


# FortiADC Layer 7 Virtual Server with Kerberos Authentication Relay Deployment Guide

**FORTINET DOCUMENT LIBRARY**

http://docs.fortinet.com

**FORTINET VIDEO GUIDE**

http://video.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

**FORTIGATE COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**

http://www.fortinet.com/training

**FORTIGUARD CENTER**

http://www.fortiguard.com

**END USER LICENSE AGREEMENT**

http://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**

Email: techdocs@fortinet.com

January 8, 2019

Layer 7 Virtual Server with Kerberos Authentication Relay Deployment Guide

# TABLE OF CONTENTS

# Change Log

| Date | Change Description |
| --- | --- |
| 2019-01-09 | Initial release. |

# Introduction

This guide details the steps required to configure FortiADC Layer 7 Virtual Server with kerberos authentication relay based on V5.2 release.

# Overview

Kerberos authentication is a computer authentication protocol that works on the basis of tickets (i.e., credentials). It provides several authentication choices, allowing nodes communicating over a non-secure network to verify each others' identity securely via a Key Distribution Center (KDC) and Service Tickets (STs). It is primarily used for client-server authentication model and provides mutual authentication by which both the client and the server verify each others' identity.

Kerberos authentication is built upon symmetric key cryptography and requires a trusted third party, and may also resort to the use of public-key cryptography in certain phases of the authentication process. By default, Kerberos Authentication Relay uses UDP port 88.

The Kerberos authentication consists of the following logical components:

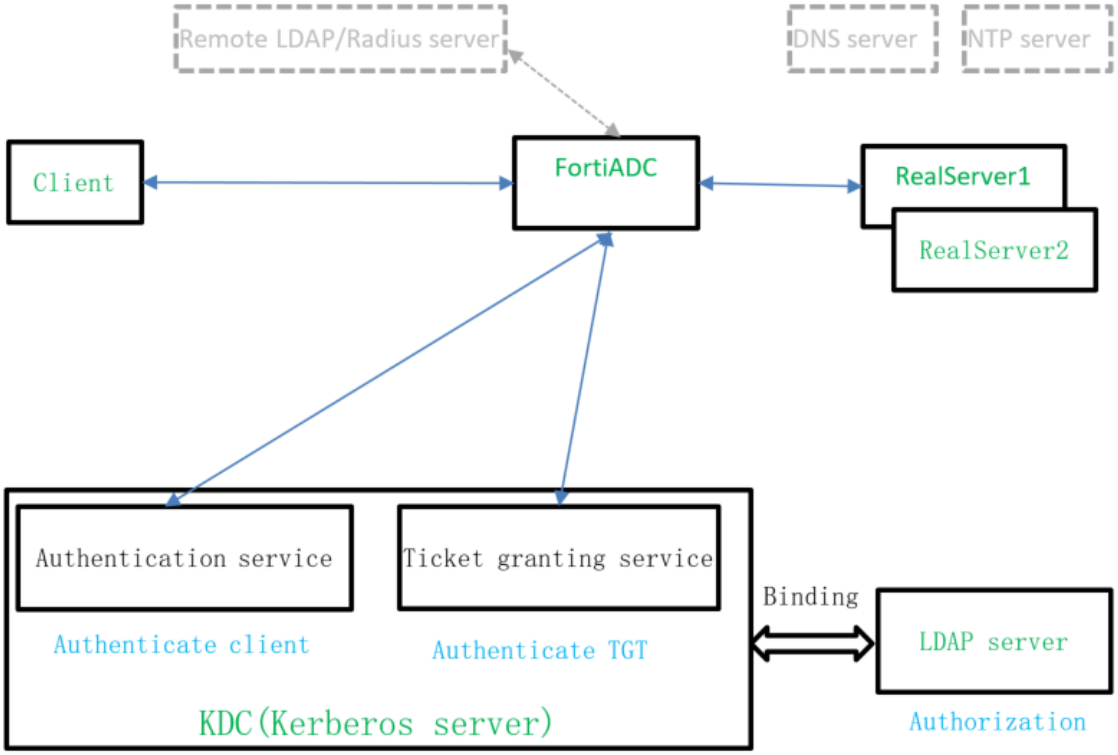
- Client
- Authentication Server (AS)
- Ticket Granting Server (TGS)
- Service Server (SS)

Often, the AS and TGS are located on the same physical server, i.e., the KDC.

If using Windows as authentication server, you will need to set up windows AD (Active Directory Domain services). Add proper Active directory users.

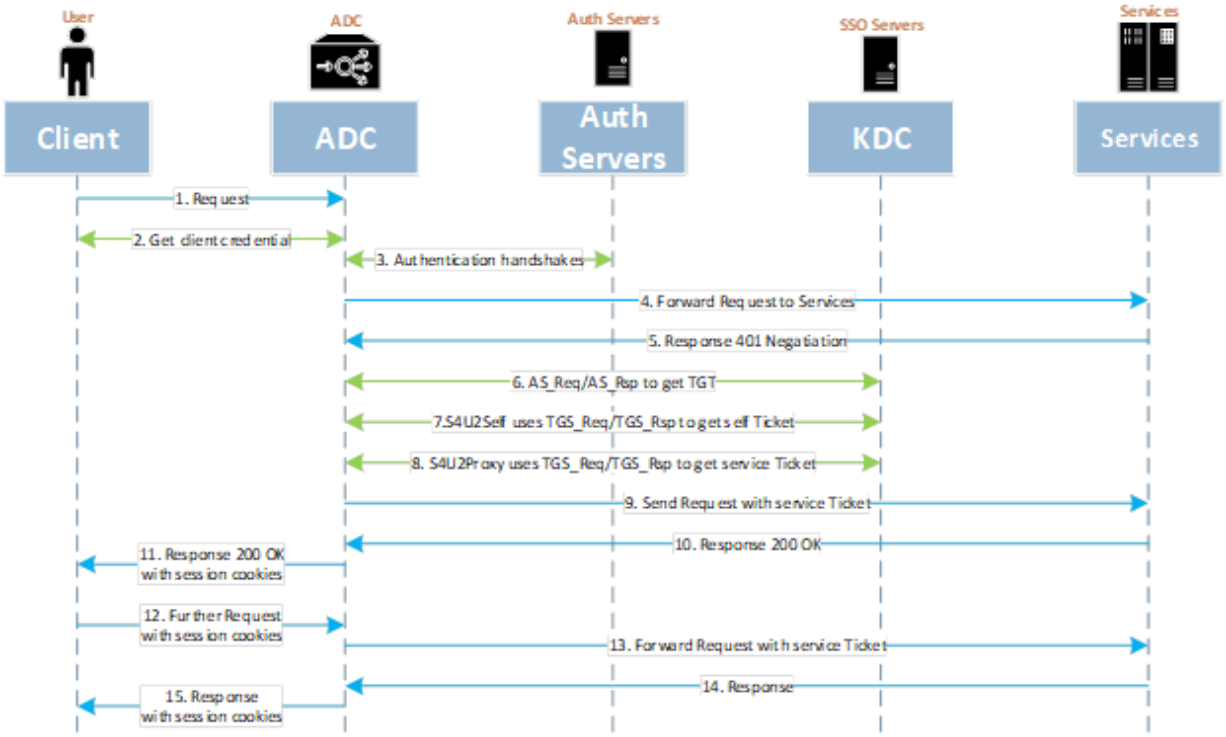
This deploy guide only provides configuration on the FortiADC. When on the Kerberos server setting, refer to the appropriate documents for the server that you chose.

# Example Topology description



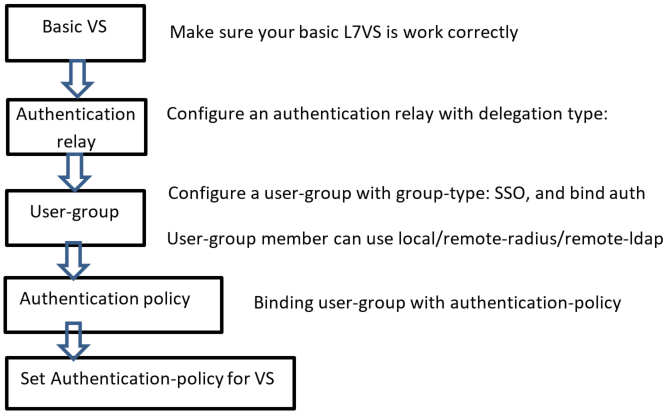

| server | hostname/IP example | note |
|---|---|---|
| DNS server | | A DNS-server is needed, since all the tested domain name should be resolved by DNS server. Ignored in this guide, I will use local hosts file. |
| NTP server | | Kerberos is time aware of, so we need a NTP server to make sure all the devices in time consistency. Ignored in this guide, make sure the time is consistency in all the test machine. |
| Client | | We will test a HTTP service, so here we need a client which had http browser. |
| Remote LDAP/Radius | | Ignored in this guide, I will use FortiADC' local user for frontend authentication. |
| Kerberos server | kerberos.example.test | The Kerberos realm: EXAMPLE.TEST |
| Ldap server | ldap.example.test | The Base DN: dc=example,dc=test |
| VirtualServer | www218.example.test | |
| RealServer | | |

# Work flow


User
ADC
Auth Servers
SSO Servers
Services
Client
ADC
Auth Servers
KDC
Services
1. Request
2. Get client credential
3. Authentication handshakes
4. Forward Request to Services
5. Response 401 Negotiation
6. AS_Req/AS_Rsp to get TGT
7.S4U2Self uses TGS_Req/TGS_Rsp to get self Ticket
8. S4U2Proxy uses TGS_Req/TGS_Rsp to get service Ticket
9. Send Request with service Ticket
10. Response 200 OK
11. Response 200 OK with session cookies
12. Further Request with session cookies
13. Forward Request with service Ticket
14. Response
15. Response with session cookies

# Configuration

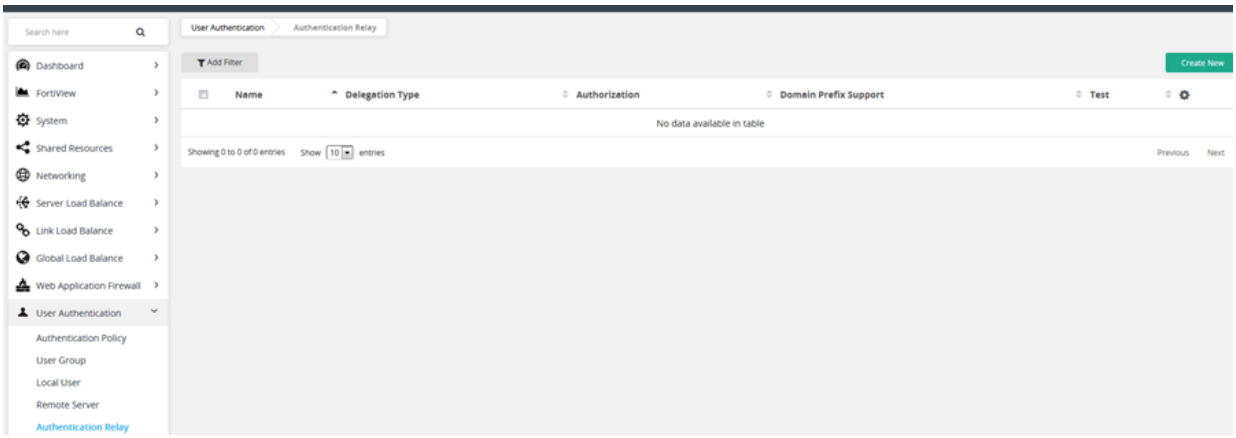
### 1. Overview

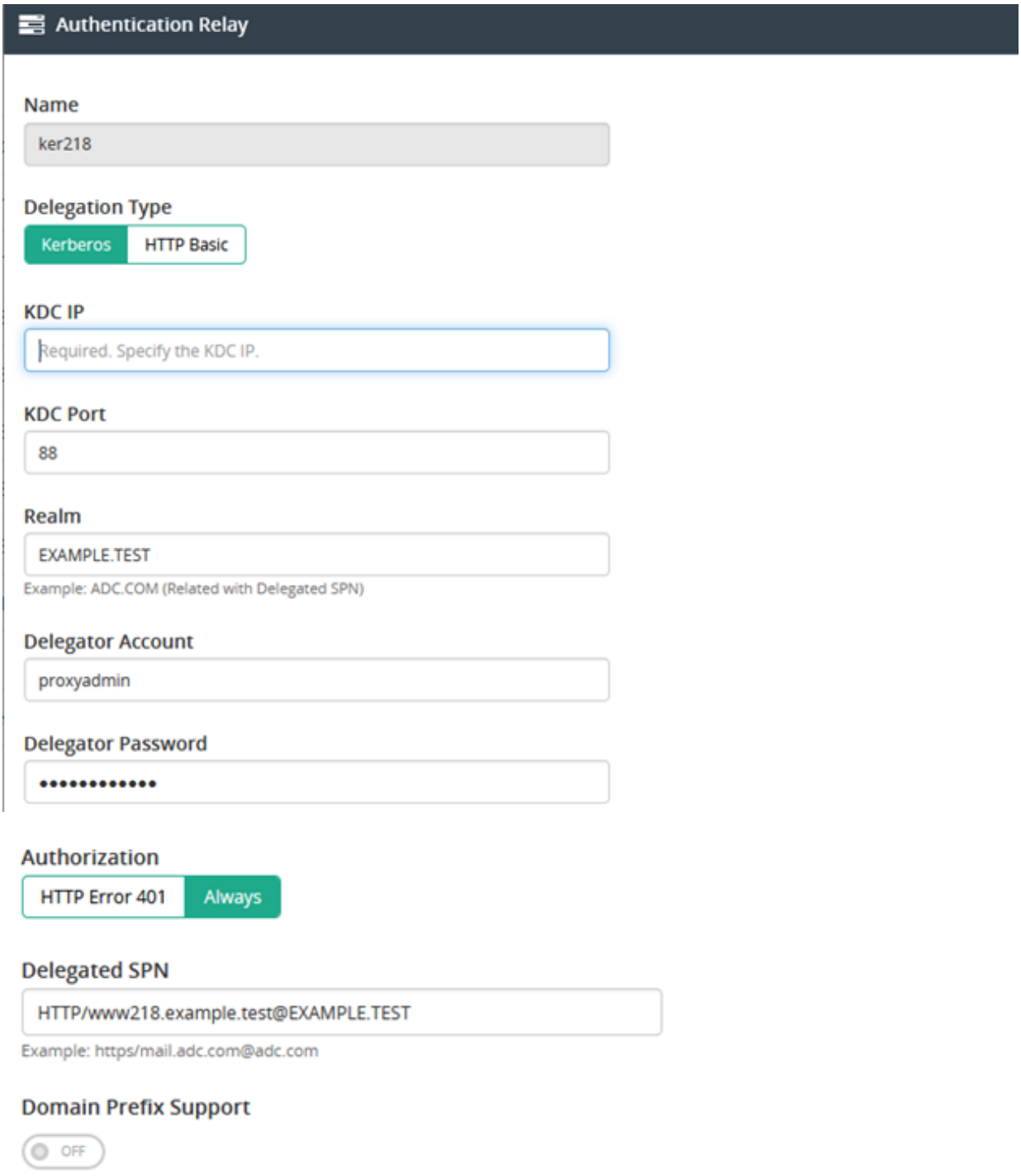



### 2. Set proper Layer 7 Virtual server

Configure a proper Layer 7 Virtual server and test it to make sure your Layer 7 Virtual server works properly.

### 3. Create a new authentication relay



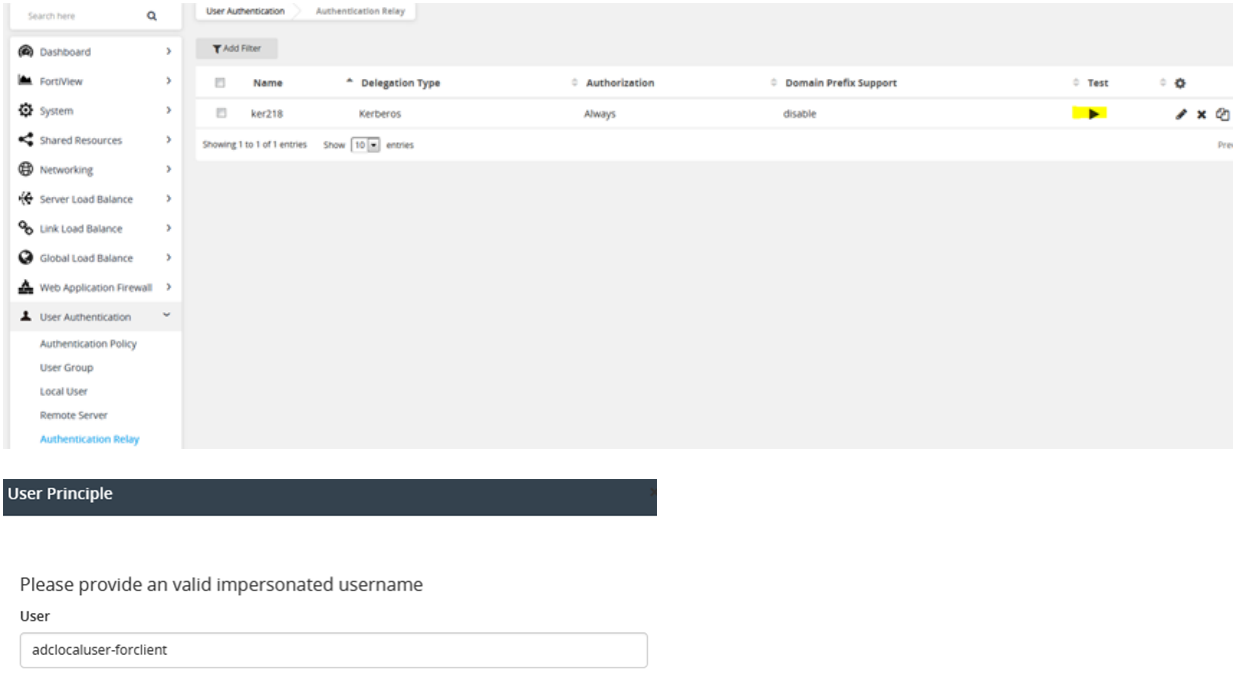



- KDC IP: Enter the IP address of the KDC
- Realm: In most cases, your Kerberos realm is your domain name, in upper-case letters.
- The Delegator Account set on the ADC must match the account set on the LDAP/AD server. This account must have the delegation attribute on the LDAP/AD server and set the Delegated SPN.
    - For example, the Delegator Account here is: proxyadmin
    - For example, the Delegated SPN here is: HTTP/www218.example.test@EXAMPLE.test

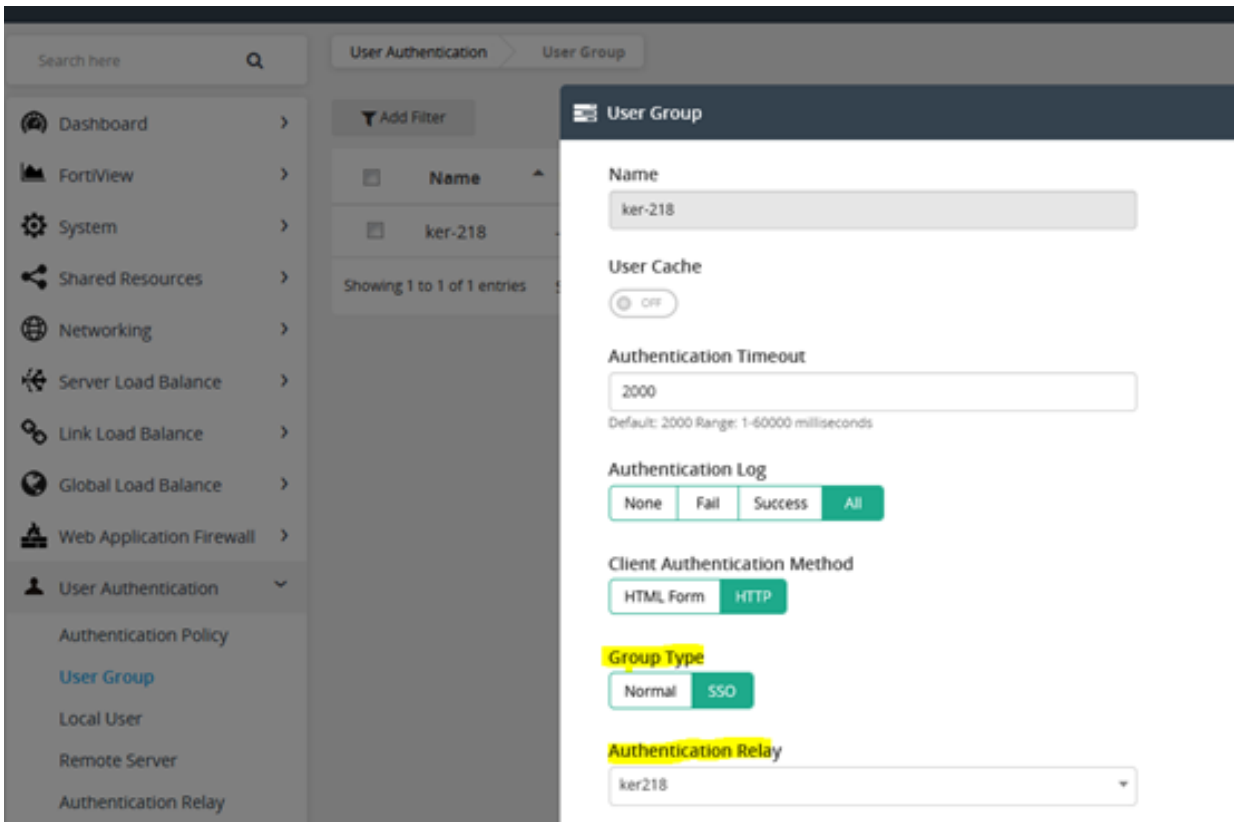
- Delegated SPN (Service principal name): Specify the delegated SPN.

### 4. Test Kerberos authentication relay

After creating a Kerberos authentication relay you can test its setting by pressing the test button, and inputting the correct username for client. If the test fails, please check the Kerberos server setting.

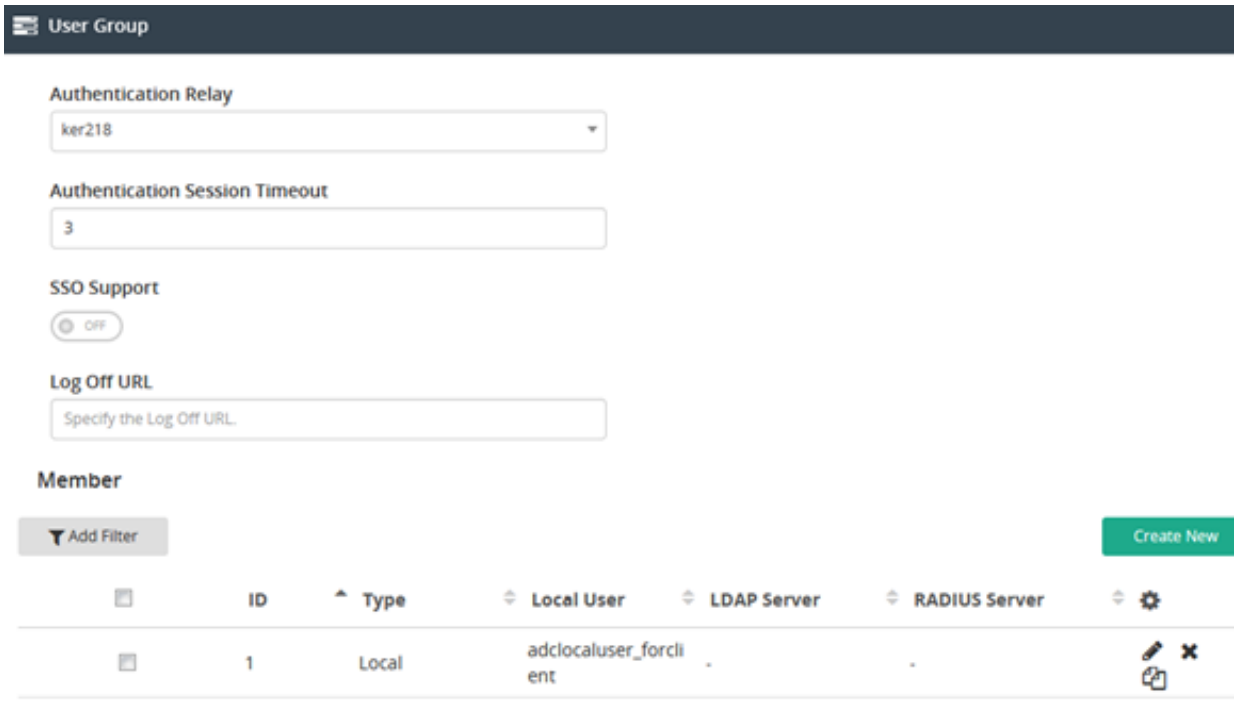


### 5. Create a user-group set group type to SSO and Authentication relay to kerberos

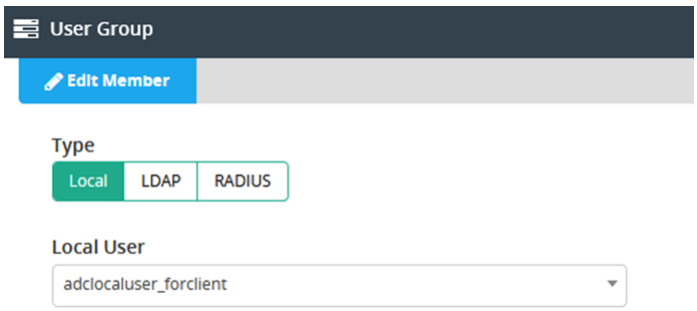



### 6. Add user group member

You can add preferred user group member for Virtual server authentication use. Here I use local Type.




When the client sends a http request to Virtual server, the FortiADC will ask the user to input a username and password. If the username and password match with the user-group member, the ADC will act as a proxy to authentication with Kerberos server by using the delegator account to get a self and service ticket.



**7. Set up authentication policy and bind it with Layer 7 HTTP(S) virtual server**