FortiGate 110C and SendQuick ConeXa One-time-Password (OTP) Configuration Guide

Prepared by

TalariaX Pte Ltd
76 Playfair Road
#08-01 LHK2
Singapore 367996
Tel: 65-62802881
Fax: 65-62806882

FORTIGATE 110C AND SENDQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

1.0 INTRODUCTION

This document is prepared as a guide to configure FortiGate 110C to integrate with SendQuick Conexa for 2-Factor Authentication with One-time-password via SMS.

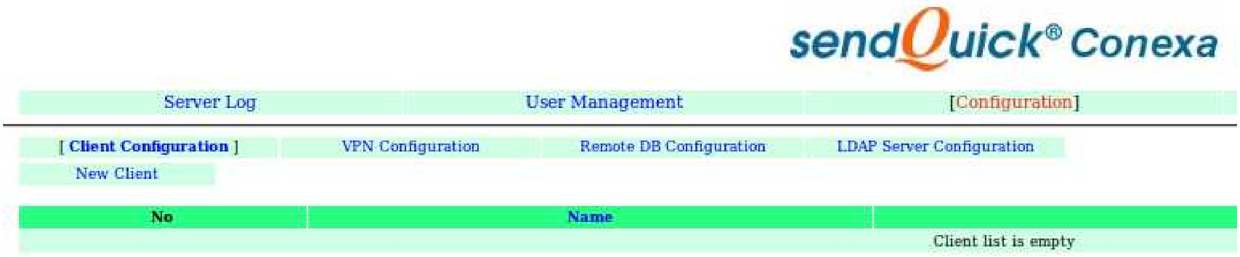
The pre-requisite is that SendQuick Conexa OTP server is configured with RADIUS on port 1812. Ensure that both applications are using the same port for radius.

2.0 CONEXA CONFIGURATION

2.1 Client Configuration

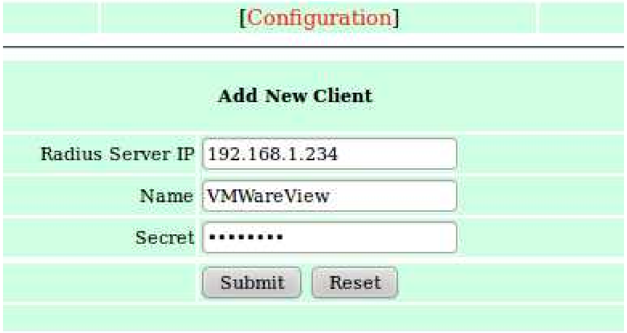
To create a new client, Go to Configuration -> Client Configuration -> New Client

2.1.1 Add New Client



No	Name	
		Client list is empty

Radius Server IP	IP address of the FortiGate 110C system.
Name	Short name of the radius client.
Secret	Shared secret of the radius client.



Add New Client

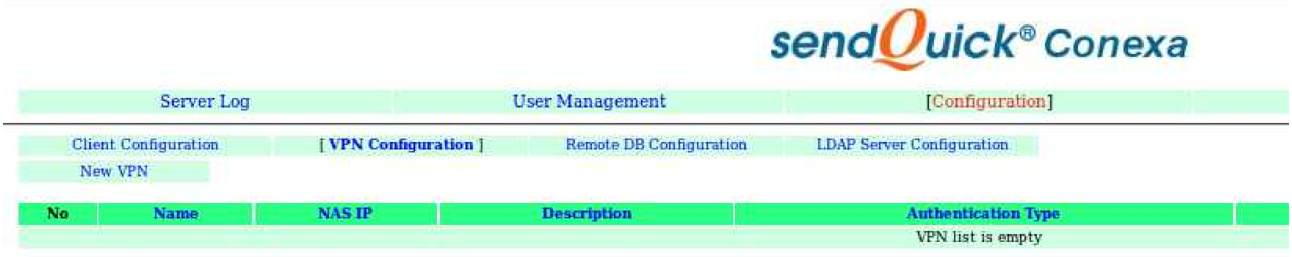
Radius Server IP: 192.168.1.234

Name: VMWareView

Secret: ••••••••

2.2 VPN Configuration

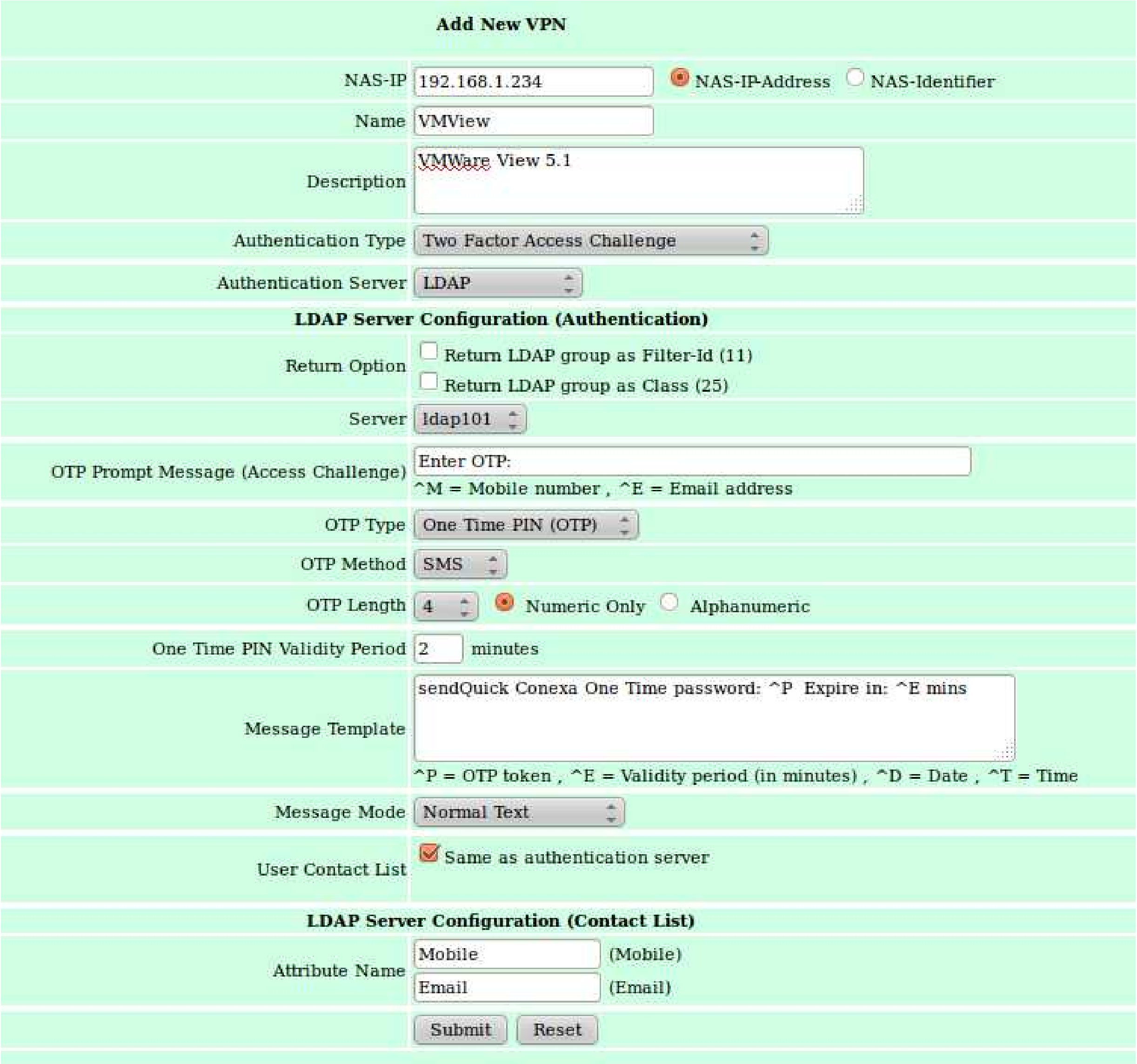
To create a new VPN, Go to Configuration -> VPN Configuration -> New VPN



No	Name	NAS IP	Description	Authentication Type
				VPN list is empty

2.2.1 Add New VPN

NAS-IP	192.168.1.234
Name	Unique name of this VPN.
Description	Description of this VPN. For reference only.
Authentication Type	Two Factor Access Challenge
Authentication Server	LDAP LDAP → Authentication through LDAP server such as Active Directory or OpenLDAP. Select LDAP server from list, which are predefined in LDAP Server Configuration page.
User Contact List	Check on 'Same as authentication server' to use the same user list in authentication server. LDAP → Select from a list of predefined LDAP servers. Mobile and email attributes are required.

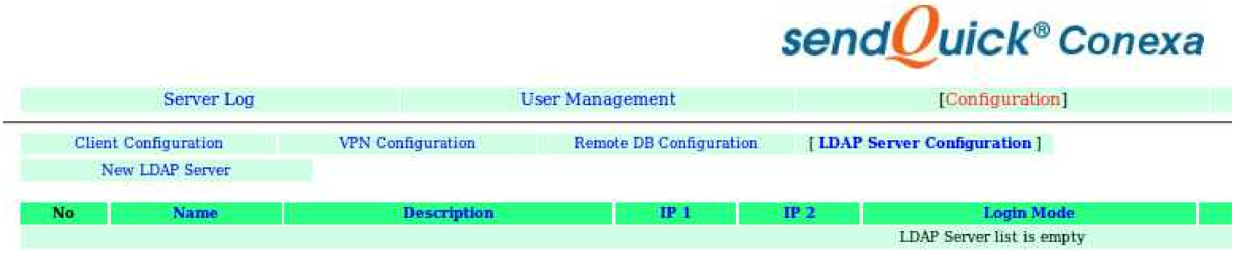


Add New VPN

NAS-IP	192.168.1.234 ● NAS-IP-Address ○ NAS-Identifier
Name	VMView
Description	VMWare View 5.1
Authentication Type	Two Factor Access Challenge
Authentication Server	LDAP
LDAP Server Configuration (Authentication)	
Return Option	□ Return LDAP group as Filter-Id (11) □ Return LDAP group as Class (25)
Server	ldap101
OTP Prompt Message (Access Challenge)	Enter OTP: ^M = Mobile number , ^E = Email address
OTP Type	One Time PIN (OTP)
OTP Method	SMS
OTP Length	4 ● Numeric Only ○ Alphanumeric
One Time PIN Validity Period	2 minutes
Message Template	sendQuick Conexa One Time password: ^P Expire in: ^E mins ^P = OTP token , ^E = Validity period (in minutes) , ^D = Date , ^T = Time
Message Mode	Normal Text
User Contact List	☑ Same as authentication server
LDAP Server Configuration (Contact List)	
Attribute Name	Mobile (Mobile) Email (Email)

2.3 LDAP Server Configuration

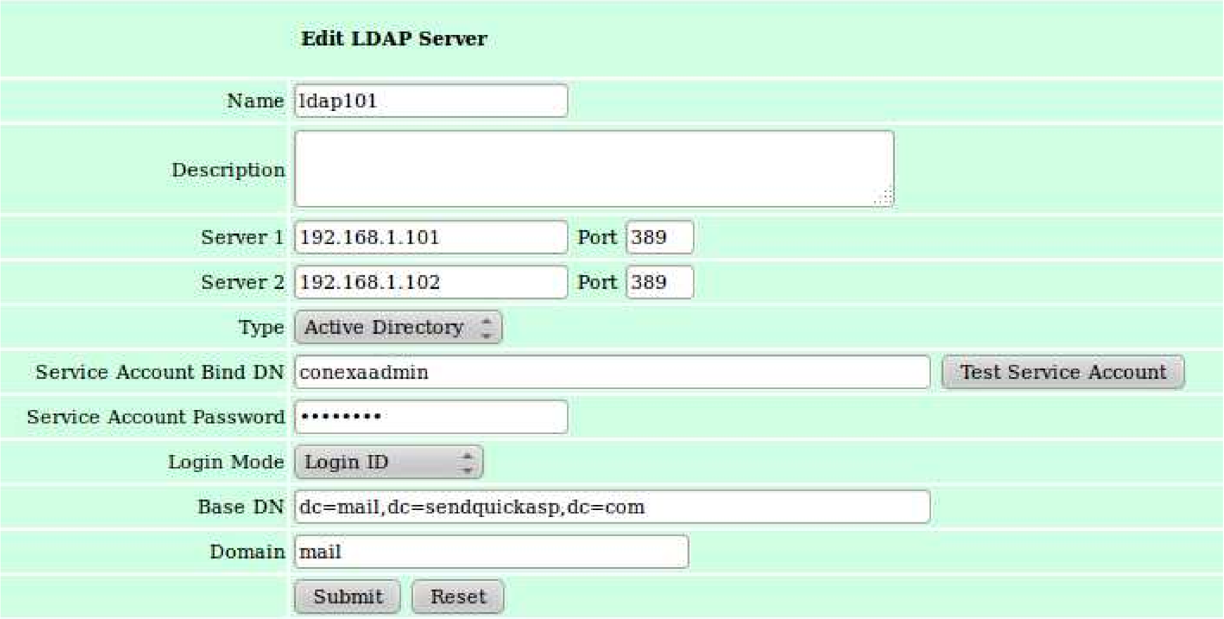
Configuration -> LDAP Server Configuration -> New LDAP Server



No	Name	Description	IP 1	IP 2	Login Mode
					LDAP Server list is empty

2.3.1 Add New LDAP Server

Name	Unique name for LDAP server, which will be used as identifier in VPN configuration .
Description	For reference only.
Server 1 & Port	LDAP Server IP and port number. LDAP default port : 389
Server 2 & Port	LDAP Server IP (Backup/Secondary) and port number. LDAP default port : 389
Service Account Name & Password	Valid login name & password, which will be used for binding and searching.
Login Mode	[Display Name | Login ID | Email] Type of login ID for this LDAP server.
Base DN	Base DN of the location of user list in LDAP.
Domain	Windows login domain for the user, apply to AD only.



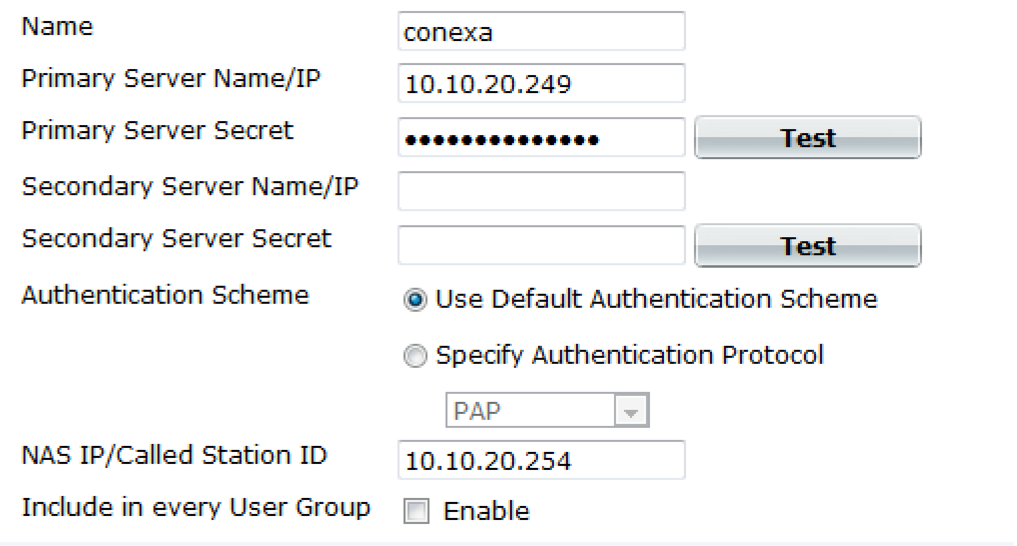
Edit LDAP Server

Name	ldap101
Description	
Server 1	192.168.1.101 Port 389
Server 2	192.168.1.102 Port 389
Type	Active Directory
Service Account Bind DN	conexaadmin
Service Account Password	••••••••
Login Mode	Login ID
Base DN	dc=mail,dc=sendquickasp,dc=com
Domain	mail

3.0 Configuring FortiGate 110C

To configure for the RADIUS authentication protocol, you need to configure a new Radius Server in FortiGate.

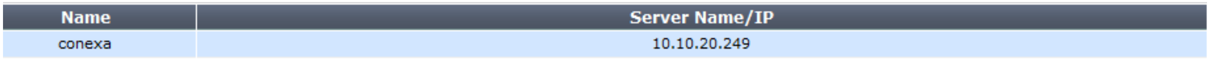
Configure a new Radius Server with sendQuick Conexa credentials as shown below:



Name	conexa	
Primary Server Name/IP	10.10.20.249	
Primary Server Secret	••••••••••••••	Test
Secondary Server Name/IP		
Secondary Server Secret		Test
Authentication Scheme	● Use Default Authentication Scheme	
	○ Specify Authentication Protocol	
	PAP	
NAS IP/Called Station ID	10.10.20.254	
Include in every User Group	□ Enable	

Insert SendQuick Conexa IP (above example 10.10.20.249) into the IP field. The NASIP (above) as the IP of FortiGate.

Once it is setup, you will see Conexa as Radius server being created, as below:



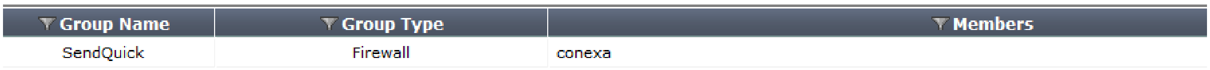
Name	Server Name/IP
conexa	10.10.20.249

You may require to configure the timeout for Radius using CLI (command line) as below:

```
conf sys global
set remoteauthtimeout 60
end
```

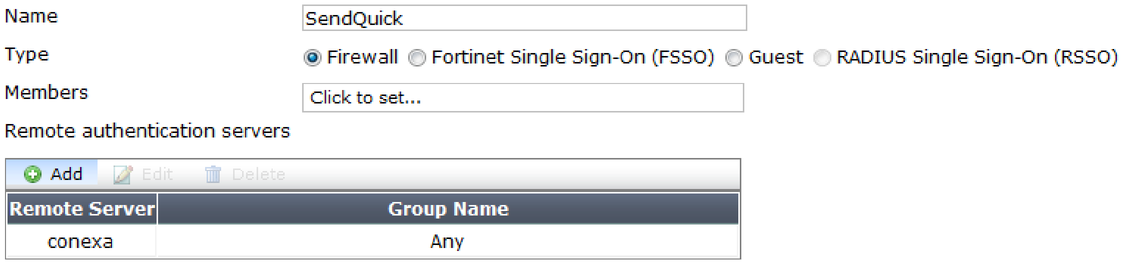
The next step is the assign a user group (or user realm) to use sendQuick Conexa (conexa radius setting) for the authentication.

Create a Usergroup (eg, Groupname = sendQuick) and assign the group to use 'conexa' as the authentication server. Once setup, you will see similar information as below:



Group Name	Group Type	Members
SendQuick	Firewall	conexa

You will need to select the Type and the selected Radius server (eg, conexa) for the group. This will ensure that these users will use sendquick Conexa for authentication.

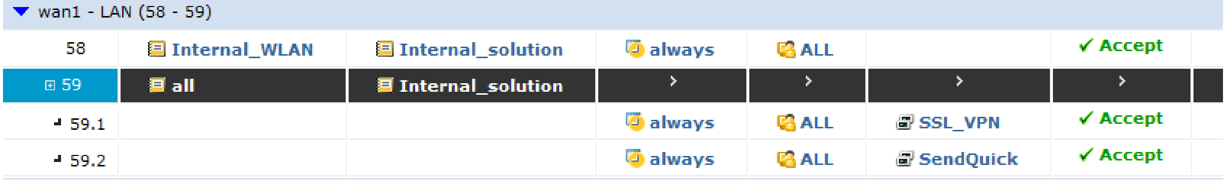


Name	SendQuick
Type	● Firewall ○ Fortinet Single Sign-On (FSSO) ○ Guest ○ RADIUS Single Sign-On (RSSO)
Members	Click to set...

Remote authentication servers

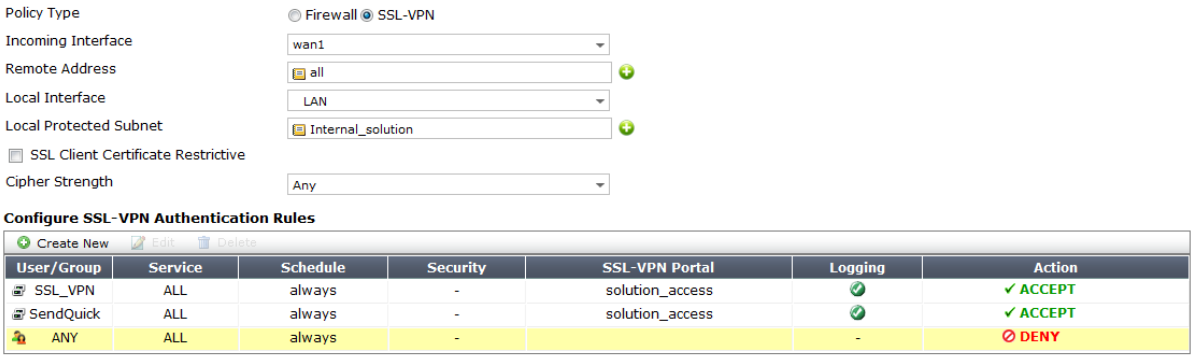
Remote Server	Group Name
conexa	Any

Lastly, you may wish to conifgure the Firewall policy to ensure all traffic is supported for the smooth operation of the 2FA with Conexa. The example is as below:



wan1 - LAN (58 - 59)

58	Internal_WLAN	Internal_solution	always	ALL		✓ Accept
59	all	Internal_solution	›	›	›	›
59.1			always	ALL	SSL_VPN	✓ Accept
59.2			always	ALL	SendQuick	✓ Accept



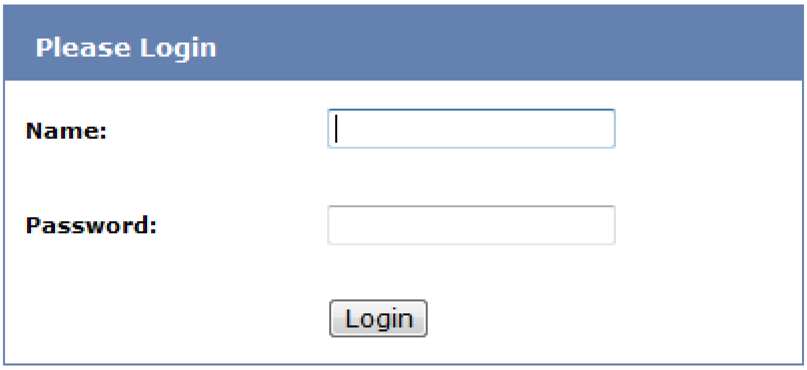
Policy Type	○ Firewall ● SSL-VPN
Incoming Interface	wan1
Remote Address	all
Local Interface	LAN
Local Protected Subnet	Internal_solution
□ SSL Client Certificate Restrictive	
Cipher Strength	Any

Configure SSL-VPN Authentication Rules

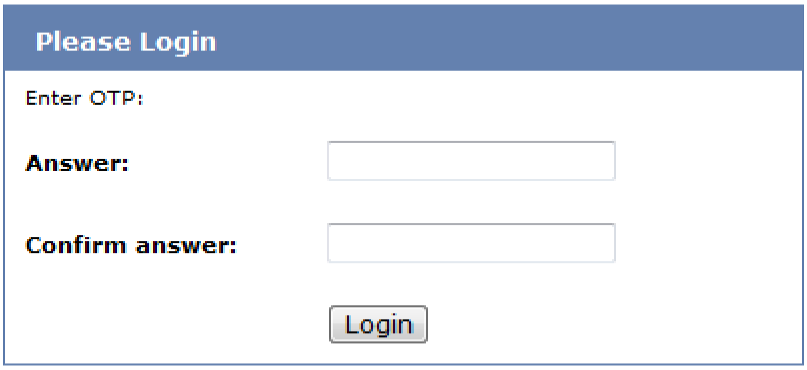
User/Group	Service	Schedule	Security	SSL-VPN Portal	Logging	Action
SSL_VPN	ALL	always	-	solution_access	✓	✓ ACCEPT
SendQuick	ALL	always	-	solution_access	✓	✓ ACCEPT
ANY	ALL	always	-		-	⊘ DENY

4.0 Testing the 2FA Integration

First, start the FortiGate 110C secure web browser (HTTPS) and you will see the login page to enter Username and Password. This is the Username and Password in the Active Directory. This is shown in the figure below.



One the Username and Password is authenticated, you will receive a SMS OTP. Enter the OTP received on both fields as shown below. Fortigate requires a confirmation of the SMS OTP to be entered in the fields, as shown below.



Please Login
Enter OTP:
Answer:
Confirm answer:
Login