External authentication with SOPHOS UTM appliances Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	Merlin House Brunel Road Theale Reading RG7 4AB	
Dorian Tomkins	Dtomkins@securenvoy.com	
	Special thanks to Tim Headicar of Foursys	

SOPHOS UTM appliance Integration Guide

This document describes how to integrate an SOPHOS UTM appliance with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

The SOPHOS UTM appliance provides - Secure Remote Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions without the complication of deploying hardware tokens or smartcards.

Two-Factor authentication is provided by the use of your PIN and your Phone to receive the onetime passcode.

SecurAccess is designed as an easy to deploy and use technology. It integrates directly into Microsoft's Active Directory and negates the need for additional User Security databases. SecurAccess consists of two core elements: a Radius Server and Authentication server. The Authentication server is directly integrated with LDAP or Active Directory in real time.

SecurEnvoy Security Server can be configured in such a way that it can use the existing Microsoft password. Utilising the Windows password as the PIN, allows the User to enter their UserID, Windows password and One Time Passcode received upon their mobile phone. This authentication request is passed via the Radius protocol to the SecurEnvoy Radius server where it carries out a Two-Factor authentication. SecurEnvoy utilises a web GUI for configuration, as does the SOPHOS UTM appliance. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Sophos UTM
SOPHOS UTM Ver. 9.312-8

SecurEnvoy
Windows 2012 R2
IIS installed with SSL certificate (required for remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v7.3.501

© 2015 SecurEnvoy Ltd. All rights reserved

Index

1.0 Pre Requisites 4

2.0 Configuration of Sophos UTM appliance for SSL VPN users 4
2.1 Add a new backend authentication RADIUS server 4

3.0 Configuration of SecurEnvoy 6
3.1 Enable Auto User creation for the RADIUS users 6
3.2 Allow RADIUS users to access the End-User Portal 7
3.3 Allow RADIUS users to use the SSL VPN client 8
3.4 Login to the user Portal and download the SSL VPN client 9
3.5 Use of RADIUS authenticated users for other components 10

4.1 Use SecurEnvoy Authentication with PPTP 11
4.2 User SecurEnvoy to authenticate administrative access 12
4.3 Use SecurEnvoy to control web surfing 13

5.0 Limitations: 13

The following table shows what token types are supported.

Token Type Supported	
Soft Token App	✓
Soft Token App Next code (Auto Resync)	✓
SMS Preload Code	✓
SMS Three Code	✓
SMS Day Code	✓
SMS Realtime	X
SMS Preload	✓
Email Three Code	✓
Email Day Code	✓
Email Realtime	X
Voice Call	X
OneSwipe (offline) via QRcode	X

© 2015 SecurEnvoy Ltd. All rights reserved

Limitations as follows:
SOPHOS UTM does not at the moment support RADIUS Access Challenge it is not possible to use token types that require two logon steps.
It is also currently not possible to customize the login screen so the OneSwipe Offline button cannot be added"

1.0 Pre Requisites

It is assumed that the Sophos UTM appliance is setup and operational. An existing Domain user can authenticate using a Domain password and access applications, your users can access through SSL VPN using local accounts or Domain accounts.

Securenvoy Security Server has a suitable account created that has read and write privileges to the Active Directory, if firewalls are between the SecurEnvoy Security server, Active Directory servers, and the Astaro Security Gateway, additional open ports will be required.
NOTE: *SecurEnvoy requires LDAP connectivity either over port 389 or 636 to the Active Directory servers and port 1645 or 1812 for RADIUS communication from the Sophos UTM appliance.*

NOTE: *Add radius profiles for each* SOPHOS UTM *appliance that requires Two-Factor Authentication.*

2.0 Configuration of SOPHOS UTM appliance for remote assess VPN users

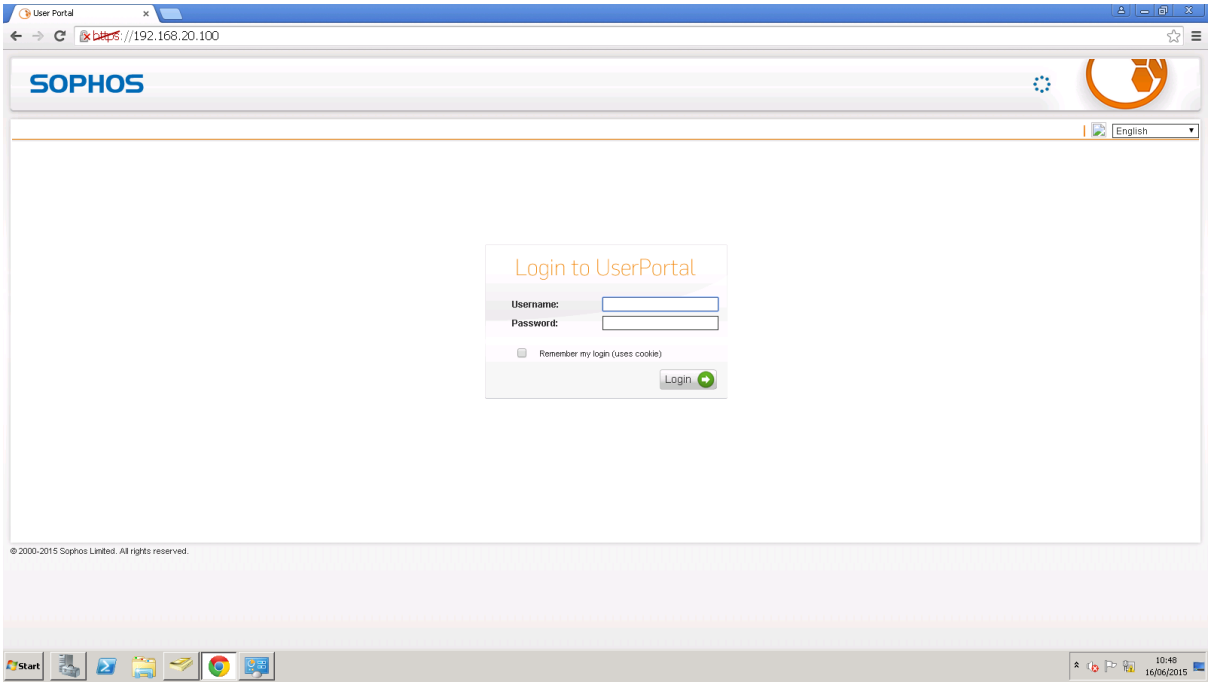
To enable a SecurEnvoy Two-Factor authentication logon to the Astaro Security Gateway UTM appliance, login to the administration interface.

See diagrams below

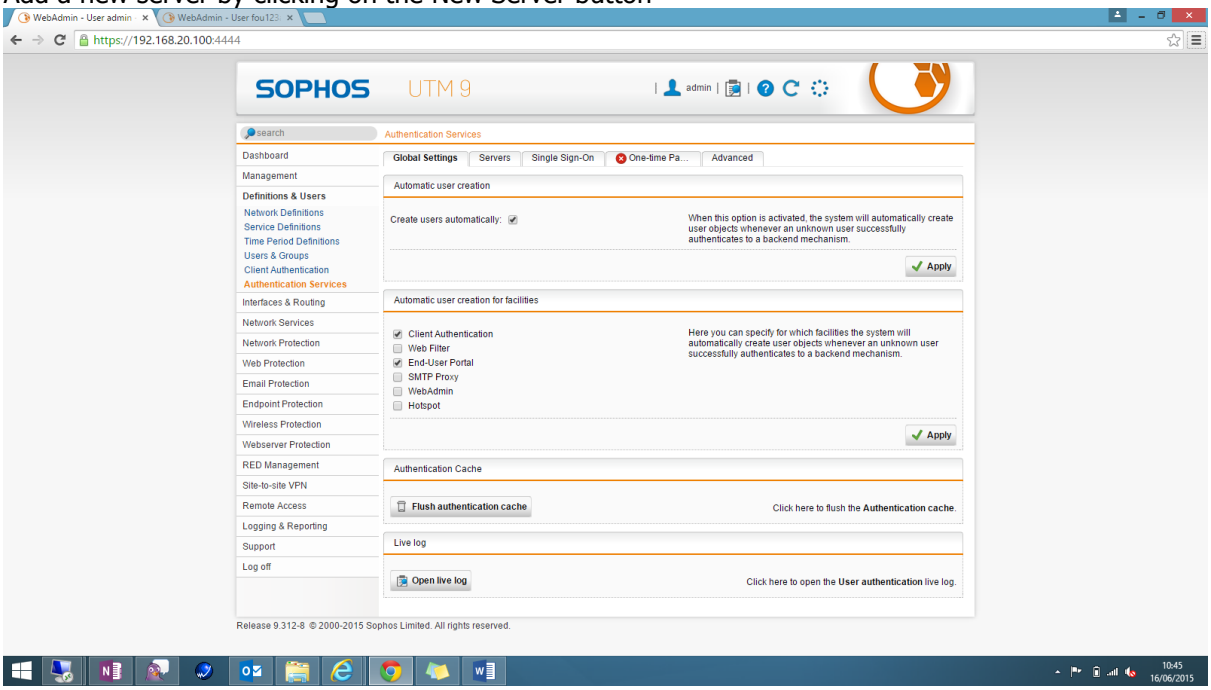
2.1 Add a new backend authentication RADIUS server

Log in to the WebAdmin interface.

© 2015 SecurEnvoy Ltd. All rights reserved



Go to Users -> Authentication -> Servers
Add a new server by clicking on the New Server button



Choose Backend: Radius
Click on the + sign next to Server and enter
Name: SecurEnvoy RADIUS server
Type: Host
Address: your SecurEnvoy IP Address

In the Pop-Up and click Save

Enter the Shared secret value according to your SecurEnvoy configuration.

Please note that the "Test" button does not work for "Test server settings" but only if you enter a valid Username: and Password: (OTP)

3.0 Configuration of SecurEnvoy

SecurEnvoy Radius configuration is set up to authenticate both the PIN and Passcode component. By default SecurEnvoy use the domain password as the PIN component. This allows an easy to use mechanism for the end user without having to first enrol for a PIN.

SecurEnvoy supplies the second factor of authentication, which is the dynamic one time passcode (OTP) which is sent to the user's mobile phone.

Launch the SecurEnvoy admin interface, by executing the Local Security Server Administration link on the SecurEnvoy Security Server.

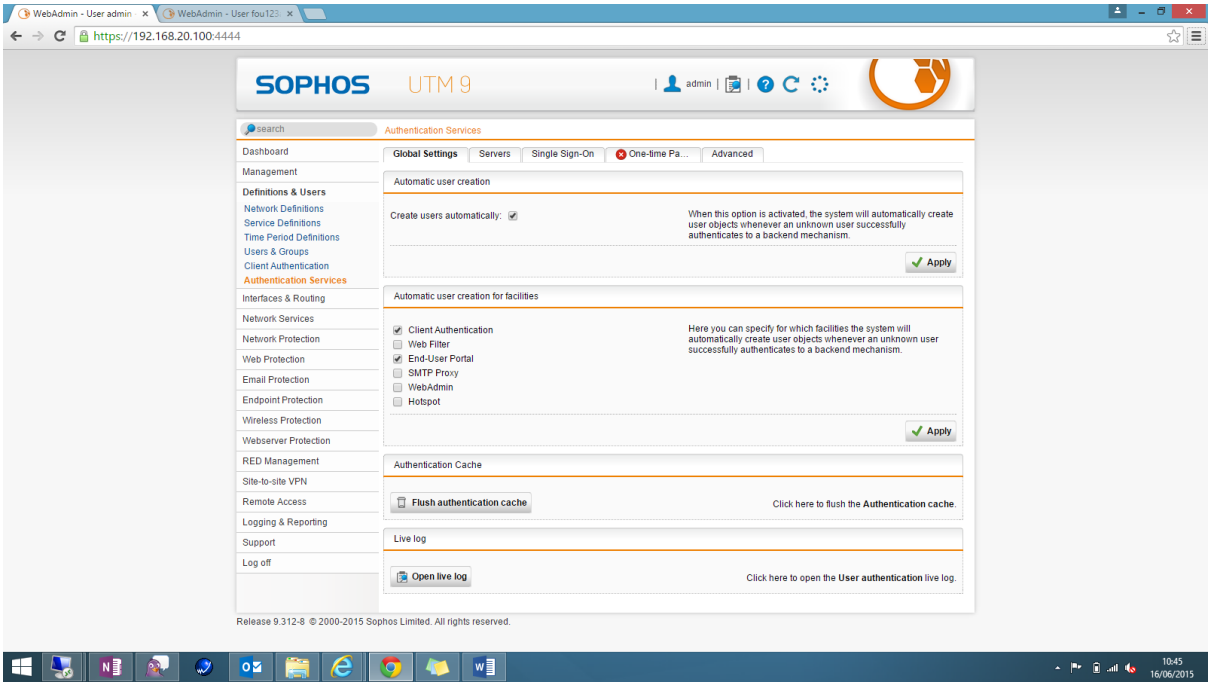
1. Click the **"Radius"** Button
2. Enter IP address and Shared secret for each Citrix Web Interface server that wishes to use **SecurEnvoy** Two-Factor authentication.
3. Make sure the "Authenticate Passcode Only (Pin not required) checkbox is unticked.



4. Press Update
5. Now Logout

3.1 Enable Auto User creation for the RADIUS users

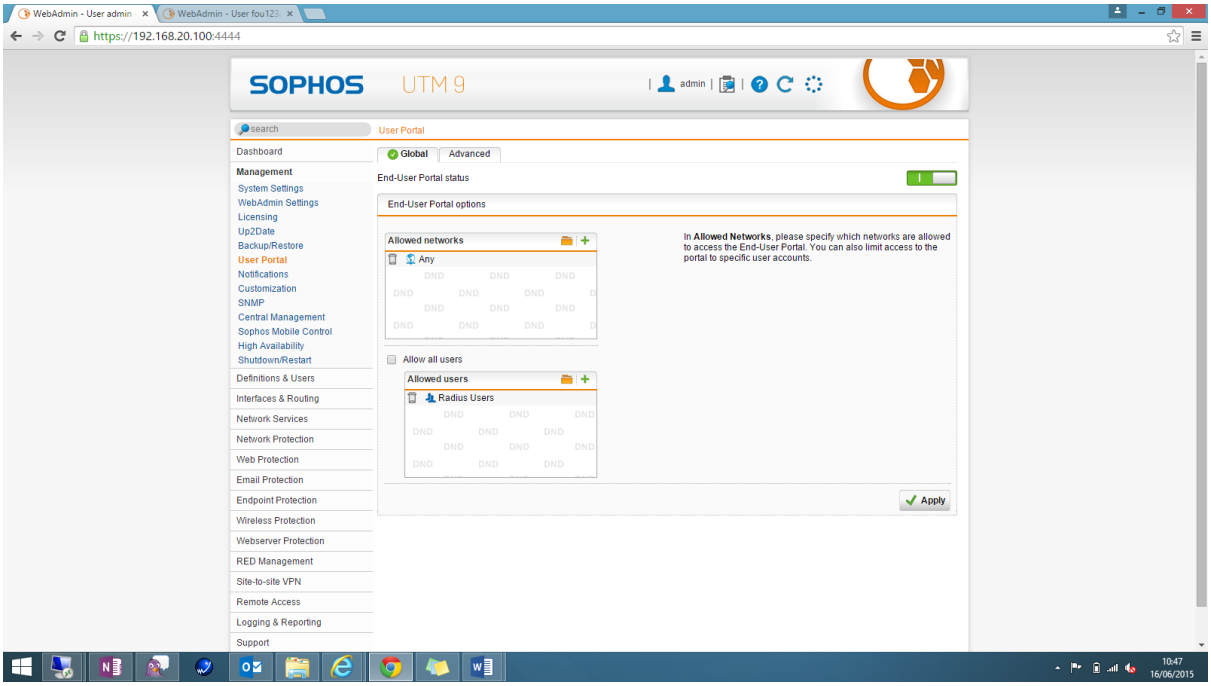
© 2015 SecurEnvoy Ltd. All rights reserved



Go to Users-> Authentication -> Global Settings and enable "Create users automatically". Now click Apply. After that choose "End-User Portal" and "SSL VPN" below and click Apply.

3.2 Allow RADIUS users to access the End-User Portal

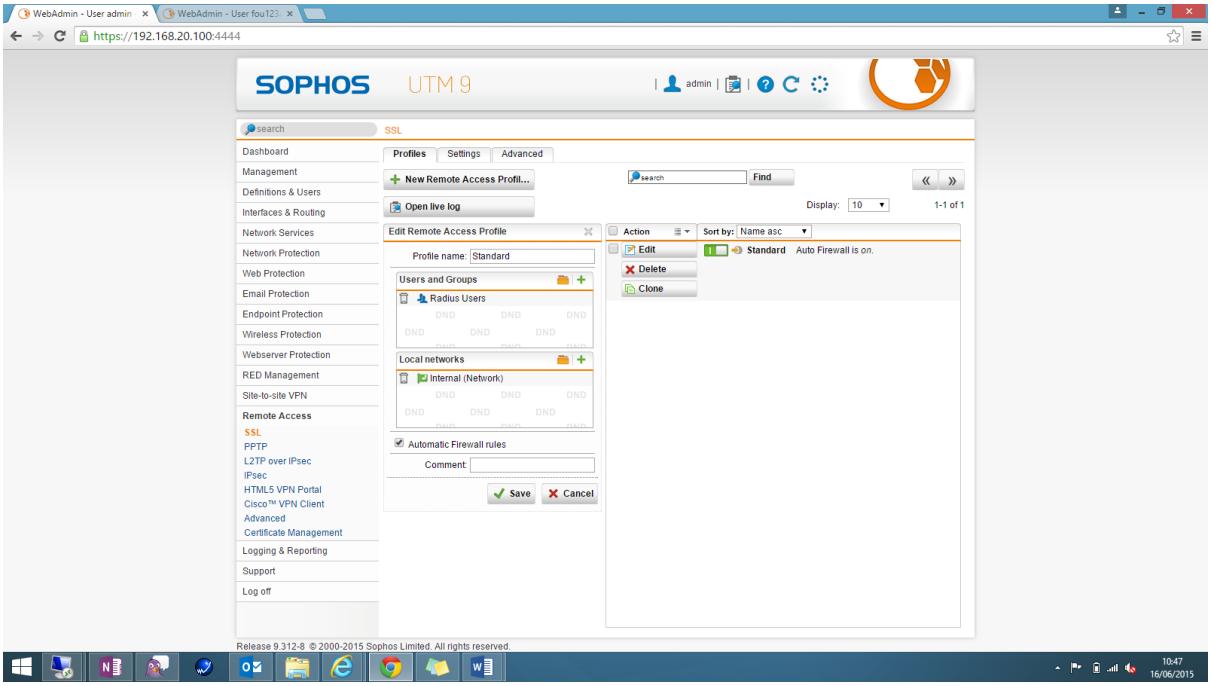
In order to get their SSL VPN client and configuration, users have to initially log in to the End User portal. Make sure that RADIUS authenticated users are allowed to log in.



Go to Management-> User Portal and add the "Radius Users" group to the list of allowed users. You can choose this group by clicking on the Folder icon and drag and drop it from the list on

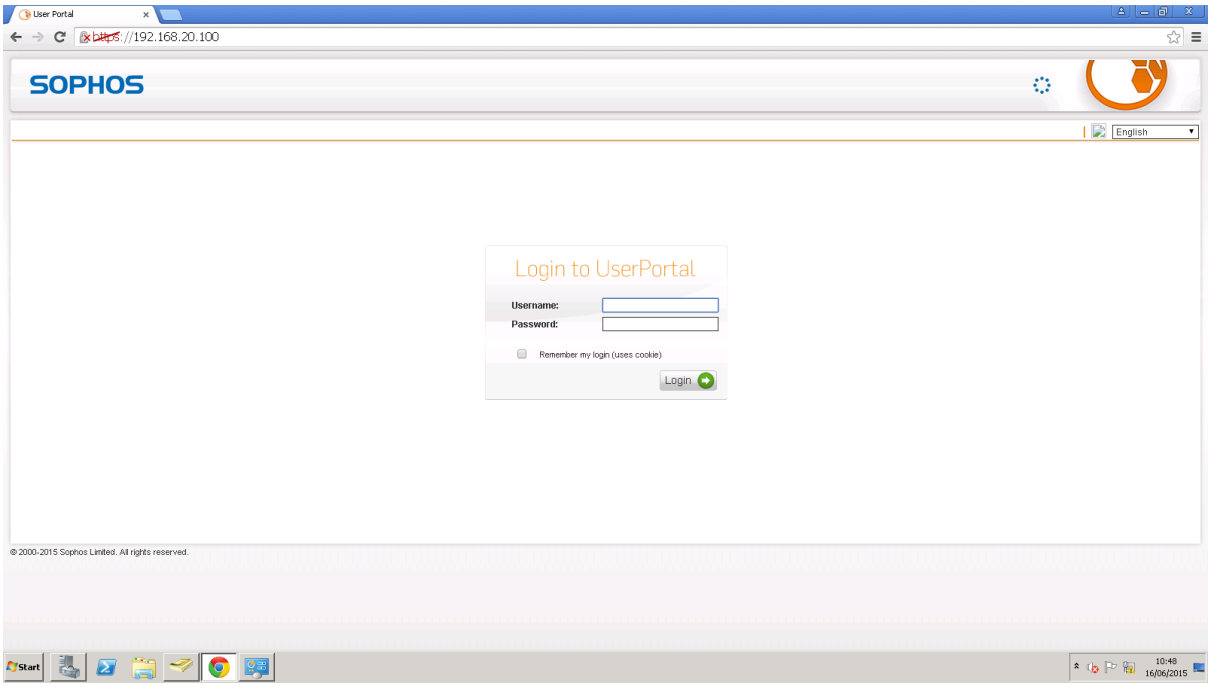
3.3 Allow RADIUS users to use the SSL VPN client

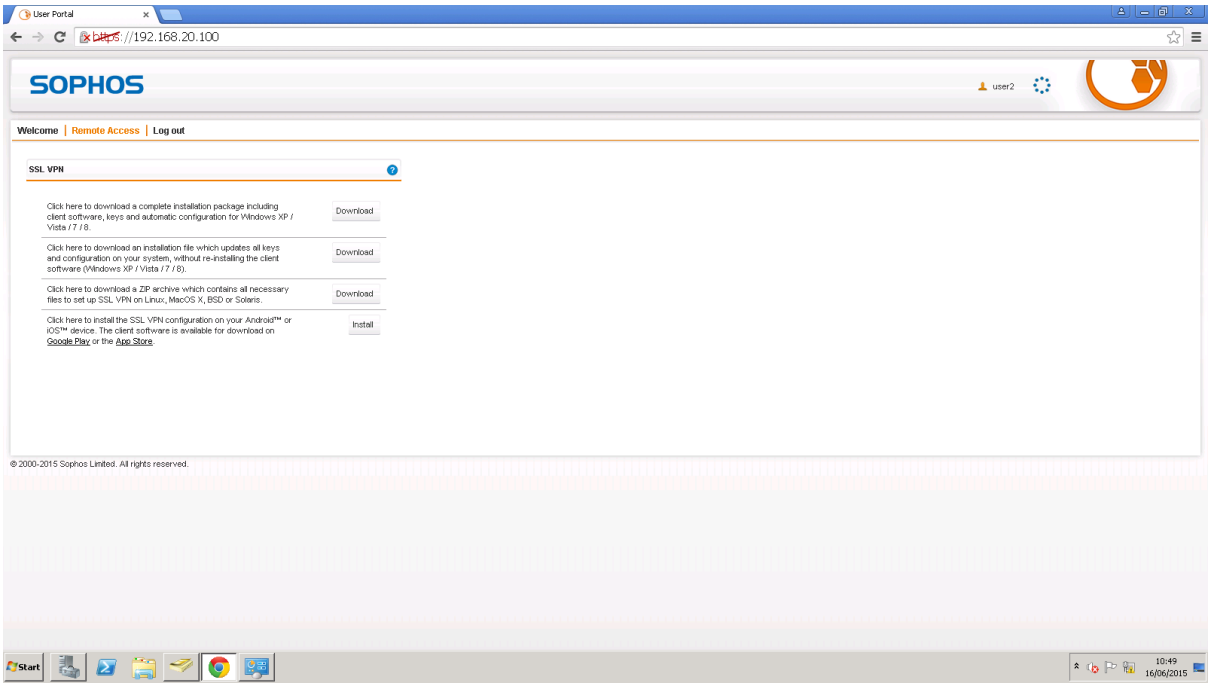
Go to Remote Access -> SSL and make sure that the Radius Users group is also listed under "Users and Groups". Again use the Folder icon and drag and drop the group in the according field.



3.4 Login to the user Portal and download the SSL VPN client

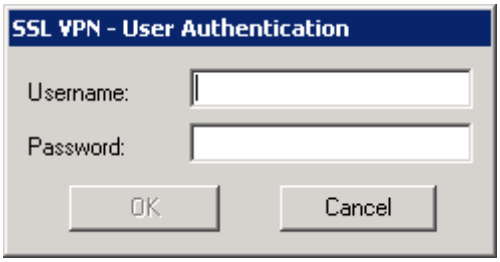
Access your user portal and log in with your SecurEnvoy Domain User ID and your assigned OTP / RADIUS password





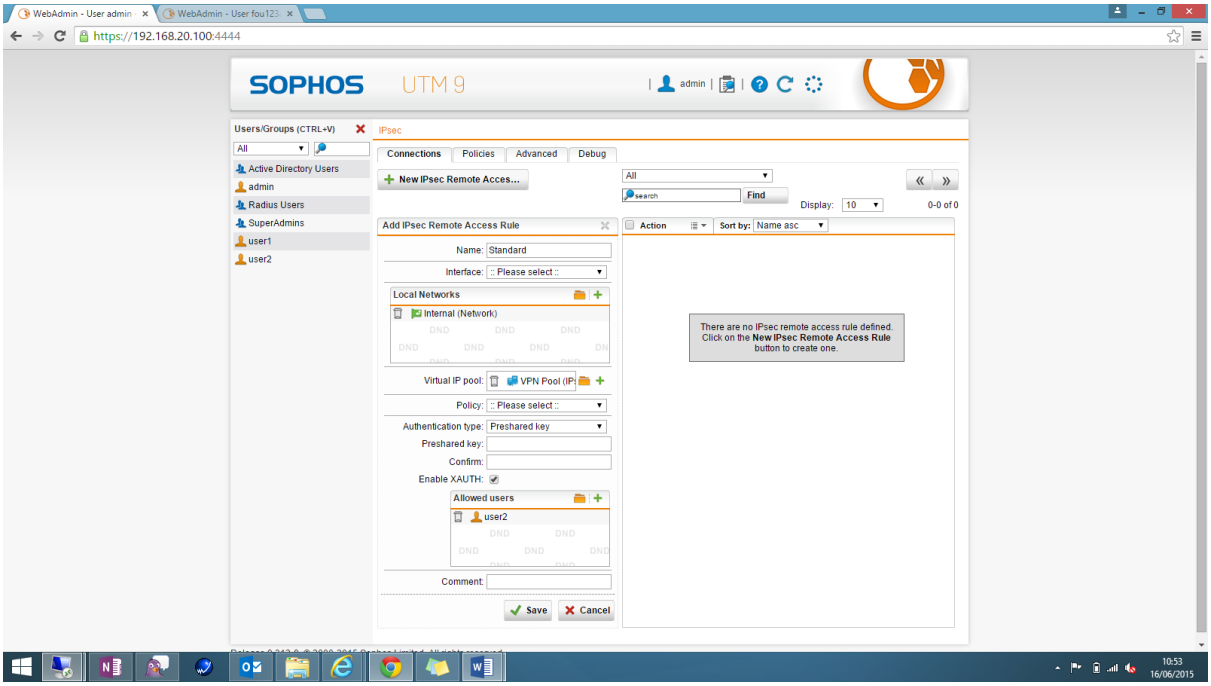
Go to Remote Access and download the SSL VPN installation package (1st link) and install it on your clients PC.

If you start the SSL connection, you can now enter your Username and your PIN+OTP under "Password:"



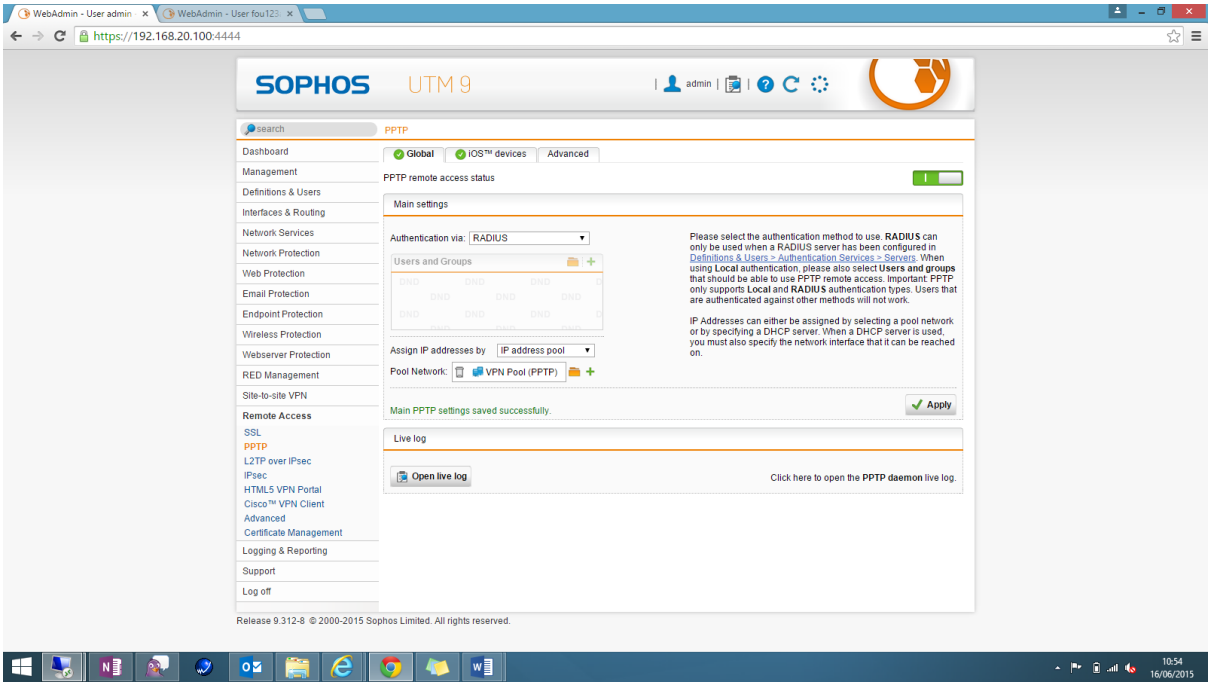
3.5 Use of RADIUS authenticated users for other components

You can also use SecurEnvoy authenticated users with IPSec VPN. Just enable the XAUTH option to check for OTP:

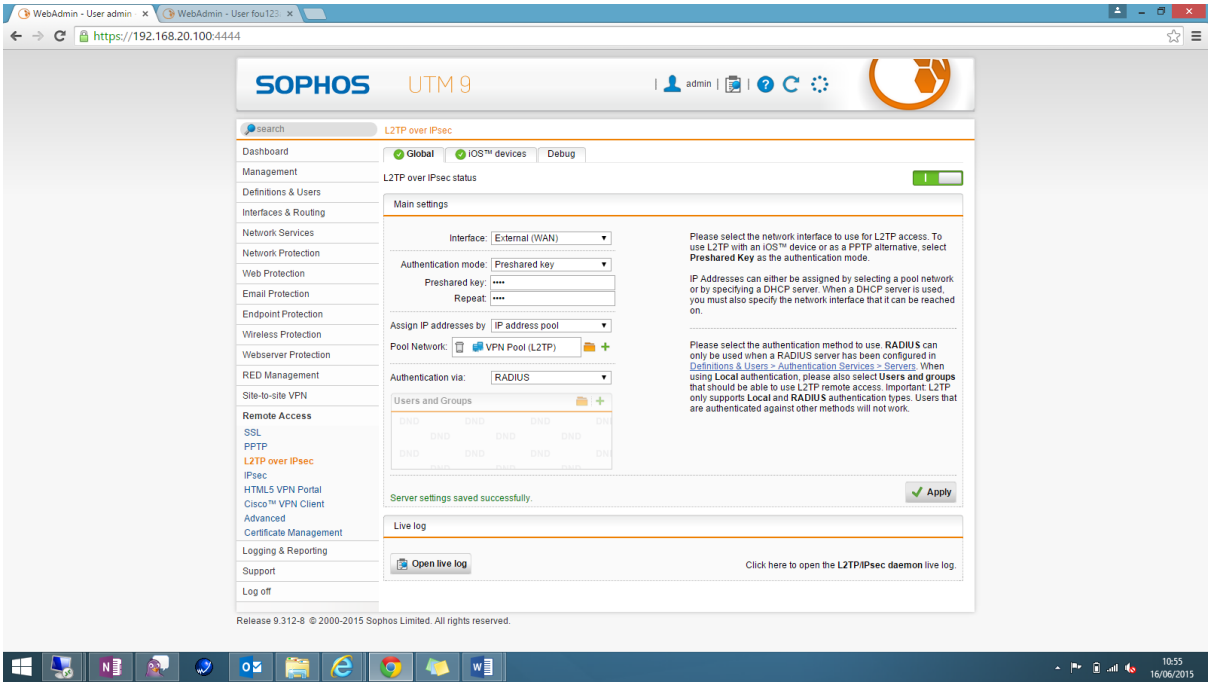


4.1 Use SecurEnvoy Authentication with PPTP

Go to Remote Access -> PPTP and change the authentication method to "RADIUS"



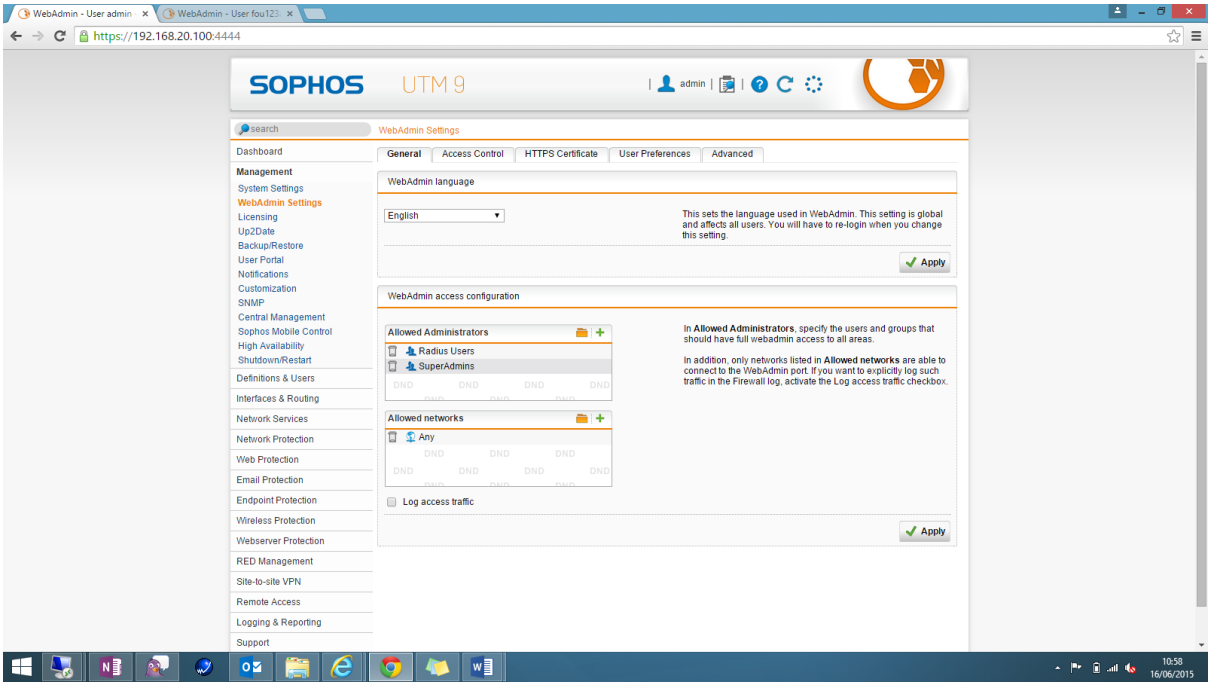
Use SecurEnvoy Authentication with L2TP over IPSec



Go to Remote Access -> L2TP over IPSec and chance Access Control -> Authentication via: to RADIUS

4.2 User SecurEnvoy to authenticate administrative access

Go to Management -> WebAdmin Settings -> Access Control and add the RADIUS Users or RADIUS group to the list of Allowed Administrators or Allowed Auditors:



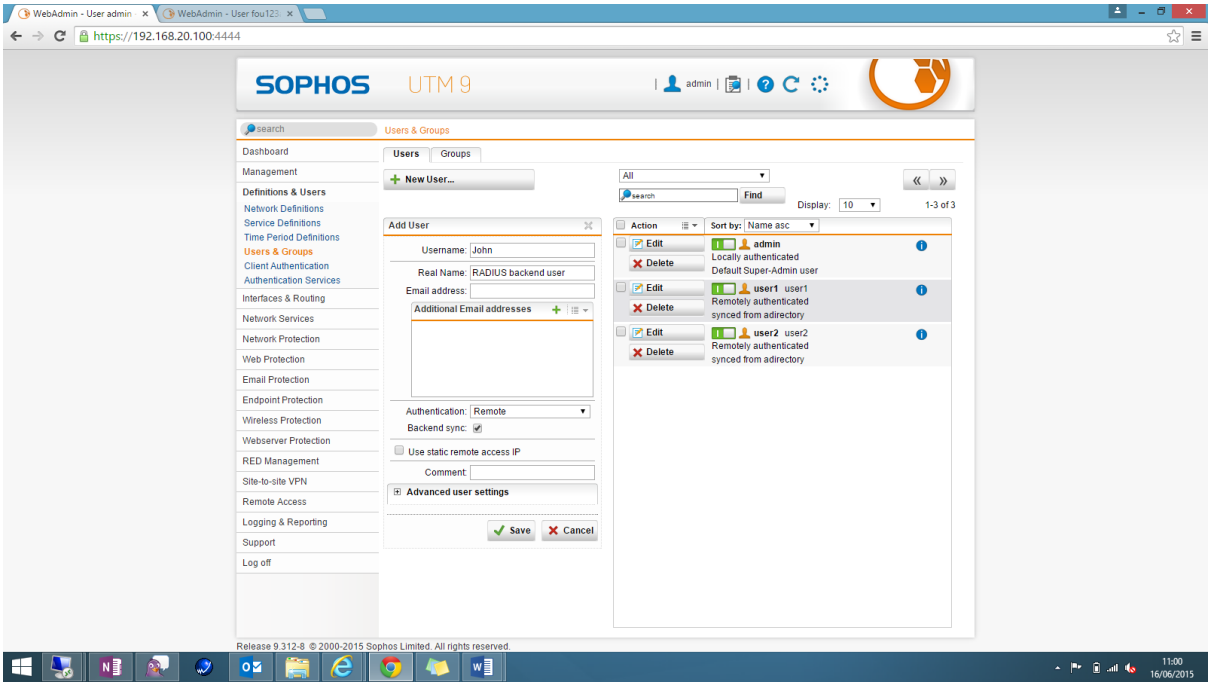
4.3 Use SecurEnvoy to control web surfing

RADIUS users can also be used to control access to the HTTP proxy.

Go to Web Security -> HTTP/S and choose either Basic User Authentication or Transparent with authentication and add the RADIUS group or single users to the list of allowed users/Groups.

Allow only single users from the SecurEnvoy RADIUS server to access specific resources
In order to limit access to specific users and not the whole SecurEnvoy user base, create local users with a matching user name. Those users are auto-generated upon first login to the User Portal but can be also pre-created by adding them manually

Go to Users -> Users and click New user...



Use the same user name as used in the backend (e.g. your Active Directory) and choose Authentication: Remote. Make sure to activate Backend sync:

You can now use this single user in every access control segment mentioned above.

5.0 Limitations:

As the SOPHOS UTM does at the moment not support Challenge-Response it is not possible to use the Real Time SMS feature. The solution only works with preloaded or timed OTPs.