Microsoft Forefront Unified Access Gateway 2010 and SendQuick ConeXa One-time-Password Configuration Guide

Prepared by

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

MICROSOFT FOREFRONT UNIFIED ACCESS GATEWAY (UAG) 2010 AND SENDQUICK CONEXA ONE TIME PASSWORD CONFIGURATION GUIDE

1.0 INTRODUCTION

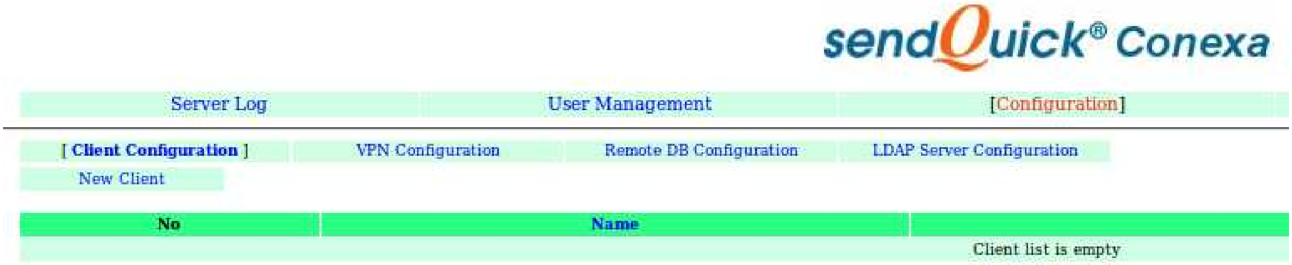
This document is prepared as a guide to configure Microsoft Forefront Unified Access Gateway 2010 (UAG) to run with SendQuick Conexa for One-time-password via SMS.

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

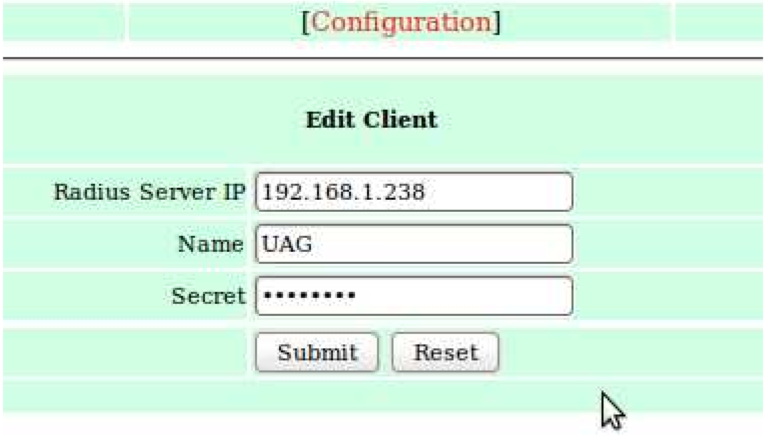
To create a new client, Go to Configuration -> Client Configuration -> New Client



Client list is empty

2.1.1 Add New Client

Radius Server IP	IP address of the UAG.
Name	Short name of the radius client.
Secret	Shared secret of the radius client.



Edit Client

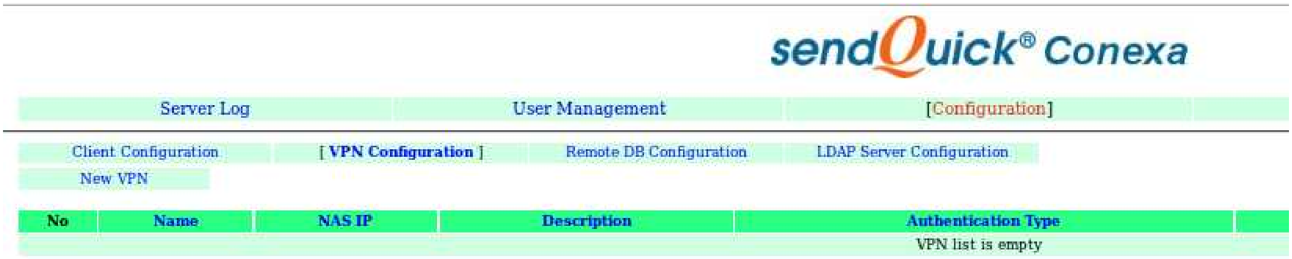
Radius Server IP 192.168.1.238

Name UAG

Secret ••••••••

2.2 VPN Configuration

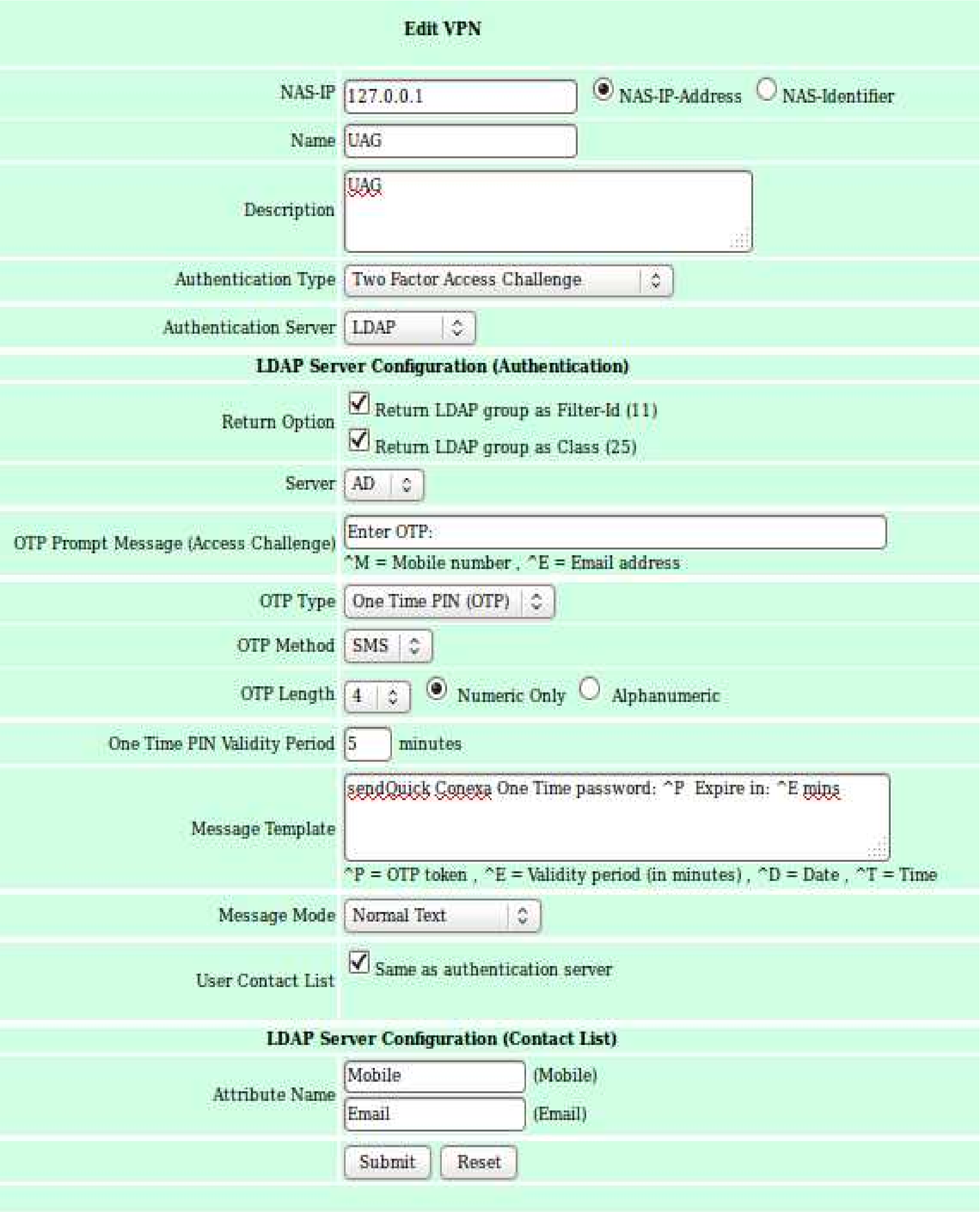
To create a new VPN, Go to Configuration -> VPN Configuration -> New VPN



No	Name	NAS IP	Description	Authentication Type
				VPN list is empty

2.2.1 Add New VPN

NAS-IP	127.0.0.1
Name	Unique name of this VPN.
Description	Description of this VPN. For reference only.
Authentication Type	Two Factor Access Challenge
Authentication Server	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.

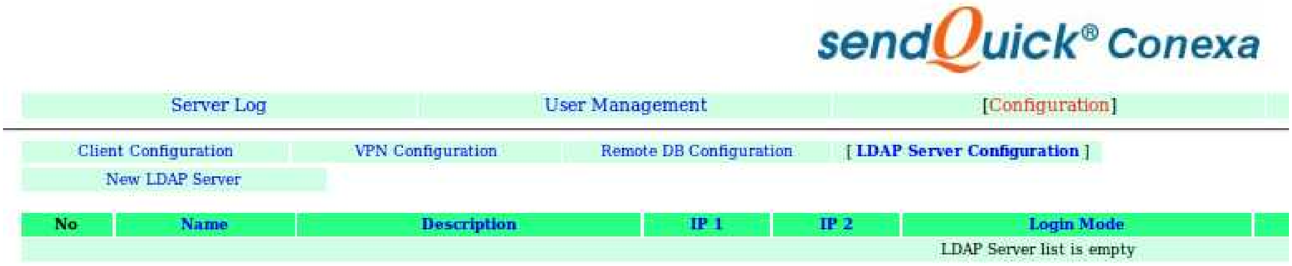


Edit VPN

NAS-IP	127.0.0.1 ● NAS-IP-Address ○ NAS-Identifier
Name	UAG
Description	UAG
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	AD
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	5 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)
	Submit Reset

2.3 LDAP Server Configuration

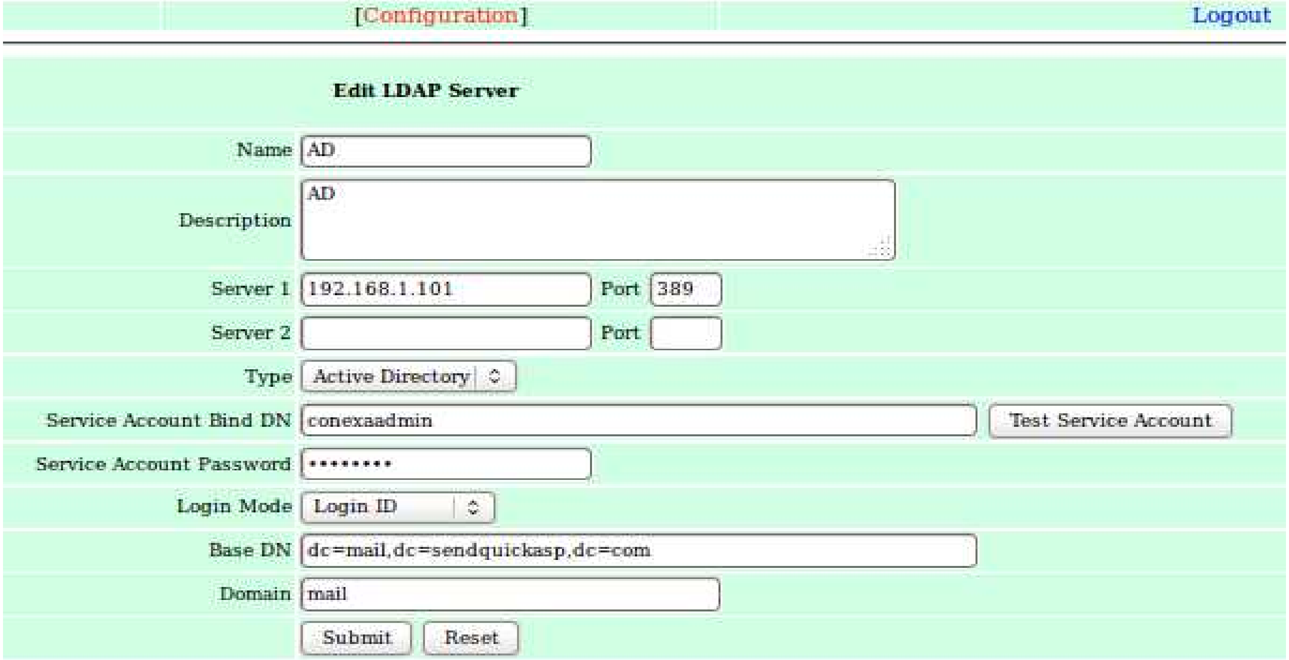
Configuraion -> LDAP Server Configuration -> New LDAP Server



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.



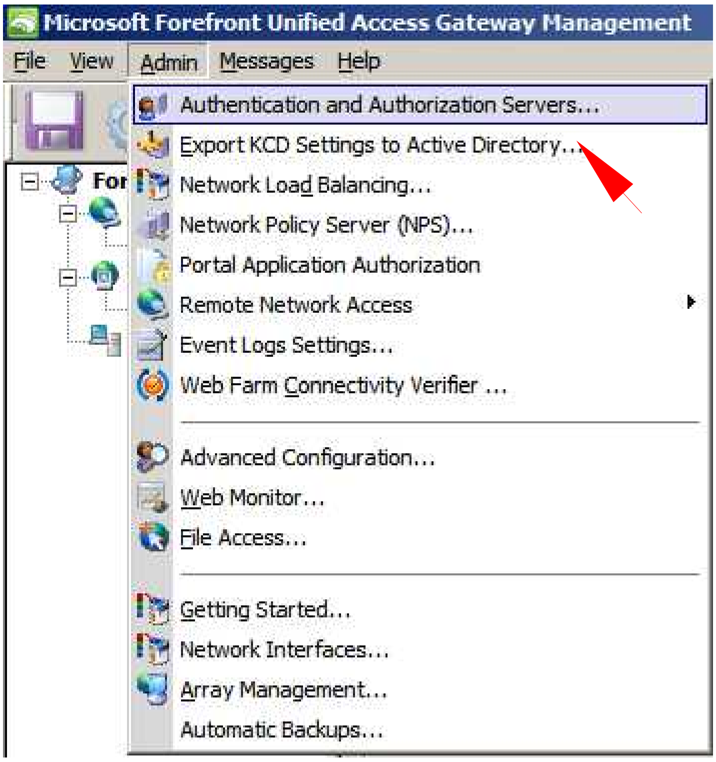
[Configuration] Logout

Edit LDAP Server

Name	AD
Description	AD
Server 1	192.168.1.101 Port 389
Server 2	Port
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

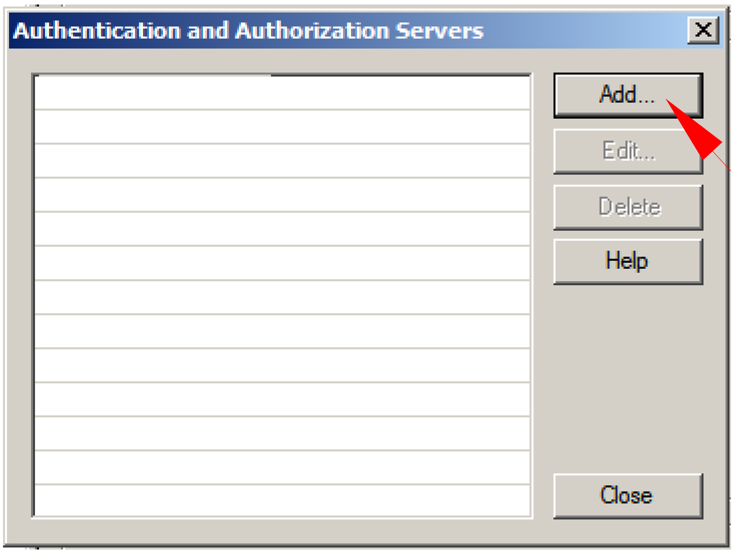
3.0 Configuring Microsoft Forefront Unified Access Gateway 2010

3.1 Click Authentication and Authorization Servers

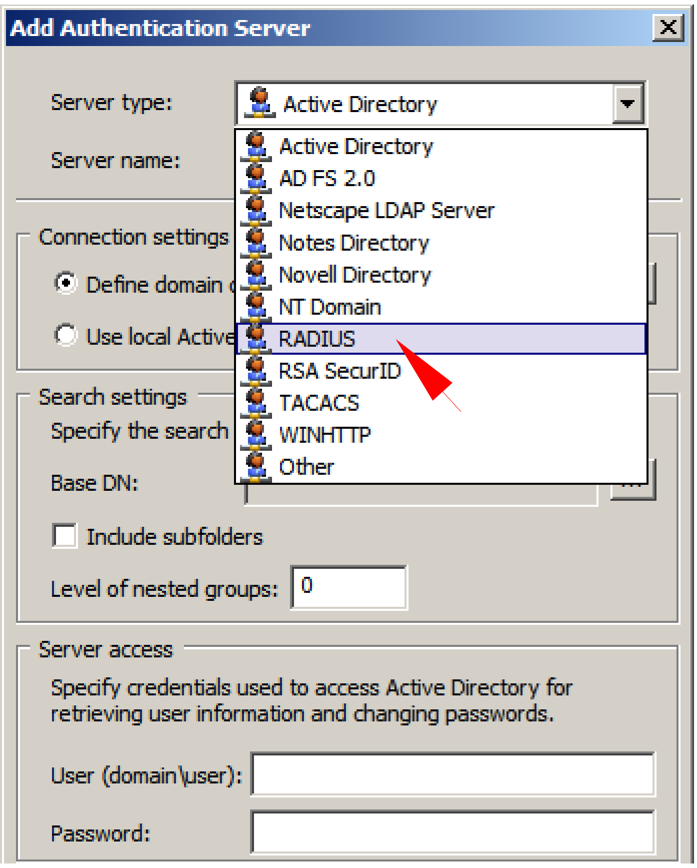


Microsoft Forefront Unified Access Gateway Management
File
View
Admin
Messages
Help
For
Authentication and Authorization Servers...
Export KCD Settings to Active Directory...
Network Load Balancing...
Network Policy Server (NPS)...
Portal Application Authorization
Remote Network Access
Event Logs Settings...
Web Farm Connectivity Verifier ...
Advanced Configuration...
Web Monitor...
File Access...
Getting Started...
Network Interfaces...
Array Management...
Automatic Backups...

3.2 Click Add



3.3 In the Server type list, Click RADIUS.



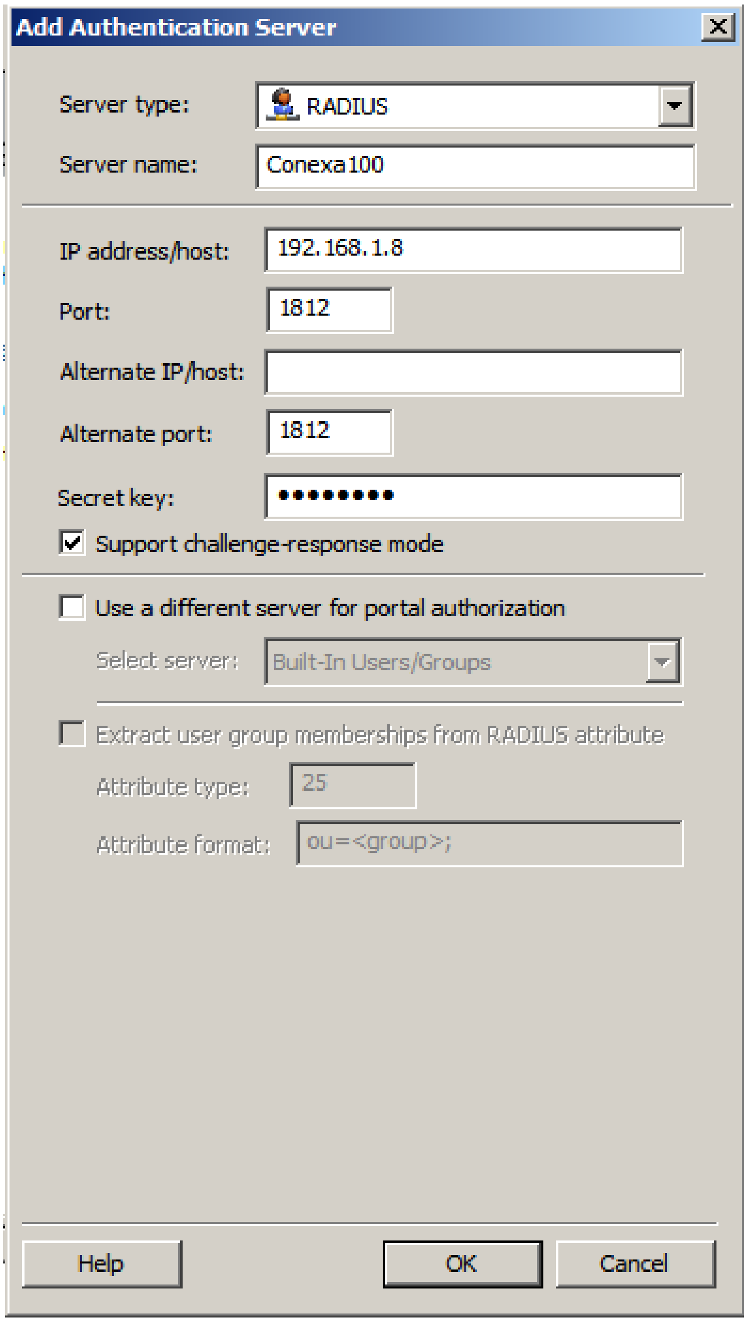
Server type: Active Directory

Level of nested groups: 0

Specify credentials used to access Active Directory for retrieving user information and changing passwords.

3.4 On the Add Authentication Server dialog box, configure the following server settings:

Server name	Name of the server, e.g Conexa100
IP address/host	IP address of sendQuick Conexa
Port	1812
Secret key	Shared secret of the sendQuick Conexa
Support challenge-response mode	Select this option



Add Authentication Server

Server type: RADIUS

Server name: Conexa100

IP address/host: 192.168.1.8

Port: 1812

Alternate IP/host:

Alternate port: 1812

Secret key: ••••••••

☑ Support challenge-response mode

□ Use a different server for portal authorization

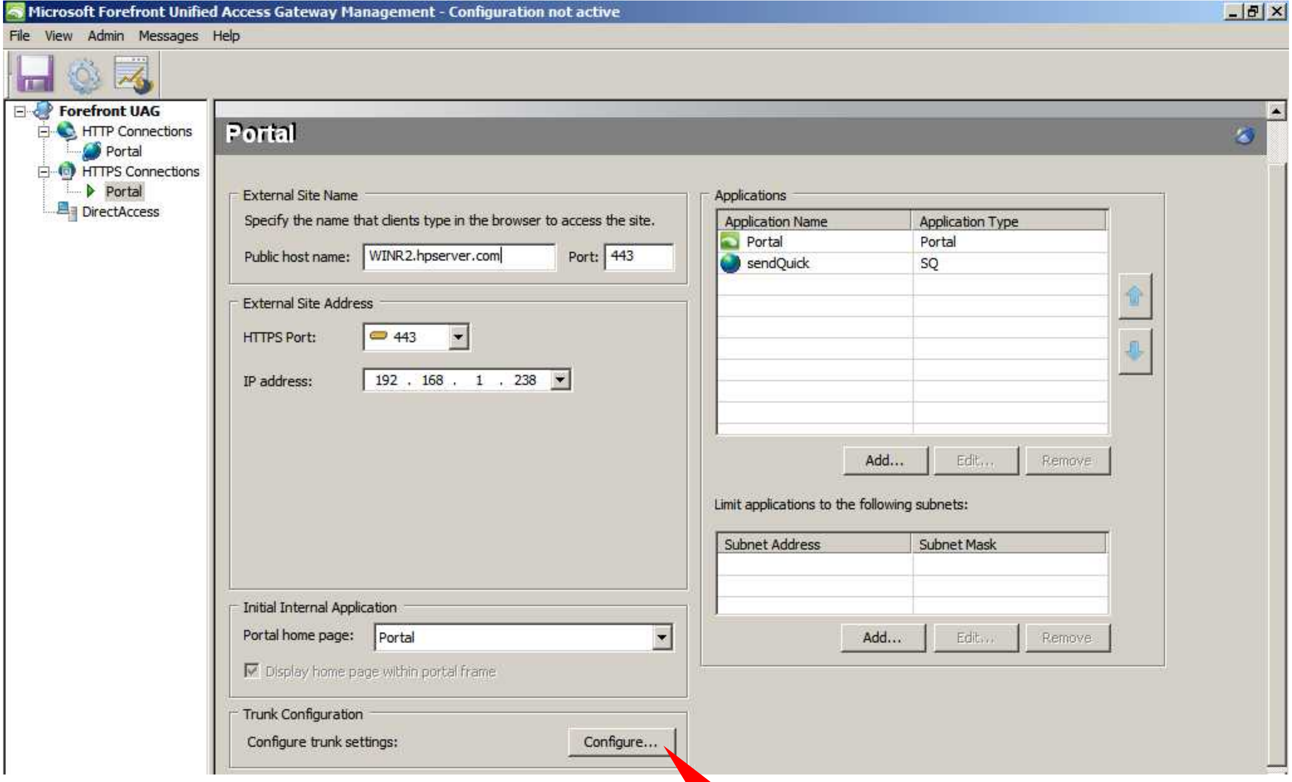
Select server: Built-In Users/Groups

□ Extract user group memberships from RADIUS attribute

Attribute type: 25

Attribute format: ou=<group>;

3.5 Click on the “Configure” button to change the authentication scheme.



External Site Name

Specify the name that clients type in the browser to access the site.

Public host name: WINR2.hpserver.com Port: 443

External Site Address

HTTPS Port: 443

IP address: 192 . 168 . 1 . 238

Initial Internal Application

Portal home page: Portal

☑ Display home page within portal frame

Trunk Configuration

Configure trunk settings:

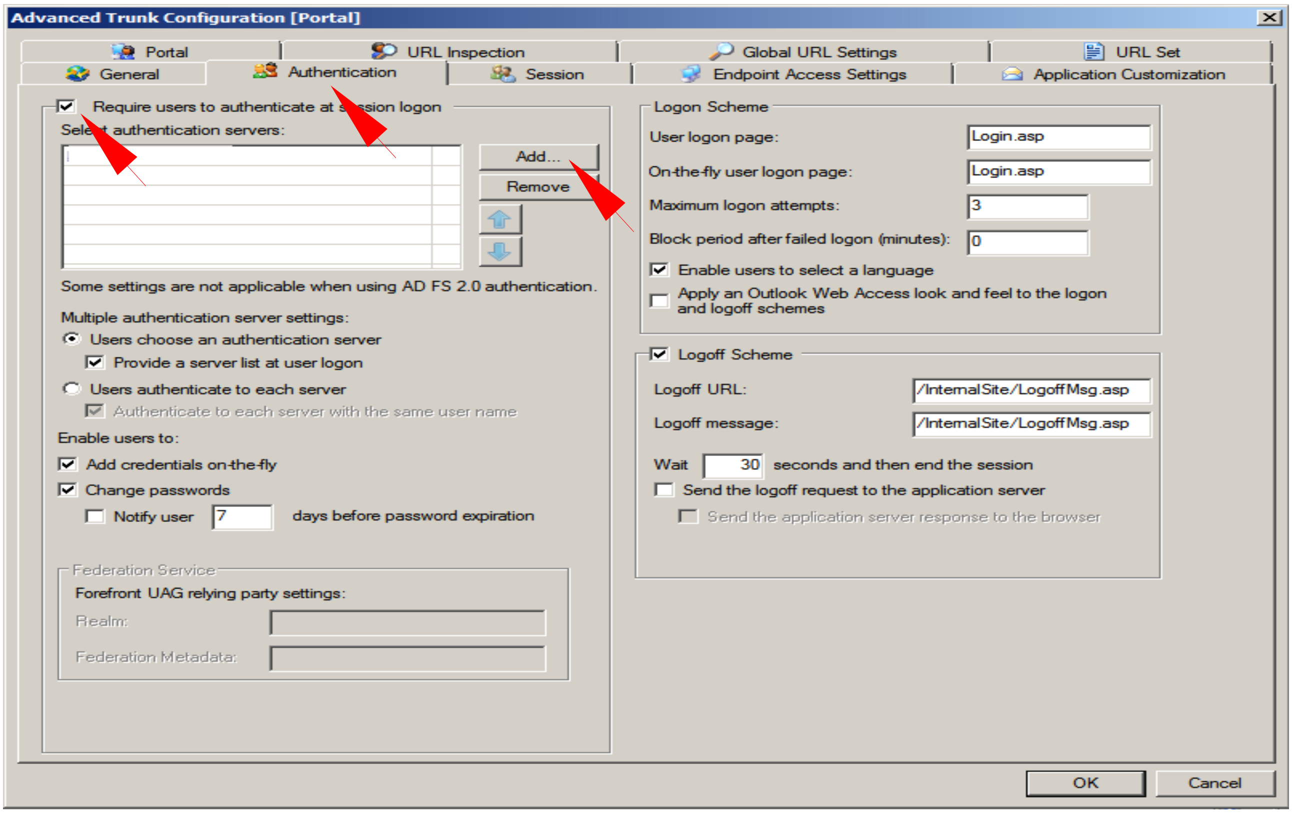
Applications

Application Name	Application Type
Portal	Portal
sendQuick	SQ

Limit applications to the following subnets:

Subnet Address	Subnet Mask

3.6 Go to Authentication tab, select “Require users to authenticate at session logon”.Then, Select “Add”.



Advanced Trunk Configuration [Portal]

☑ Require users to authenticate at session logon

Select authentication servers:

Some settings are not applicable when using AD FS 2.0 authentication.

Multiple authentication server settings:

● Users choose an authentication server

☑ Provide a server list at user logon

○ Users authenticate to each server

☑ Authenticate to each server with the same user name

Enable users to:

☑ Add credentials on-the-fly

☑ Change passwords

□ Notify user 7 days before password expiration

Federation Service

Forefront UAG relying party settings:

Realm:

Federation Metadata:

Logon Scheme

User logon page: Login.asp

On-the-fly user logon page: Login.asp

Maximum logon attempts: 3

Block period after failed logon (minutes): 0

☑ Enable users to select a language

□ Apply an Outlook Web Access look and feel to the logon and logoff schemes

☑ Logoff Scheme

Logoff URL: /InternalSite/LogoffMsg.asp

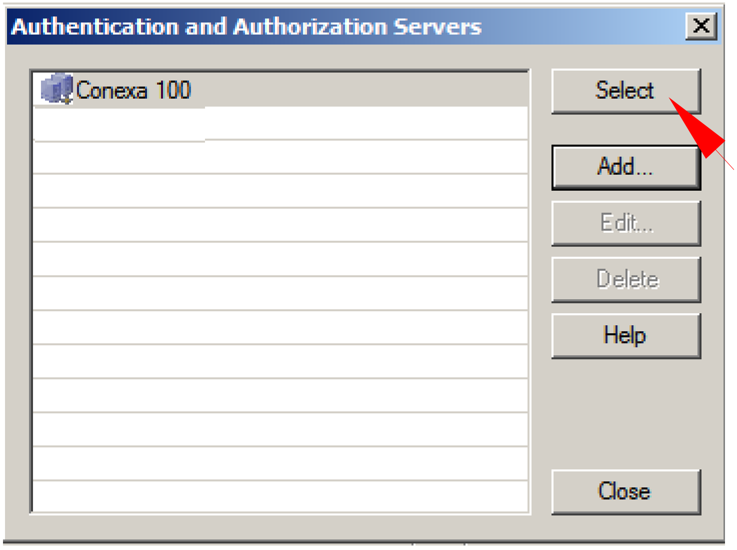
Logoff message: /InternalSite/LogoffMsg.asp

Wait 30 seconds and then end the session

□ Send the logoff request to the application server

□ Send the application server response to the browser

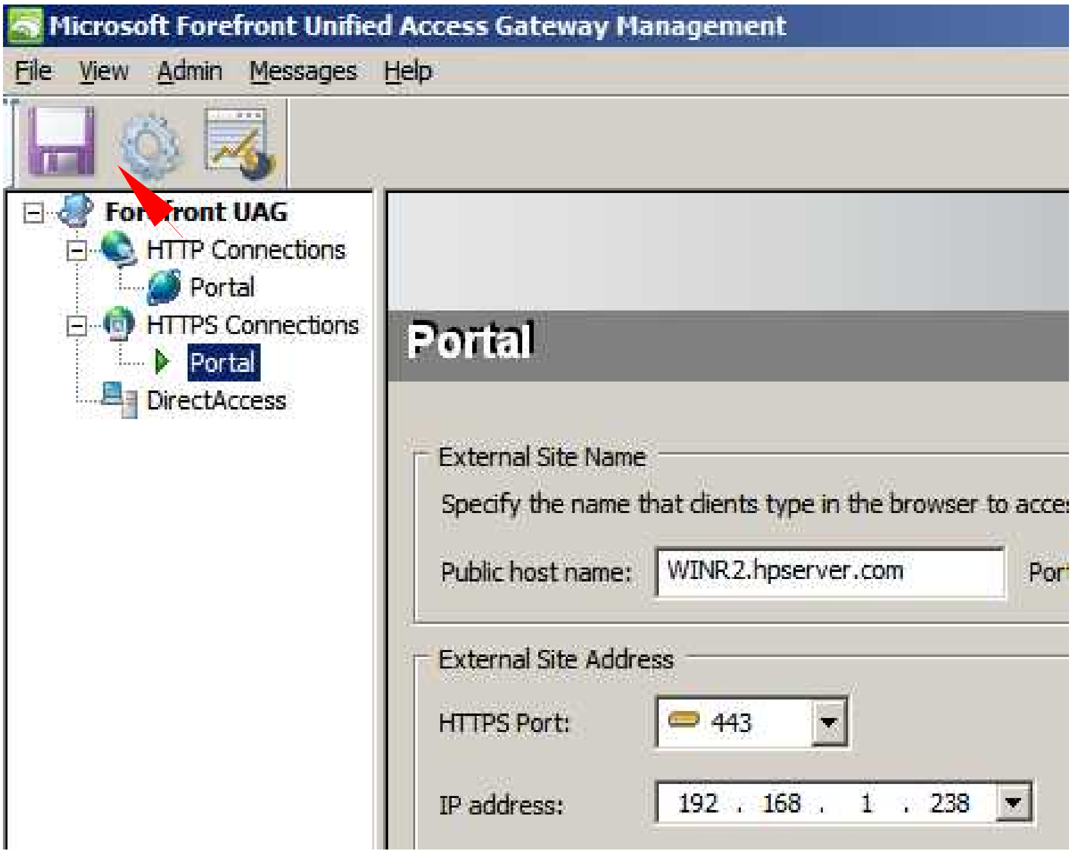
3.7 Select Conexa Server.



Authentication and Authorization Servers

Conexa 100

3.8 Save and activate the configuration.



Microsoft Forefront Unified Access Gateway Management
File View Admin Messages Help
Forefront UAG
HTTP Connections
Portal
HTTPS Connections
Portal
DirectAccess
Portal

External Site Name

Specify the name that clients type in the browser to acce

Public host name: WINR2.hpserver.com Por

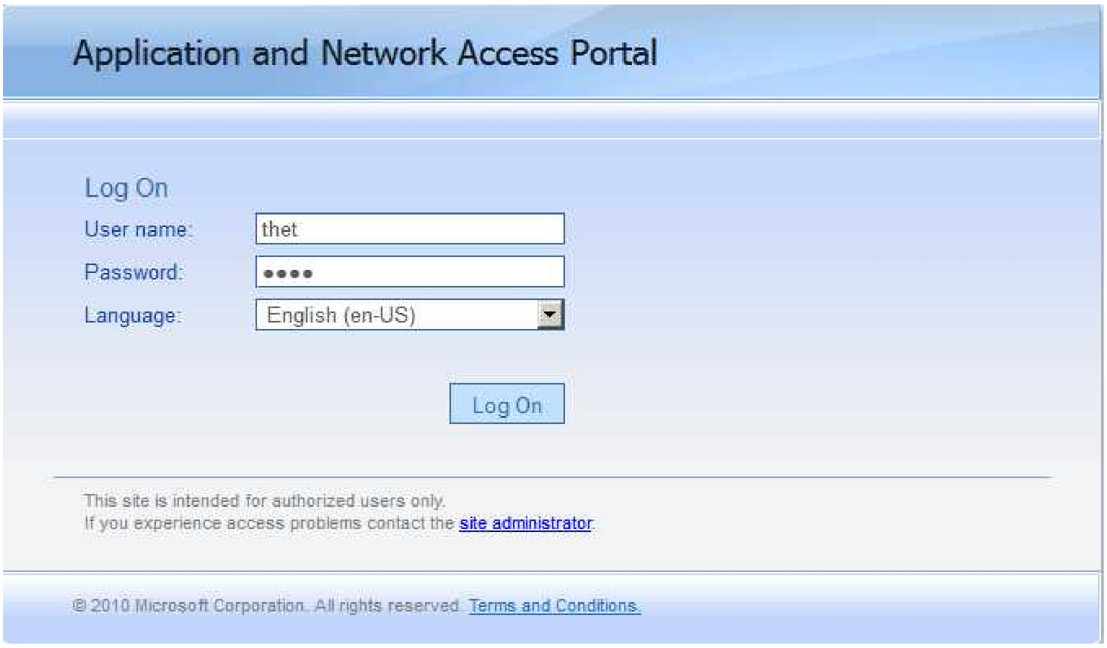
External Site Address

HTTPS Port: 443

IP address: 192 . 168 . 1 . 238

4.0 Testing

4.1 Enter user name and password, click “Log On” button.



Application and Network Access Portal

Log On

User name: thet

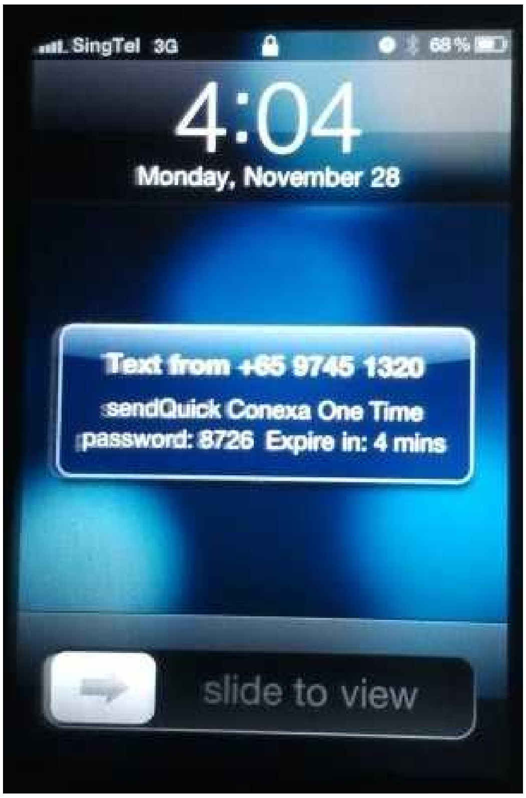
Password: ●●●●

Language: English (en-US)

This site is intended for authorized users only.
If you experience access problems contact the site administrator.

© 2010 Microsoft Corporation. All rights reserved. Terms and Conditions.

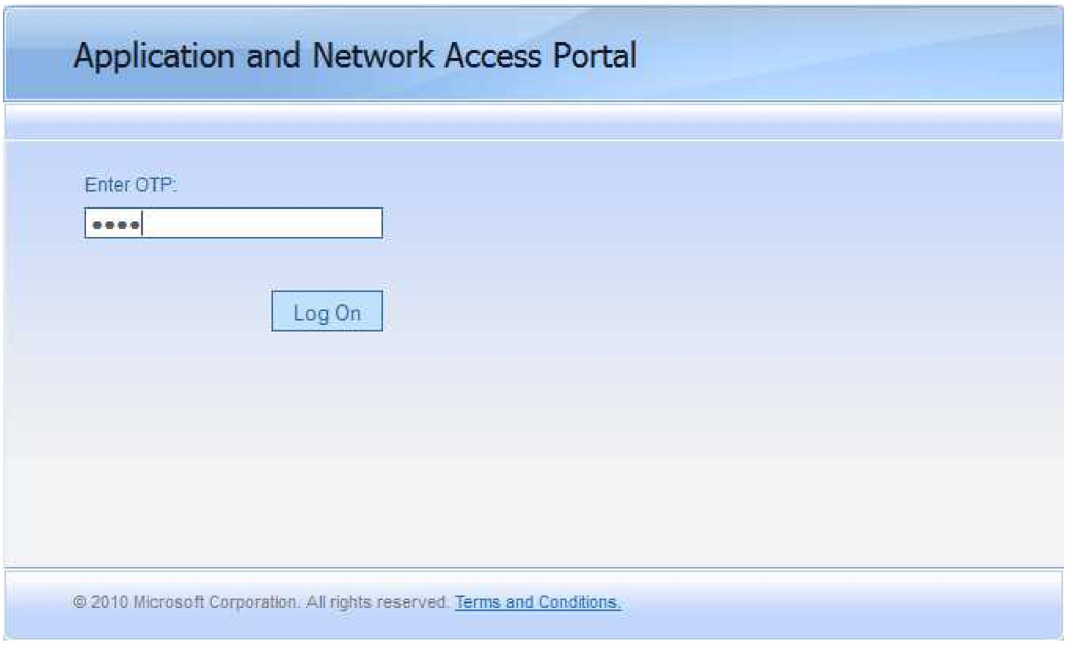
4.2 You will receive a one-time password to your mobile phone.



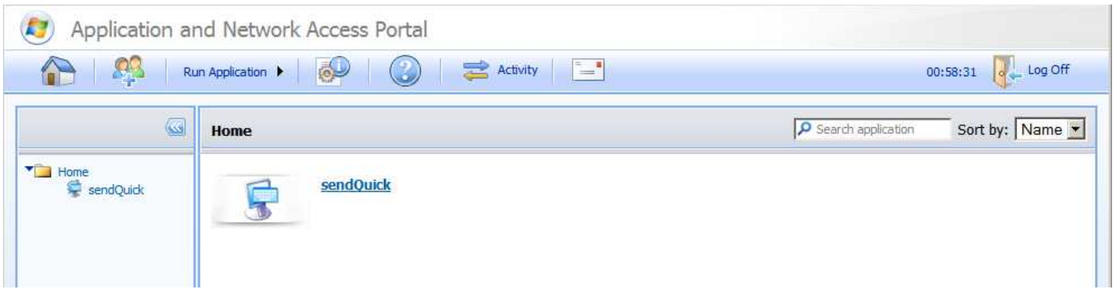
Text from +65 9745 1320

sendQuick Conexa One Time password: 8726 Expire in: 4 mins

4.3 Enter the one-time password and click the “Log On”.



Application and Network Access Portal
Enter OTP:
••••
Log On
© 2010 Microsoft Corporation. All rights reserved. Terms and Conditions.



Application and Network Access Portal
Run Application
Activity
00:58:31
Log Off
Home
Search application
Sort by: Name
Home
sendQuick
sendQuick