QUICK START GUIDE

SecurEnvoy SecurAccess

Abstract

This document walks you through an installation of the SecurEnvoy SecurAccess product within your environment quickly and easily.

Document Version 1.12

Michael Urgero

murgero@securenvoy.com

Contents

Getting Started 2

Things You Will Need 2

Microsoft Windows 2008 R2 or Windows 2012 R2 2

Authentication Processing Topology 3

Installation of Microsoft IIS Web Services and Microsoft .Net 3.5 4

Configure AdminSDHolder Permissions 8

Installing & Configuring SecurEnvoy SecurAccess 11

Configure your RADIUS Client 21

Registering your First Device 22

Support for Your Trial 25

What's Next 25

Getting Started

The purpose of this document is to outline the general steps for the installation and validation of the SecurEnvoy SecurAccess Two-factor Authentication Solution within your environment quickly and easily.

The SecurEnvoy SecurAccess Two-Factor Authentication Solution has many features and options. We will not be covering all features and options in this guide. The intent of this guide is to provide instruction for the initial implementation and allow customers to explore additional features as they see fit.

Advanced configuration features are not covered here. If you are looking for advanced configuration instructions, please follow the advanced configuration guide.

At the end of this guide you will have a fully functional environment.

Things You Will Need

This document will assume that the reader is a network and systems administrator with administrative level access to the systems required for this implementation, listed below. If you do not currently have this level of access to the environment, you should obtain it before you continue.

To properly implement SecurEnvoy SecurAccess you will need the following;

- A single Microsoft Windows 2008 R2 or 2012 R2 Server, either physical or virtual.
- Administrative Access to your Microsoft Active Directory.
- Download the SecurEnvoy SecurAccess product latest version.

Download is available here: https://www.securenvoy.com/products/securaccess/key-features.shtm

Microsoft Windows 2008 R2 or Windows 2012 R2

Here are some basic items to cover about the server you chose to use.

- Your server can be physical or virtual.
- Your selection of which server version you choose does not impact the implementation.
- Please assure that your server is fully patched as a best practice.
- There is no requirement for the SecurEnvoy SecurAccess server to be a member of the Active Directory.

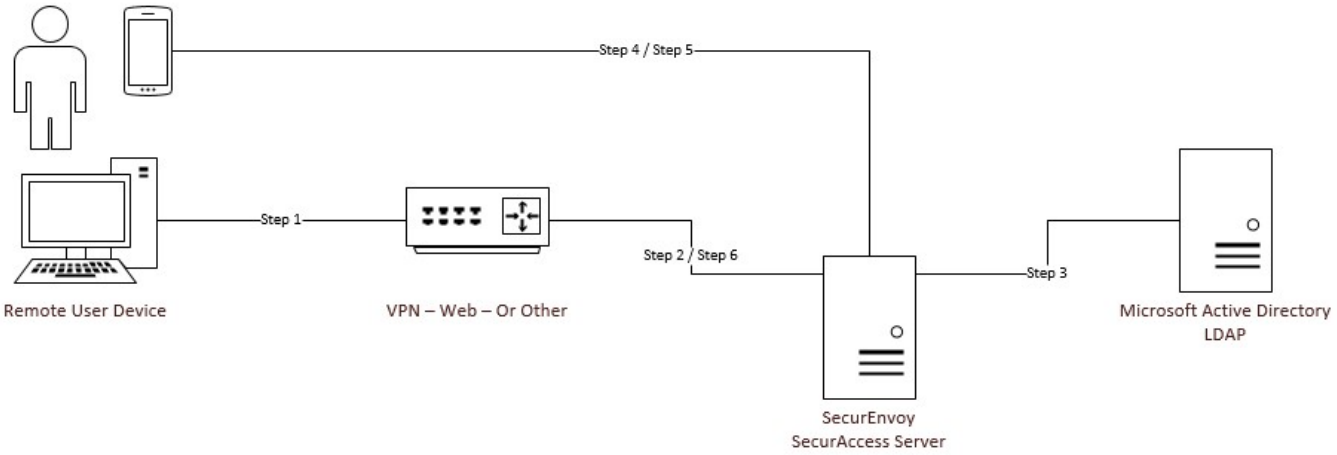
Examples;

- Microsoft Windows 2012 R2 Virtual Guest on VMware ESX and is a member of the Active Directory.
- Microsoft Windows 2008 R2 Physical Server in a workgroup.

Either of the above examples will work.

Authentication Processing Topology

In the below simplified diagram, we are showing a VPN, using RADIUS with SecurEnvoy SecurAccess Two Factor Authentication and a Microsoft Active Directory.



Step 1: The user on a device (internal or external) makes a request for authentication to a VPN, Web Site or some other application which uses RADIUS authentication.

Step 2: A RADIUS authentication package is delivered to the SecurEnvoy SecurAccess Server for processing.

Step 3: LDAP Credentials are validated against the Microsoft Active Directory.

Step 4: Using information from the Active Directory user account, an Approve / Decline message is delivered to the users mobile device.

Step 5: The user approves the authentication by acknowledging the message. This causes the SecurEnvoy Phone App to send Secure Passcodes to the SecurEnvoy Server.

Step 6: The SecurEnvoy Server returns a 'Good to Go' message to the VPN.

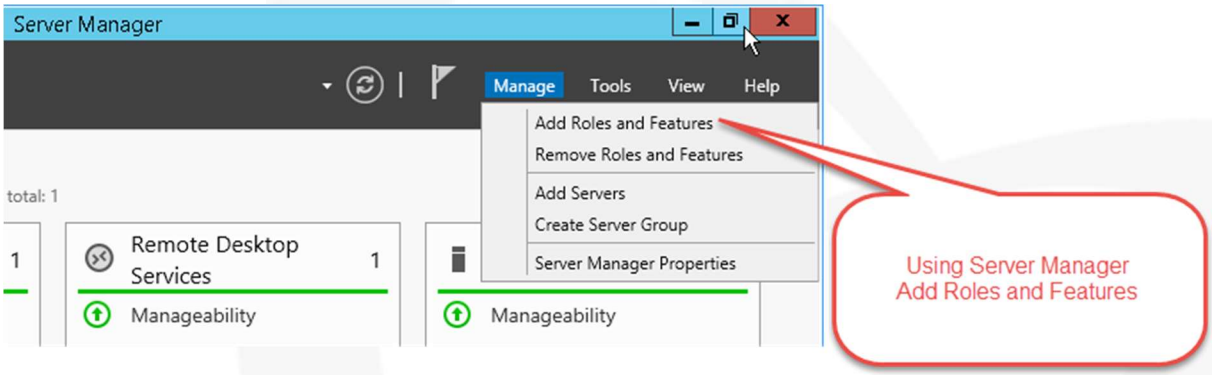
It's important to note that there are many options and methods for delivering the second factor authentication. In our example and for the purposes of this quick start guide, we're keeping it as simple as possible.

As you explore the product and its features, you'll find the many options available and we encourage you to try ones that you would want to work with in your environment.

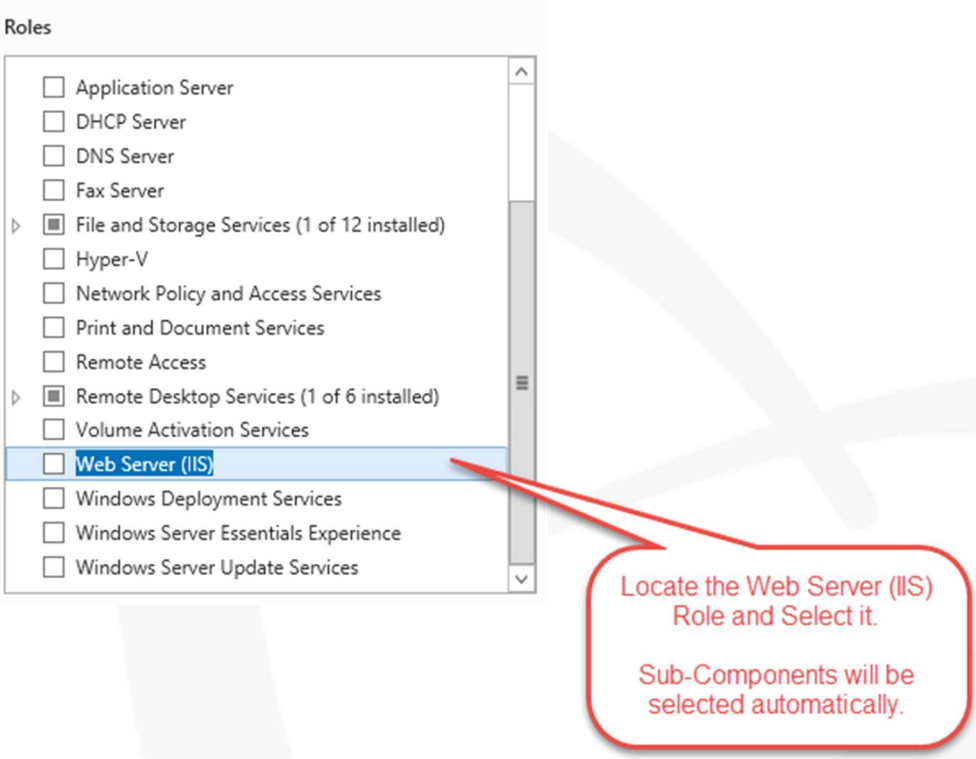
Installation of Microsoft IIS Web Services and Microsoft .Net 3.5

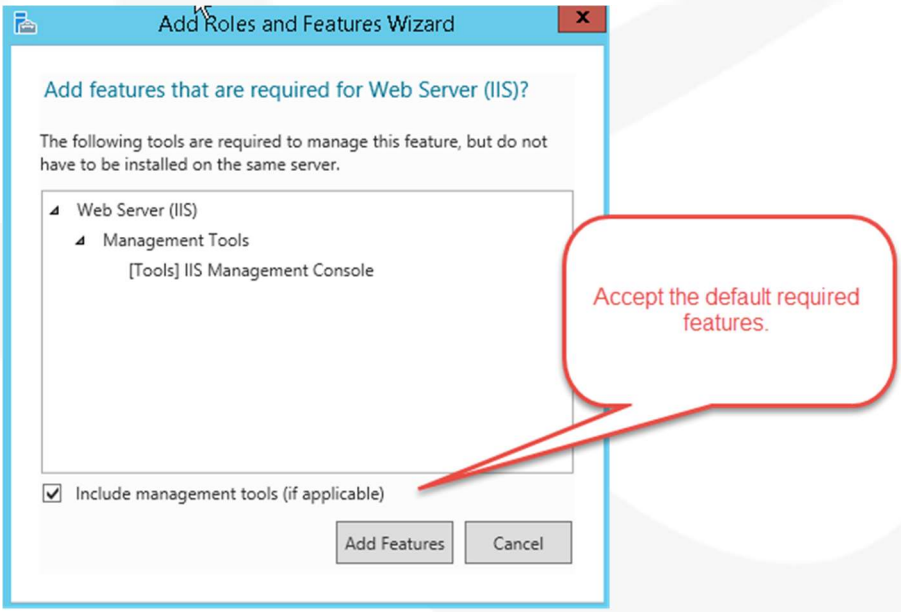
The SecurEnvoy SecurAccess Two Factor Authentication Solution uses http and https for communication. This allows you to use the solution both internally and externally easily.

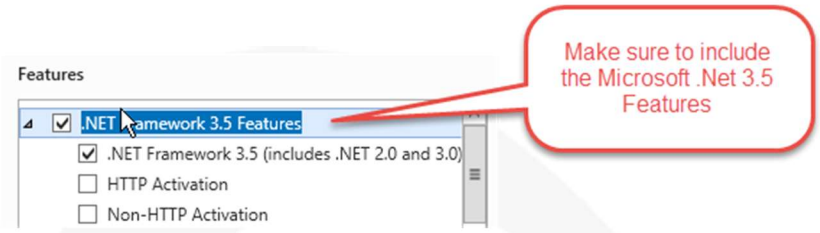
We will begin the implementation with the web components that are required for the SecurAccess. Microsoft IIS Web Services and Microsoft .Net 3.5.

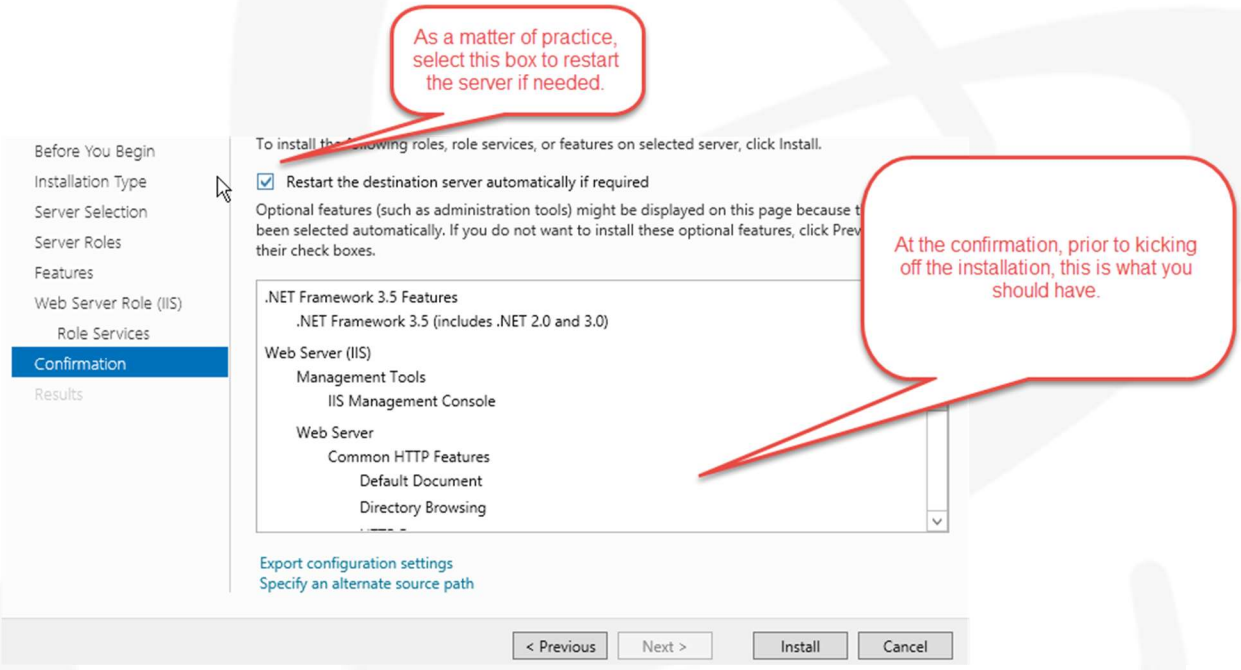


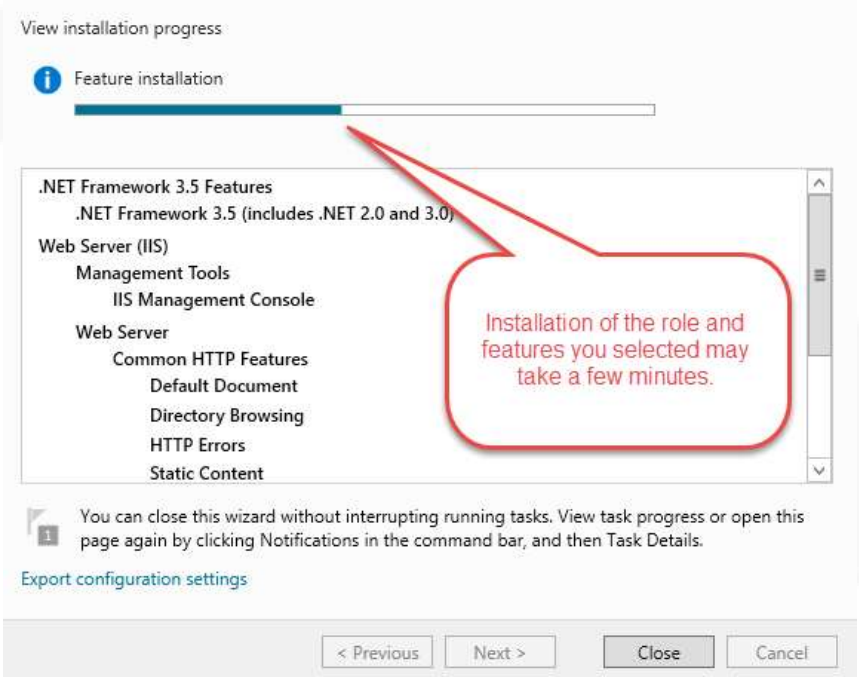


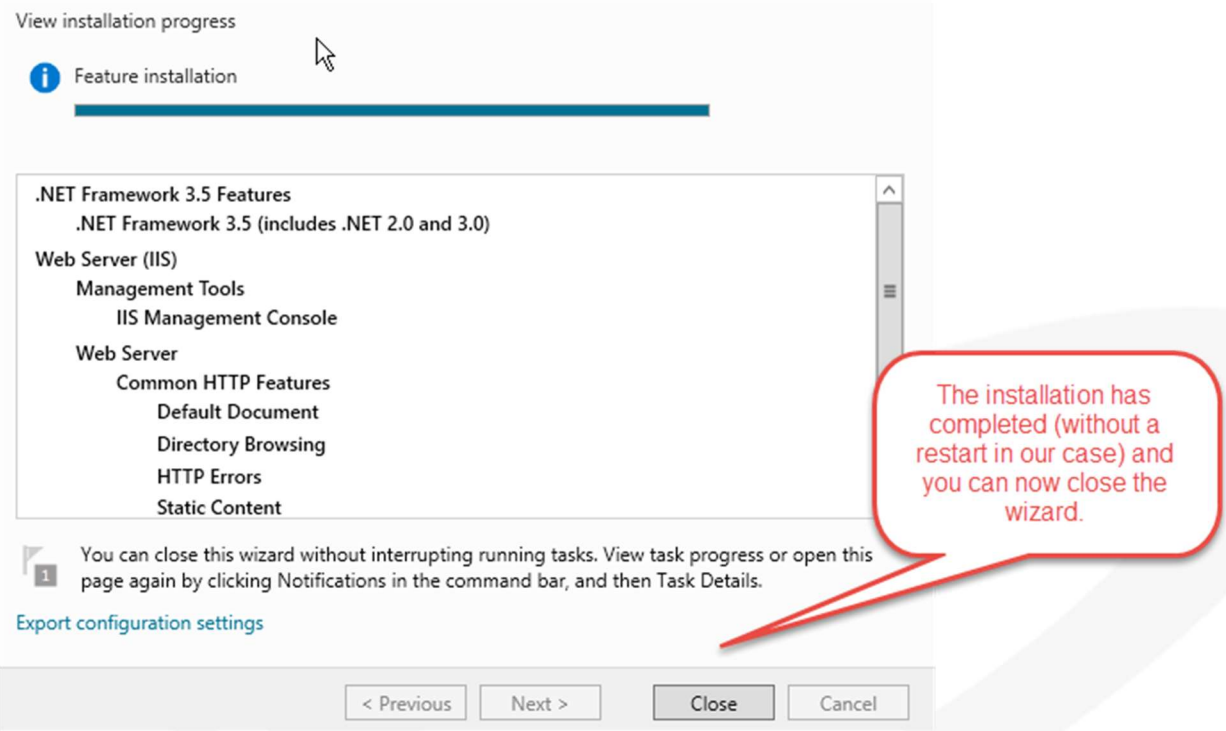

Roles
Application Server
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services (1 of 6 installed)
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Essentials Experience
Windows Server Update Services
Locate the Web Server (IIS) Role and Select it.
Sub-Components will be selected automatically.


Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
Accept the default required features.


Features
.NET Framework 3.5 Features
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
HTTP Activation
Non-HTTP Activation
Make sure to include the Microsoft .Net 3.5 Features


As a matter of practice, select this box to restart the server if needed.
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Restart the destination server automatically if required
.NET Framework 3.5 Features
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
At the confirmation, prior to kicking off the installation, this is what you should have.
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel


View installation progress
Feature installation
.NET Framework 3.5 Features
.NET Framework 3.5 (includes .NET 2.0 and 3.0)
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Installation of the role and features you selected may take a few minutes.
You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.
Export configuration settings
< Previous
Next >
Close
Cancel



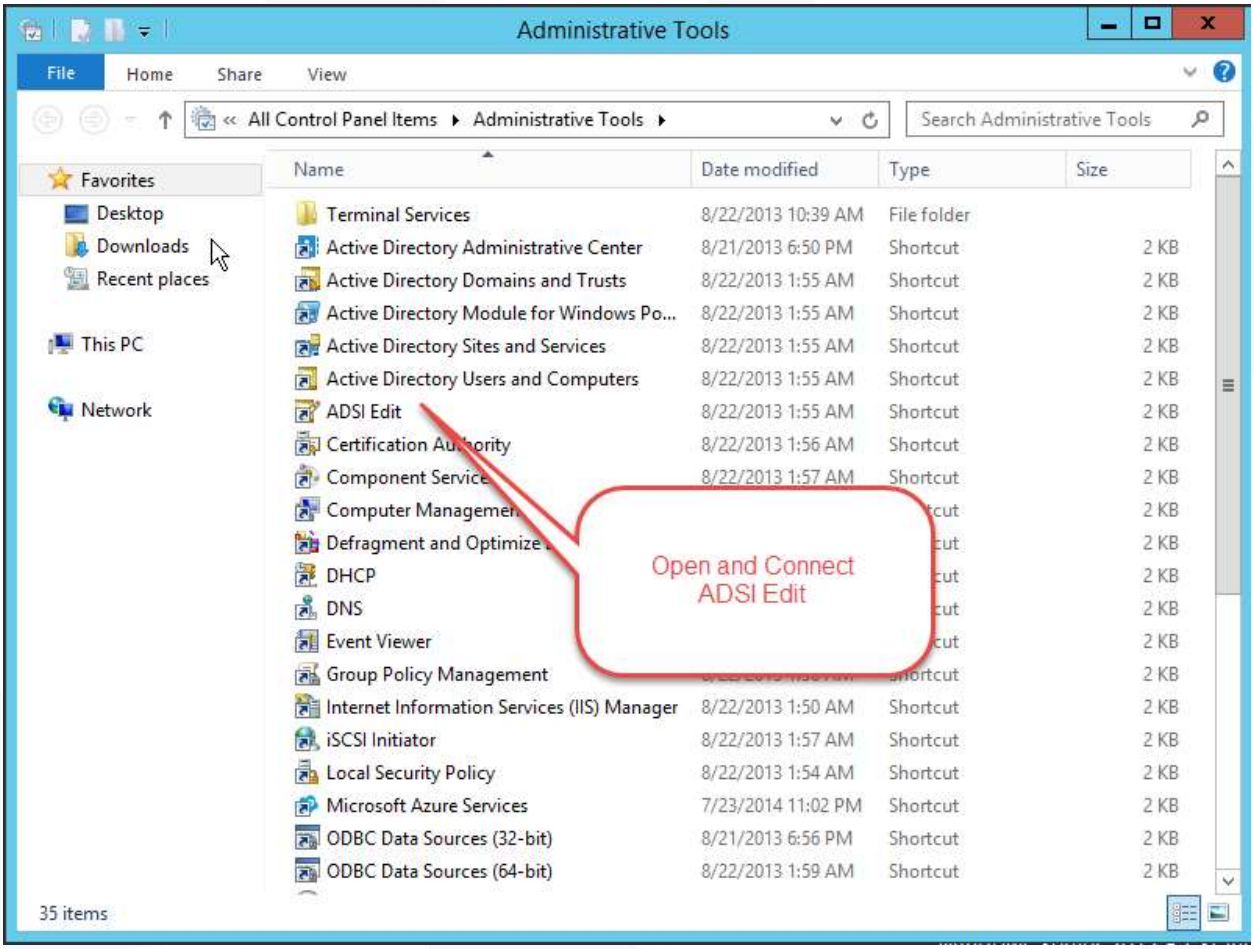
As a matter of practice, we recommend restarting the server even if it does not restart by itself during the implementation.

This will complete the prerequisite installation of Microsoft Services.

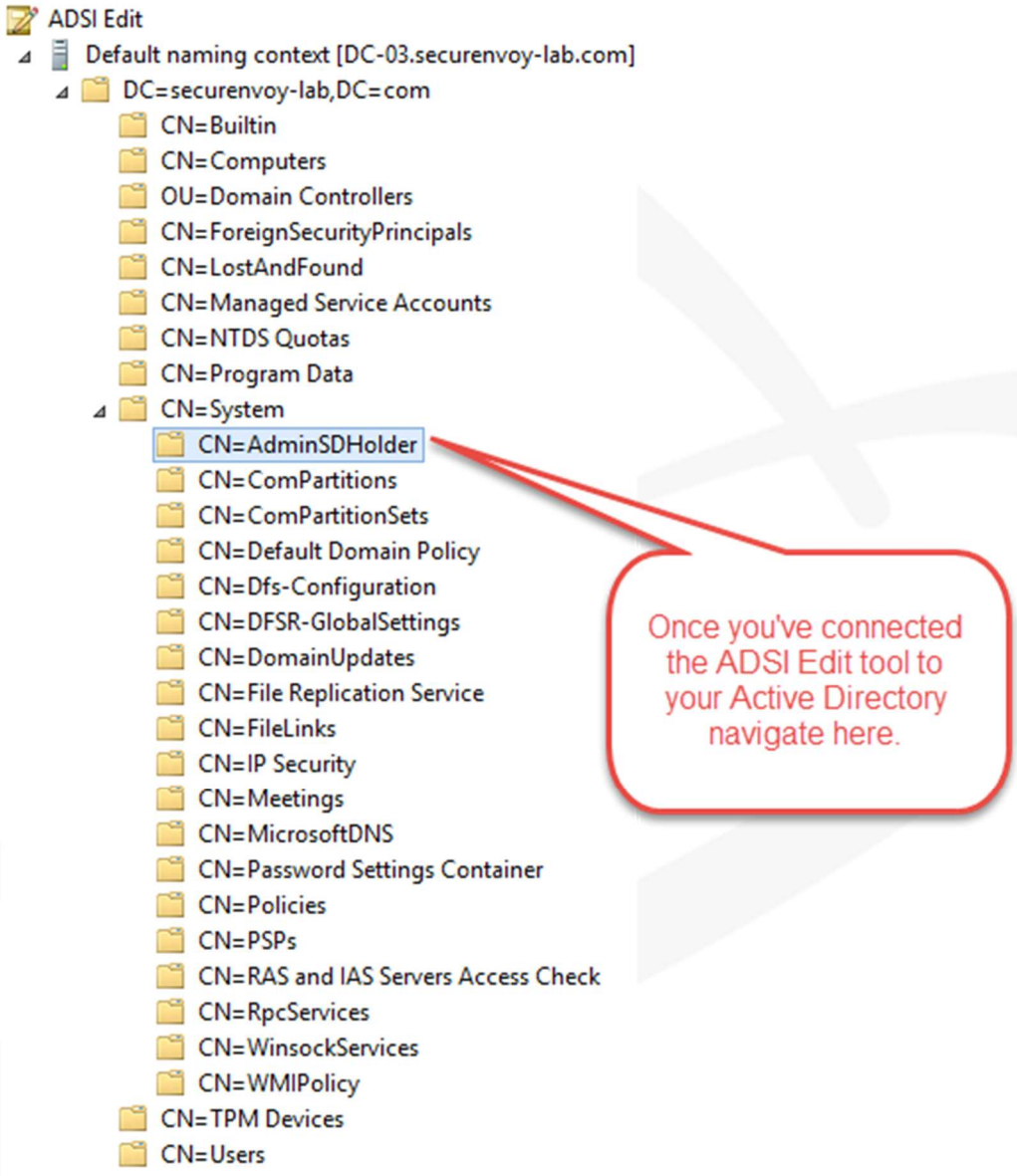
Configure AdminSDHolder Permissions

In Microsoft Windows 2008 R2 and 2012 R2 Active Directory environments it is necessary to enable permission inheritance on this object so that the SecurEnvoy Service account can write back to a users' phone number fields. Without this, the service account would require elevated permissions.

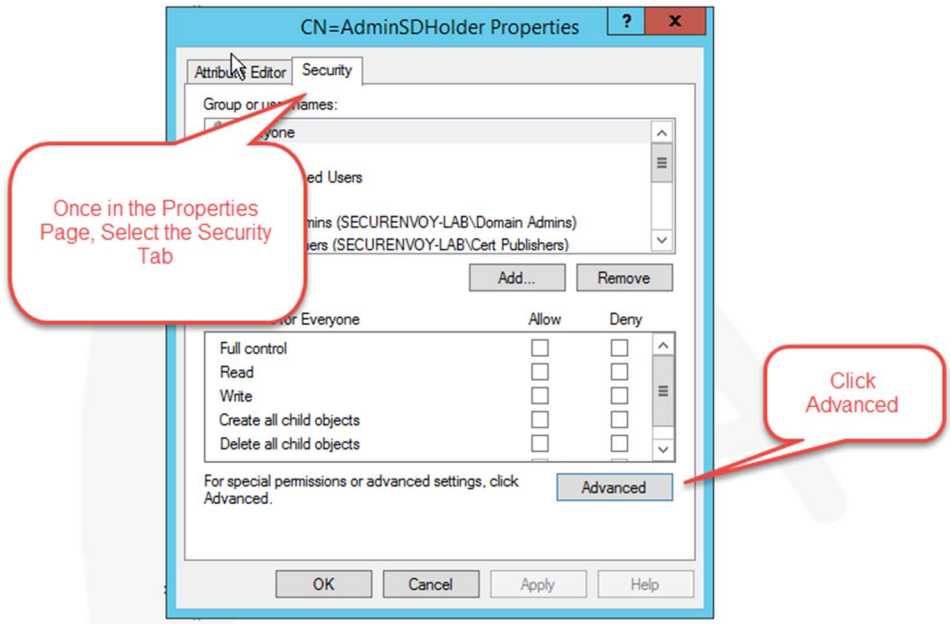
On your domain controller;

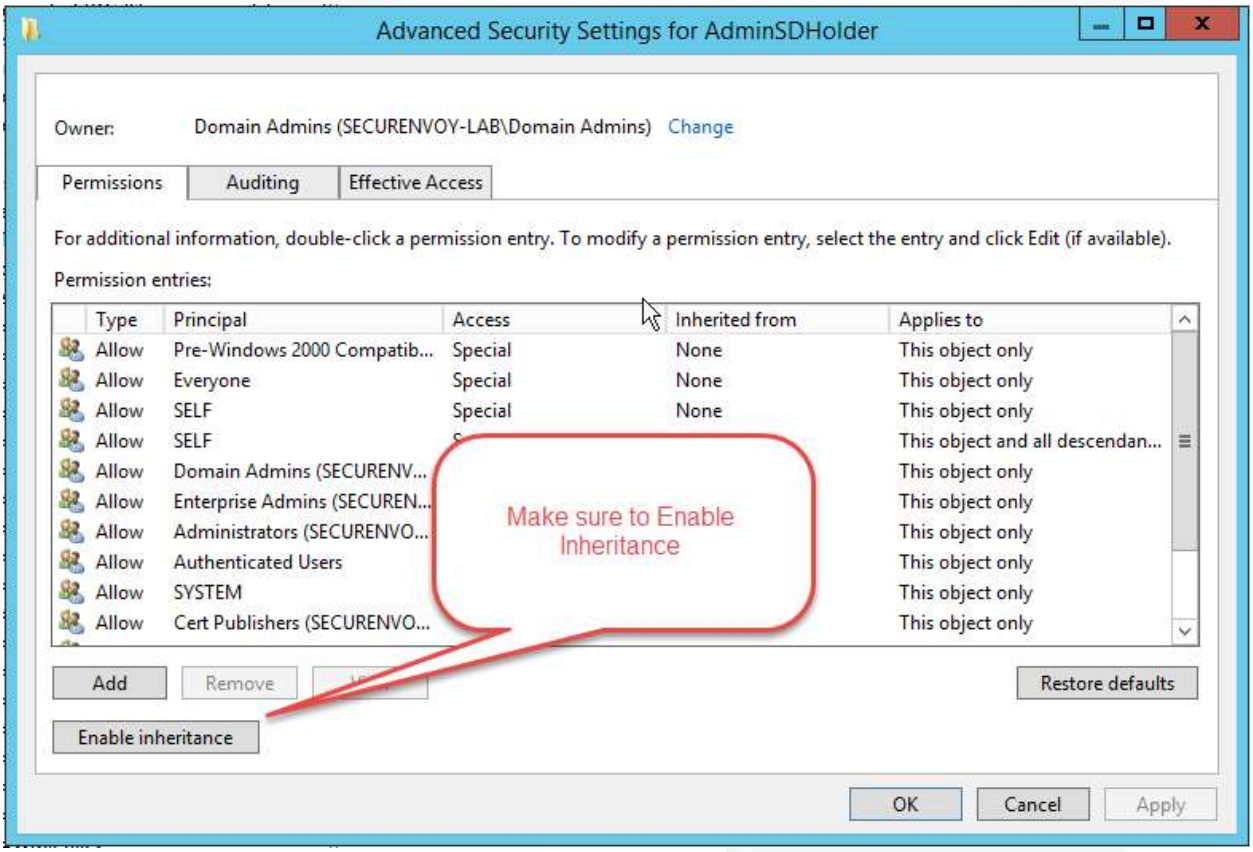


You need to establish a connection to the Active Directory where the Service Account resides.



Right click on the AdminSDHolder container and select the Properties.


CN=AdminSDHolder Properties
Attribute Editor
Security
Group or user names:
Add...
Remove
Allow
Deny
Full control
Read
Write
Create all child objects
Delete all child objects
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply
Help
Once in the Properties Page, Select the Security Tab
Click Advanced


Advanced Security Settings for AdminSDHolder
Owner: Domain Admins (SECURENVOY-LAB\Domain Admins) Change
Permissions
Auditing
Effective Access
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).
Permission entries:
Type
Principal
Access
Inherited from
Applies to
Allow Pre-Windows 2000 Compatib... Special None This object only
Allow Everyone Special None This object only
Allow SELF Special None This object only
Allow SELF This object and all descendan...
Allow Domain Admins (SECURENV... This object only
Allow Enterprise Admins (SECUREN... This object only
Allow Administrators (SECURENVO... This object only
Allow Authenticated Users This object only
Allow SYSTEM This object only
Allow Cert Publishers (SECURENVO... This object only
Add
Remove
Restore defaults
Enable inheritance
OK
Cancel
Apply
Make sure to Enable Inheritance

Installing & Configuring SecurEnvoy SecurAccess

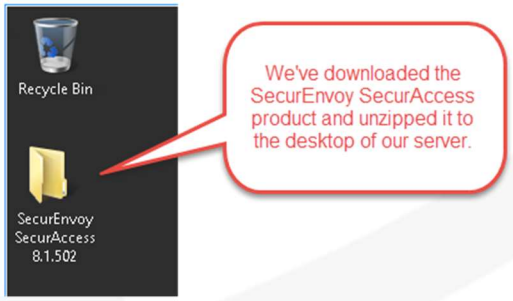
The following steps are required to configure the SecurEnvoy SecurAccess product for use. Please note that this configuration is for trials and some components, like Secure LDAP and HTTPS are not used in these examples. If you require these for your trial, please reference the SecurEnvoy SecurAccess Administrators Guide that was included in your download.

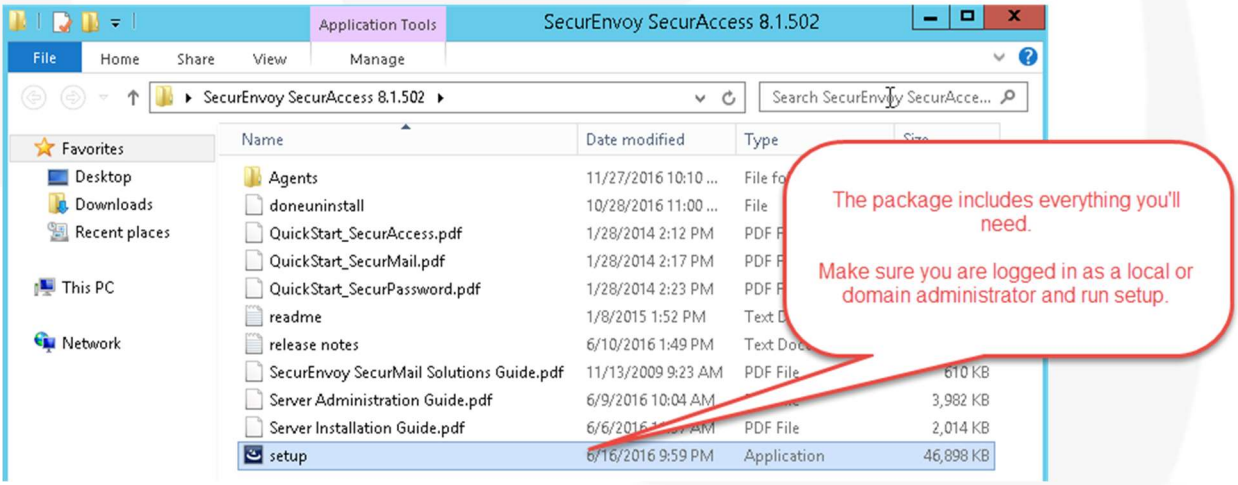
We suggest gathering the following before getting started to make things easy.

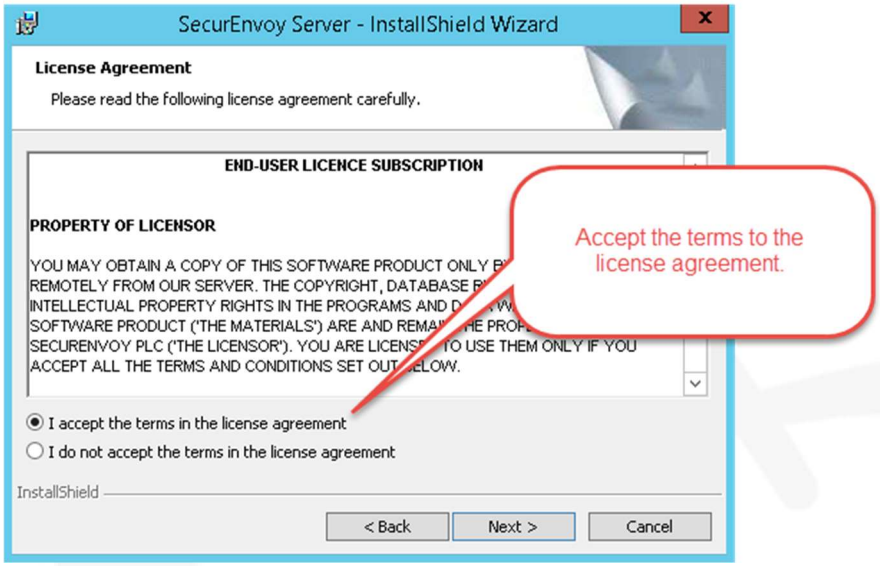
- Microsoft Active Directory Service FQDN and NetBIOS name
- FQDN for at least one Domain Controller
- Create (or use) a Service Account – only needs to be a domain user.
- Email server FQDN
- Email account with credentials

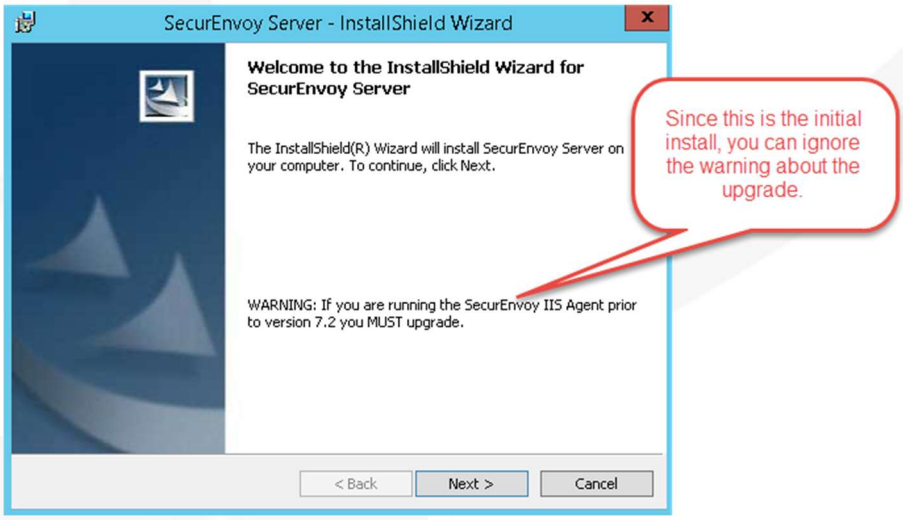
We will begin with the base installation of the SecurEnvoy SecurAccess product.

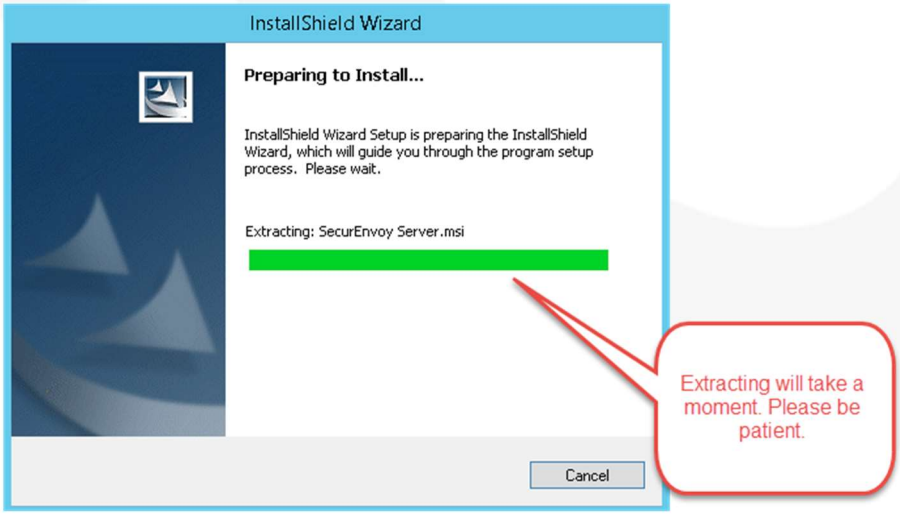
Download is available here: https://www.securenvoy.com/products/securaccess/key-features.shtm

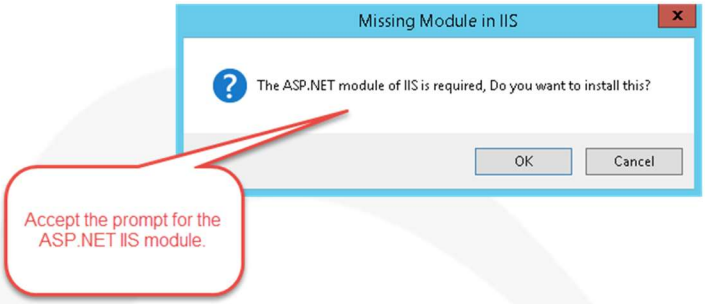


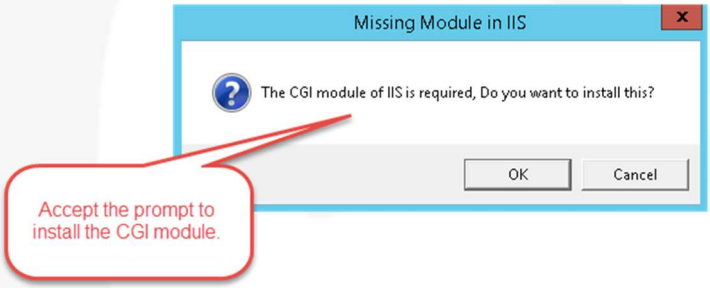



SecurEnvoy Server - InstallShield Wizard
License Agreement
Please read the following license agreement carefully.
END-USER LICENCE SUBSCRIPTION
PROPERTY OF LICENSOR
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel
Accept the terms to the license agreement.


SecurEnvoy Server - InstallShield Wizard
Welcome to the InstallShield Wizard for SecurEnvoy Server
The InstallShield(R) Wizard will install SecurEnvoy Server on your computer. To continue, click Next.
WARNING: If you are running the SecurEnvoy IIS Agent prior to version 7.2 you MUST upgrade.
< Back
Next >
Cancel
Since this is the initial install, you can ignore the warning about the upgrade.


InstallShield Wizard
Preparing to Install...
InstallShield Wizard Setup is preparing the InstallShield Wizard, which will guide you through the program setup process. Please wait.
Extracting: SecurEnvoy Server.msi
Cancel
Extracting will take a moment. Please be patient.

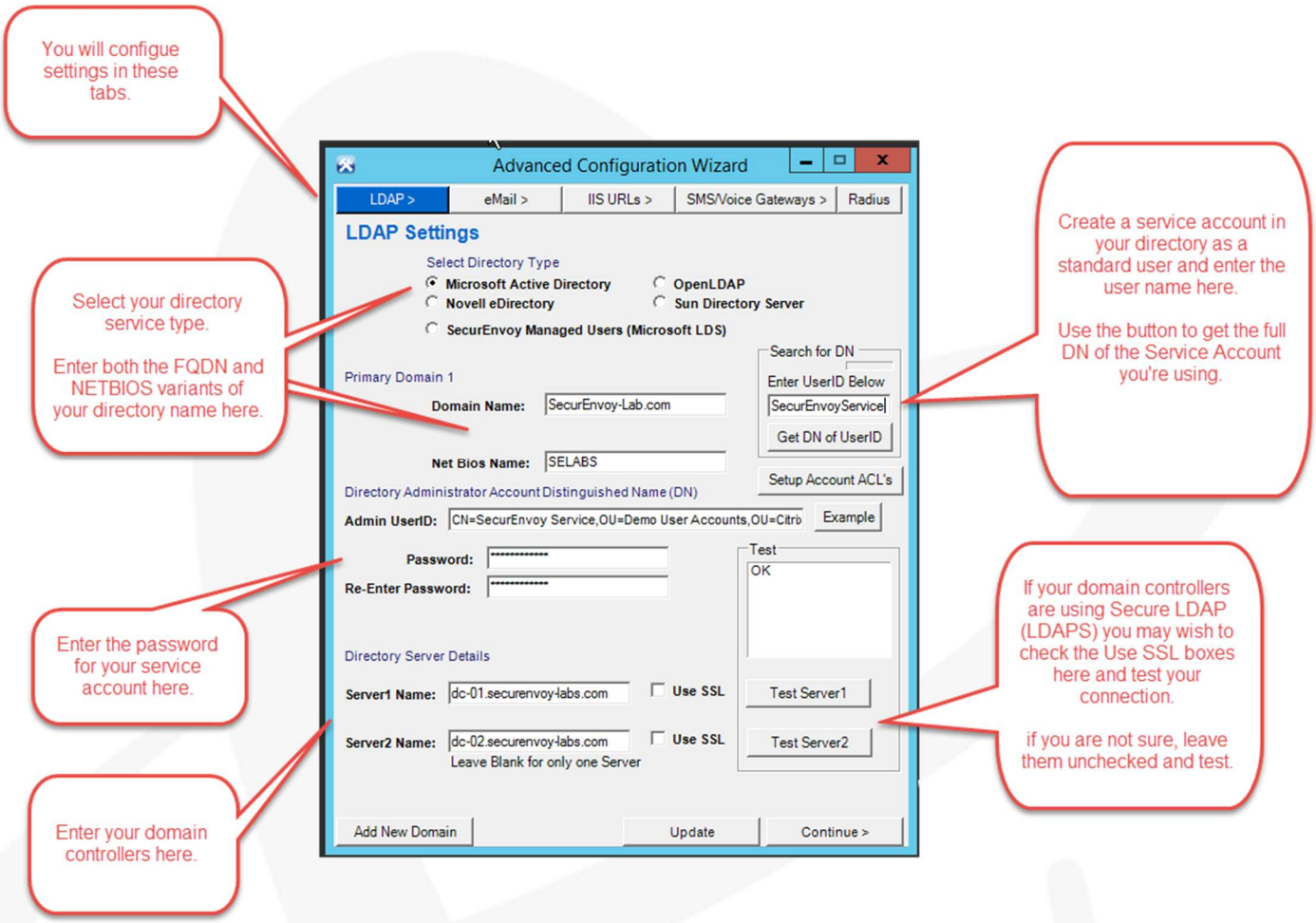

Missing Module in IIS
The ASP.NET module of IIS is required, Do you want to install this?
OK
Cancel
Accept the prompt for the ASP.NET IIS module.


Missing Module in IIS
The CGI module of IIS is required, Do you want to install this?
OK
Cancel
Accept the prompt to install the CGI module.


Advanced Configuration Wizard
SecurEnvoy
Advanced Configuration
What type of installation is this?
New Installation
Additional Server (Replica)
Upgrade
Since this is the first and only server you'll be installing for the trial, select New Installation.
Continue

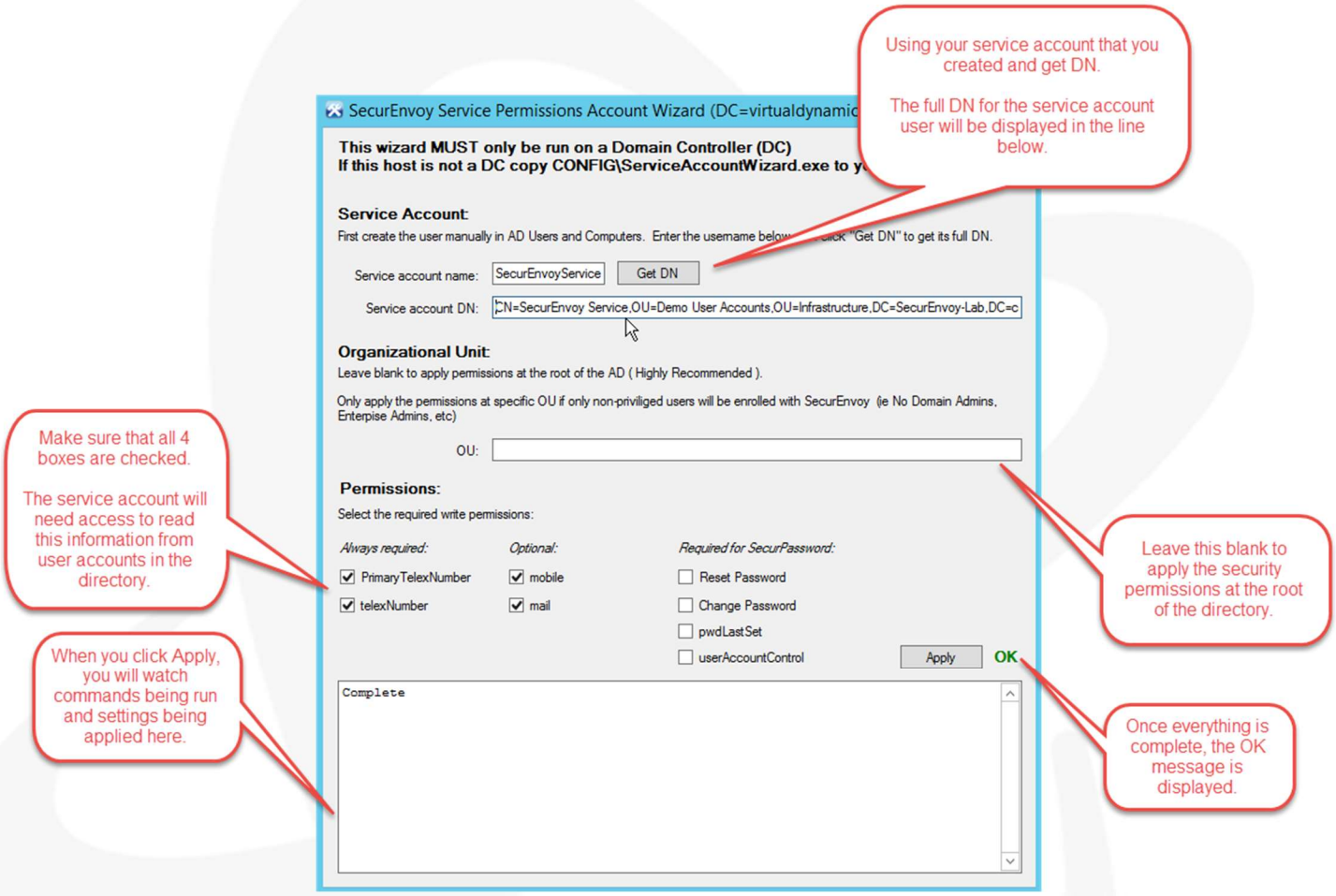


The advanced configuration wizard uses a series of tabs where you enter detailed information related to your configuration. If this is the first time you are configuring the system, you will notice that each time you click continue, services will be installed and started.



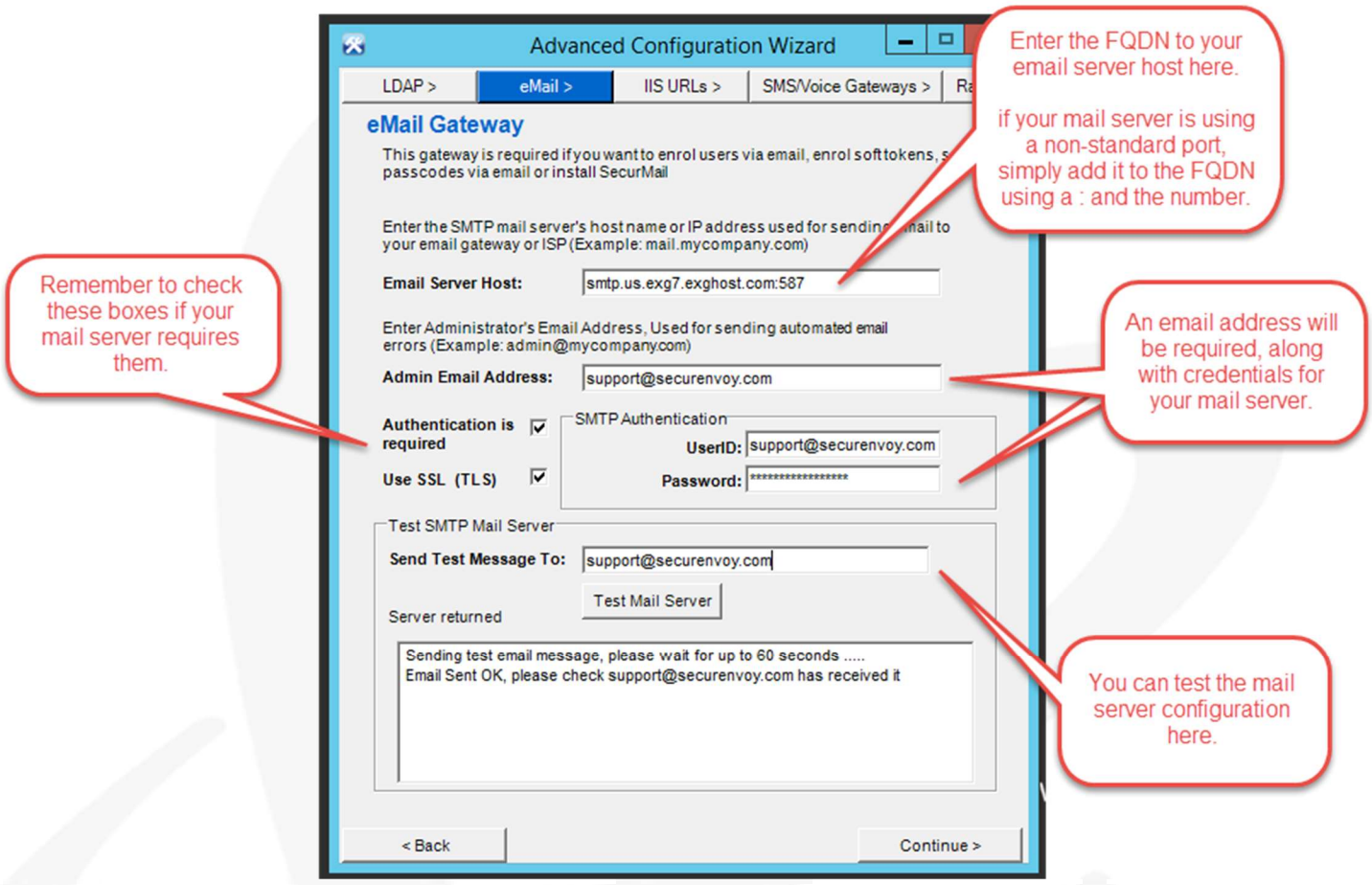
The SecurEnvoy SecurAccess product will need to communicate with your directory services to perform authentication functions. The above configuration represents a Microsoft Active Directory configuration.

Once you have completed the configuration on the previous screen, you will be required to click the button Setup Account ACL's and when you do, you'll make special security changes to the service account user in the Active Directory.



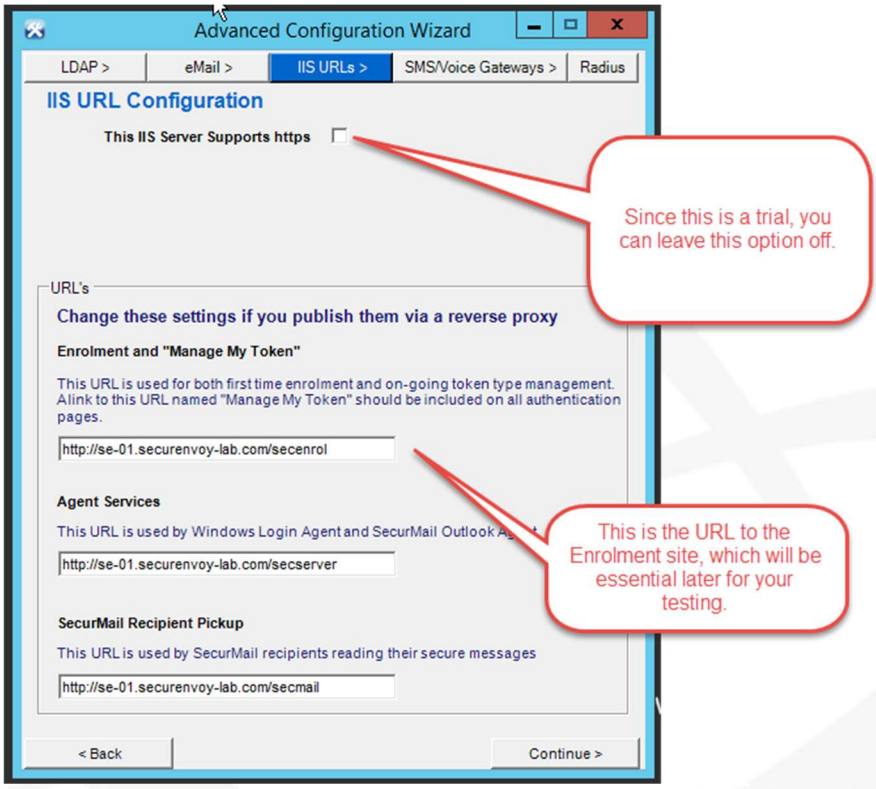
These security changes to the service account are essential to the proper function of the solution. The service account needs to read and sometimes write details to user accounts in the Microsoft Active Directory, like phone numbers and email addresses.

When completed, simply close this window.

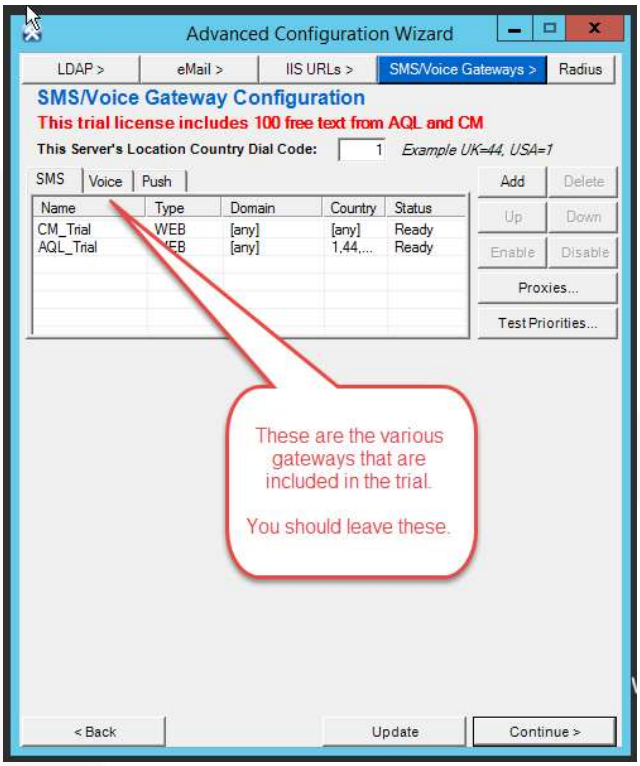


The SecurEnvoy SecurAccess product will use this email configuration to deliver enrolment instructions to users as well as system alerts to the system administrator.

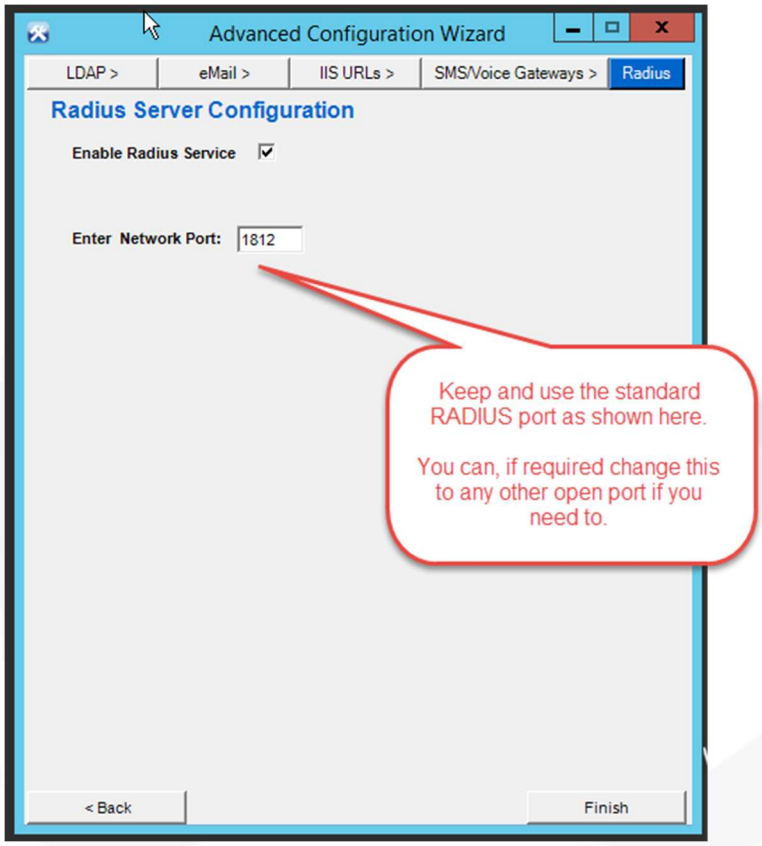
Please make sure to validate your settings here by sending a test message.



In later steps, users will be delivered an email requesting that they enroll in the system. The email will contain this URL.



There are three tabs of gateways – SMS, Voice and Push. The this is how the SecurEnvoy SecurAccess solution will deliver security details to users for logon.


Advanced Configuration Wizard
LDAP >
eMail >
IIS URLs >
SMS/Voice Gateways >
Radius
Radius Server Configuration
Enable Radius Service
Enter Network Port:
1812
Keep and use the standard RADIUS port as shown here.
You can, if required change this to any other open port if you need to.
< Back
Finish

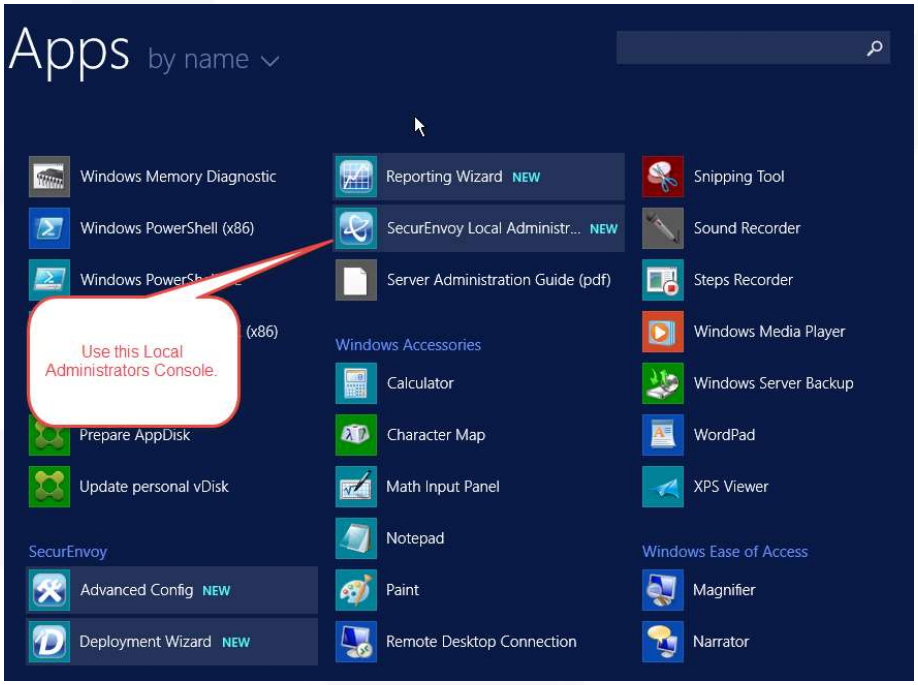
Configure your RADIUS Client

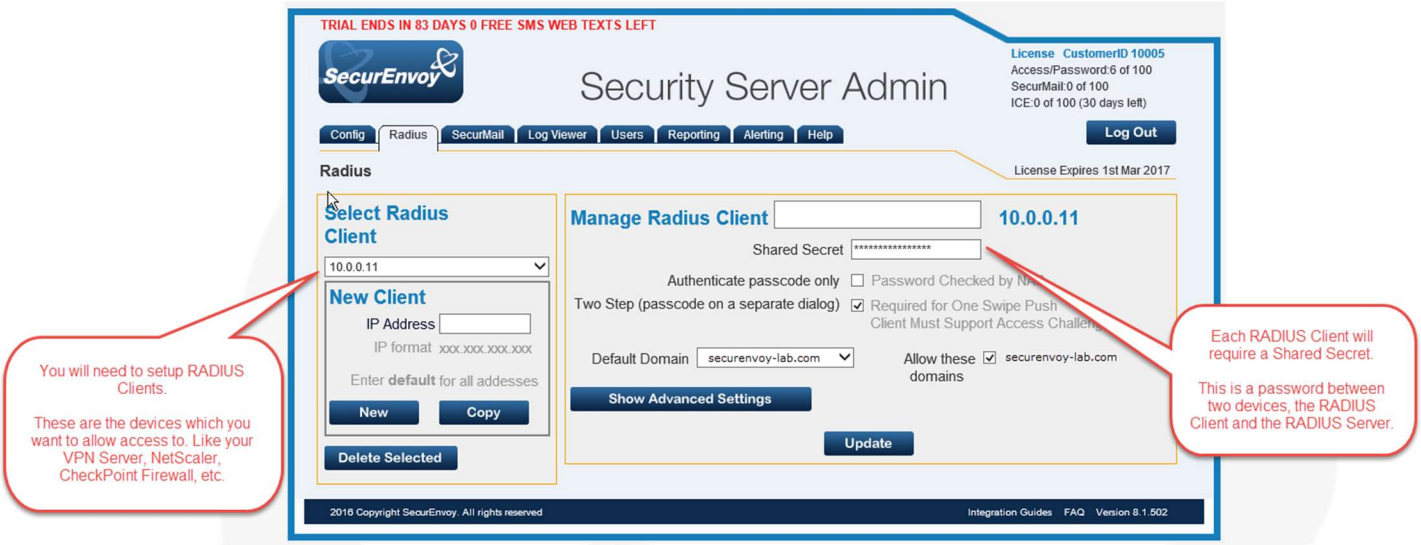
Now that you have completed the setup and configuration of the SecurEnvoy SecurAccess Server, you will need to configure and allow other devices to work with it. That process begins with creating security entries to allow devices to communicate. These are called RADIUS Clients.

A RADIUS Client would be something like your VPN Server, Citrix NetScaler, Check Point Firewall VPN, etc. When you are configuring a RADIUS Client, you'll need to do two things.

- IP Address of your RADIUS Client
- A Shared Secret

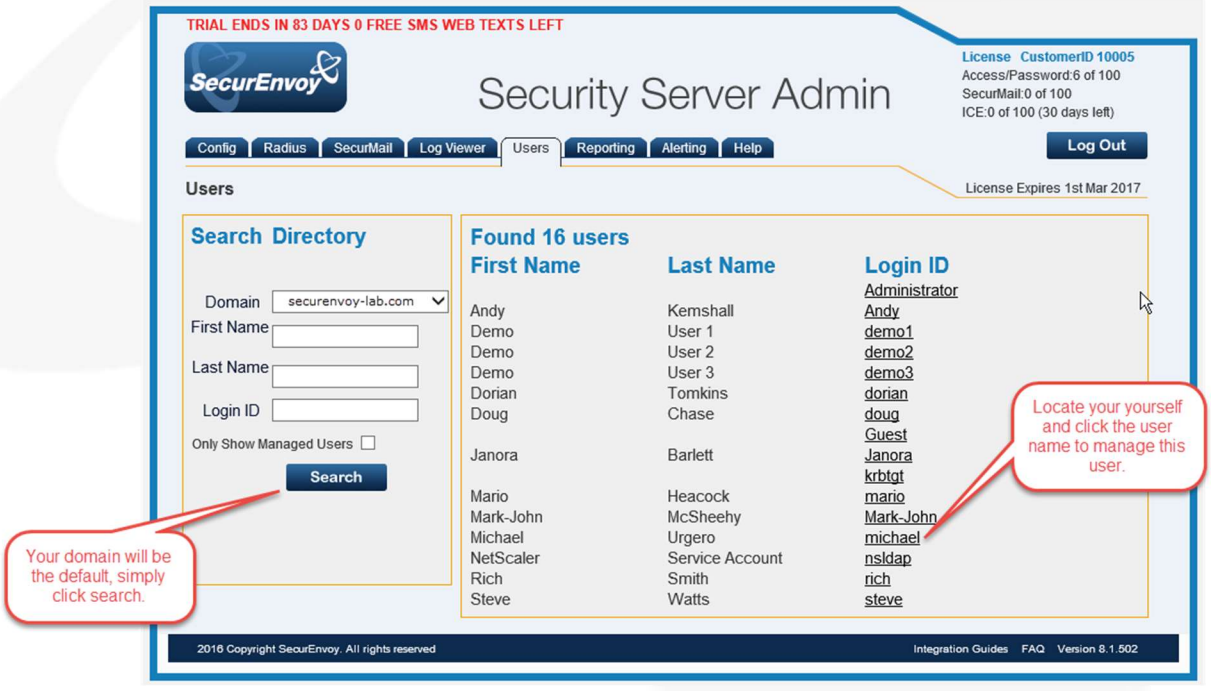
A Shared Secret is a password or passphrase that these two devices will use to validate each other. For the trial, you can keep these simple, but for a production environment they should be complex. It's also important to know that you can have more than one RADIUS Client and that the Shared Secret can be different for each RADIUS Client.

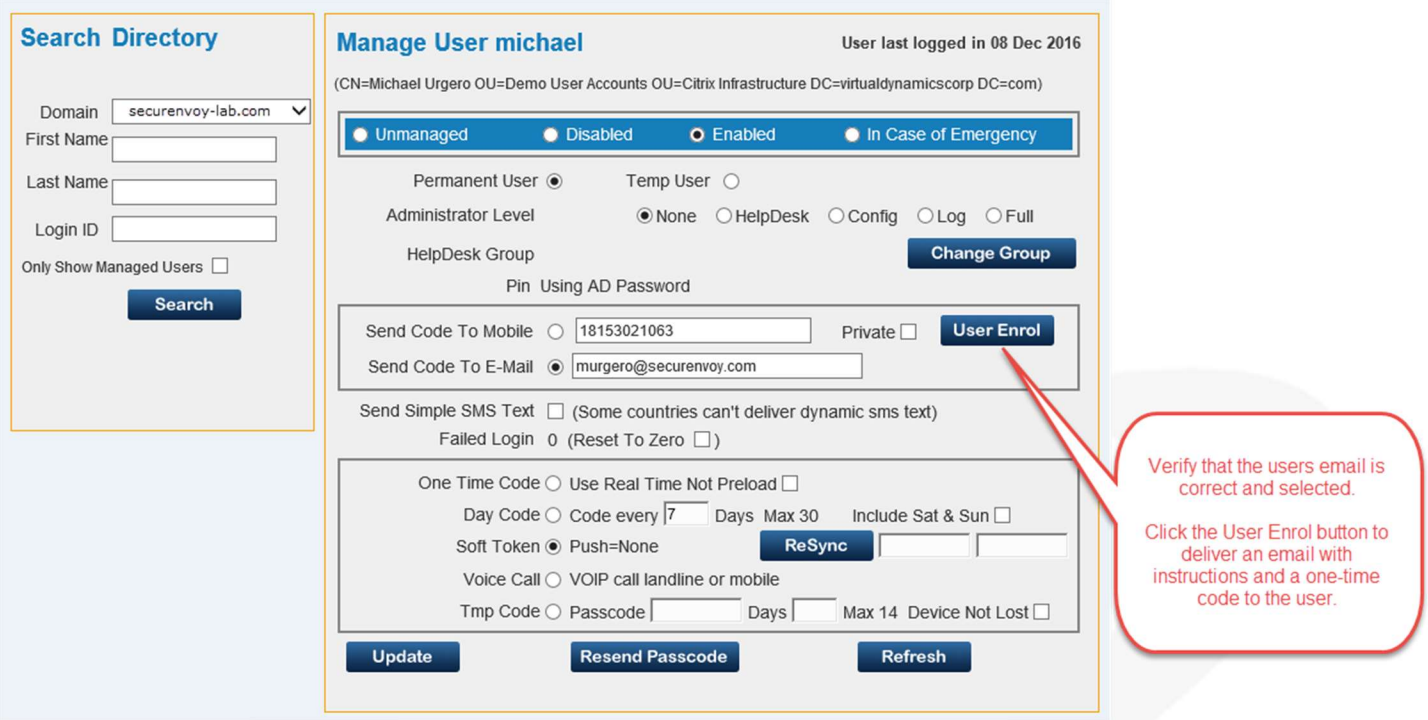




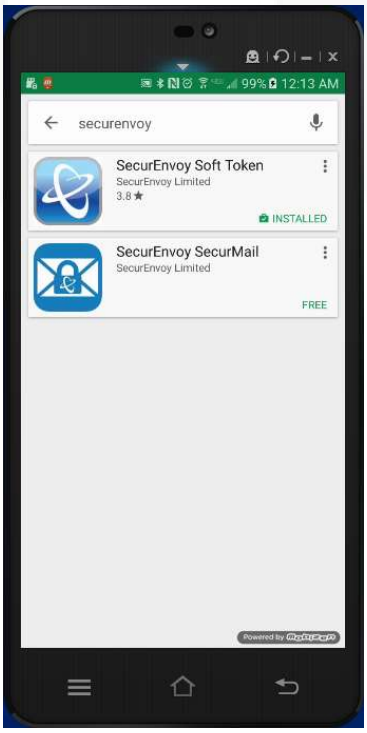
Registering your First Device

SecurEnvoy SecurAccess Soft Tokens need to be registered to the system to work. To do this, navigate to the User Tab. It will be important to note a few things here, in this configuration for the trial we are searching the entire directory and that means your list of users may be long.





The system will use the email configuration you specified earlier to deliver a message to the user. This email will contain the URL for enrolment as well as a one-time code that they will need to complete their authentication.



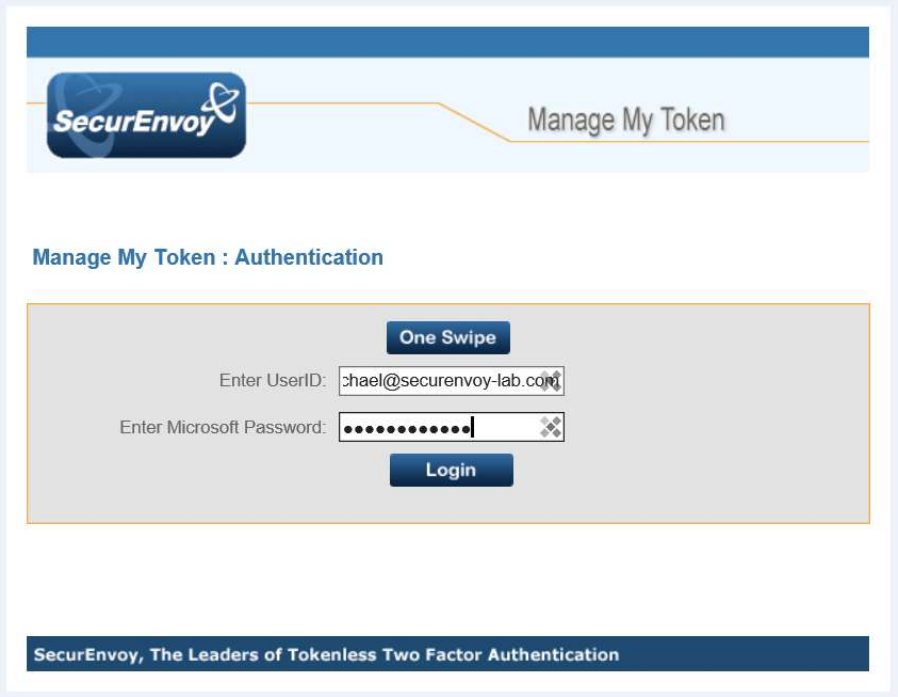
From the user side, you will need to load the SecurEnvoy Soft Token Application on your smart phone device.

SecurEnvoy has applications in all the major markets, simply search for SecurEnvoy.

When you locate the SecurEnvoy Soft Token Application, install to your smart phone device. You will receive several prompts that need to be accepted.

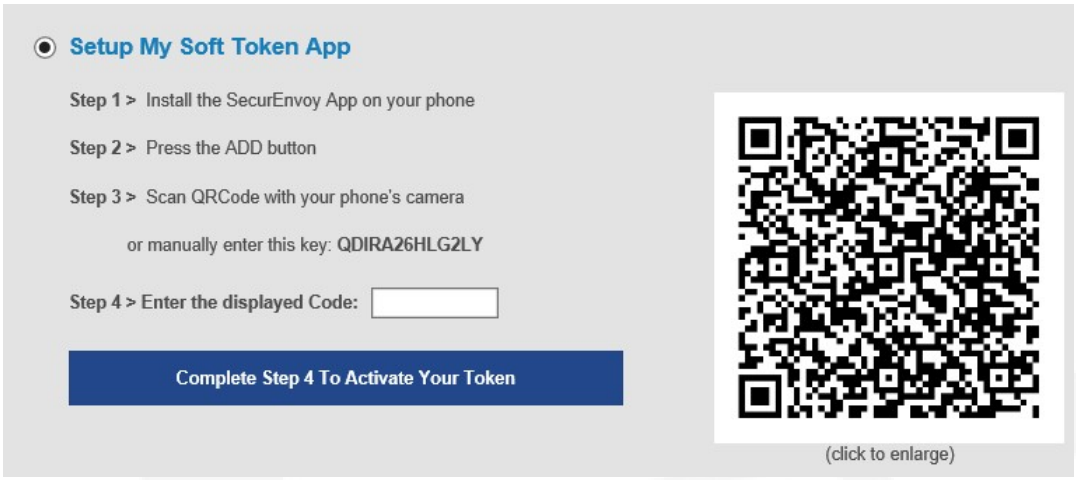
Once you have completed the installation of the SecurEnvoy Soft Token Application from the market, you will need to get ready for enrolment and have probably received an enrolment email by now.

Navigate your browser to the following URL: http://<yourserverFQDN>/secenrol. You should reference the IIS URLs page from the SecurEnvoy SecurAccess Advanced Configuration tool on your server to get this address.



You will logon to this site with your Microsoft Active Directory Credentials and will be prompted for the one-time code that you received in your enrolment email to setup your token.

You'll setup your SecurEnvoy SecurAccess Soft Token using the QR Code shown on the page. The QR Code contains the URL that the SecurEnvoy SecurAccess server will use to communicate with your Soft Token.



Once your token is activated, you're ready to go. You will now need to configure your VPN, Citrix NetScaler, CheckPoint Firewall or other service for RADIUS authentication.

SecurEnvoy SecurAccess works with many different vendors and is a the most flexible two-factor authentication solution on the market today.

Support for Your Trial

We're happy to help you get things setup and running. If you have any questions or need help with your trial, please reach out to us – we would be happy to help.

What's Next

Now that you have the SecurEnvoy SecurAccess Two-Factor Authentication configuration completed, you will need to refer to the integration guide for the product that you're working with.

- Citrix RADIUS Integration
- Palo Alto VPN Firewall Integration
- Cisco VPN Integration

And many more. Please refer to our web site for additional product integration.