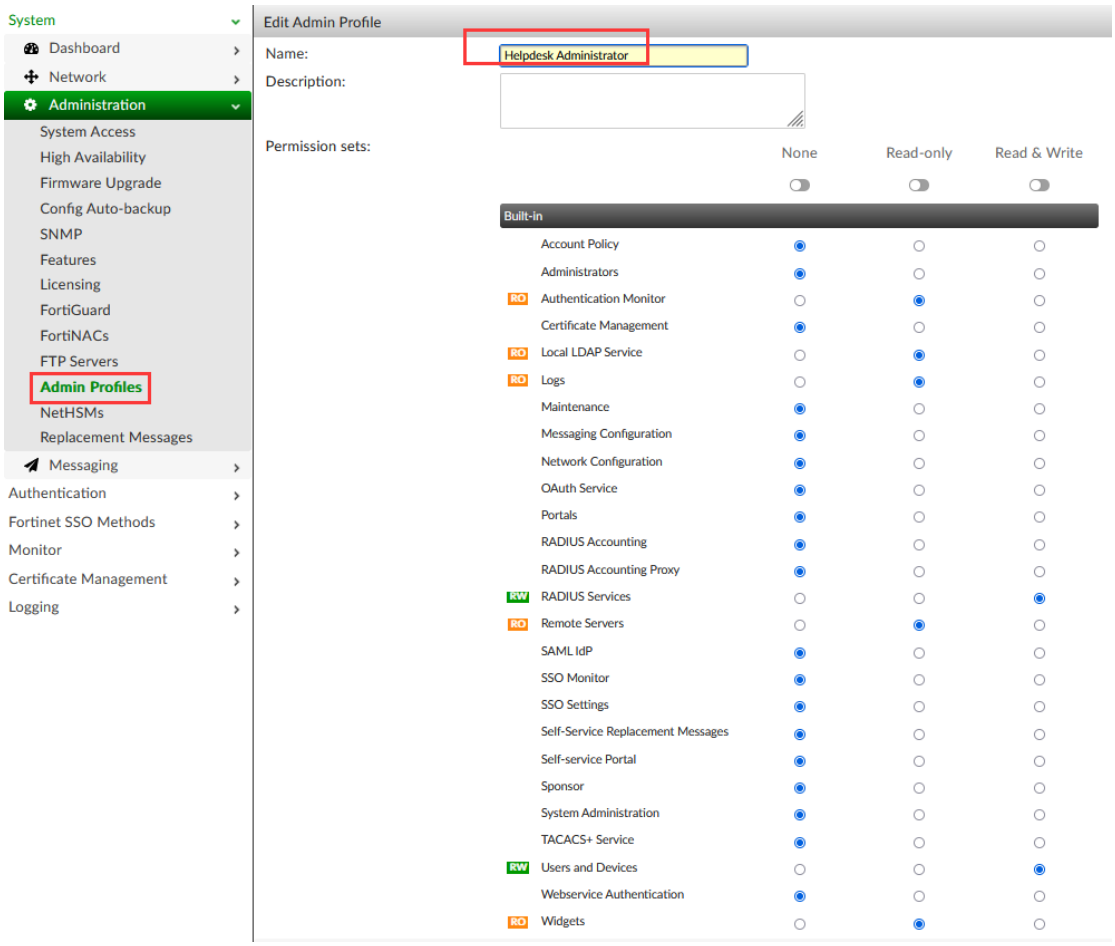
FAC 默认的管理员为 admin, 可以在此页面对 admin 管理员帐号进行管理.



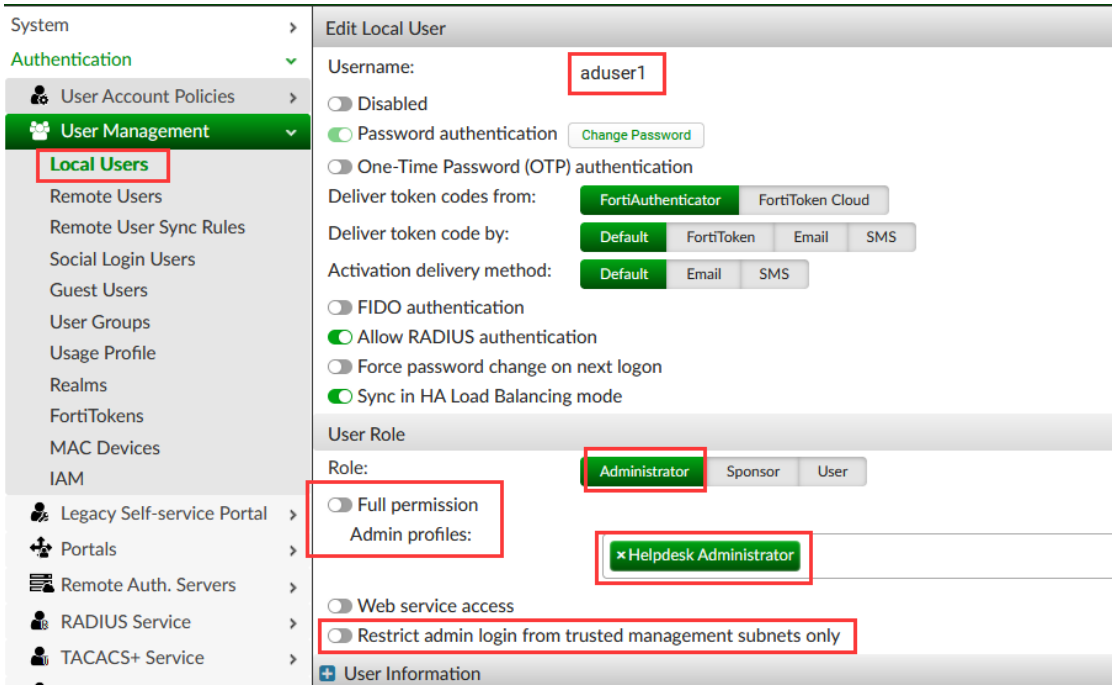
1.2 其它管理员操作

对于其它管理员操作, 可以在下面界面设置管理的操作权限:





然后在建立的 admin 帐号下调用:

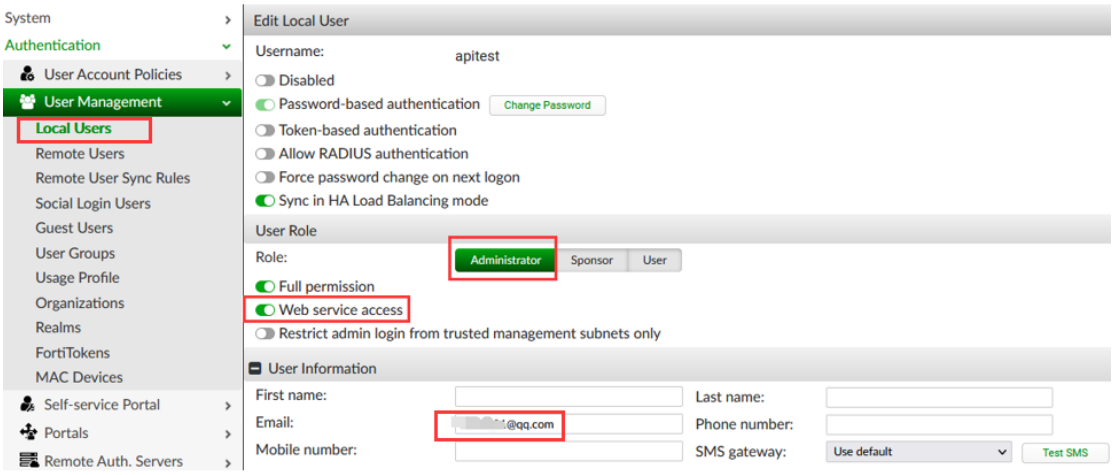


上面的界面也可以设置管理员登录的信任主机.

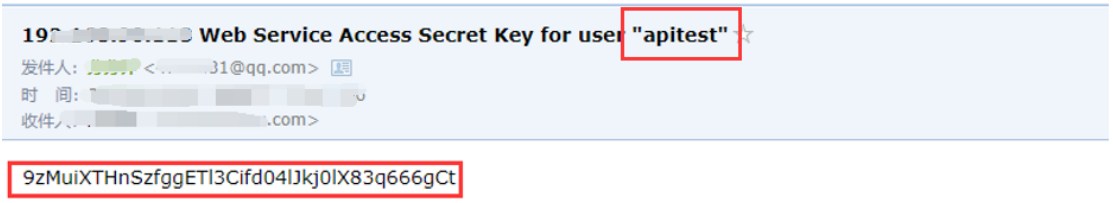
1.3 REST API 管理员

在很多用户场景需要使用 REST API 访问 FAC，对 FAC 进行一些管理和操作.

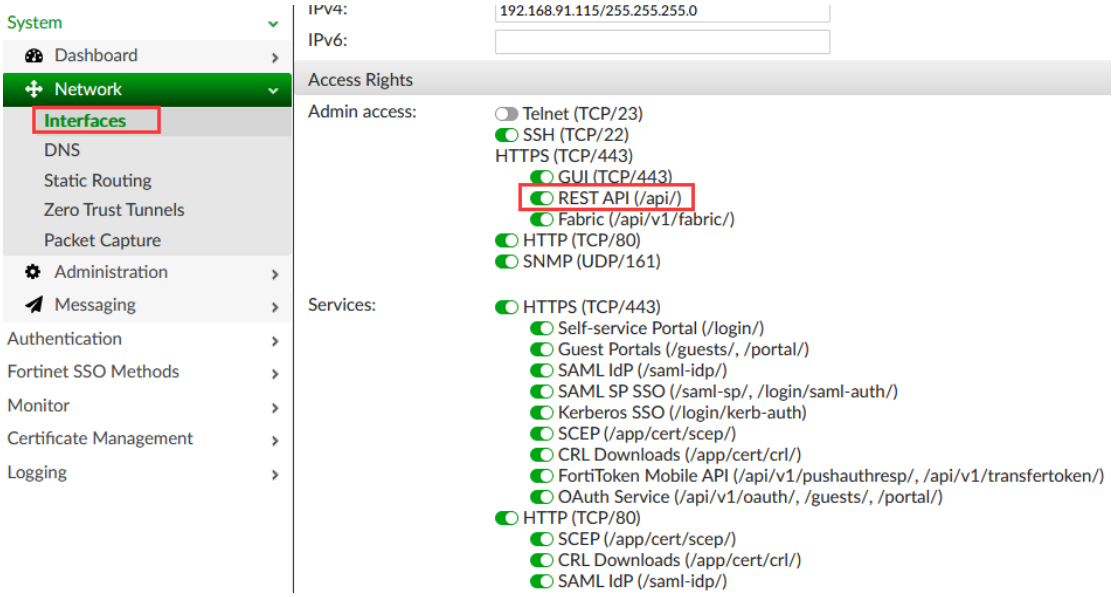
在下面界面创建 API 访问帐号:



开启后 API 用户的设置的邮箱会收到 API 访问的密码:



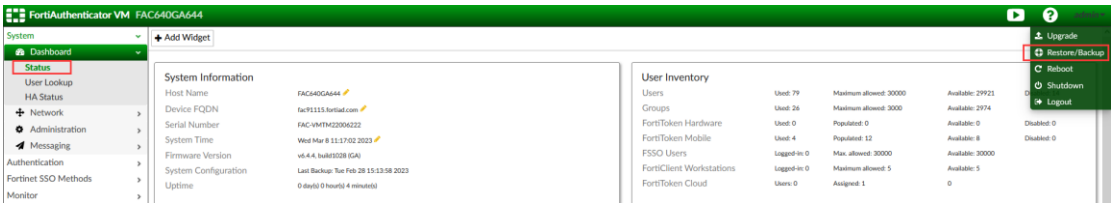
注意: FAC 的接口下也需要开启 API 访问:



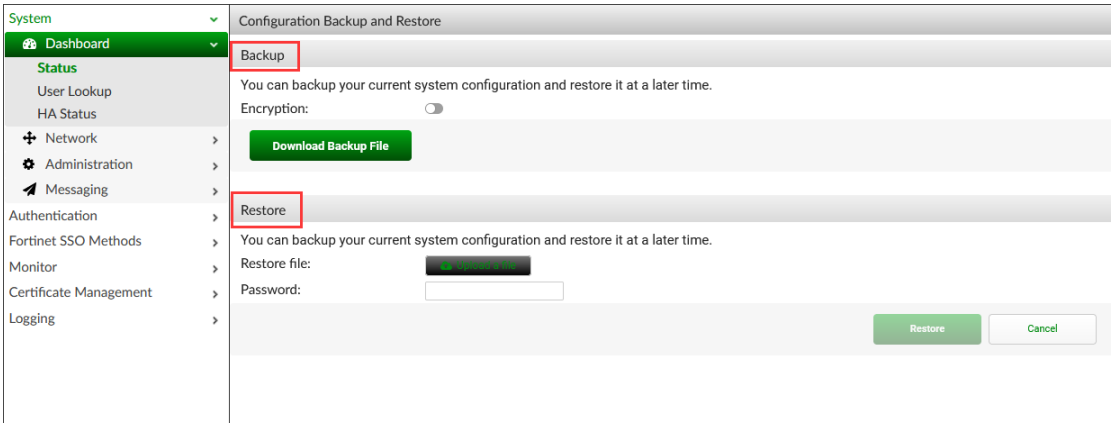
FAC REST API 的使用，请参考 FAC 的 API 指导手册.

2. 系统配置文件备份和恢复

建议每次修改配置前后，备份一下 FAC 的配置文件，如果是 FACVM，定期备份虚机快照:



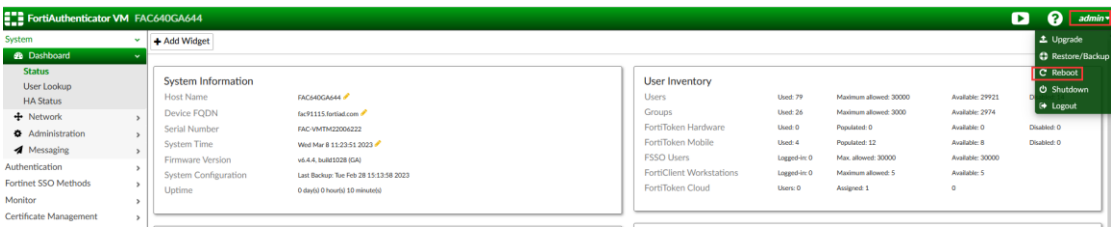
在下面的操作界面可以选择备份配置文件或是恢复 FAC 的配置文件(请谨慎操作):



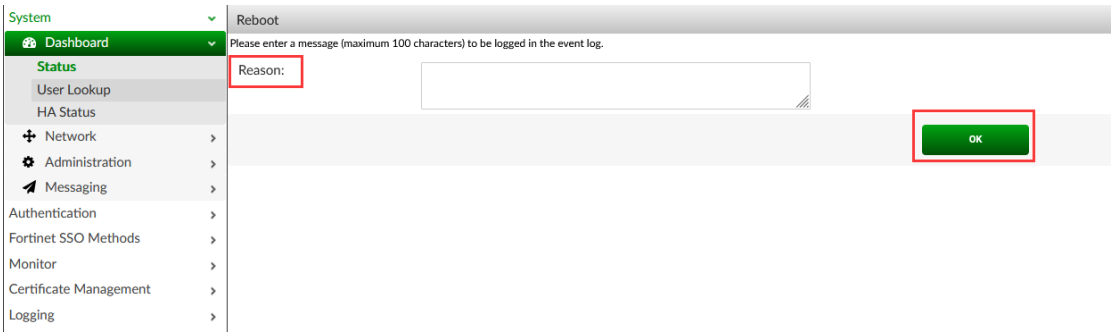
注意: FAC 的配置文件跟防火墙不通，不是可读文件，如果需要把 FAC 的配置文件在不通 FAC 平台间转化的话，请联系 Fortinet 售后支持;

3. 设备重启

点击”Reboot” 可重启 FAC:

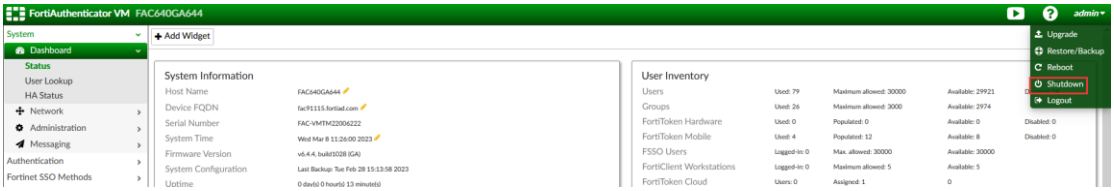


可以备上设备重启原因:

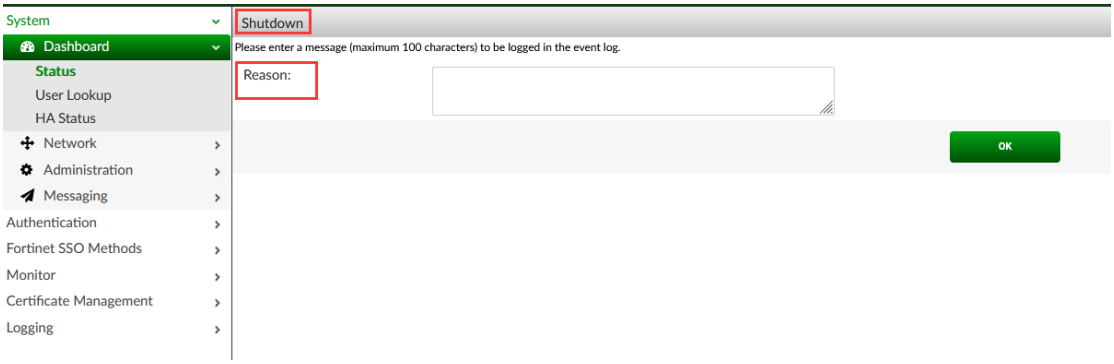


4. 设备关机

点击”Shutdown” 可给设备关机:

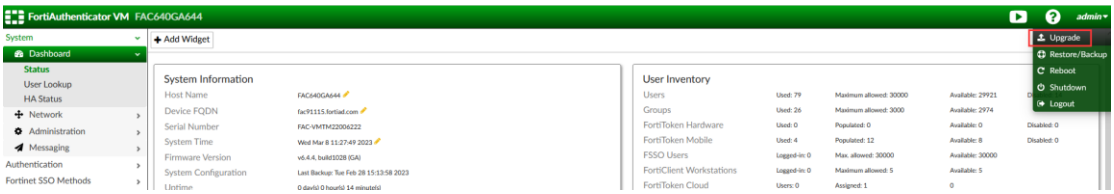


备上设备关机原因:

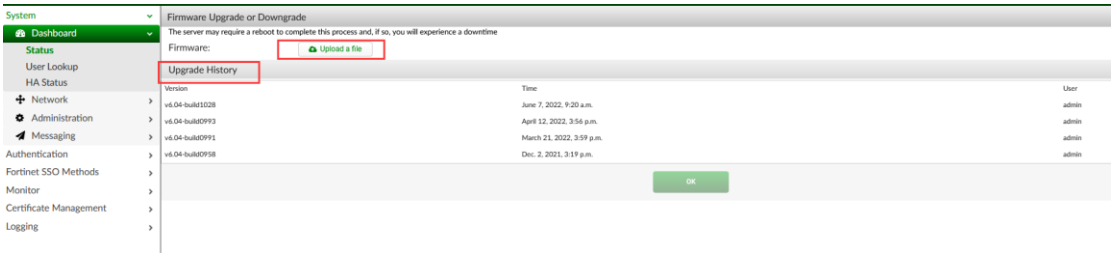


5. 设备升级

点击”Upgrade” 可升级 FAC 的版本:



在防火墙的升级界面，可以看到之前的升级历史记录:



设备升级后会自动重启:

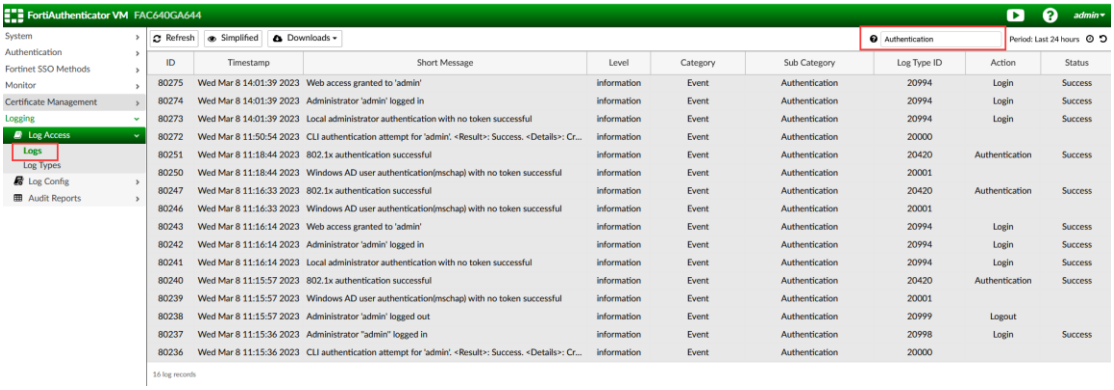
注意:

- 在升级 FAC 之前，请备份设备的配置文件，如果是 FACVM，请备份设备虚机快照.
- 在升级 FAC 之前,请仔细阅读要升级的版本的版本发布说明，特别是升级说明(Upgrade instructions)这个章节,需要特别关注:
  - 是否需要先升级到过渡版本
  - 有些虚机平台比如 FACKVM 或 FACXEN 的旧版本需要在升级之前先扩容虚机硬盘

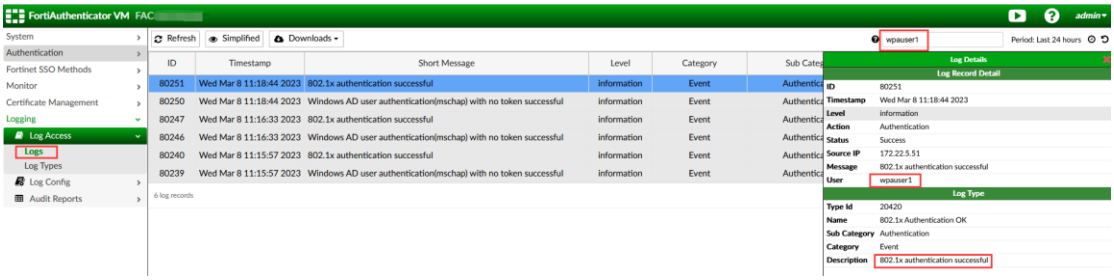
6. FAC 日志相关

6.1 日志查看

在下面界面可以看到 FAC 的所有日志信息:

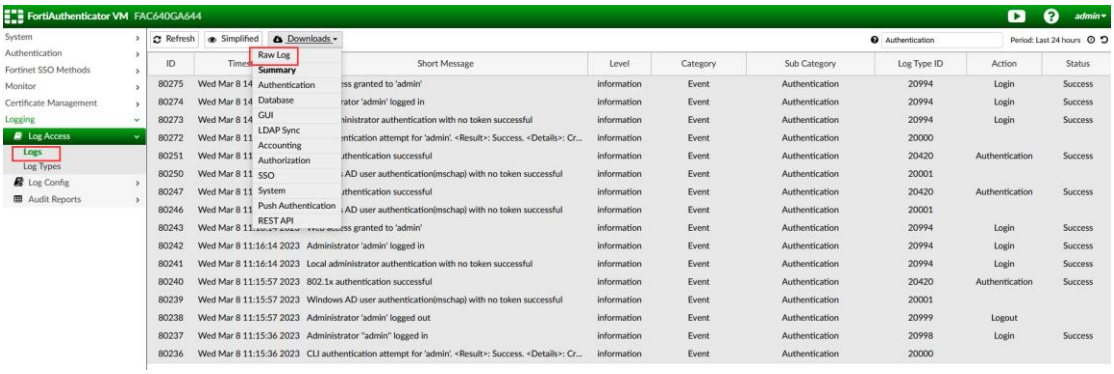


日志支持关键字搜索查找，比如查找某个用户的认证日志:



6.2 日志下载

点击”Download”的”Raw Log”可以下载日志:



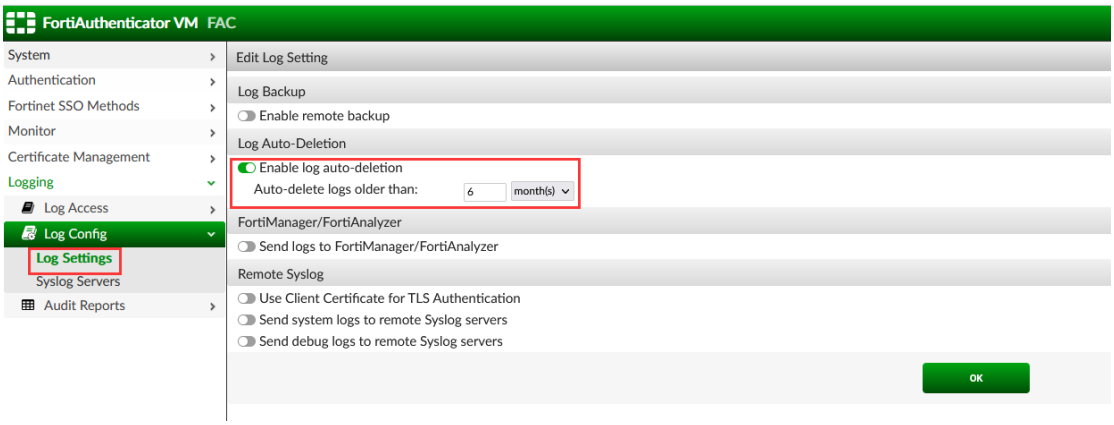
注意: 如果日志量比较大的话，那日志下载也会比较慢.

6.3 日志设置

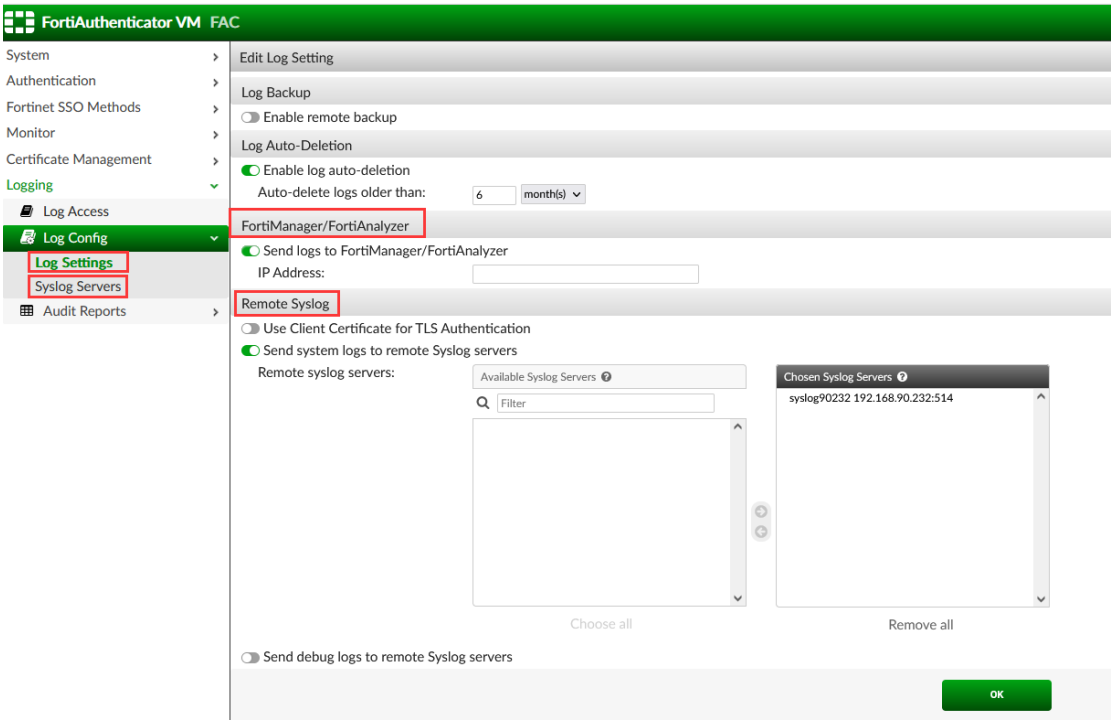
在下面界面可以设置日志的相关参数:

设置日志回滚时间:

因为 FAC 的日志是存储在 FAC 的数据库中，如果 FAC 的日志量太大的话，会影响 FAC 的其它数据库相关的操作进而影响 FAC 的认证，所以一般建议日志的保存时间不要超过 6 个月.

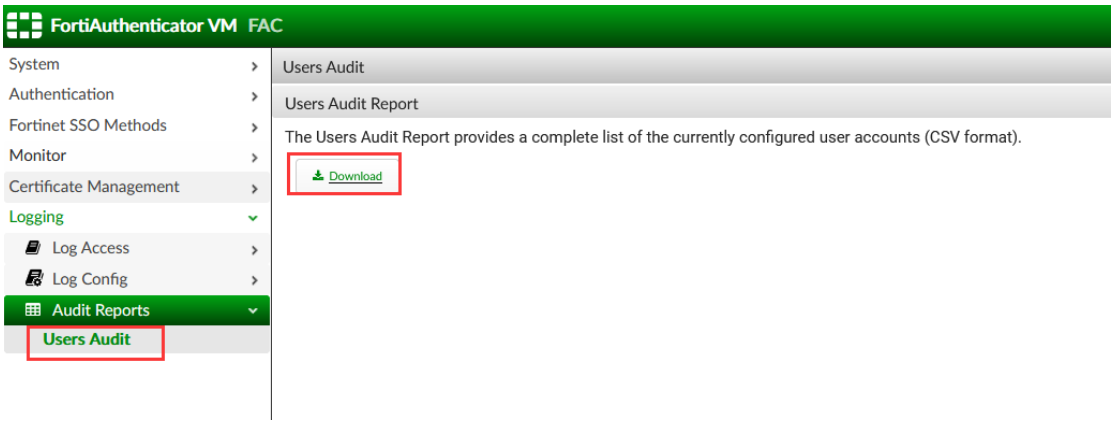


把日志基于 syslog 发送给外部设备，比如 FortiManager/FortiAnalyzer 或第三方的 syslog server:



6.4 用户审计

可以下载用户审计报告，获取 FAC 上所有 Local 和 Remote LDAP 用户的信息，包括用户的帐号信息，token 信息，以及帐号建议的时间和最后一次用户做认证的时间.



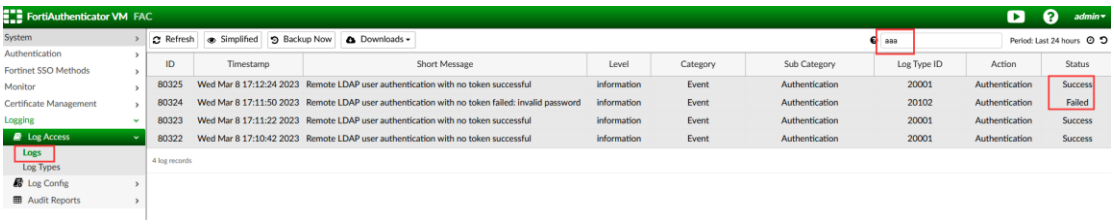
四. 常见问题及 debug 方法

1. FAC 的 debug 方法

FAC 的 debug 日志有三种，一种是 Log 日志，一种是 debug 日志，还有一个是 debug 报告，Log 日志和 Debug 日志在我们遇到问题时可自己查看分析，debug 报告包含详细的 debug 信息，需要发给研发，由研发来分析定位问题.

1.1 Log 日志

Log 日志一般显示 FAC 的系统操作或是认证结果，比如显示用户认证结果，用户 token 分配结果等，虽然 FAC 的 Log 日志不会有详细的相关信息，比如下面查看用户 aaa 的认证日志记录:



这个是能看到认证的结果，但是看不到认证的过程;

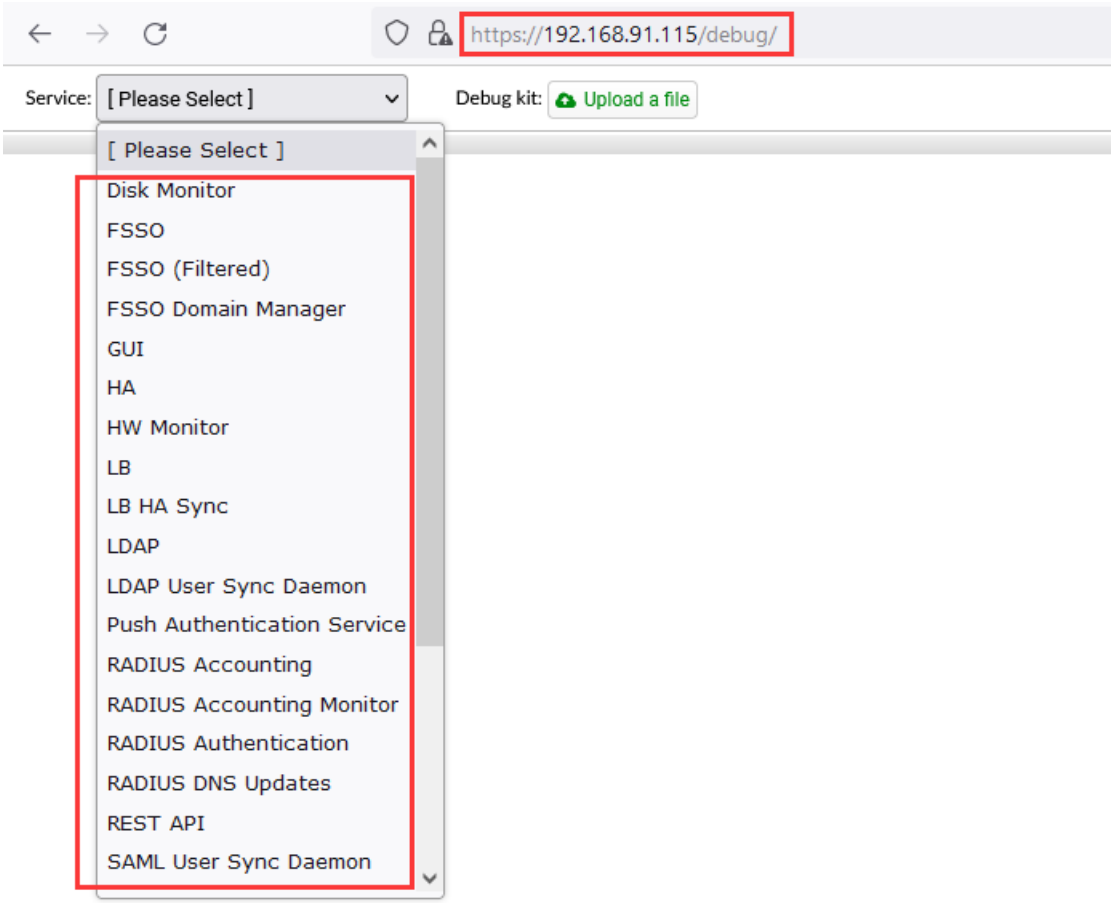
但是 FAC 的 Log 日志记录的比较全面，所有 FAC 相关的操作和处理都会有日志记录，所以当我们需要查询或定位问题时，先检查搜索一下日志会非常有帮助.

1.2 Debug 日志

FAC 的 debug 日志是基于模块的，访问每个模块的日志，可以看到详细的信息和过程.

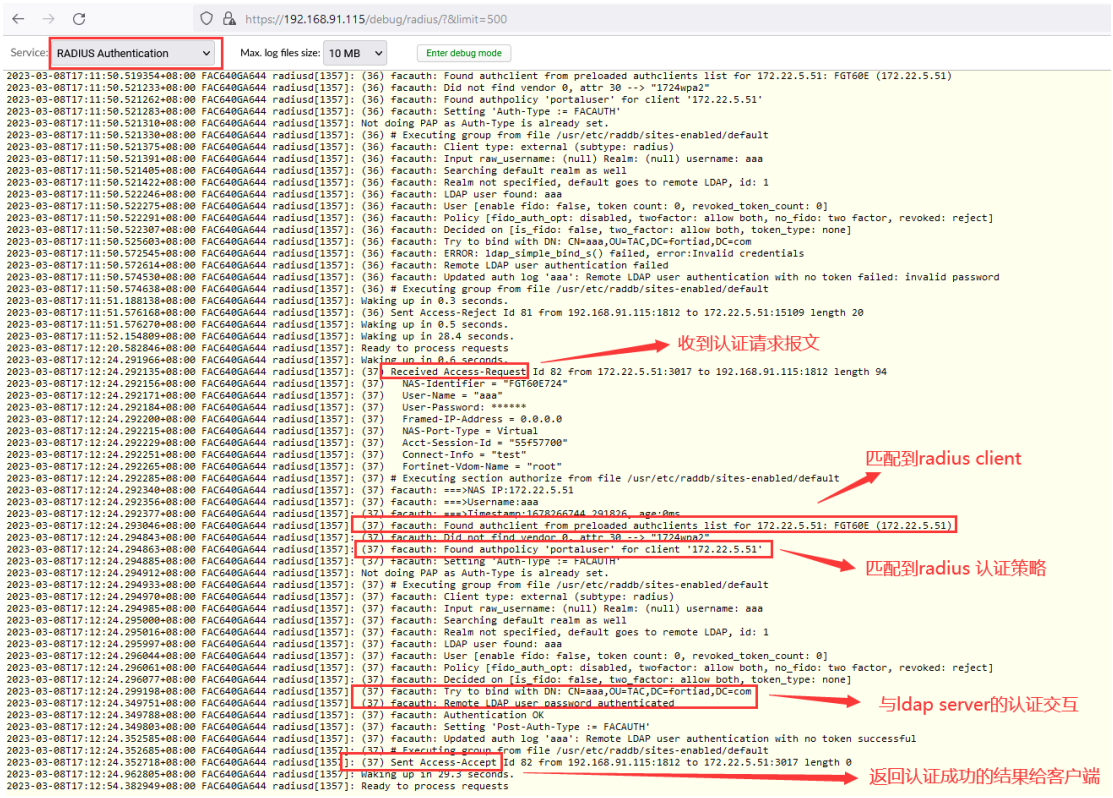
访问 FAC 的下面地址，可以进入 FAC 的 debug 日志页面:

https://fac_ip_address/debug/



当我们需要 debug 某个模块时，就选择相应的模块.

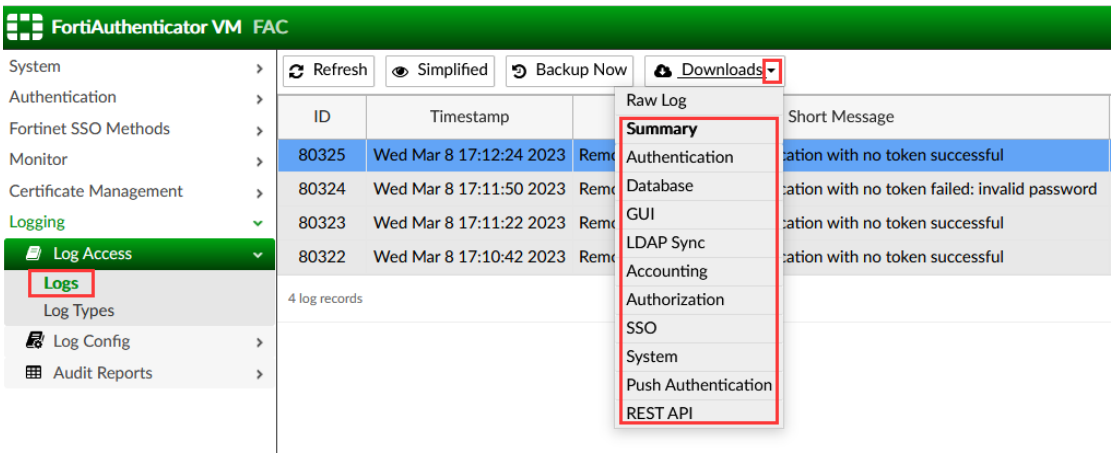
比如我们经常遇到比较多的问题是跟认证相关，那就可以选择 RADIUS Authentication，以下是一个用户认证的完整处理过程:



1.3 Debug 报告

在处理某些问题时，基于 Log 日志和 Debug 日志也不能分析问题，那么我们就需要相关的 debug 报告，然后把 debug 报告发送个研发来做更进一步的分析.

在下面页面可以下载相关模块的 Debug 报告.



1.4 报文抓取

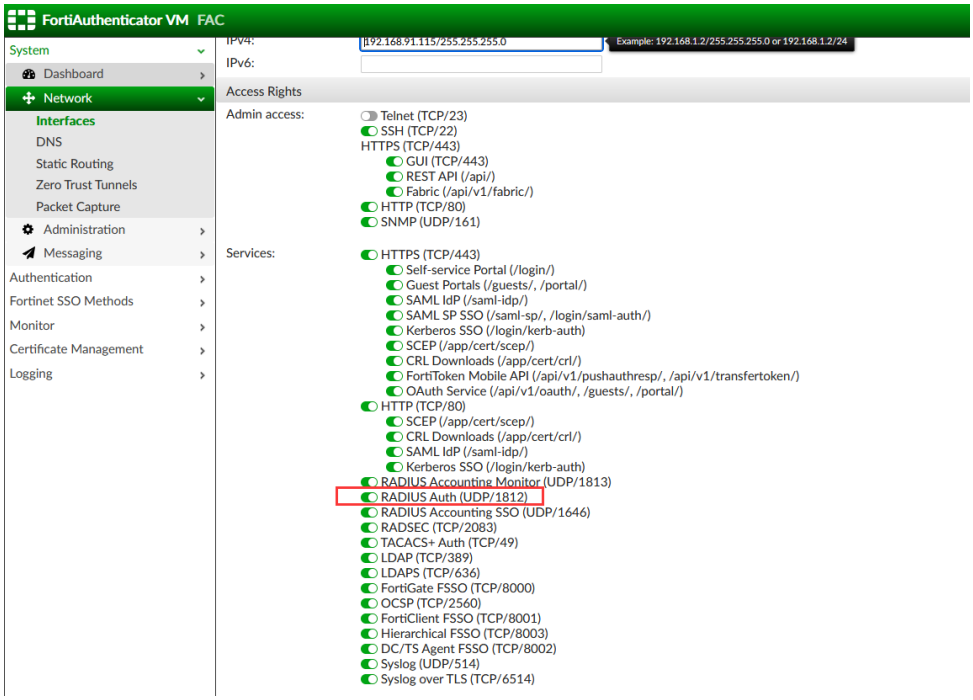
在 FAC 上也可以开启报文抓取，以便于更进一步分析问题，最多可抓取 10000 个报文:

2. 常见问题的处理方法

在 FAC 的使用过程中,遇到问题后，首先先检查一下 FAC 的 Log 日志，可以查找出问题的时间点的日志或是基于某些用户或是关键字来检查日志，大部分问题都可以通过查看 Log 日志或 Debug 日志找到原因. 以下列举了一些在 FAC 的日常使用中遇到的问题已经处理办法.

2.1 用户认证失败,没有日志显示

当用户认证失败时，首先基于这个用户来检查一下 Log 日志,如果 FAC 上没有相关用户认证的日志,则需要检查一下相关配置，比如 FAC 的接口是否开启 radius 认证:

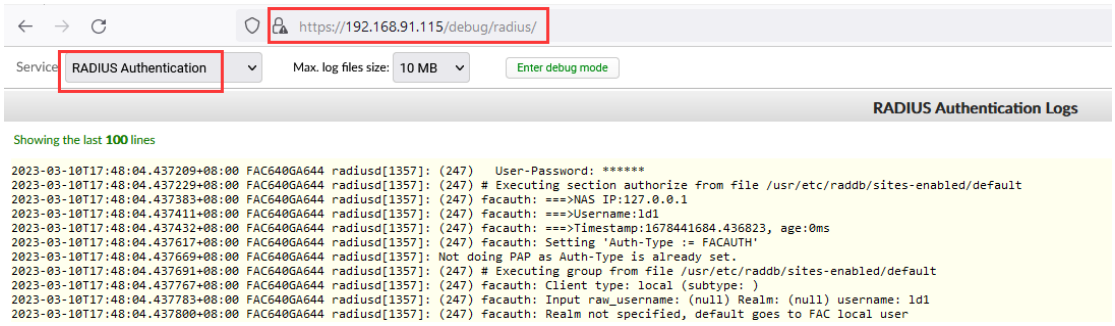


比如 FAC 上配置的 radius client 是否正确, radius secret 可以是否正确.

2.2 用户日志显示认证失败

当用户认证失败时，首先基于这个用户来检查一下 Log 日志,如果不能得到认证失败的原因,那可以检查一下 debug 日志, debug 日志里面会有详细的认证过程日志:

https://fac_ip_address/debug/radius/



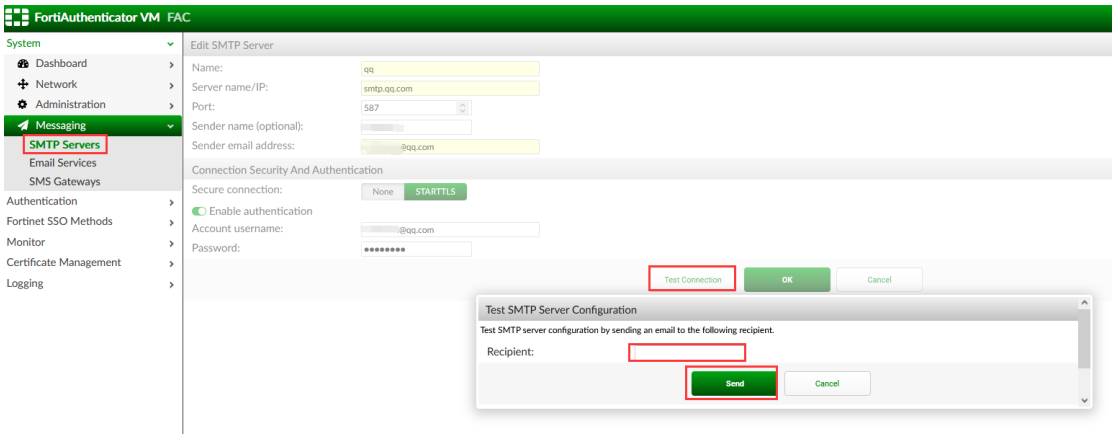
请注意: FAC 的所有用户相关的日志，包括 FAC 的 GUI 页面登录,radius 认证/saml 认证等都可以在上面的 debug 页面看到用户认证的详细信息和过程;

2.3 用户 token 分配失败

用户 token 分配失败分两种情况，一种是 FAC 跟 Fortinet 后台通讯失败导致 token 分配失败，这种情况需要检查 FAC 的通讯链路,以及确保 FAC 的上网策略中没有 SSL 检测之类的策略;

还有一种 token 分配失败情况是无法发送 token 激活的邮件

首先需要确保用户的邮箱地址设置正确,其次需要检查一下 SMTP 服务器是否工作正常，比如在 SMTP 设置的界面做一下邮箱测试:



如果邮箱测试失败，可以通过抓包检查一下 FAC 跟 SMTP server 之间的通讯报文.

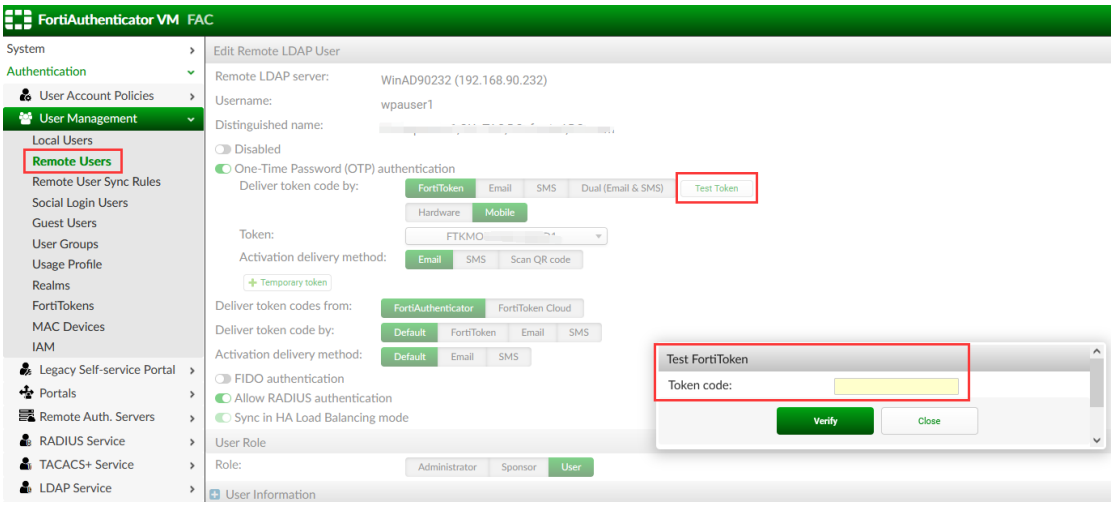
2.4 ldap 用户输入正确的密码，但是 FAC 日志显示认证失败，密码错误

这种情况一般有两种原因，一种是用户本身密码的问题，比如密码过期了，可以在别的设备上使用这个密码登录一下，以检查密码状态是否正常;

还有一种原因就是此用户在 ldap server 的目录发生了变化,比如从一个 OU 迁移到另外一个 OU，迁移后 FAC 上没有及时同步这个用户的信息，解决办法是在 FAC 上使用这个用户改变后的同步规则再同步一下这个用户;

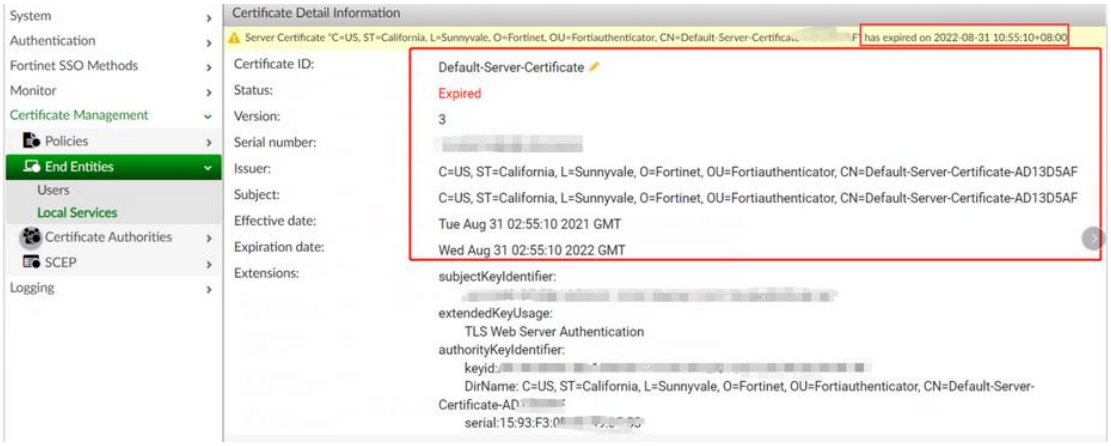
2.5 用户输入正确 token 后, FAC 日志依然显示 token 认证失败

出现这种情况可能是因为用户端的 token 跟 FAC 侧的 token 产生了偏移，解决办法是对用户的 token 做一下 token 测试，输入连续的两个 token 来进行 token 纠偏:



2.6 FAC 自带的证书显示过期

有些旧版本自带的证书有效期比较端，到期后显示证书过期

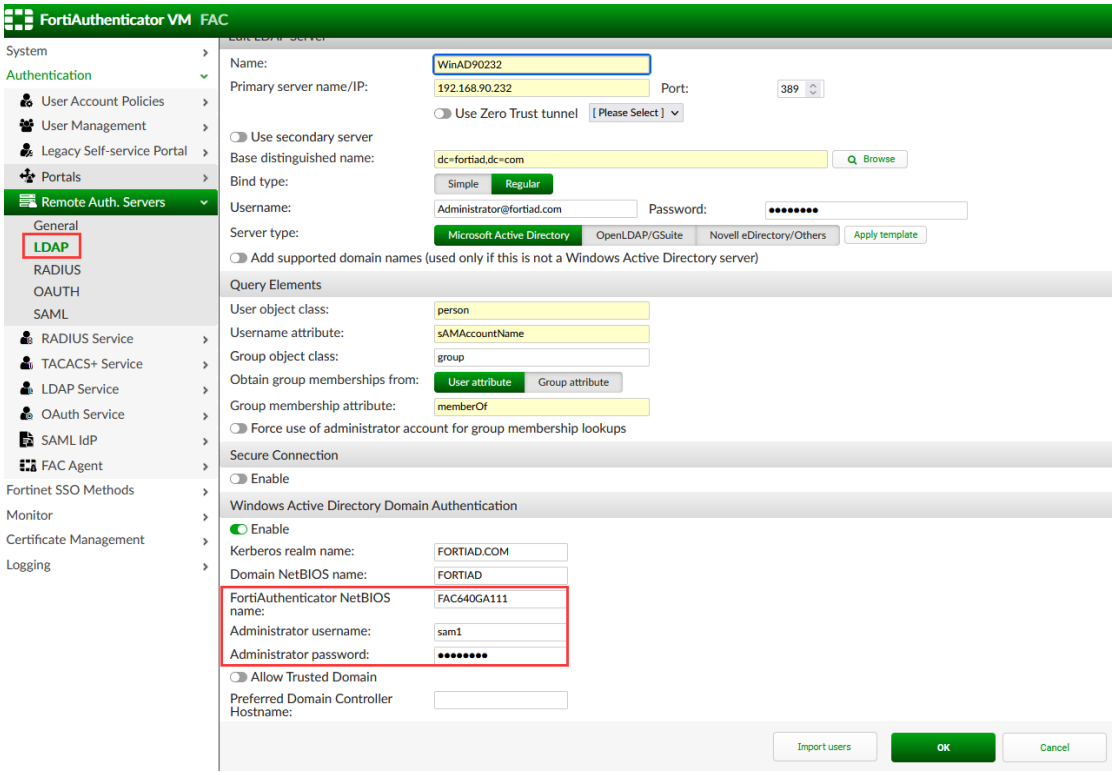


下面三个方法都可以解决这个问题:

- 重新安装一下 FAC 的 License
- 升级一下 FAC 的版本
- 证书过期后重启一下 FAC

2.7 FAC 加入到 AD 域失败

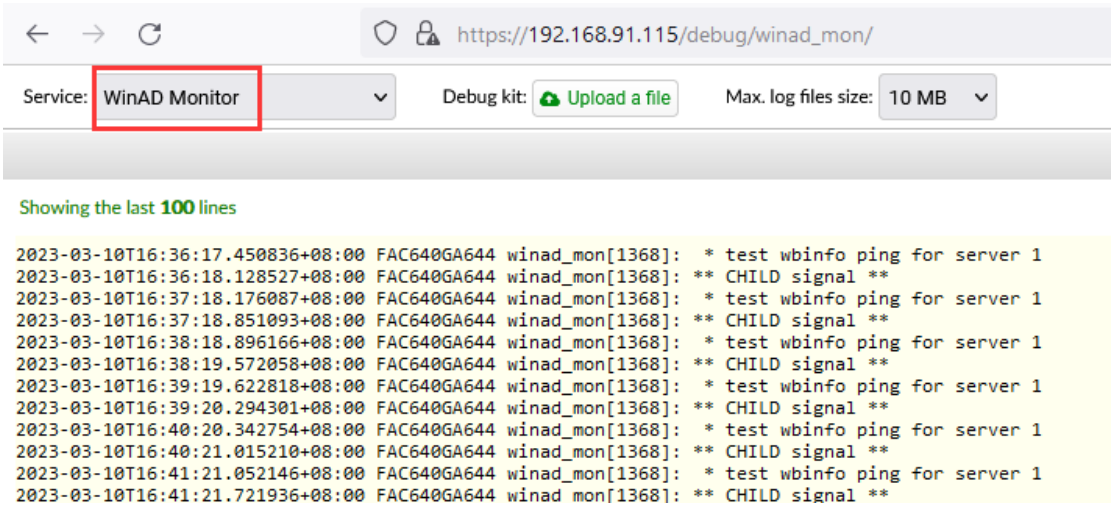
- 需要确认一下 FAC 的时间跟 AD 域的时间是否一致
- 其次需要确认相关设置是否正确:



包括上面 FAC NetBIOS 的名字以及帐号和密码是否正确和匹配. 比如要保证 FAC NetBIOS 没有使用过并且 AD 域内的设备没有只用这个名字;

- 如果已经加域成功了，但是想修改配置的登录帐号，也会导致 FAC 掉域，如果要修改登录帐号，则必须同时修改 FAC NetBIOS 名字.

- 检查 FAC 加域的 debug 日志



- 最后如果不好定位问题，需要在 FAC 上抓 FAC 跟 AD 域之间的通讯报文来分析这个问题;

2.8 HA A-P 模式无法建立或配置不同步

- 首先需要检查 FAC 设备是否型号和软件版本都一致
- 登录 FAC 的命令行, ping 一下对端 FAC 的管理地址;
- 抓 FAC 的管理接口报文，检查 FAC 之间的心跳通讯是否正常, FAC 之间会基于心跳接口建立 vpn 通道，使用 UDP port 720 和 169.254.0.x 的地址来通讯，一般来说主机地址是 169.254.0.1，备机地址是 169.254.0.2，这两个地址可以互相 ping 通;
- 检查一下 FAC 的 HA debug 日志，https://fac_ip/debug/slony/

2.9 HA LB 模式无法建立或配置不同步

- 检查 FAC 之间是否有基于 UDP port 721 的通讯, FAC 基于此端口来建立链接;
- 检查 FAC 之间基于 UDP port 1194 的通讯, FAC 之间基于此端口进行通讯;
- 如果链接有问题，可以在 LB Node 的"HA Status"页面点击"Reconnect" 来重新建立链接;
- 可以在 LB node 的 https://fac_lb_node_ip/debug/lb/ 页面检查 LB Node 与 Master 之间的通讯的 debug 日志;
- 如果配置不同步，可以在 LB Node 的"HA Status"页面点击"Rebuild Tables" 来出发配置重新同步;
- 可以在 LB node 的 https://fac_lb_node_ip/debug/lb_sync/ 页面检查 LB Node 与 Master 之间的配置同步的 debug 日志;