External authentication with Citrix Xen App (Web Interface) version 5 Authenticating Users Using SecurAccess Server by SecurEnvoy

Contact information		
SecurEnvoy	www.securenvoy.com	0845 2600010
	1210 Parkview Arlington Business Park Theale Reading RG7 4TY	
Phil Underwood	Punderwood@securenvoy.com	
	Special thanks to Jan Jonker of ICTaurus for the Citrix configuration	http://www.ictaurus.nl

Citrix Xen App (Web Interface v5) (Radius) Integration Guide

This document describes how to integrate a Citrix Xen App (Web Interface) with SecurEnvoy two-factor Authentication solution called 'SecurAccess'.

The Citrix Xen App (Web Interface) provides - Secure Remote Access to the internal corporate network.

SecurAccess provides two-factor, strong authentication for remote Access solutions (such as Citrix Secure Gateway series), 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. All notes within this integration guide refer to this type of approach.

The equipment used for the integration process is listed below:

Citrix
Citrix Xen App (Web Interface) ver. 5.x

SecurEnvoy
Windows 2003 server SP1
IIS installed with SSL certificate (required for remote administration)
Active Directory installed or connection to Active Directory via LDAP protocol.

SecurAccess software release v5.3.501

© 2005 SecurEnvoy Ltd. All rights reserved

Index

1.0 Pre Requisites 3
2.0 Configuration of Citrix using Radius 4
2.1 Citrix Web Interface Radius configuration 4
3.0 Configuration of SecurEnvoy 6
4.0 SecurEnvoy and Citrix in a Managed Services Environment 7

Additonal Configuration

4.1 Additional Citrix configuration for UPN support 8

1.0 Pre Requisites

It is assumed that the Citrix Xen App (Web Interface) *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 Citrix server, 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 Citrix® Web Interface.*

NOTE: *Add radius profiles for each Citrix server® that requires Two-Factor Authentication.*

© 2005 SecurEnvoy Ltd. All rights reserved

2.0 Configuration of Citrix using Radius

Citrix now has the ability to utilise the RADIUS protocol for user authenticating.

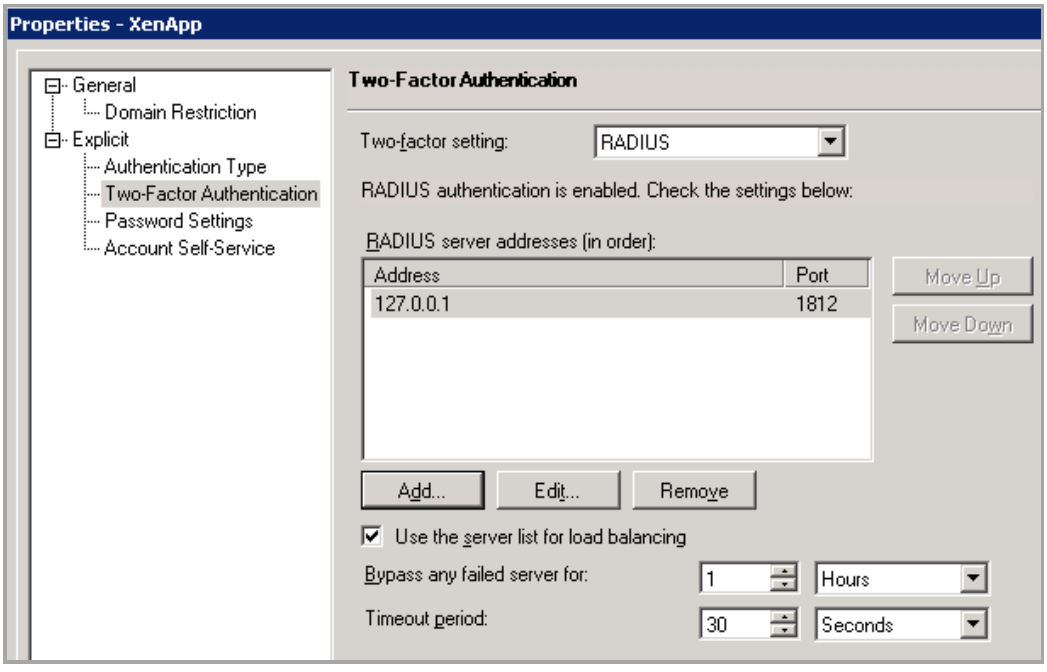
It is recommended to use the RADIUS protocol for authentication, as it allows existing Citrix Web Login pages to be utilised. The standard Citrix pages are used which allows greater flexibility and less overhead when updating the Citrix software, as there is no need to customise the Web Login page..

2.1 Citrix Web Interface Radius configuration

Navigate to the Citrix Web Interface and select the web site that requires SecurEnvoy authentication.

Then select authentication methods, Explicit 2 Factor Authentication and finally select Radius.

Click “ADD” and enter the IP address of the SecurEnvoy server and the port number (1812 = default)



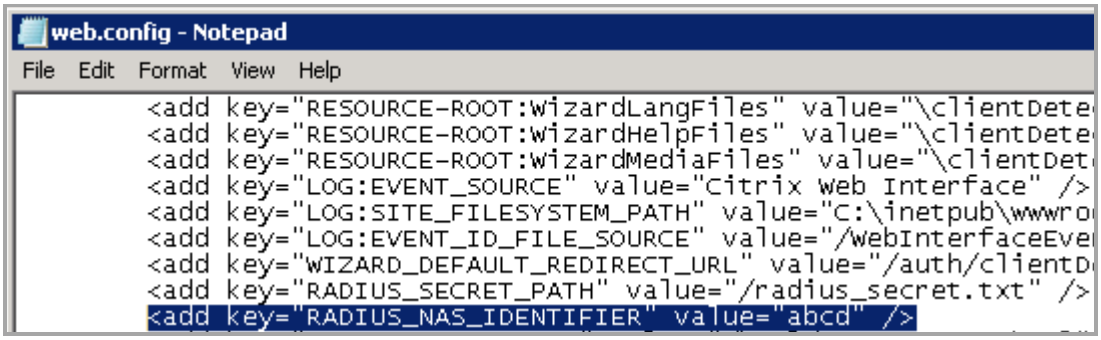
Navigate to \inetpub\wwwroot\Citrix\yourwebsite and edit the web.config file,
NOTE: before proceeding it is recommended that this file is backed up.

Search for *RADIUS_NAS_IDENTIFIER* and enter a text string to identify this Radius profile, in this example we have used “abcd”.

Therefore the entry will show as "RADIUS_NAS_IDENTIFIER" value="abcd" />

Save all changes to this file. If a Citrix repair site action is carried out in the Citrix Web interface console this file is going to be restored to its original state. So whenever you need to do a repair, copy the modified file back to this place after the repair.

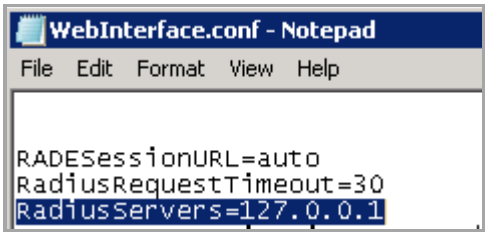
© 2005 SecurEnvoy Ltd. All rights reserved



Navigate to: \inetpub\wwwroot\Citrix\yourwebsite\conf\ and open the webinterface.conf file

NOTE: before proceeding it is recommended that this file is backed up.

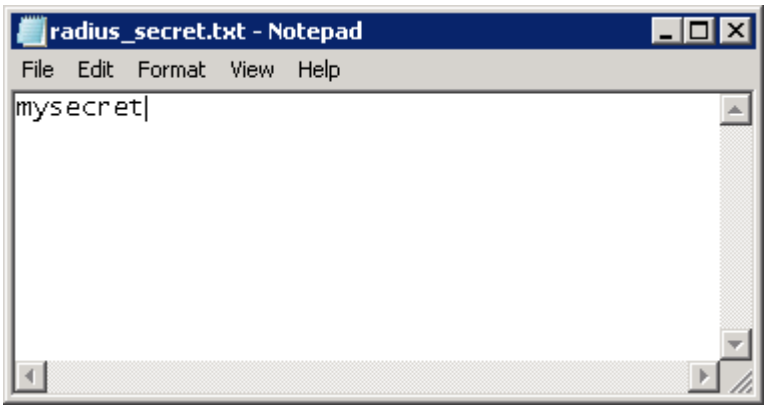
Open with a text editor and find :radiusservers and check if the address of the SecurEnvoy is correct:



Finally navigate to \inetpub\wwwroot\Citrix\yourwebsite\conf and create a text file called “radius_secret.txt” edit this file and enter a Radius shared secret value and save all changes.

This is the same Radius shared secret value that will be used upon the SecurEnvoy server Radius configuration

NOTE: It is recommended to keep a copy of this file in case of deletion or a Citrix site repair is carried out.



© 2005 SecurEnvoy Ltd. All rights reserved

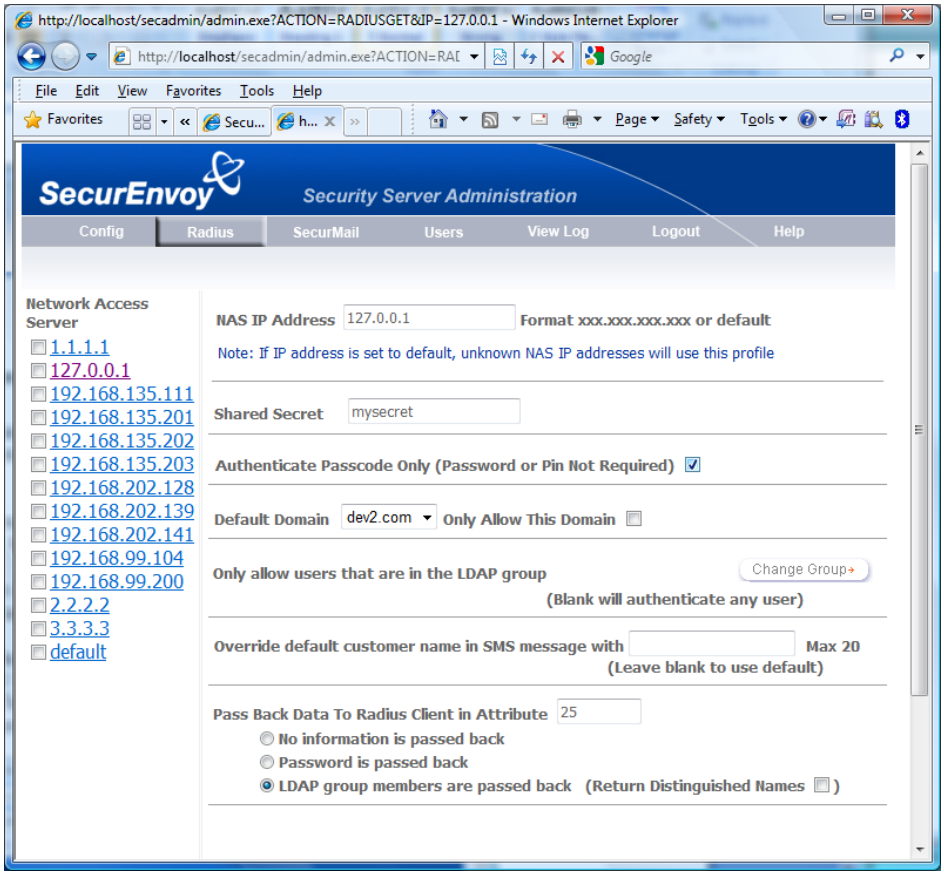
3.0 Configuration of SecurEnvoy

To help facilitate an easy to use environment, SecurEnvoy can be set up to only authenticate the passcode component as both authentication servers that are required to authenticate a remote user.

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 ticked.



4. Press Update
5. Now Logout

© 2005 SecurEnvoy Ltd. All rights reserved

4.0 SecurEnvoy and Citrix in a Managed Services Environment (Multiple UPN Suffix support)

Within a Citrix Managed Services Environment, there is typically a single domain model but supporting many Managed services customers; these are generally logically separated by OU within the Microsoft Active Directory domain.

Microsoft Active Directory domain controllers can authenticate a user with two distinct ways. The first is support for pre Windows 2000 logon name (samaccountname), the second is support for User Logon name (User-Principal-Name or UPN).

When a user authenticates the short name is checked against the Active Directory for the actual domain, however as this is a managed services environment they is only one domain, so any duplication of user accounts will cause an error.

See example:

You have one domain named W23.com and have added some domain suffixes like W24.com and W25.com and there are 3 users with the same username in these domain(suffixes) so we have :

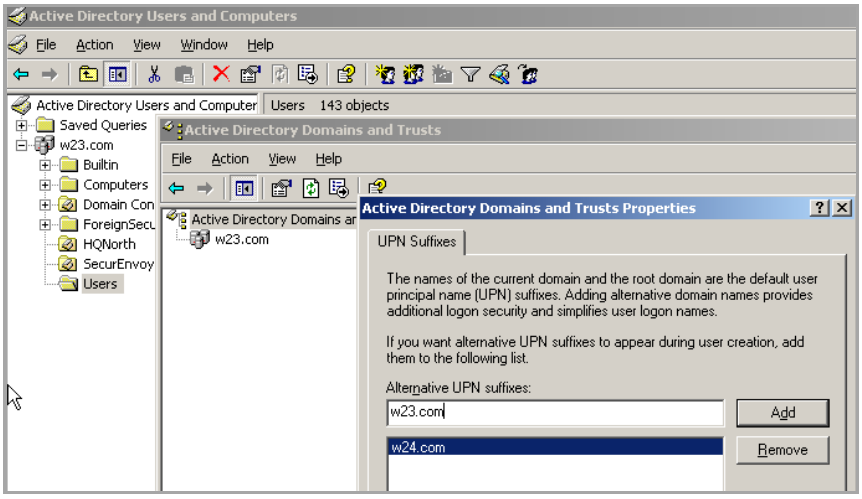
testuser@ W23.com (pre windows2000 logon name: testuser)
testuser@ W24.com (pre windows2000 logon name: testuser_W24)
testuser@ W25.com (pre windows2000 logon name: testuser_W25)

In default behaviour when Citrix utilises 2 Factor Authentication, it will automatically remove the domain component and forward only the short name, so only “testuser” is submitted to the active directory . In normal circumstances (no identical usernames) this will work fine. But in this case not since there are 3 identical usernames.

What happens in this case is that the Active Directory checks this name to its pre windows 2000 name database and comes up with the first username of “testuser” it matches.

The recommended solution to overcome this issue is to use User-Principal-Name or UPN authentication.
Multiple UPN suffixes are allowed in the same domain and can be configured then there is some extra action required. For example:

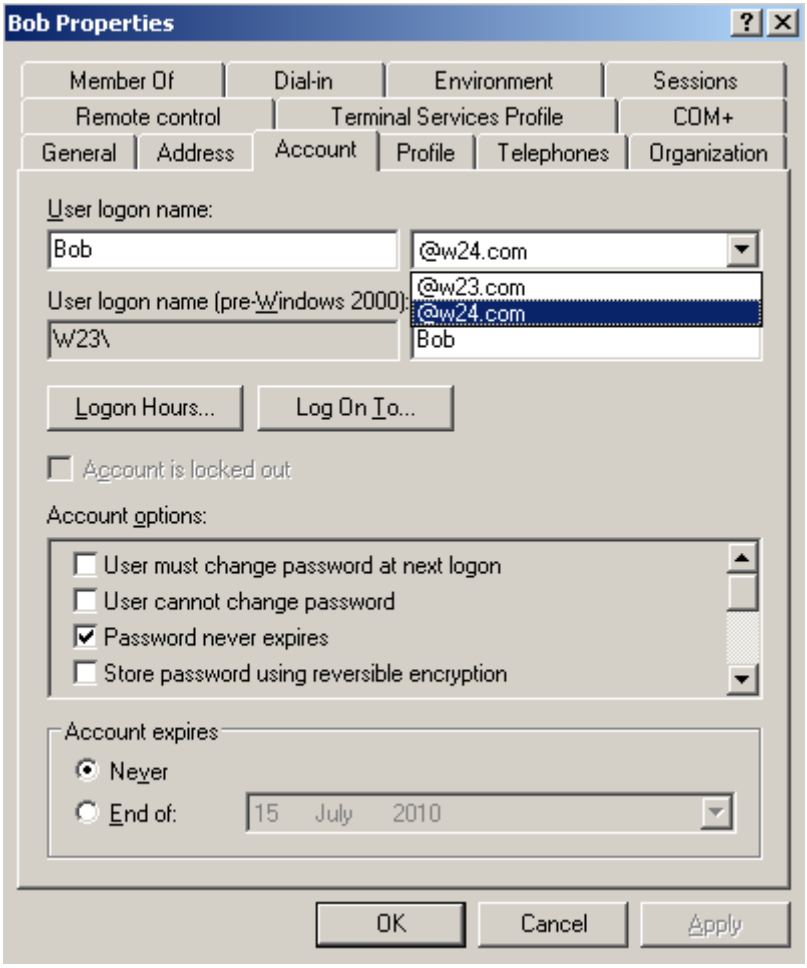
Run the Active Directory Domains and Trusts MMC, create additional UPN suffixes as required.



© 2005 SecurEnvoy Ltd. All rights reserved

After the UPN suffixes have been created, when a new user is created or an existing user is edited, the User logon Name (UPN) will have a drop down box so that the correct UPN suffix can be applied.

NOTE: *The pre Windows 2000 logon name must be unique for the domain*



4.1 Additional Citrix configuration for UPN support

Navigate to
\inetpub\wwwroot\Citrix\yourwebsite\app_code\PagesJava\com\citrix\wi\pageutils

NOTE: before proceeding it is recommended that this file is backed up.

Edit the TwoFactorAuth.java

Locate the following section: :

```
public static String getUserName(UPNCredentials token, boolean fullyQualified) {
        if (fullyQualified) {
        return token.getShortDomain() + "\\" + token.getShortUserName();
        } else {
        return token.getShortUserName();
        }
```

© 2005 SecurEnvoy Ltd. All rights reserved

}

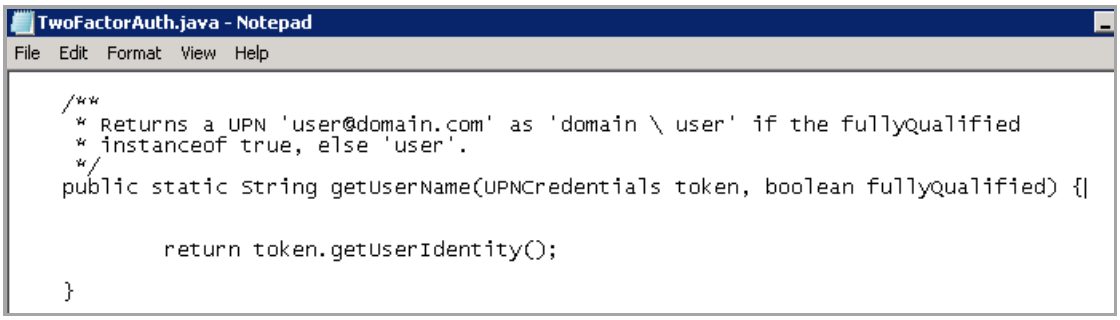
Now replace this with:

public static String getUserName(UPNCredentials token, boolean fullyQualified) {

return token.getUserIdentity();

}

Save all changes (Please keep a copy of this file)



© 2005 SecurEnvoy Ltd. All rights reserved