# Configuring RADIUS and Remote Authentication Servers using FortiAuthenticator and BuyPass Code

*Shanaz Khan*
*SE Fortinet Norway*

## Topology

FortiAuthenticator configured as a RADIUS server and connected to LDAP and FortiGate.

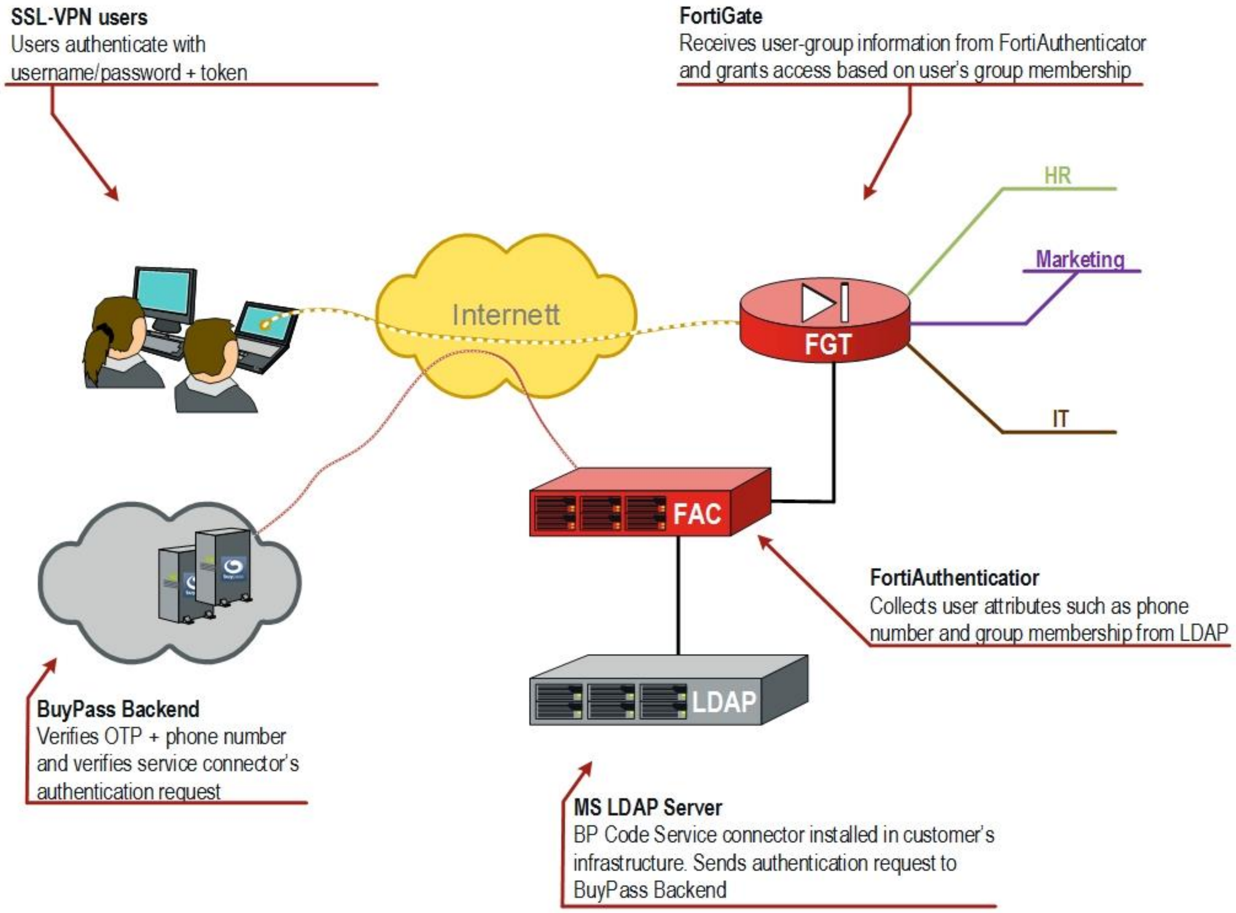

SSL-VPN users
Users authenticate with username/password + token
FortiGate
Receives user-group information from FortiAuthenticator and grants access based on user's group membership
HR
Marketing
IT
Internett
FGT
FAC
FortiAuthenticatior
Collects user attributes such as phone number and group membership from LDAP
LDAP
BuyPass Backend
Verifies OTP + phone number and verifies service connector's authentication request
MS LDAP Server
BP Code Service connector installed in customer's infrastructure. Sends authentication request to BuyPass Backend

Figure 1 Sample topology

The configuration discussed in this document was tested with the following setup for users, groups, and, memberships:

| Group | Member | Resource |
|---|---|---|
| IT | dollyduck | Esxi Server (10.188.10.10) |
| HR | donaldduck | FAZ (10.188.2.5) |
| Marketing | mickeymouse | FML (10.188.100.10) |

Table 1 Users' access to resources

## Software versions

The configuration discussed in this document was tested with the following firmware versions:

- FortiAuthenticator  GA 6.0.1
- FortiGate 6.2.0
- Windows Server 2016
- Windows 10
- BuyPass Code Service Connector
- BuyPass Code token App for mobile phone

## Prerequisites

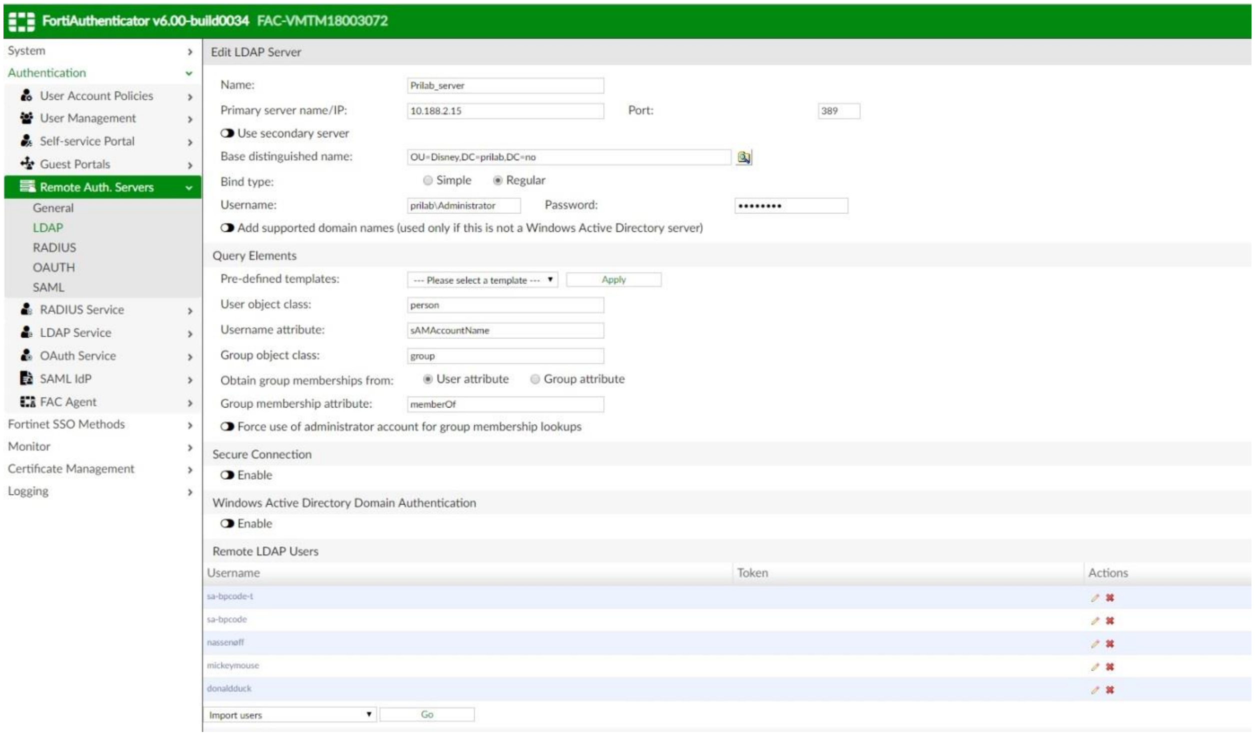
This documentation is based on BuyPass Service Connector already installed on MS LDAP server as well as the necessary users and groups defined in customer's AD domain structure.

## FortiAuthenticator basic setup

1) Configure IP and DNS on the FortiAuthenticator

## Configure Remote Auth. Servers (LDAP)

1) Go to **Authentication** -> **Remote Authentication Servers** -> **LDAP** and select **Create New**
2) Enter the remote LDAP server information



Edit LDAP Server

Name: Prilab_server

Primary server name/IP: 10.188.2.15 Port: 389

◑ Use secondary server

Base distinguished name: OU=Disney,DC=prilab,DC=no

Bind type: ○ Simple ● Regular

Username: prilab\Administrator Password: ••••••••

◑ Add supported domain names (used only if this is not a Windows Active Directory server)

Query Elements

Pre-defined templates: --- Please select a template --- ▾ Apply

User object class: person

Username attribute: sAMAccountName

Group object class: group

Obtain group memberships from: ● User attribute ○ Group attribute

Group membership attribute: memberOf

◑ Force use of administrator account for group membership lookups

Secure Connection

◑ Enable

Windows Active Directory Domain Authentication

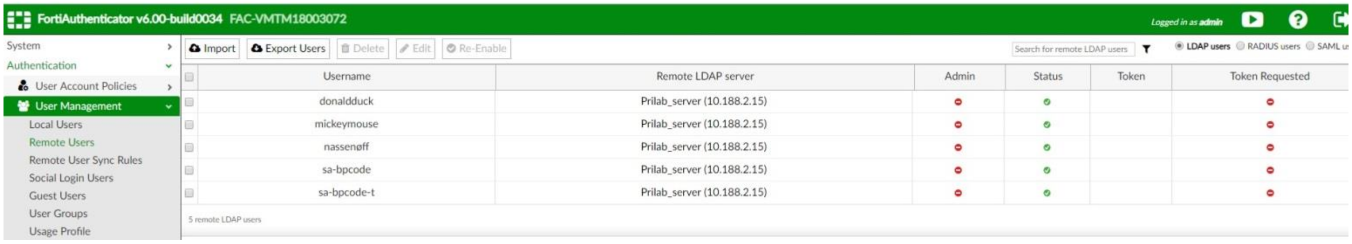
◑ Enable

Remote LDAP Users

| Username | Token | Actions |
|---|---|---|
| sa-bpcode-t | | ✎ ✖ |
| sa-bpcode | | ✎ ✖ |
| nassenøff | | ✎ ✖ |
| mickeymouse | | ✎ ✖ |
| donaldduck | | ✎ ✖ |

Import users ▾ Go

3) You should able to see the LDAP users replicated under **Remote Users**

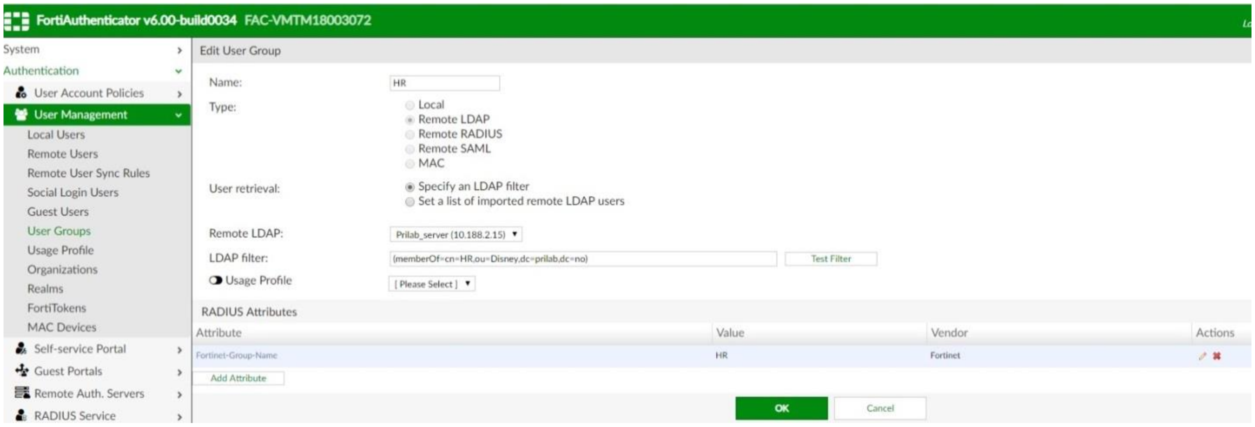


| □ | Username | Remote LDAP server | Admin | Status | Token | Token Requested |
|---|---|---|---|---|---|---|
| □ | donaldduck | Prilab_server (10.188.2.15) | ⊖ | ✓ | | ⊖ |
| □ | mickeymouse | Prilab_server (10.188.2.15) | ⊖ | ✓ | | ⊖ |
| □ | nassenøff | Prilab_server (10.188.2.15) | ⊖ | ✓ | | ⊖ |
| □ | sa-bpcode | Prilab_server (10.188.2.15) | ⊖ | ✓ | | ⊖ |
| □ | sa-bpcode-t | Prilab_server (10.188.2.15) | ⊖ | ✓ | | ⊖ |

5 remote LDAP users

## Create User Group

1) Go to **User Management** -> **User Groups** -> **Create New**
2) Select **Type** Remote LDAP
3) **User retrieval**: Specify an LDAP filter
4) **Remote LDAP**: Select a remote LDAP server
5) **LDAP filter**: specify a filter and Test Filter to verify the correct user(s) in the group
6) **Radius Attributes** -> **Add Attribute**. **Vendor**: Fortinet, **Attribute ID**: Fortinet-Group-Name. **Value**: HR (repeat the above steps for the all necessary groups, in this case HR, IT, Marketing SSLVPN)



Edit User Group

Name: HR

Type: ○ Local ● Remote LDAP ○ Remote RADIUS ○ Remote SAML ○ MAC

User retrieval: ● Specify an LDAP filter ○ Set a list of imported remote LDAP users

Remote LDAP: Prilab_server (10.188.2.15) ▾

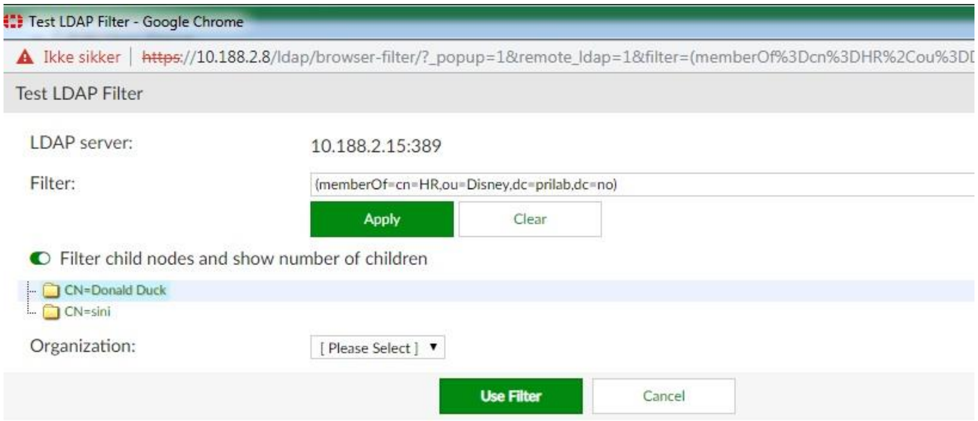
LDAP filter: (memberOf=cn=HR,ou=Disney,dc=prilab,dc=no)

Usage Profile: [ Please Select ] ▾

RADIUS Attributes

| Attribute | Value | Vendor | Actions |
|---|---|---|---|
| Fortinet-Group-Name | HR | Fortinet | |

Note – the Value for this attribute (HR in the above example) is the attribute sent with every user member of the LDAP group specified, and this is what FortiGate uses to match users against its local group.



~~https~~://10.188.2.8/ldap/browser-filter/?_popup=1&remote_ldap=1&filter=(memberOf%3Dcn%3DHR%2Cou%3DI

Test LDAP Filter

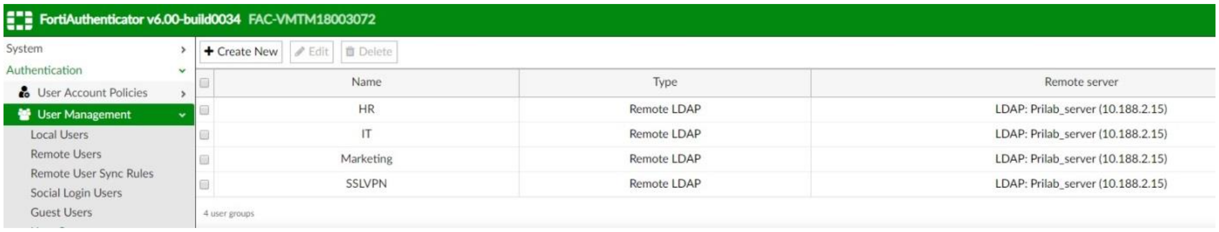
LDAP server: 10.188.2.15:389

Filter: (memberOf=cn=HR,ou=Disney,dc=prilab,dc=no)

Filter child nodes and show number of children

- CN=Donald Duck
- CN=sini

Organization: [ Please Select ] ▾

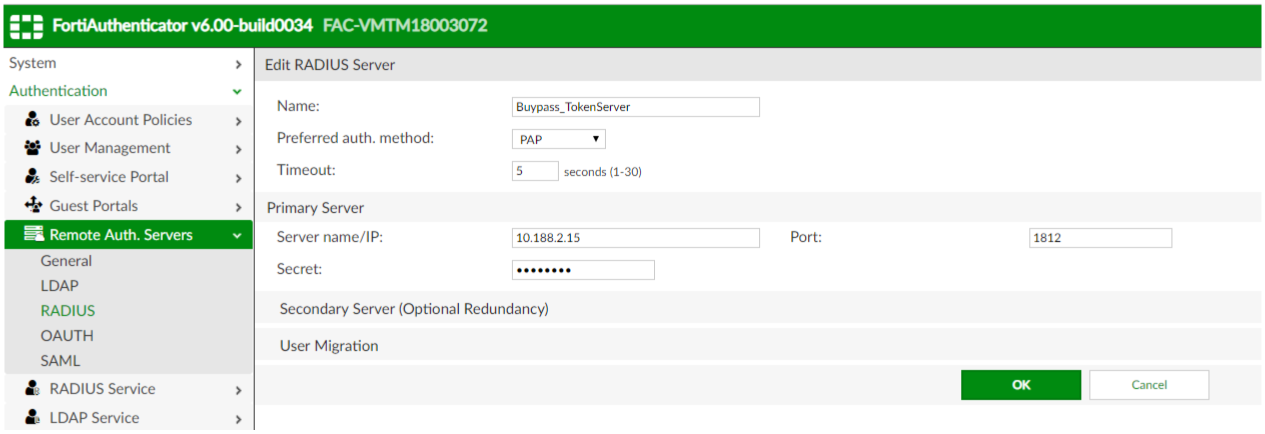


| Name | Type | Remote server |
|---|---|---|
| HR | Remote LDAP | LDAP: Prilab_server (10.188.2.15) |
| IT | Remote LDAP | LDAP: Prilab_server (10.188.2.15) |
| Marketing | Remote LDAP | LDAP: Prilab_server (10.188.2.15) |
| SSLVPN | Remote LDAP | LDAP: Prilab_server (10.188.2.15) |

4 user groups

## Remote Authentication Servers

1) Go to **Remote Auth. Servers** -> **RADIUS** -> **Create New**
2) Give it a suitable new, in this sample configuration we'll call it BuyPass_TokenServer
3) **Preferred auth. method**: select appropriate method (must be same as in RADIUS configuration on Fortigate)
4) **Servername/IP**: IP address of the server where the BuyPass Code Service Connector is running (in this sample configuration, BPSC is running on the Domain Controller)
5) **Port**: 1812, **Secret**: must be same as in RADIUS configuration on Fortigate)



Edit RADIUS Server

Name: Buypass_TokenServer

Preferred auth. method: PAP

Timeout: 5 seconds (1-30)

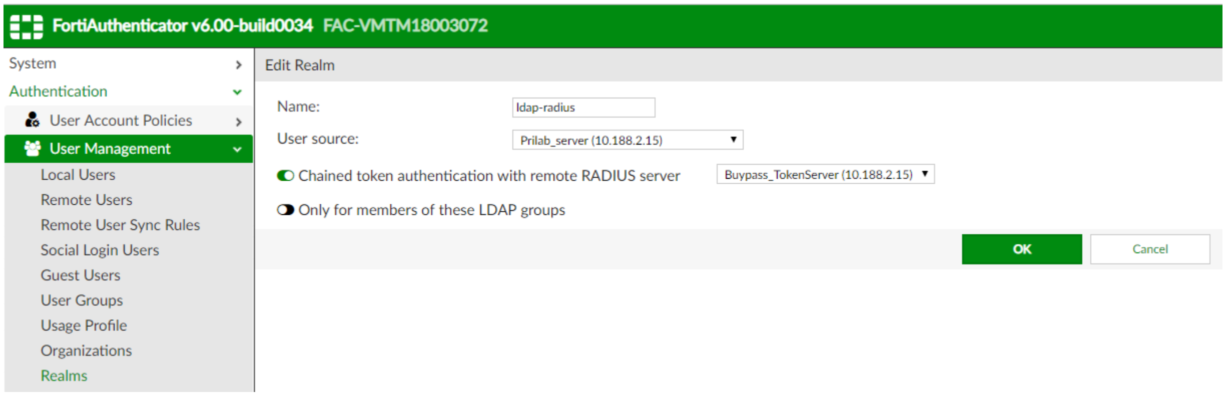
Primary Server

Server name/IP: 10.188.2.15 Port: 1812

Secret: ••••••••

## Realms

1) Go to **Authentication** -> **User Management** **->** **Realms** -> **Create New**
2) Create a new realm pointing to your LDAP server.
3) **Chained token authentication with remote RADIUS server:** select the RADIUS server created in previous step (Remote Auth.Servers)



Edit Realm

Name: ldap-radius

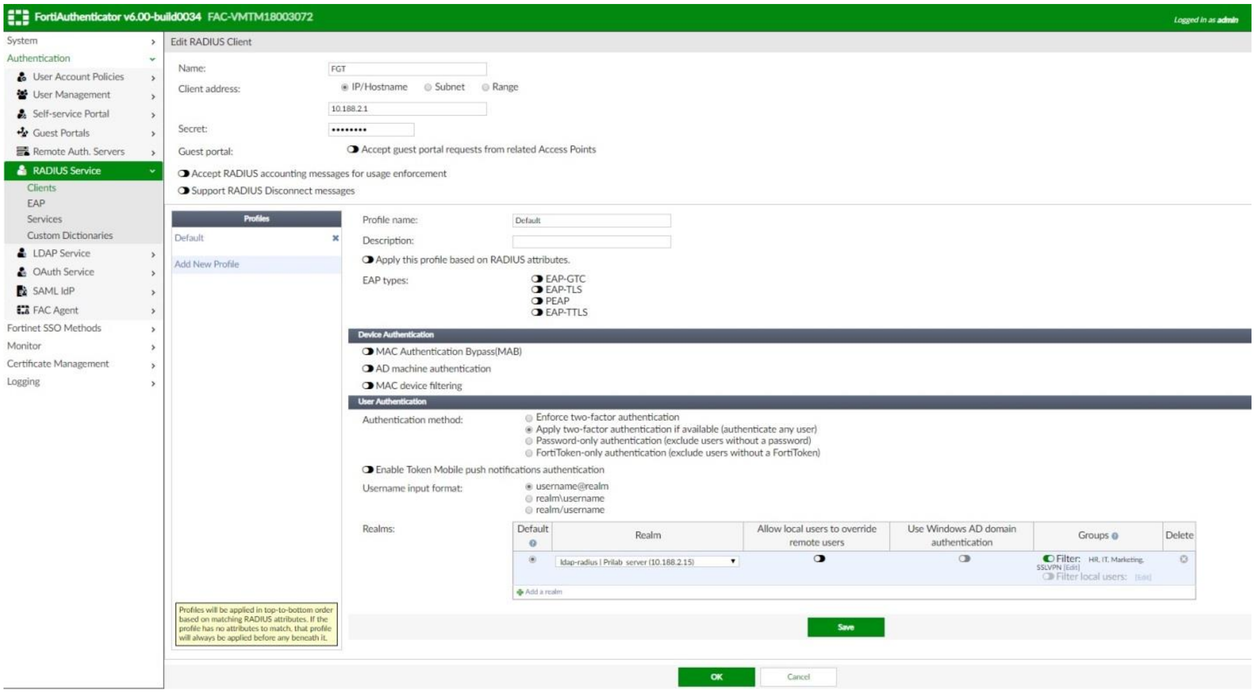
User source: Prilab_server (10.188.2.15)

Chained token authentication with remote RADIUS server: Buypass_TokenServer (10.188.2.15)

Only for members of these LDAP groups

## Configuring RADIUS client

1) Go to **Authentication** -> **RADIUS Services** -> **Clients**
2) **Client name/IP**: the IP address of the FortiGate
3) **Secret**: The RADIUS passphrase that the FortiGate unit will use



Edit RADIUS Client

Name: FGT

Client address: ● IP/Hostname ○ Subnet ○ Range

10.188.2.1

Secret: ••••••••

Guest portal: Accept guest portal requests from related Access Points

Accept RADIUS accounting messages for usage enforcement

Support RADIUS Disconnect messages

Profile name: Default

Description:

Apply this profile based on RADIUS attributes.

EAP types: EAP-GTC, EAP-TLS, PEAP, EAP-TTLS

MAC Authentication Bypass(MAB)

AD machine authentication

MAC device filtering

Authentication method:
○ Enforce two-factor authentication
● Apply two-factor authentication if available (authenticate any user)
○ Password-only authentication (exclude users without a password)
○ FortiToken-only authentication (exclude users without a FortiToken)

Enable Token Mobile push notifications authentication

Username input format:
● username@realm
○ realm\username
○ realm/username

Realms:

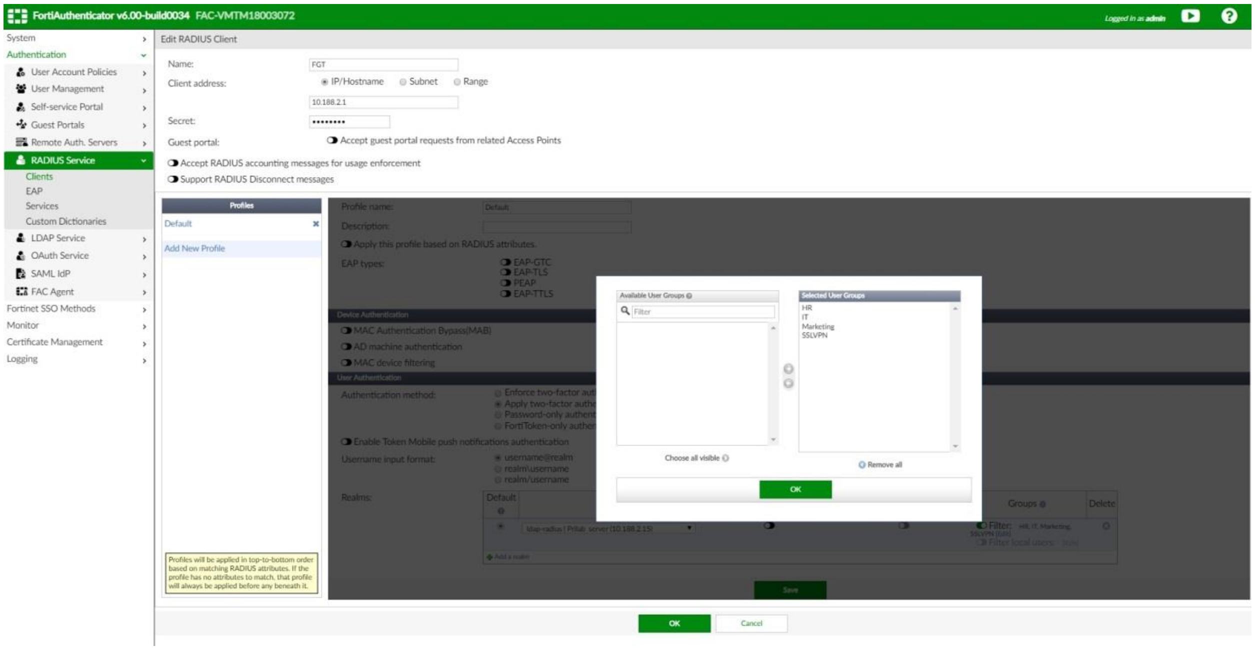
| Default | Realm | Allow local users to override remote users | Use Windows AD domain authentication | Groups | Delete |
|---|---|---|---|---|---|
| ● | ldap-radius \| Prilab server (10.188.2.15) | | | Filter: HR, IT, Marketing, SSLVPN [Edit]<br>Filter local users: [Edit] | |

Profiles will be applied in top-to-bottom order based on matching RADIUS attributes. If the profile has no attributes to match, that profile will always be applied before any beneath it.

4) Keep **Default** profile. **User Authentication** -> **Authentication method**: *Apply two-factor authentication if available (authenticate any user)*
5) **Realms**
   I. Select the remote realm we created in **Realms**

II. **Groups**: enable filter and select the local group(s) we created in **User Groups** (no need to enable Allow local users to override remote users + Use Windows AD domain authentication)

III. **Groups**: enable filter and select the local group we created in **User Groups. Save -> OK**



FortiAuthenticator v6.00-build0034 FAC-VMTM18003072

Edit RADIUS Client

Name: FGT

Client address: ● IP/Hostname ○ Subnet ○ Range

10.188.2.1

Secret: ••••••••

Guest portal: Accept guest portal requests from related Access Points

Accept RADIUS accounting messages for usage enforcement

Support RADIUS Disconnect messages

Profiles: Default, Add New Profile

Profile name: Default

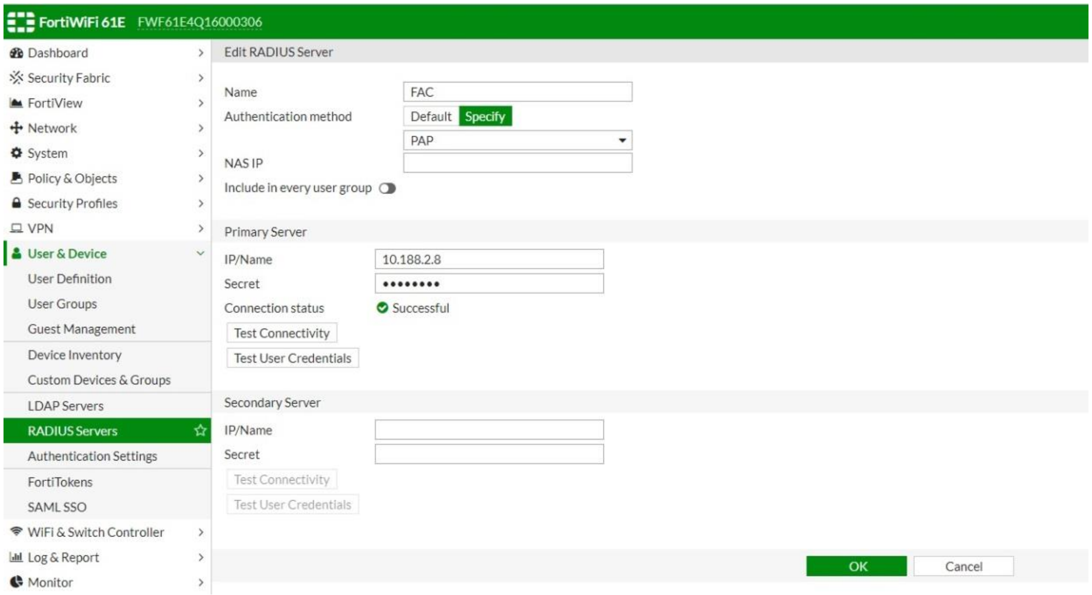
Profiles will be applied in top-to-bottom order based on matching RADIUS attributes. If the profile has no attributes to match, that profile will always be applied before any beneath it.

Selected User Groups: HR, IT, Marketing, SSLVPN

Realms: ldap-radius | Prilab server (10.188.2.15) — Filter: HR, IT, Marketing, SSLVPN

## Configure the FortiGate for RADIUS authentication

- Go to **User & Device** -> **RADIUS Servers** and select **Create New**



FortiWiFi 61E FWF61E4Q16000306

Edit RADIUS Server

Name: FAC

Authentication method: Default [✓ Specify]

PAP

NAS IP:

Include in every user group: off

Primary Server

IP/Name: 10.188.2.8

Secret: ••••••••

Connection status: Successful

Secondary Server

IP/Name:

Secret:

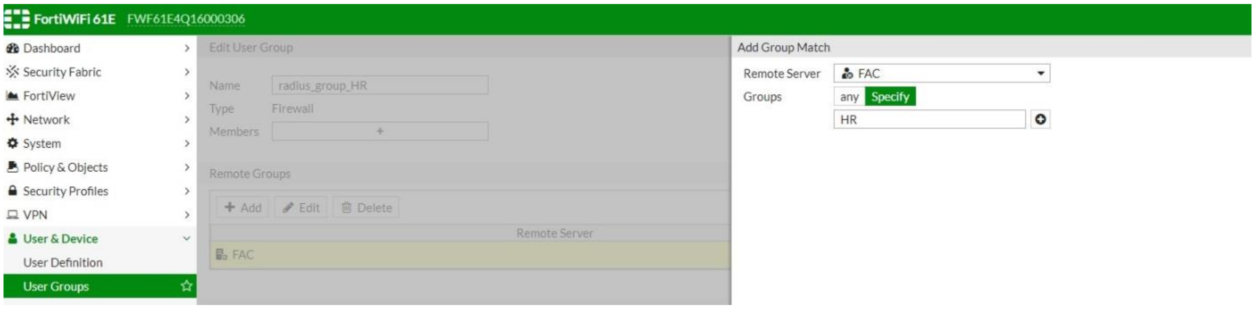
- **Name**: the FortiAuthenticator, in this case called FAC. Specify Authentication method and IP address of the FortiAuthenticator (FAC).
- **Secret**: same passphrase as specified for RADIUS Client configuration on FortiAuthenticator.
- **Test Connectivity**: verify the connection between FortiGate and FortiAuthenticator.

## User Groups

We need to create local groups on Fortigate, corresponding to the groups created on FortiAuthenticator (HR, IT, Marketing, SSLVPN)

1) **User & Device** -> **User Groups** and select **Create New**
2) **Name**: Give it a suitable **name**
3) **Type**: Firewall
4) **Remote Groups** -> **Add** and select the remote RADIUS Server created previously (fac).
5) **Groups: Specify** and give it a name (corresponding to FortiAuthenticator group name)

Note – By default this value is '*Any*', and with this value, FortiGate will ignore radius attributes received. So in order to match attribute HR, instead of *Any*, select HR.



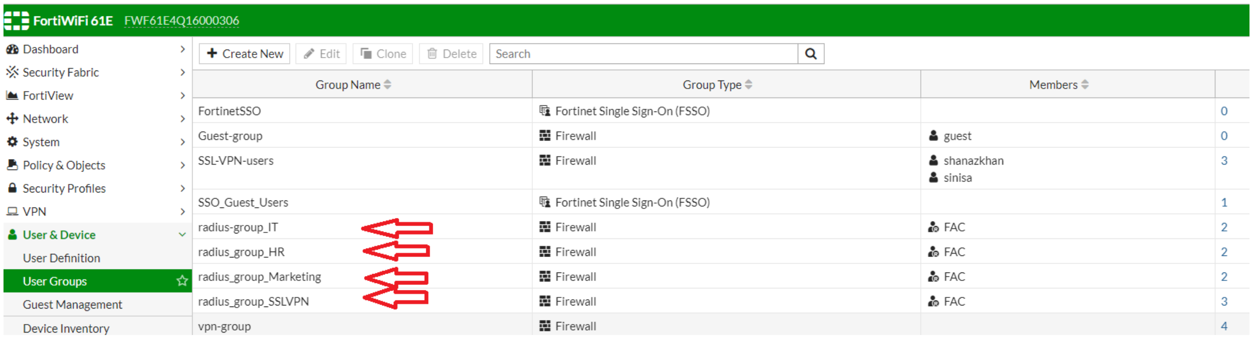
Name: radius_group_HR
Type: Firewall
Members:

| Remote Server |
|---|
| FAC |

Remote Server: FAC
Groups: any [✓ Specify]
HR

Now every user that arrives with e.g. an attribute 'HR' will be matched against *radius_group_HR* group.

Repeat the above steps for all necessary groups (in this case, HR, IT, Marketing, SSLVPN)

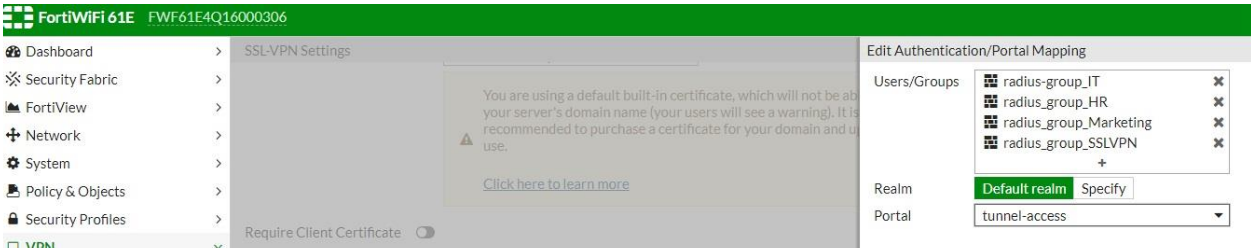


| Group Name | Group Type | Members | |
|---|---|---|---|
| FortinetSSO | Fortinet Single Sign-On (FSSO) | | 0 |
| Guest-group | Firewall | guest | 0 |
| SSL-VPN-users | Firewall | shanazkhan<br>sinisa | 3 |
| SSO_Guest_Users | Fortinet Single Sign-On (FSSO) | | 1 |
| radius-group_IT | Firewall | FAC | 2 |
| radius_group_HR | Firewall | FAC | 2 |
| radius_group_Marketing | Firewall | FAC | 2 |
| radius_group_SSLVPN | Firewall | FAC | 3 |
| vpn-group | Firewall | | 4 |

## SSL VPN Settings

**VPN** -> **SSL-VPN Settings**

- Specify **Listen on Interface(s)** – in this case wan1 + **Listen on port** 10443
- **Restrict Access**: Allow access from any host
- **Tunnel Mode Client settings** -> Address Range: Automatically assign addresses
- Specify **DNS Server(s)**
- **Authentication/Portal Mapping**: Create New, select the necessary group(s), keep default **realm** and assign **portal** tunnel-access



You are using a default built-in certificate, which will not be ab your server's domain name (your users will see a warning). It is recommended to purchase a certificate for your domain and u use.

Click here to learn more

Require Client Certificate

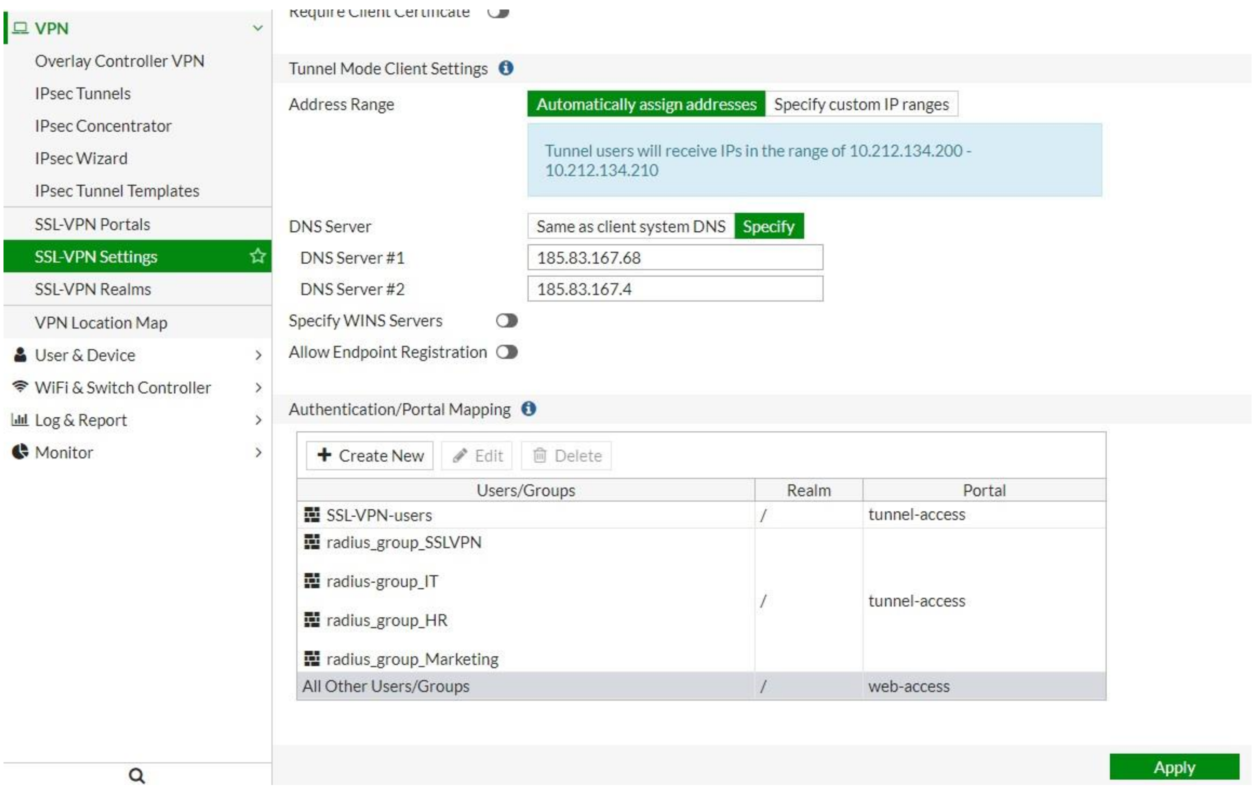
Edit Authentication/Portal Mapping

Users/Groups: radius-group_IT, radius_group_HR, radius_group_Marketing, radius_group_SSLVPN

Realm: Default realm | Specify

Portal: tunnel-access

All the necessary groups will now show up in the Authentication/Portal Mapping window:



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

DNS Server #1: 185.83.167.68

DNS Server #2: 185.83.167.4

Specify WINS Servers

Allow Endpoint Registration

Authentication/Portal Mapping

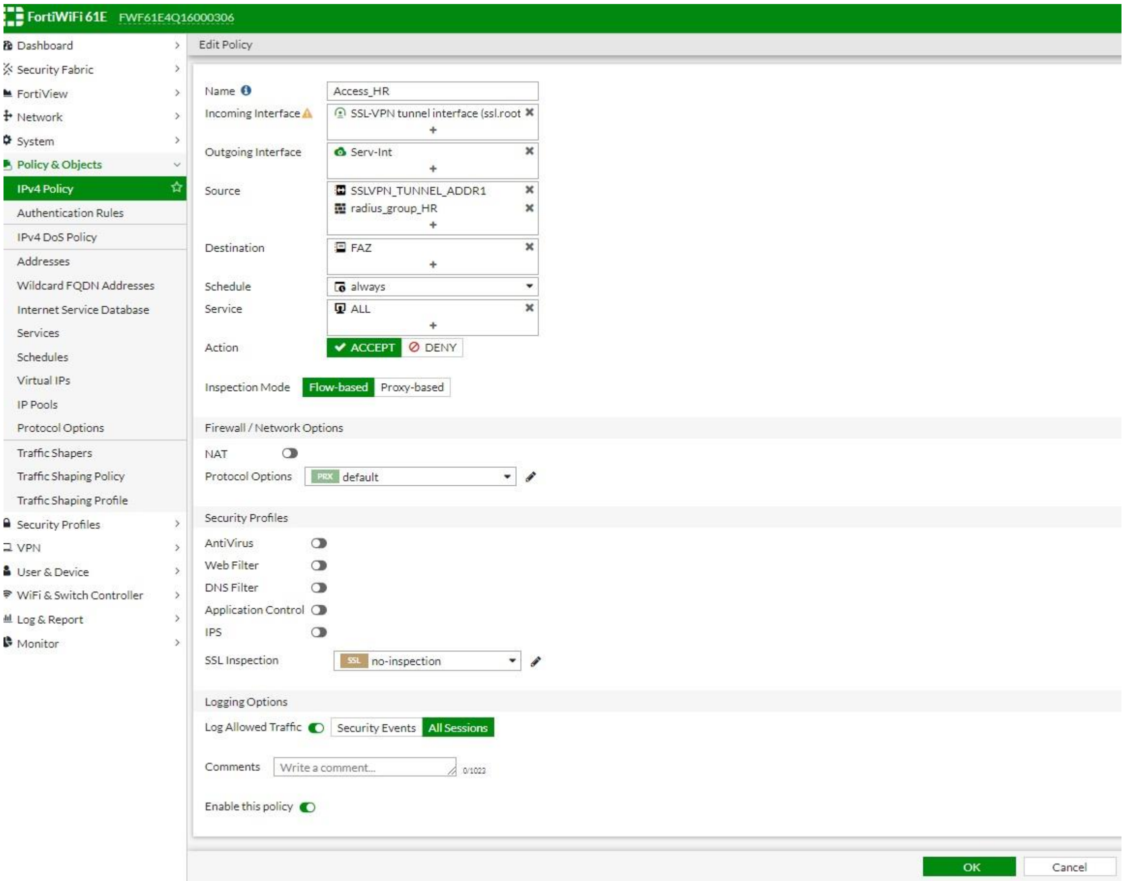
| Users/Groups | Realm | Portal |
|---|---|---|
| SSL-VPN-users | / | tunnel-access |
| radius_group_SSLVPN<br>radius-group_IT<br>radius_group_HR<br>radius_group_Marketing | / | tunnel-access |
| All Other Users/Groups | / | web-access |

## SSL-VPN Portals

- Edit **tunnel-access**, make sure that **Tunnel mode** is enabled
- **Enable Split Tunneling:** when enabled, only traffic that matches the destination address in the respective policy will be routed through the tunnel. (In this case, split tunneling is not enabled as I wish my test users to also access Internet through the tunnel).
- **Source IP Pools:** select SSLVPN_TUNNEL_ADDR1 (automatically created in the tunnel mode client settings)

## Firewall Policies

- Create policies to grant access to your users connecting though SSLVPN. This is also where we grant users access to resources based on their group membership.



Edit Policy

| | |
|---|---|
| Name | Access_HR |
| Incoming Interface | SSL-VPN tunnel interface (ssl.root |
| Outgoing Interface | Serv-Int |
| Source | SSLVPN_TUNNEL_ADDR1<br>radius_group_HR |
| Destination | FAZ |
| Schedule | always |
| Service | ALL |
| Action | ACCEPT |
| Inspection Mode | Flow-based |

Firewall / Network Options

| | |
|---|---|
| NAT | ○ |
| Protocol Options | PRX default |

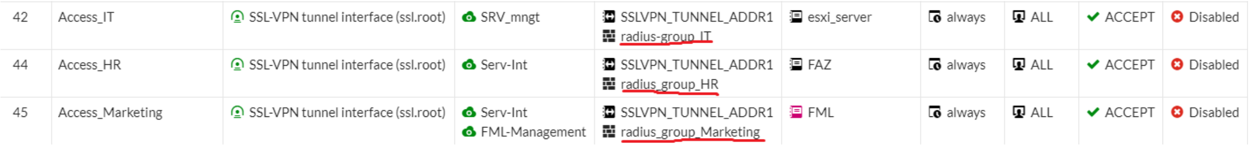
Security Profiles

| | |
|---|---|
| AntiVirus | ○ |
| Web Filter | ○ |
| DNS Filter | ○ |
| Application Control | ○ |
| IPS | ○ |
| SSL Inspection | SSL no-inspection |

Logging Options

| | |
|---|---|
| Log Allowed Traffic | ● All Sessions |
| Comments | Write a comment... 0/1023 |
| Enable this policy | ● |

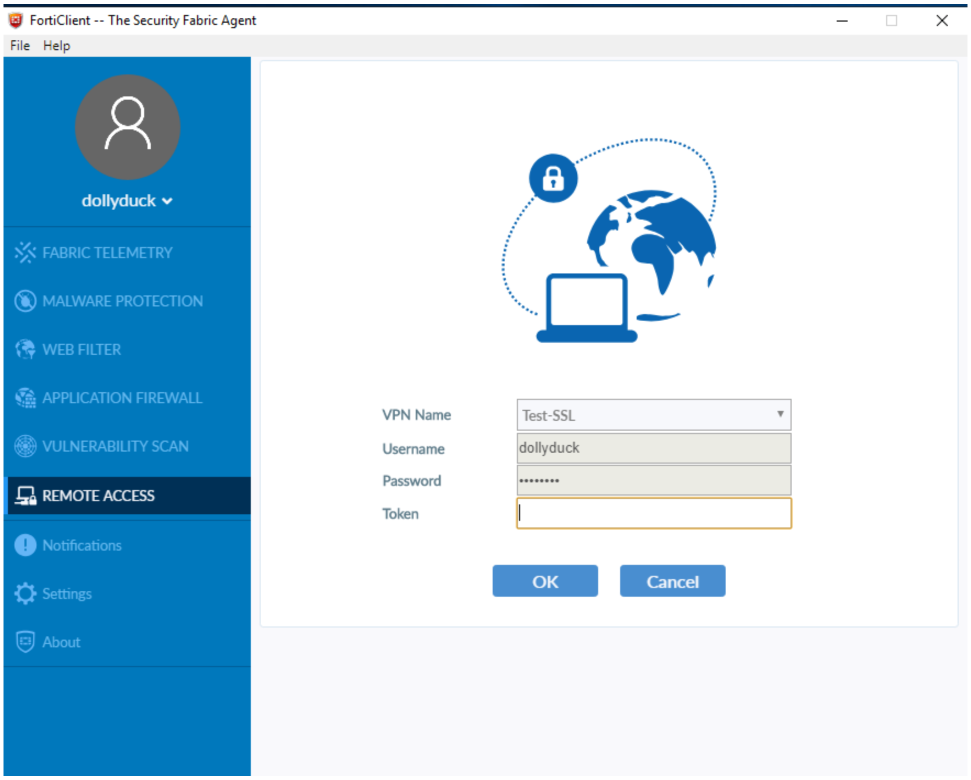
- Create a separate policy for each group, with the same Incoming Interface – *SSLVPN tunnel interface (ssl.root)*. The differentiator will be the source groups we add in addition to *SSLVPN_TUNNEL_ADDR1*



| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 42 | Access_IT | SSL-VPN tunnel interface (ssl.root) | SRV_mngt | SSLVPN_TUNNEL_ADDR1<br>radius-group_IT | esxi_server | always | ALL | ✓ ACCEPT | Disabled |
| 44 | Access_HR | SSL-VPN tunnel interface (ssl.root) | Serv-Int | SSLVPN_TUNNEL_ADDR1<br>radius_group_HR | FAZ | always | ALL | ✓ ACCEPT | Disabled |
| 45 | Access_Marketing | SSL-VPN tunnel interface (ssl.root) | Serv-Int<br>FML-Management | SSLVPN_TUNNEL_ADDR1<br>radius_group_Marketing | FML | always | ALL | ✓ ACCEPT | Disabled |

## Testing

- Once you've completed the above configuration, you can test connecting a user to SSL-VPN, e.g. our test user dollyduck:



VPN Name: Test-SSL

Username: dollyduck

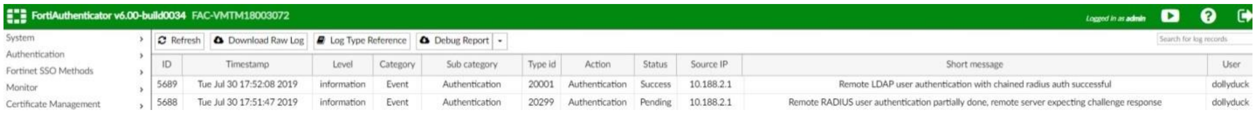
Password: ••••••••

Token:

The test user is asked for Token after username/password. BuyPass token code is typed and the test user connects successfully, as shown in FortiAuthenticator logs

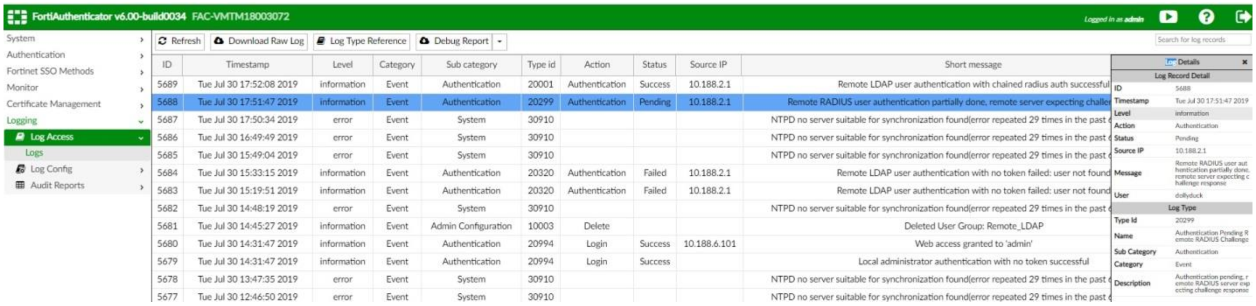
## Fortiauthenticator Logs

- FortiAuthenticator logs shows successful connection.



| ID | Timestamp | Level | Category | Sub category | Type id | Action | Status | Source IP | Short message | User |
|---|---|---|---|---|---|---|---|---|---|---|
| 5689 | Tue Jul 30 17:52:08 2019 | information | Event | Authentication | 20001 | Authentication | Success | 10.188.2.1 | Remote LDAP user authentication with chained radius auth successful | dollyduck |
| 5688 | Tue Jul 30 17:51:47 2019 | information | Event | Authentication | 20299 | Authentication | Pending | 10.188.2.1 | Remote RADIUS user authentication partially done, remote server expecting challenge response | dollyduck |

- View log details. The detailed logs may also be useful for troubleshooting

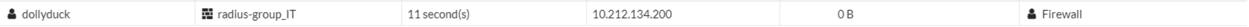


| ID | Timestamp | Level | Category | Sub category | Type id | Action | Status | Source IP | Short message |
|---|---|---|---|---|---|---|---|---|---|
| 5689 | Tue Jul 30 17:52:08 2019 | information | Event | Authentication | 20001 | Authentication | Success | 10.188.2.1 | Remote LDAP user authentication with chained radius auth successful |
| 5688 | Tue Jul 30 17:51:47 2019 | information | Event | Authentication | 20299 | Authentication | Pending | 10.188.2.1 | Remote RADIUS user authentication partially done, remote server expecting challe |
| 5687 | Tue Jul 30 17:50:34 2019 | error | Event | System | 30910 | | | | NTPD no server suitable for synchronization found(error repeated 29 times in the past |
| 5686 | Tue Jul 30 16:49:49 2019 | error | Event | System | 30910 | | | | NTPD no server suitable for synchronization found(error repeated 29 times in the past |
| 5685 | Tue Jul 30 15:49:04 2019 | error | Event | System | 30910 | | | | NTPD no server suitable for synchronization found(error repeated 29 times in the past |
| 5684 | Tue Jul 30 15:33:15 2019 | information | Event | Authentication | 20320 | Authentication | Failed | 10.188.2.1 | Remote LDAP user authentication with no token failed: user not found |
| 5683 | Tue Jul 30 15:19:51 2019 | information | Event | Authentication | 20320 | Authentication | Failed | 10.188.2.1 | Remote LDAP user authentication with no token failed: user not found |
| 5682 | Tue Jul 30 14:48:19 2019 | error | Event | System | 30910 | | | | NTPD no server suitable for synchronization found(error repeated 29 times in the past |
| 5681 | Tue Jul 30 14:45:27 2019 | information | Event | Admin Configuration | 10003 | Delete | | | Deleted User Group: Remote_LDAP |
| 5680 | Tue Jul 30 14:31:47 2019 | information | Event | Authentication | 20994 | Login | Success | 10.188.6.101 | Web access granted to 'admin' |
| 5679 | Tue Jul 30 14:31:47 2019 | information | Event | Authentication | 20994 | Login | Success | | Local administrator authentication with no token successful |
| 5678 | Tue Jul 30 13:47:35 2019 | error | Event | System | 30910 | | | | NTPD no server suitable for synchronization found(error repeated 29 times in the past |
| 5677 | Tue Jul 30 12:46:50 2019 | error | Event | System | 30910 | | | | NTPD no server suitable for synchronization found(error repeated 29 times in the past |

Log Details

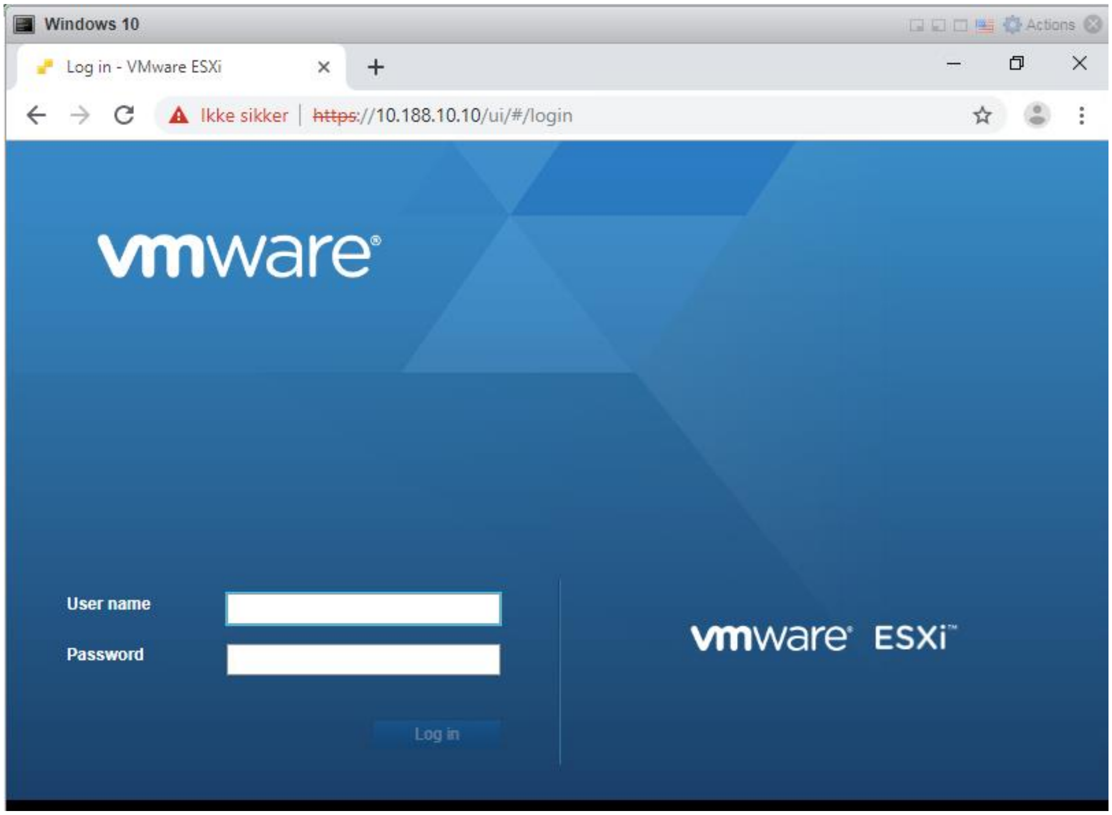
| Log Record Detail | |
|---|---|
| ID | 5688 |
| Timestamp | Tue Jul 30 17:51:47 2019 |
| Level | information |
| Action | Authentication |
| Status | Pending |
| Source IP | 10.188.2.1 |
| Message | Remote RADIUS user authentication partially done, remote server expecting challenge response |
| User | dollyduck |
| **Log Type** | |
| Type Id | 20299 |
| Name | Authentication Pending Remote RADIUS Challenge |
| Sub Category | Authentication |
| Category | Event |
| Description | Authentication pending, remote RADIUS server expecting challenge response |

On the FortiGate, Monitor → Firewall User Monitor displays our test user as connected:

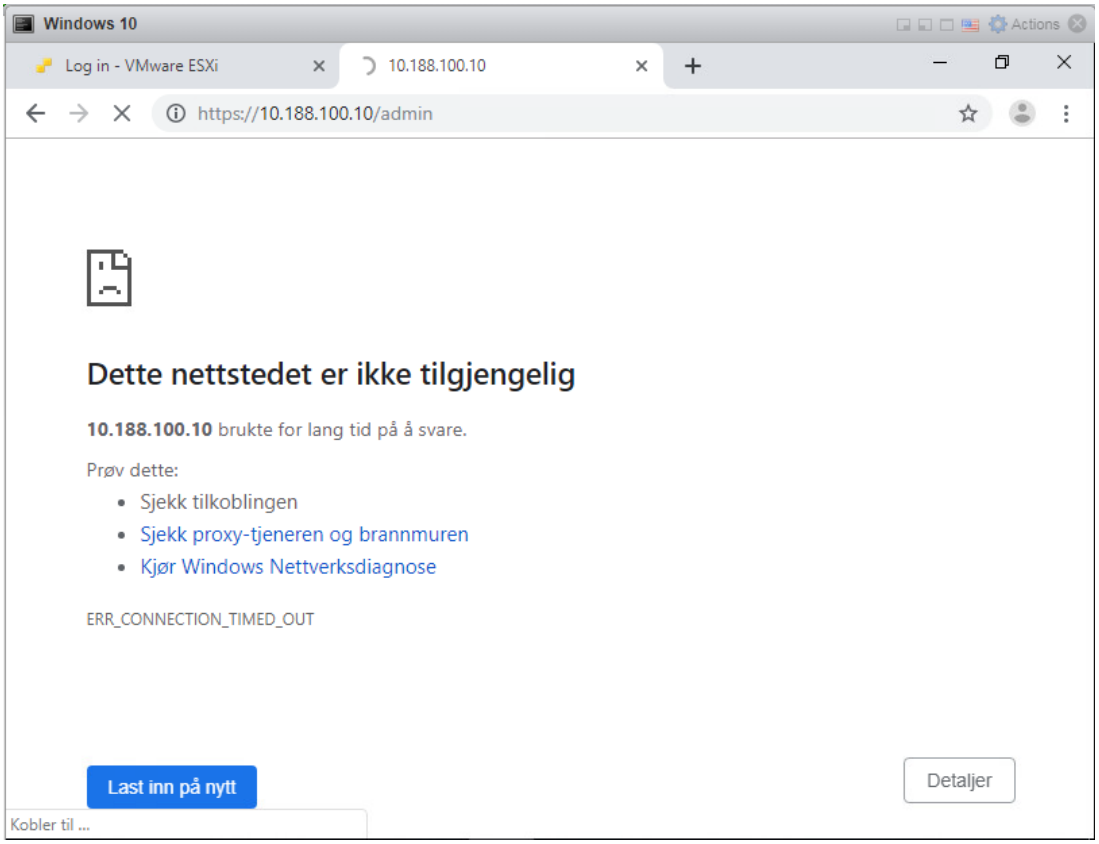


| | | | | | |
|---|---|---|---|---|---|
| dollyduck | radius-group_IT | 11 second(s) | 10.212.134.200 | 0 B | Firewall |

Test user may now access network resources according to defined security policies. In our sample configuration, test user dollyduck belongs to AD Group IT. Our FortiGate policies grant group IT access to the esxi server only:



The test user is not allowed to access e.g. FortiMail (10.188.100.10)



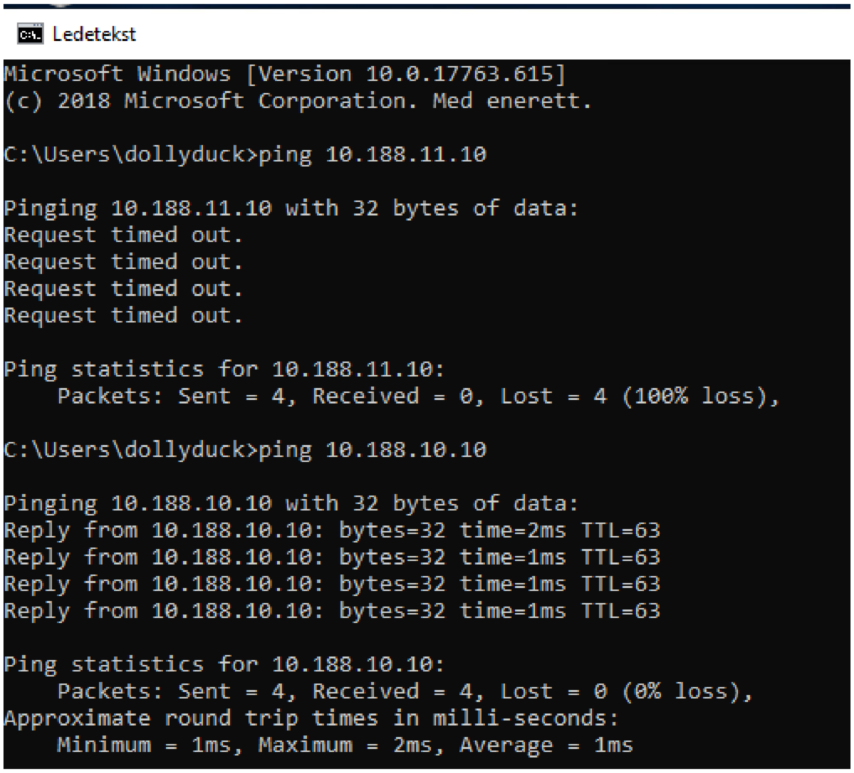
Dette nettstedet er ikke tilgjengelig

**10.188.100.10** brukte for lang tid på å svare.

Prøv dette:

- Sjekk tilkoblingen
- Sjekk proxy-tjeneren og brannmuren
- Kjør Windows Nettverksdiagnose

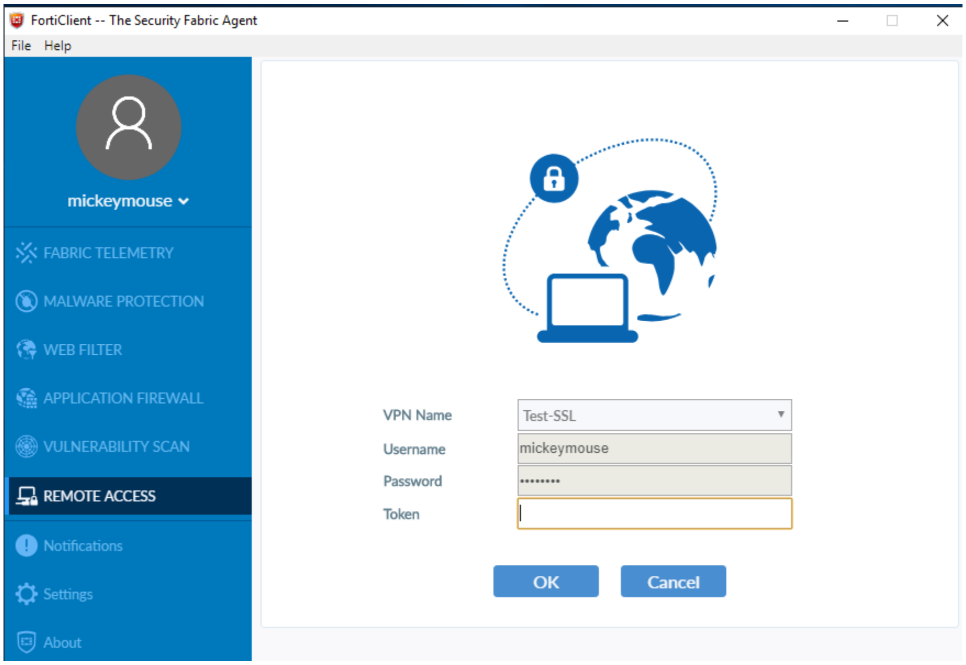
ERR_CONNECTION_TIMED_OUT



```
Microsoft Windows [Version 10.0.17763.615]
(c) 2018 Microsoft Corporation. Med enerett.

C:\Users\dollyduck>ping 10.188.11.10

Pinging 10.188.11.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.188.11.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\dollyduck>ping 10.188.10.10

Pinging 10.188.10.10 with 32 bytes of data:
Reply from 10.188.10.10: bytes=32 time=2ms TTL=63
Reply from 10.188.10.10: bytes=32 time=1ms TTL=63
Reply from 10.188.10.10: bytes=32 time=1ms TTL=63
Reply from 10.188.10.10: bytes=32 time=1ms TTL=63

Ping statistics for 10.188.10.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms
```

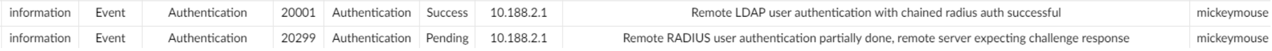
Let’s test with a user belonging to another group, e.g. mickeymouse → group Marketing.

As with test user donalduck, this test user is asked for buypass token in addition to username/password.



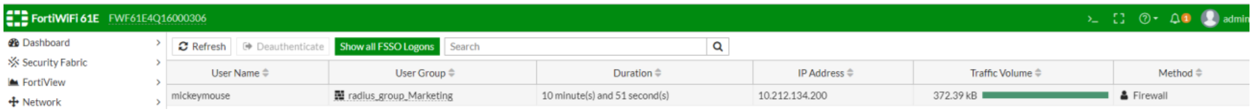
| | |
|---|---|
| VPN Name | Test-SSL |
| Username | mickeymouse |
| Password | •••••••• |
| Token | |

FortiAuthenticator verifies successful login



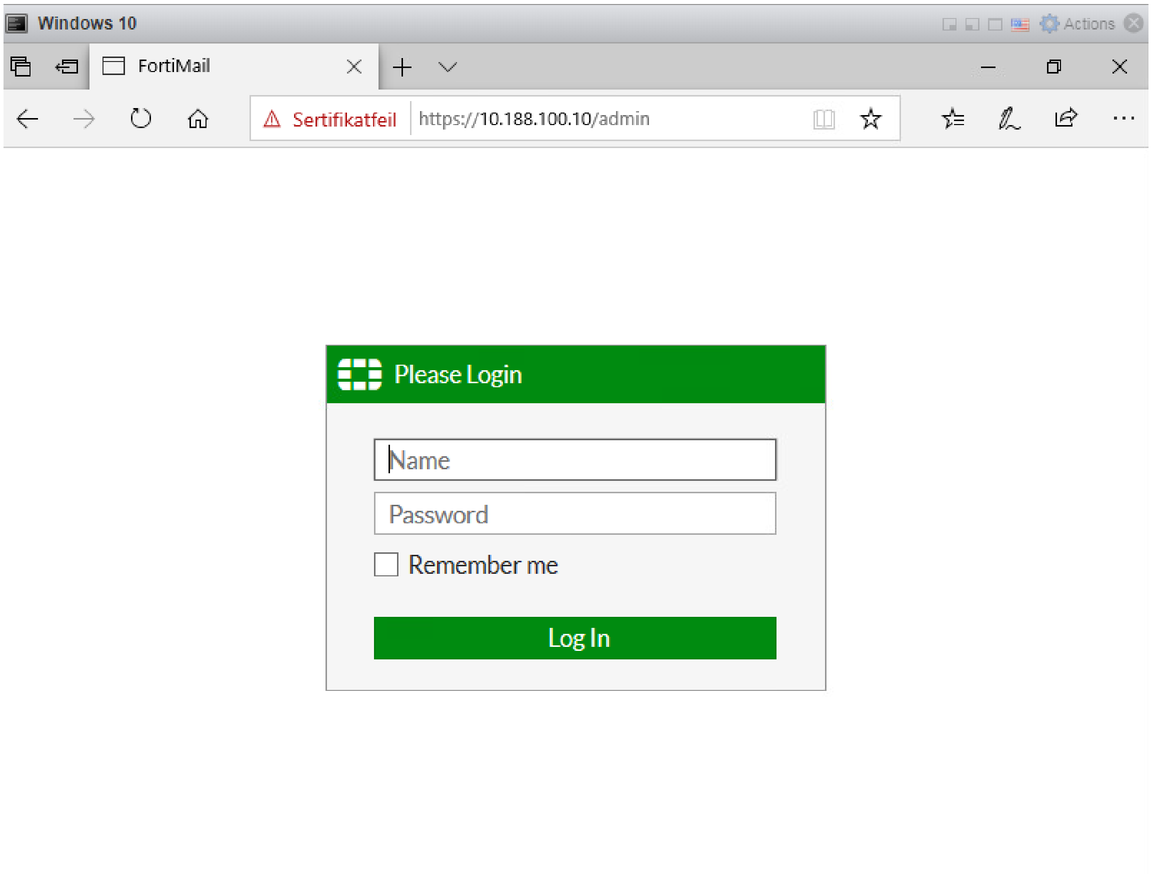
| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| information | Event | Authentication | 20001 | Authentication | Success | 10.188.2.1 | Remote LDAP user authentication with chained radius auth successful | mickeymouse |
| information | Event | Authentication | 20299 | Authentication | Pending | 10.188.2.1 | Remote RADIUS user authentication partially done, remote server expecting challenge response | mickeymouse |

FortiGate, Monitor → Firewall User Monitor, displays our test user as connected.



| User Name | User Group | Duration | IP Address | Traffic Volume | Method |
|---|---|---|---|---|---|
| mickeymouse | radius_group_Marketing | 10 minute(s) and 51 second(s) | 10.212.134.200 | 372.39 kB | Firewall |

Once connected, Test user mickey mouse has access to FortiMail, as per firewall policies.


Windows 10
Actions
FortiMail
Sertifikatfeil
https://10.188.100.10/admin
Please Login
Name
Password
□ Remember me
Log In