SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

Installation & Configuration Guide v9.4.501

Authenticating Users Using SecurAccess Server by SecurEnvoy

SecurEnvoy SecurAccess Security Server Installation & Configuration Guide

Table of Contents

DISCLAIMER 3
LEGAL 3
GETTING STARTED 4
Things You Will Need 4
Authentication Processing Topology 4
SYSTEM INSTALLATION 5
Installation of Microsoft IIS Web Service 6
INSTALLING & CONFIGURING SECURENVOY SECURACCESS 11
Downloading our Software 11
Installing SecurAccess 12
Welcome to the System Installer 12
License Agreement 13
Installation Path 13
Select Setup Type 14
CONFIGURE YOUR SERVICE ACCOUNT 17
SECURENVOY SERVICE PERMISSIONS ACCOUNT WIZARD 17
CONFIGURING SECURENVOY SECURACCESS 19
SECURENVOY SECURACCESS DASHBOARD 24
Dashboard Components 24
CONFIGURE RADIUS CLIENT CONNECTIONS 26
REGISTERING YOUR FIRST DEVICE 28
UPGRADING YOUR SERVER 31
Prior to Upgrade 31
Post Upgrade Tasks 33
INSTALLING AN ADDITIONAL SECURENVOY SERVER 33
SUPPORT 34
APPENDIX – SETTING SERVICE ACCOUNT PERMISSIONS MANUALLY 35
APPENDIX – TCP / UDP COMMUNICATIONS / FIREWALL PORTS 39

Disclaimer

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage

Legal

All rights reserved. No parts of this work may be reproduced in any form or by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and / or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

Getting Started

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

The SecurEnvoy 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 refer to the Help section in the SecurEnvoy Admin Console.

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 Microsoft Windows 2012 R2, 2016 or 2019 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/en-us/support#id4

- 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 Security server to be a member of the Active Directory.

Microsoft's standard practices for hardware requirements are sufficient for the implementation.

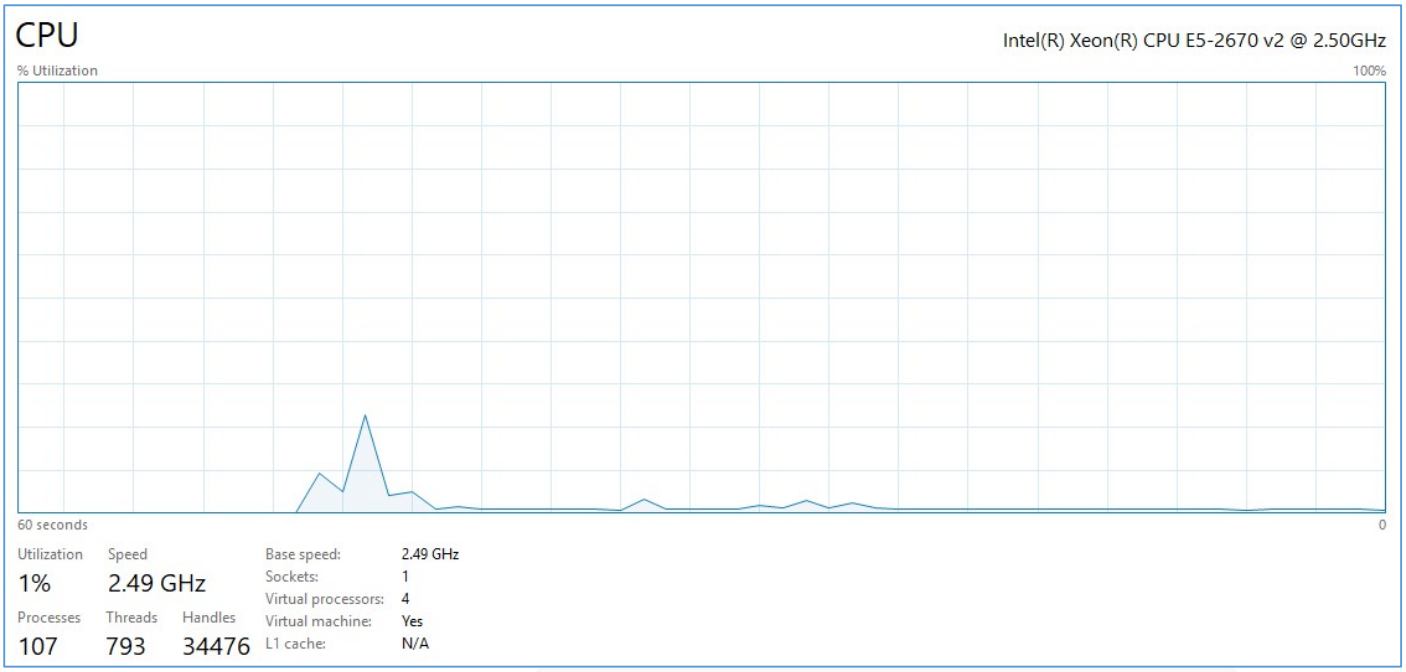
Authentication Processing Topology

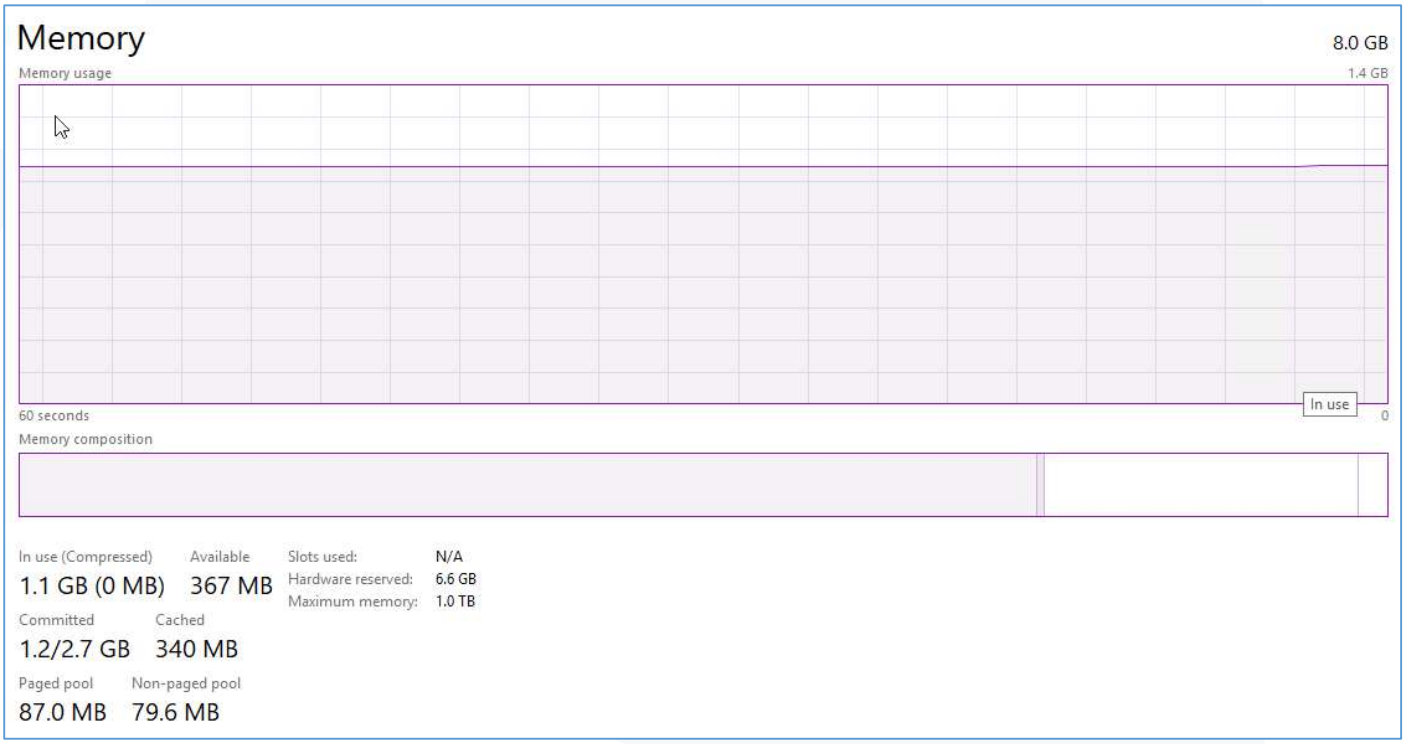
SecurEnvoy SecurAccess will integrate with any solution that can use RADIUS, such as; A10, Amazon Web Services, F5, IBM, Microsoft, Oracle, SalesForce, VMware, Barracuda, Check Point, Cisco, Citrix, Juniper, Palo Alto, SonicWall, Sophos, WatchGuard, Linux and many others.

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

System Installation

The Microsoft Windows 2019 Server that we used in our lab to document this installation process for the SecurAccess Security Server Product has the following technical specifications.

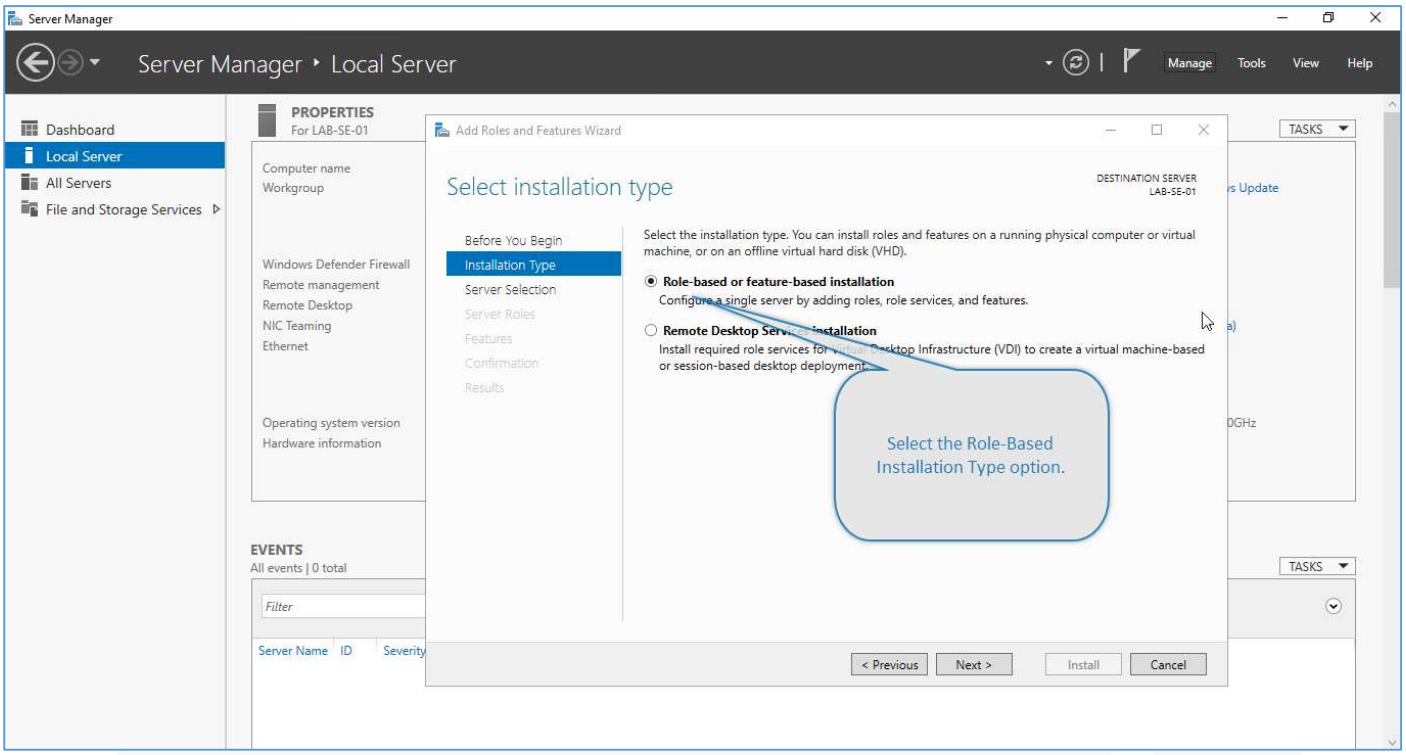


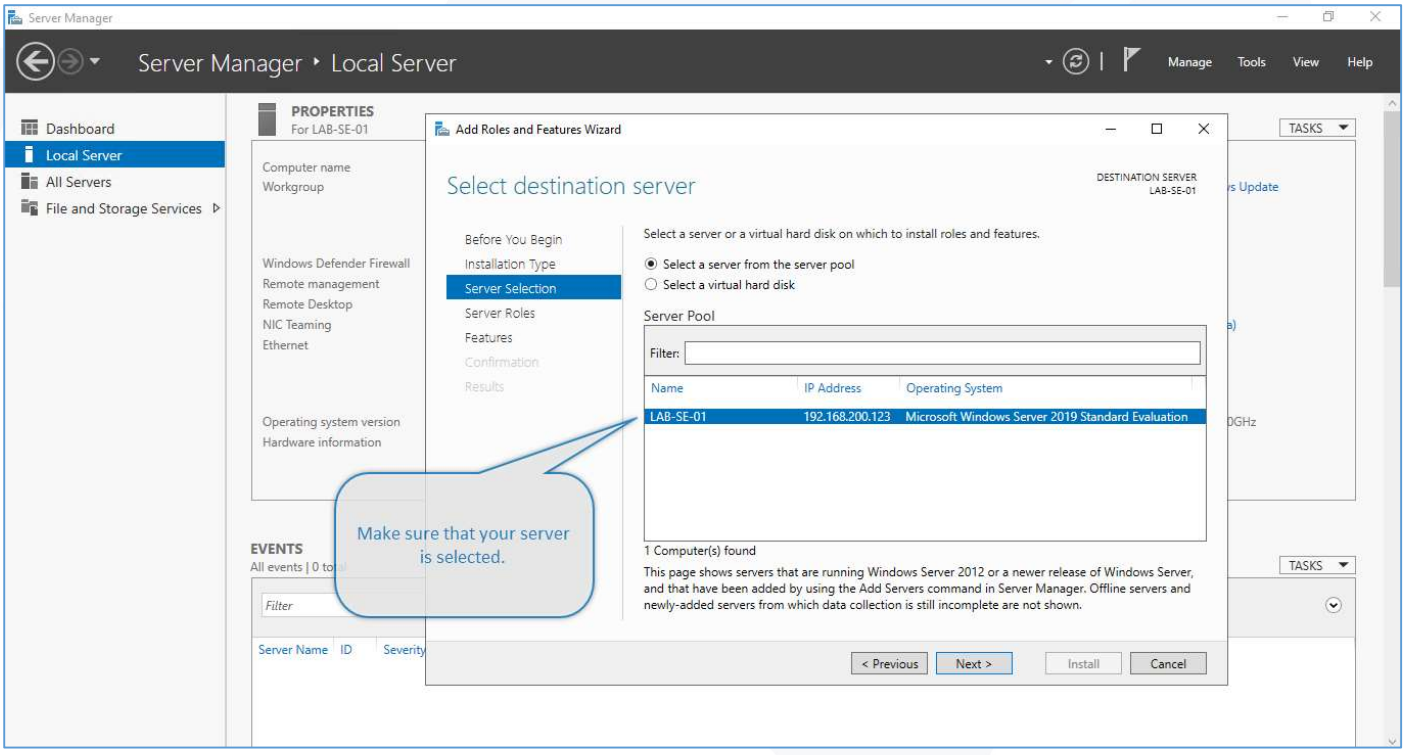


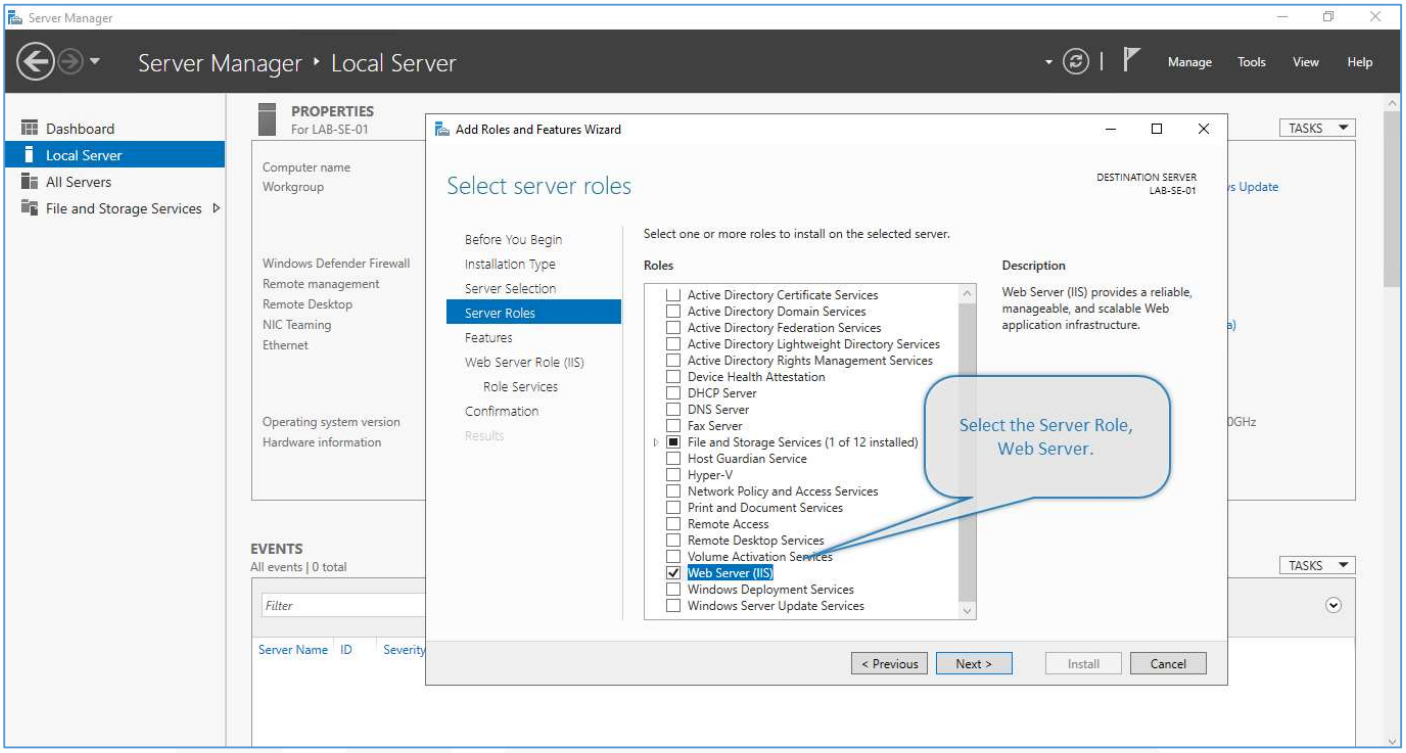
Installation of Microsoft IIS Web Service

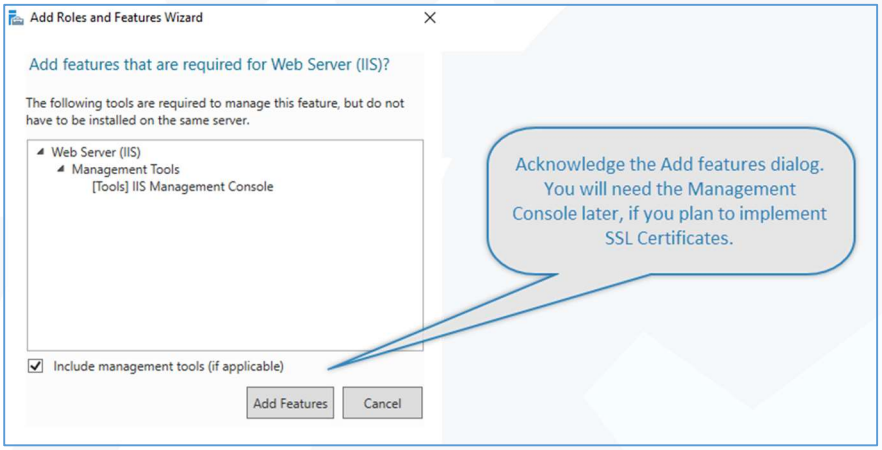
Microsoft IIS Web Services is a required Windows feature for our product. This will allow you to use either http or https (with a required SSL Certificate) as appropriate for your deployment, both internally and externally.

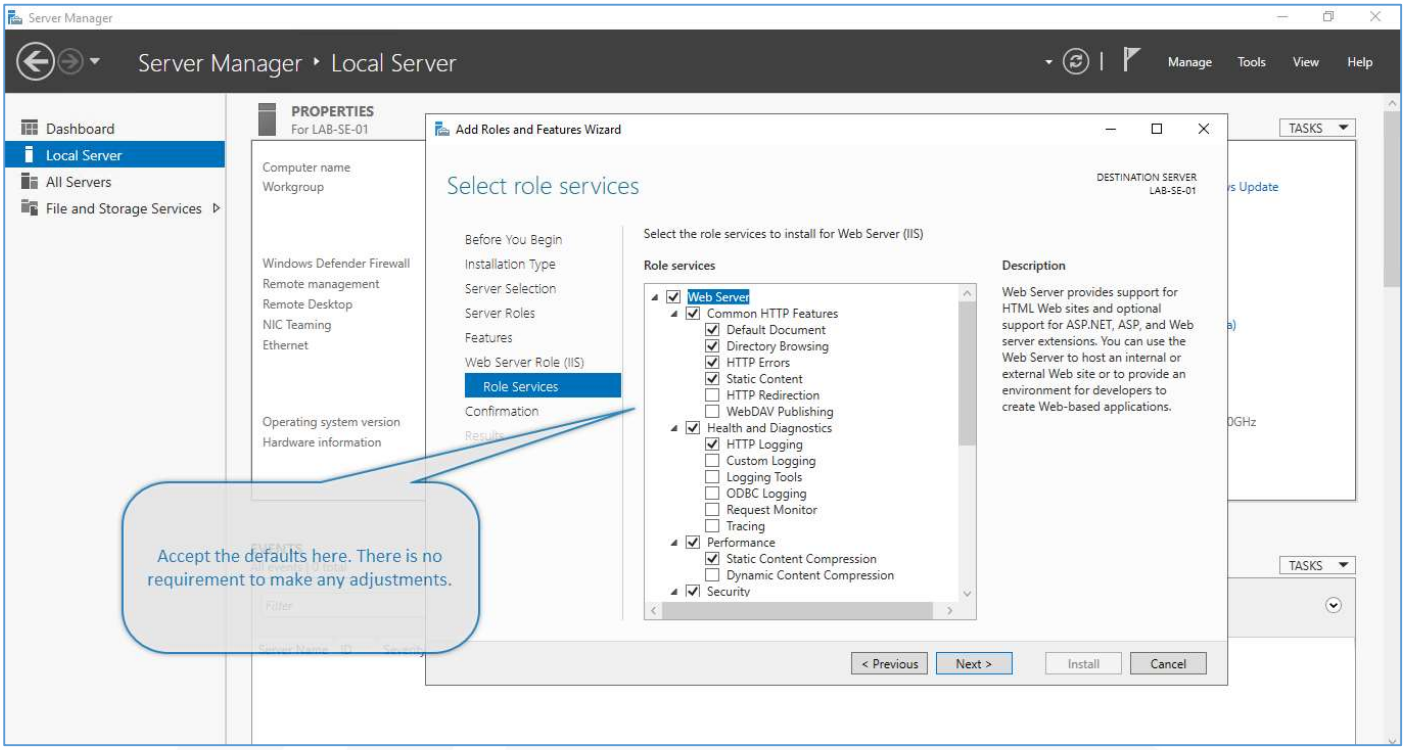
Using Server Manager, Add Roles and Features Wizard;

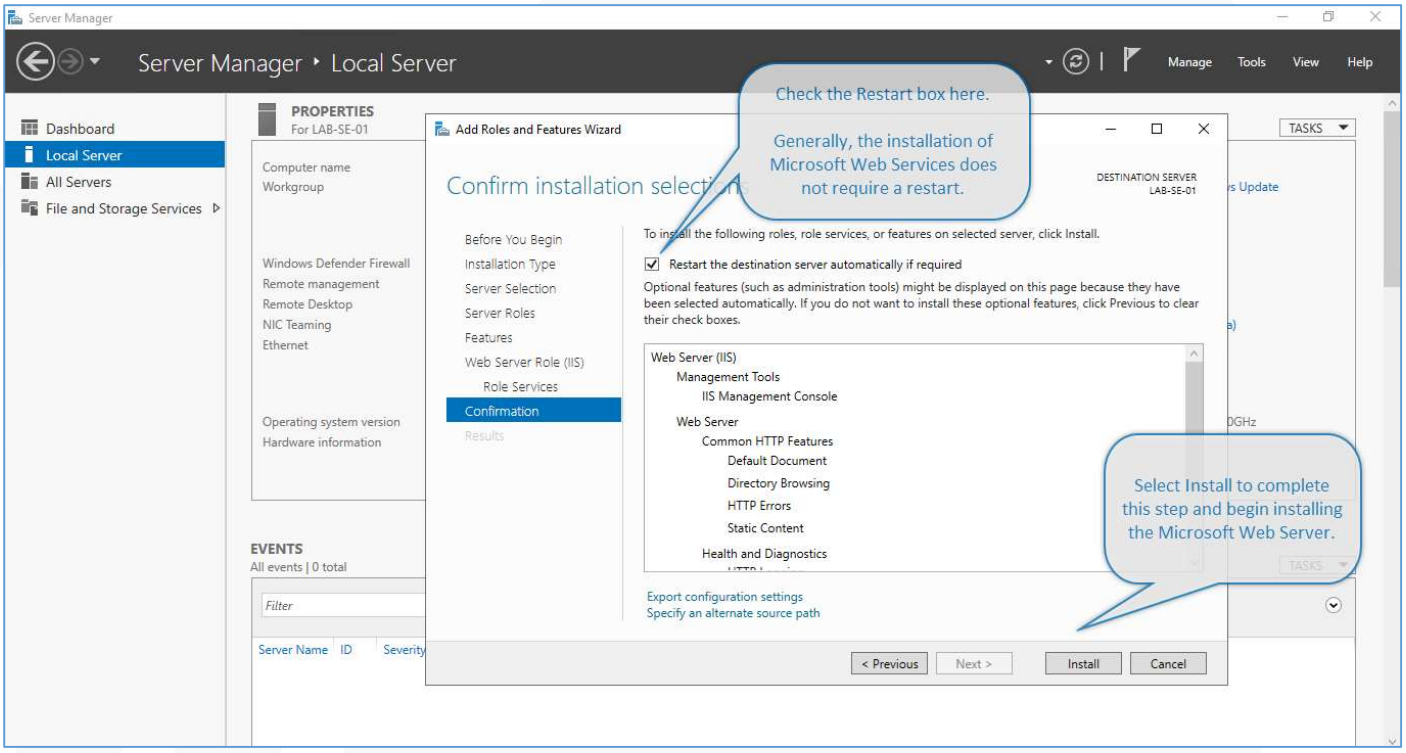


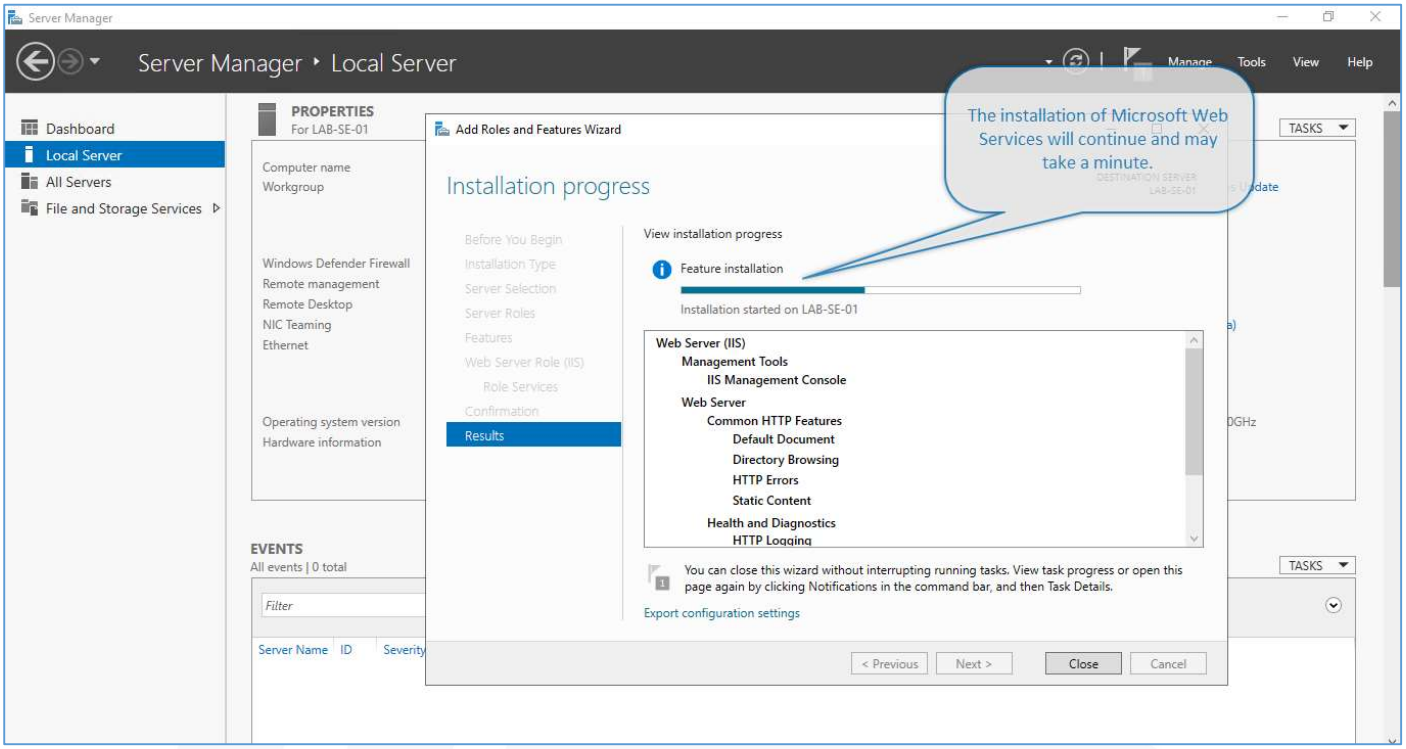


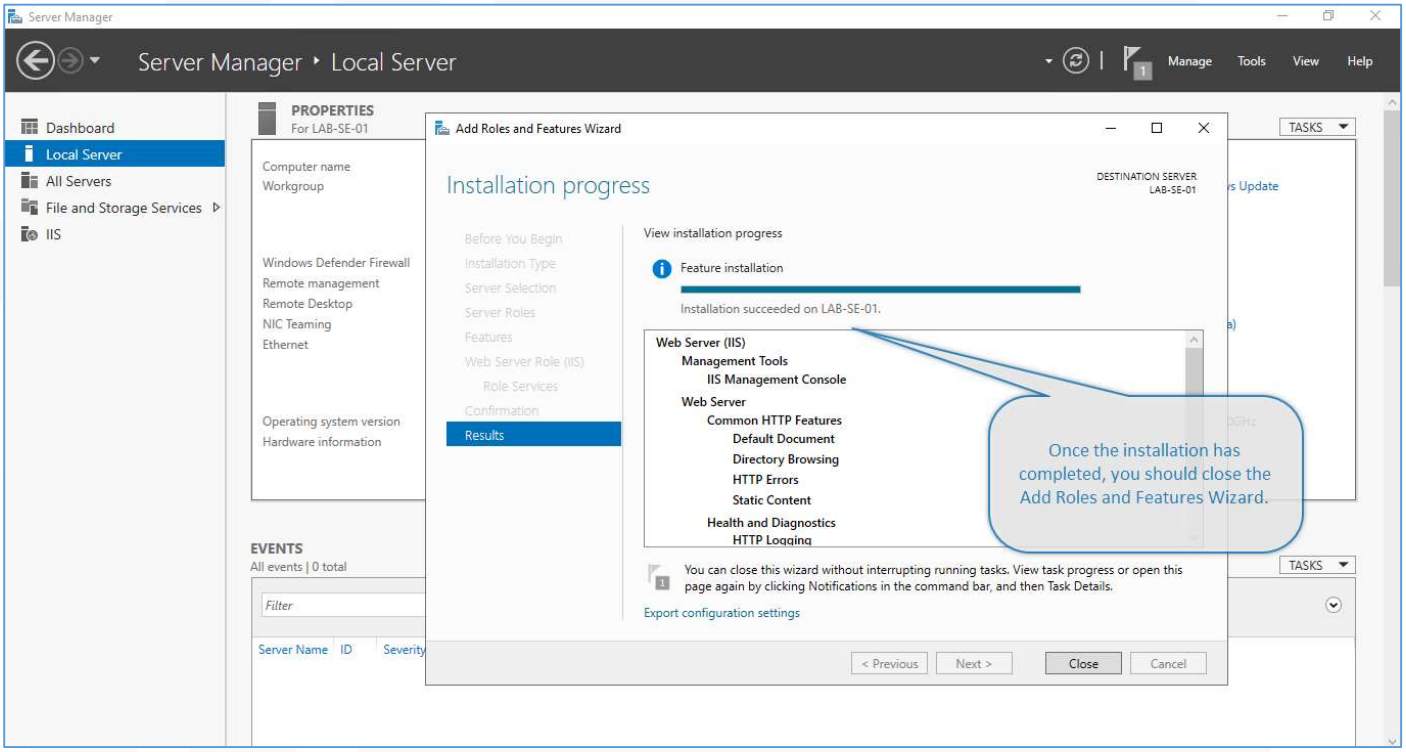

Server Manager
Server Manager • Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For LAB-SE-01
Computer name
Workgroup
Windows Defender Firewall
Remote management
Remote Desktop
NIC Teaming
Ethernet
Operating system version
Hardware information
EVENTS
All events | 0 total
Filter
Server Name
ID
Severity
TASKS
Add Roles and Features Wizard
Select server roles
DESTINATION SERVER
LAB-SE-01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select one or more roles to install on the selected server.
Roles
Active Directory Certificate Services
Active Directory Domain Services
Active Directory Federation Services
Active Directory Lightweight Directory Services
Active Directory Rights Management Services
Device Health Attestation
DHCP Server
DNS Server
Fax Server
File and Storage Services (1 of 12 installed)
Host Guardian Service
Hyper-V
Network Policy and Access Services
Print and Document Services
Remote Access
Remote Desktop Services
Volume Activation Services
Web Server (IIS)
Windows Deployment Services
Windows Server Update Services
Description
Web Server (IIS) provides a reliable, manageable, and scalable Web application infrastructure.
Select the Server Role, Web Server.
< Previous
Next >
Install
Cancel

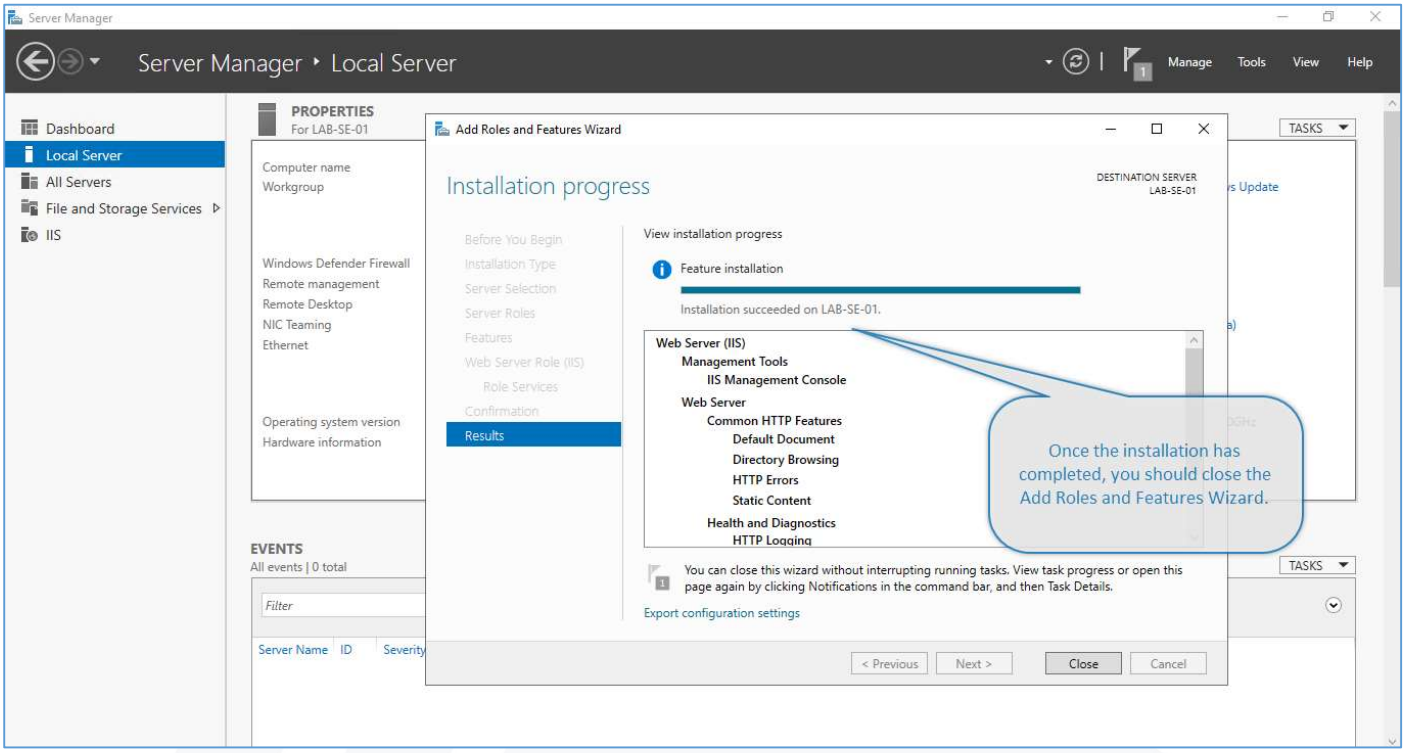

Add Roles and Features Wizard
Add features that are required for Web Server (IIS)?
The following tools are required to manage this feature, but do not have to be installed on the same server.
Web Server (IIS)
Management Tools
[Tools] IIS Management Console
Include management tools (if applicable)
Add Features
Cancel
Acknowledge the Add features dialog. You will need the Management Console later, if you plan to implement SSL Certificates.


Server Manager
Server Manager • Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For LAB-SE-01
Computer name
Workgroup
Windows Defender Firewall
Remote management
Remote Desktop
NIC Teaming
Ethernet
Operating system version
Hardware information
TASKS
Add Roles and Features Wizard
Select role services
DESTINATION SERVER
LAB-SE-01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Web Server (IIS)
Role services
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
HTTP Redirection
WebDAV Publishing
Health and Diagnostics
HTTP Logging
Custom Logging
Logging Tools
ODBC Logging
Request Monitor
Tracing
Performance
Static Content Compression
Dynamic Content Compression
Security
Description
Web Server provides support for HTML Web sites and optional support for ASP.NET, ASP, and Web server extensions. You can use the Web Server to host an internal or external Web site or to provide an environment for developers to create Web-based applications.
< Previous
Next >
Install
Cancel
Accept the defaults here. There is no requirement to make any adjustments.


Server Manager
Server Manager • Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For LAB-SE-01
Computer name
Workgroup
Windows Defender Firewall
Remote management
Remote Desktop
NIC Teaming
Ethernet
Operating system version
Hardware information
EVENTS
All events | 0 total
Filter
Server Name
ID
Severity
TASKS
Add Roles and Features Wizard
Confirm installation selections
DESTINATION SERVER
LAB-SE-01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
To install the following roles, role services, or features on selected server, click Install.
Restart the destination server automatically if required
Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
Export configuration settings
Specify an alternate source path
< Previous
Next >
Install
Cancel
Check the Restart box here.
Generally, the installation of Microsoft Web Services does not require a restart.
Select Install to complete this step and begin installing the Microsoft Web Server.


Server Manager
Server Manager • Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
PROPERTIES
For LAB-SE-01
Computer name
Workgroup
Windows Defender Firewall
Remote management
Remote Desktop
NIC Teaming
Ethernet
Operating system version
Hardware information
TASKS
EVENTS
All events | 0 total
Filter
Server Name
ID
Severity
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
LAB-SE-01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation started on LAB-SE-01
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging
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
The installation of Microsoft Web Services will continue and may take a minute.


Server Manager
Server Manager • Local Server
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
File and Storage Services
IIS
PROPERTIES
For LAB-SE-01
Computer name
Workgroup
Windows Defender Firewall
Remote management
Remote Desktop
NIC Teaming
Ethernet
Operating system version
Hardware information
TASKS
EVENTS
All events | 0 total
Filter
Server Name
ID
Severity
Add Roles and Features Wizard
Installation progress
DESTINATION SERVER
LAB-SE-01
Before You Begin
Installation Type
Server Selection
Server Roles
Features
Web Server Role (IIS)
Role Services
Confirmation
Results
View installation progress
Feature installation
Installation succeeded on LAB-SE-01.
Web Server (IIS)
Management Tools
IIS Management Console
Web Server
Common HTTP Features
Default Document
Directory Browsing
HTTP Errors
Static Content
Health and Diagnostics
HTTP Logging
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
Once the installation has completed, you should close the Add Roles and Features Wizard.



Pro Tip: For this installation, we've temporarily disabled the Microsoft Windows Firewall and Internet Explorer Enhanced Security for Administrators. If you plan to re-enable the Microsoft Windows Firewall after the installation is complete, we will guide you through the creation of a rule for RADIUS.

Installing & Configuring SecurEnvoy SecurAccess

The following steps are required to configure the SecurEnvoy SecurAccess product for use. We suggest that you gather the following listed items before getting started and have them available.

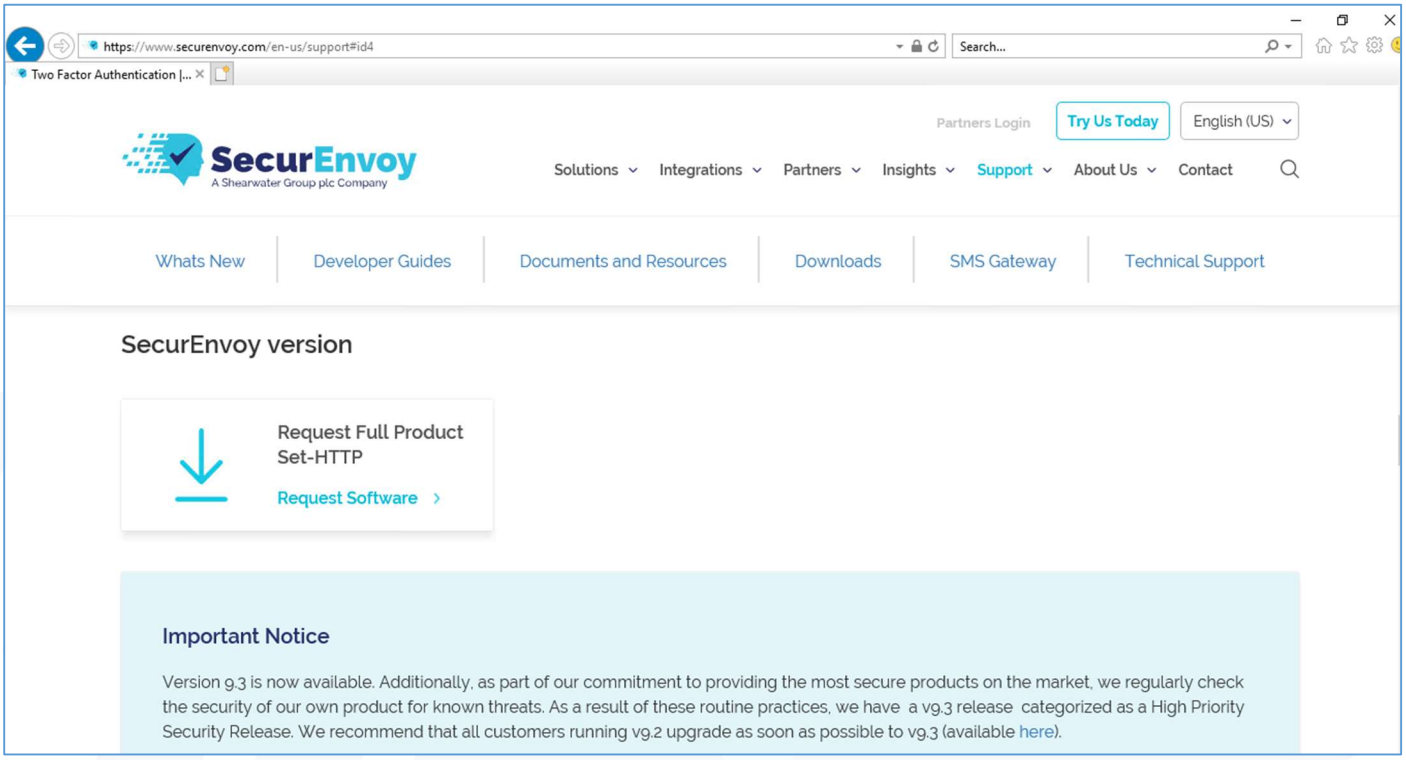
Note: This is the basic configuration to get the system installed and ready for use. Secure LDAP and SSL Certificates are strongly recommended for a production build. We cover those items further in this document.

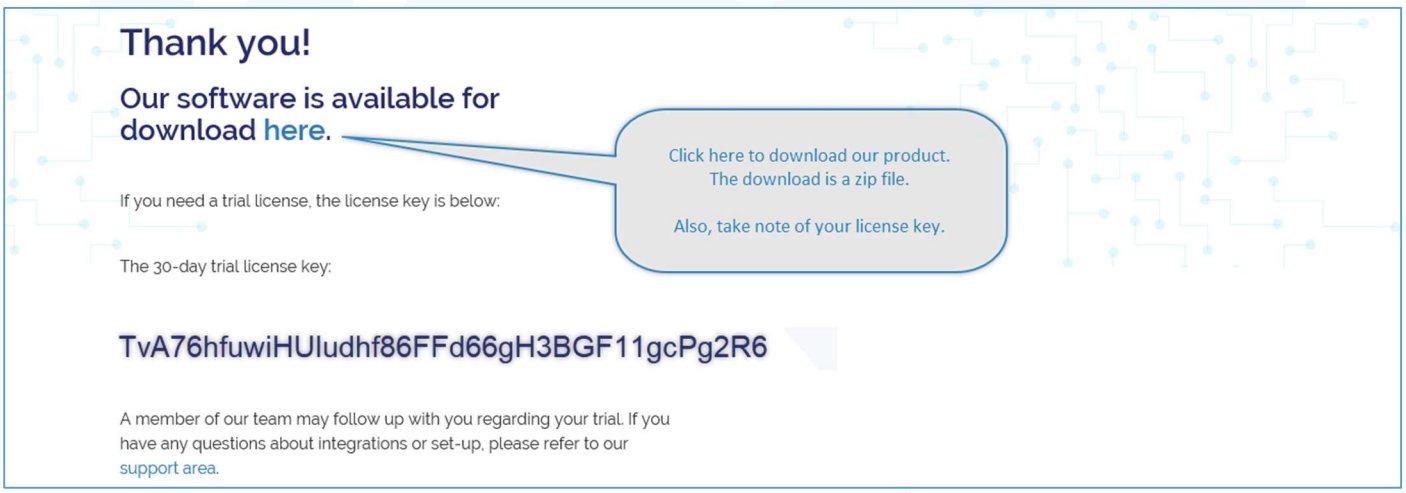
Currently, you'll need;

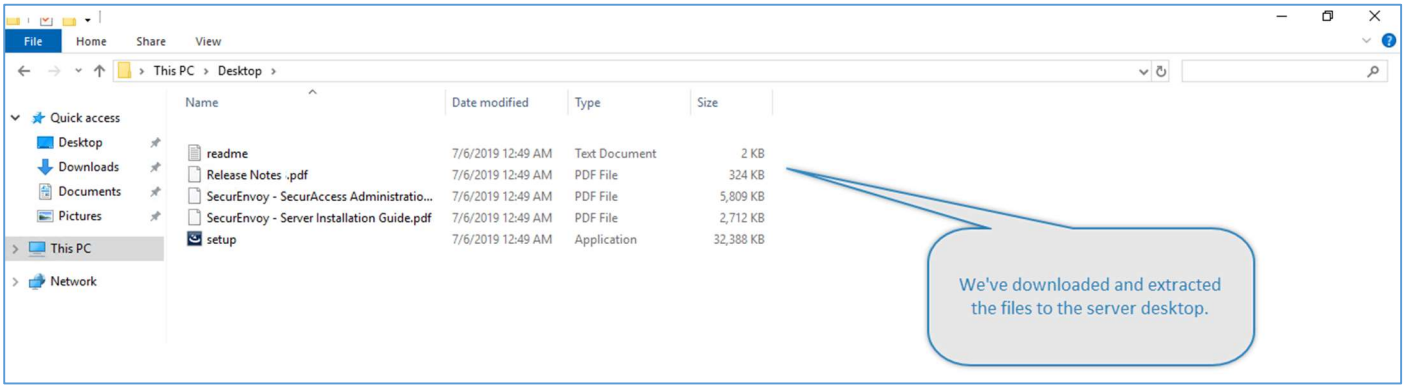
- Microsoft Active Directory Domain FQDN and NetBIOS Name
- FQDN for at least one Domain Controller, two recommended
- Create (or use) an existing Service Account from your Active Directory
- SMTP Server FQDN, including port and encryption requirements
- Email Account credentials

Downloading our Software

You can find the most current version of our software available on our web site, shown below.





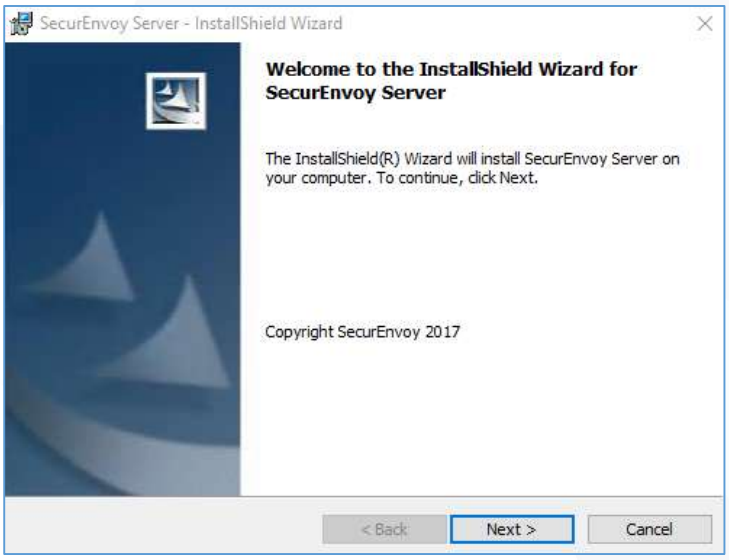


We suggest extracting the files on the server to which you intend to install the product. Here we've extracted them to the desktop of the server. You can extract our download anywhere you like.

Installing SecurAccess

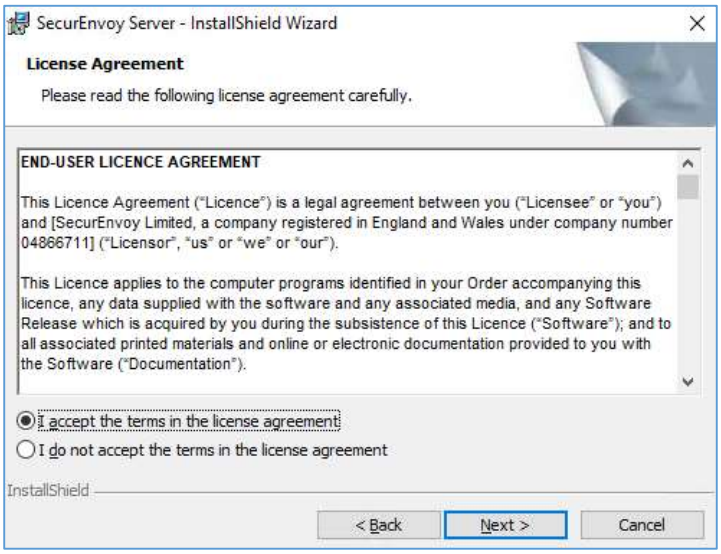
As we prepare to run setup.exe, it's important to remember that Active Directory membership for the SecurEnvoy SecurAccess Server is optional. If your server is part of the Active Directory, you should logon as a Domain or Local Administrator to complete the following steps.

Welcome to the System Installer



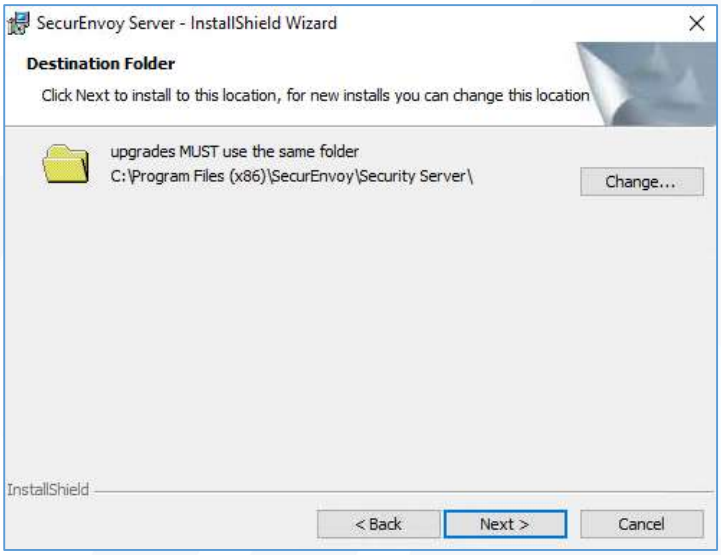
License Agreement

Please review and accept our licensing terms to continue.



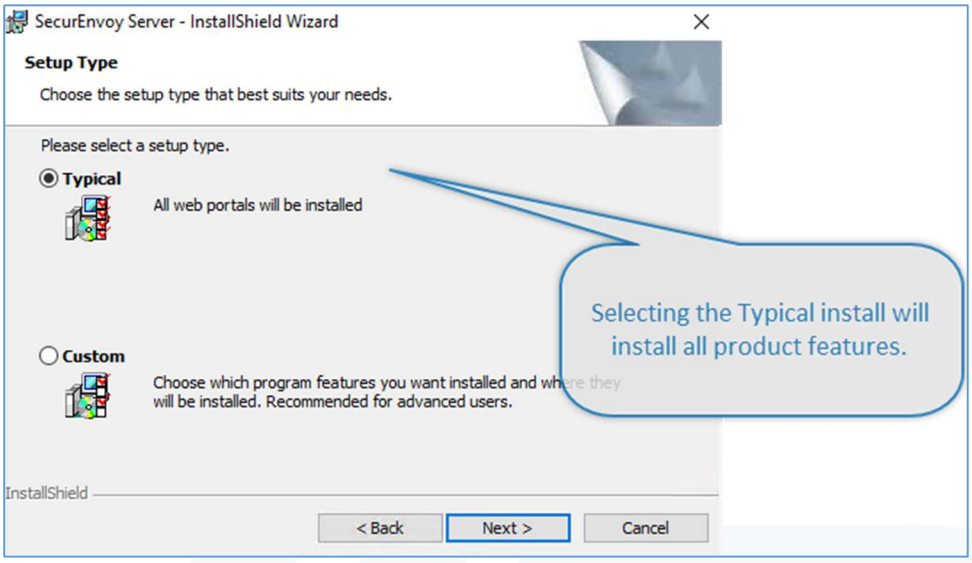
Installation Path

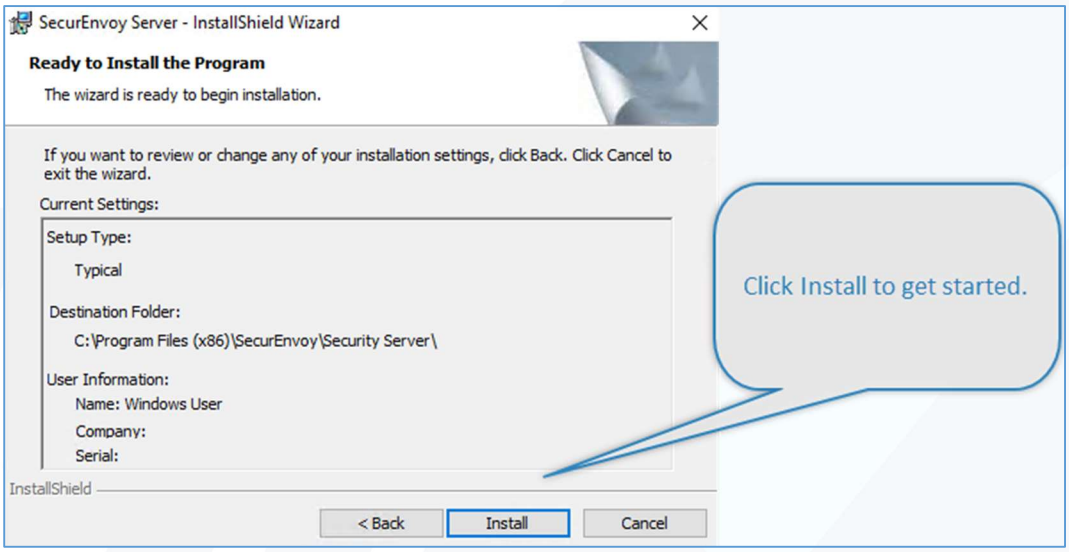
Although we recommend keeping the default installer path, you are free to change it to meet any requirements you may have. Please remember this, as you may find the default path referenced in some of our other documents.



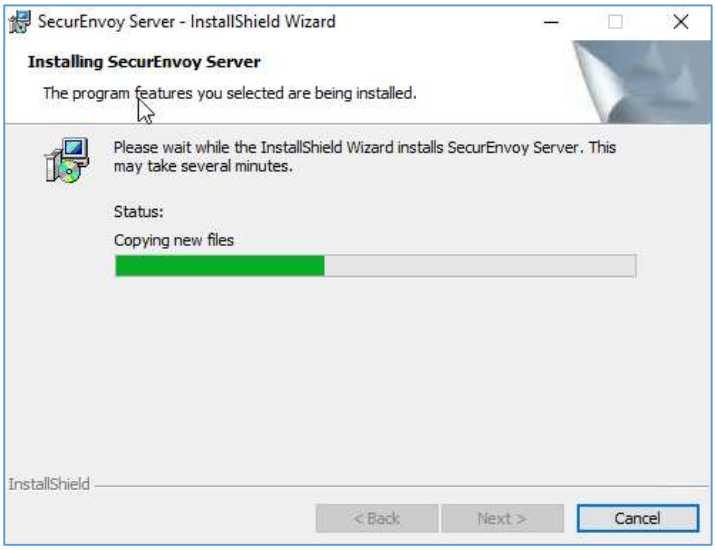
Select Setup Type

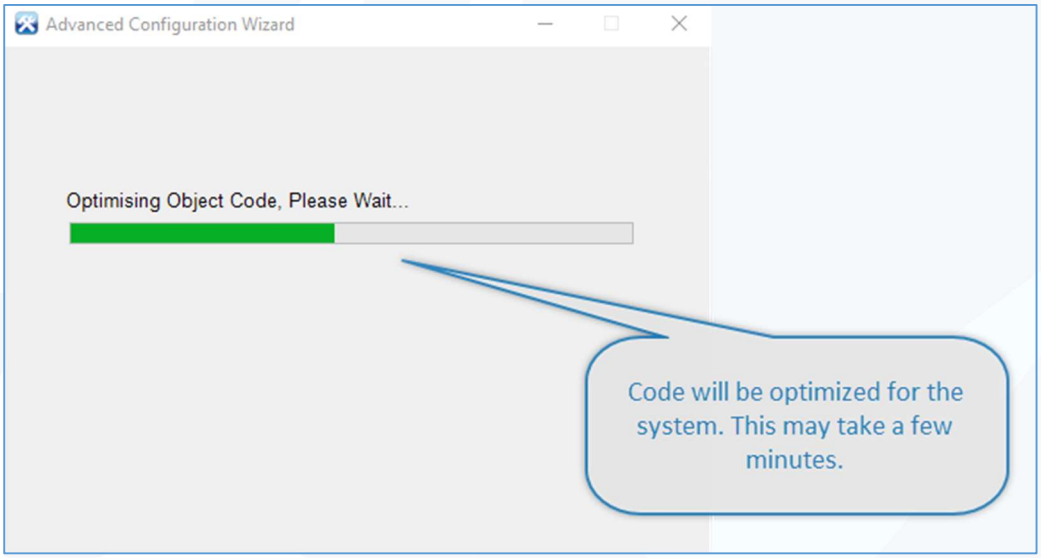
The typical install will install all features on the system. A custom install gives you the opportunity to select specific components. It's recommended that you use the typical installer, unless you are performing an advanced installation.



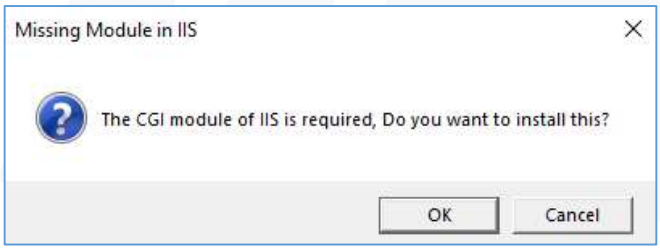


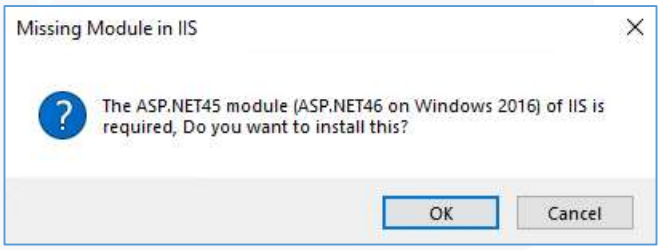
The installer will now begin running through the tasks of installing the system.

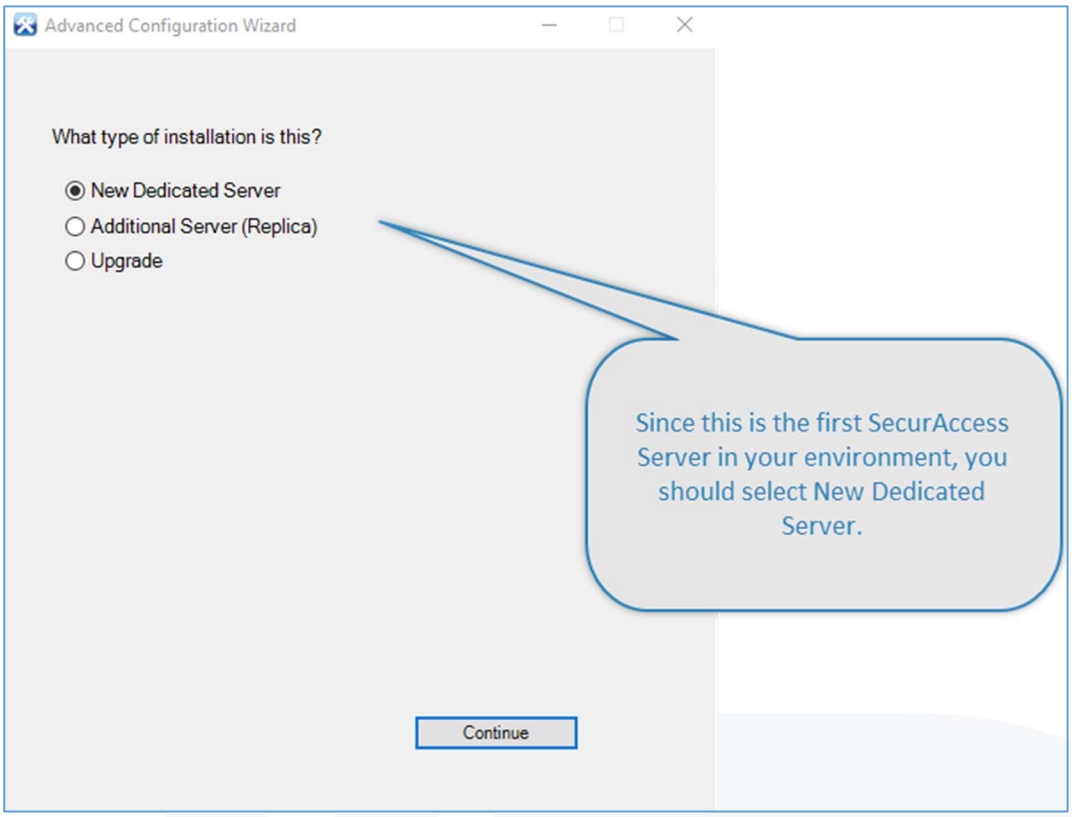


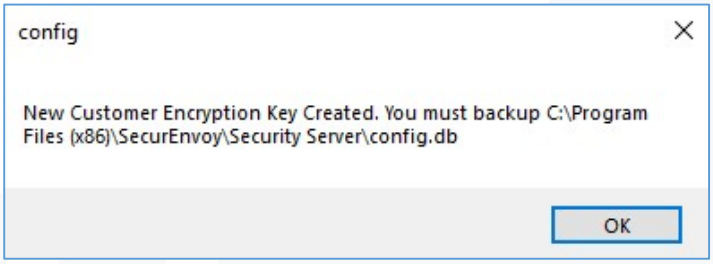


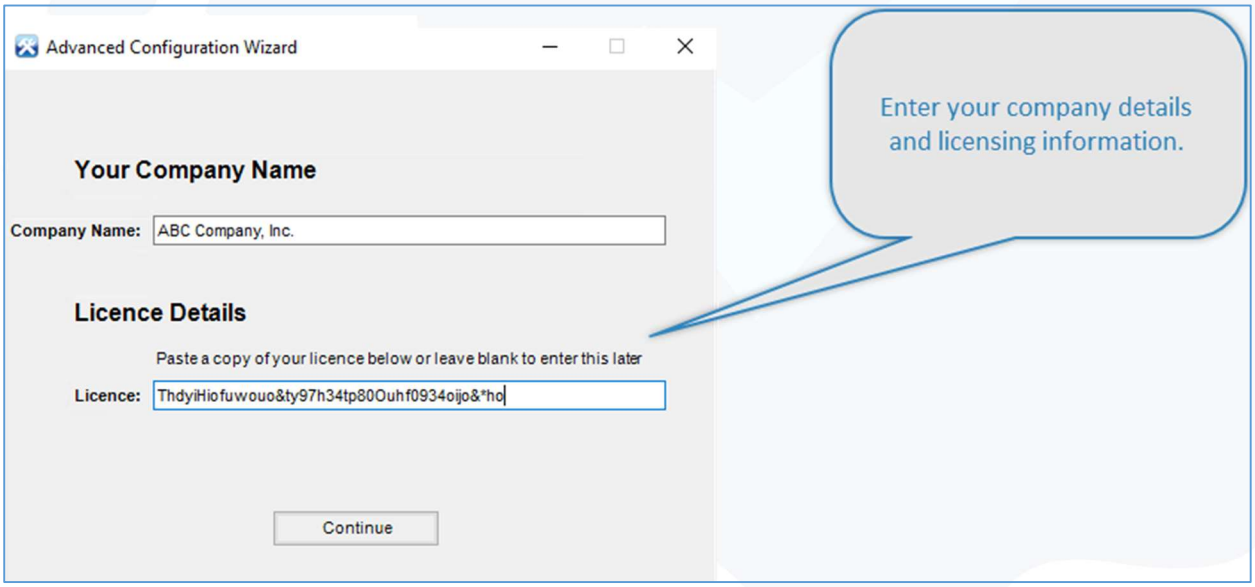
Most (if not all) systems will require the CGI module and the ASP.NET 4.5 Module, you'll be prompted and should accept.






Advanced Configuration Wizard
What type of installation is this?
New Dedicated Server
Additional Server (Replica)
Upgrade
Since this is the first SecurAccess Server in your environment, you should select New Dedicated Server.
Continue


config
New Customer Encryption Key Created. You must backup C:\Program Files (x86)\SecurEnvoy\Security Server\config.db
OK


Advanced Configuration Wizard
Your Company Name
Company Name: ABC Company, Inc.
Licence Details
Paste a copy of your licence below or leave blank to enter this later
Licence: ThdyiHiofuwouo&ty97h34tp80Ouhf0934oijo&*ho
Continue
Enter your company details and licensing information.

Configure Your Service Account

For our system to query the Active Directory for usernames and passwords, we need an account with permissions to do that function. We strongly recommend that you create a general user account in the Active Directory to serve as the service account. This account does not need to be a Domain Administrator, it can be a simple standard user.

Pro Tip: It's advisable to set the password on this account to never expire.

The LDAP Admin service account used by SecurEnvoy for SecurAccess and SecurPassword require Active Directory permissions as follows:

- Read All User Attributes (Default Permission for all users)
- Write Access To "PrimaryTelexNumber" also referred to as "Telex Number"
- Write Access To "Telex Number Other"

Optionally, to allow user Mobile and Email address attributes to be updated from the SecurEnvoy admin GUI:

- Write Access To Mobile Number (Optional)
- Write Access To E-Mail Address (Optional)

For SecurPassword and Integrated Desktop Logon:

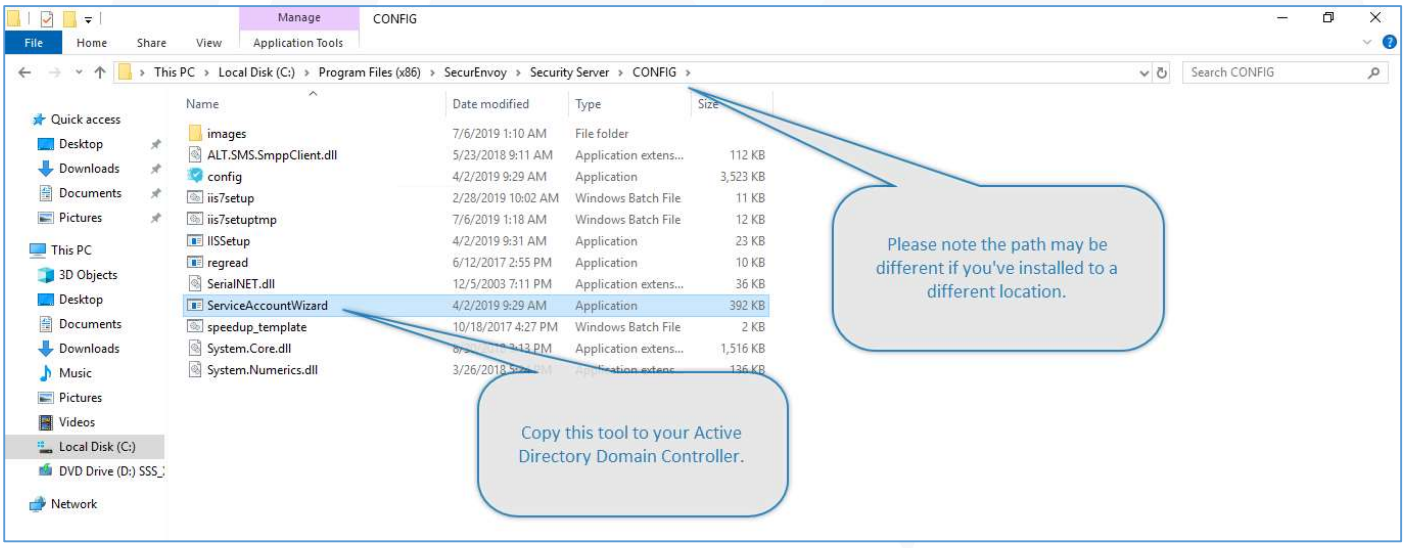
- User Object: "Reset Password"
- User Object: "Change Password"

Note: It's important to remember that although you may logon to the SecurEnvoy SecurAccess Management console as a Domain Administrator, the service account is still the account that will reach the Active Directory.

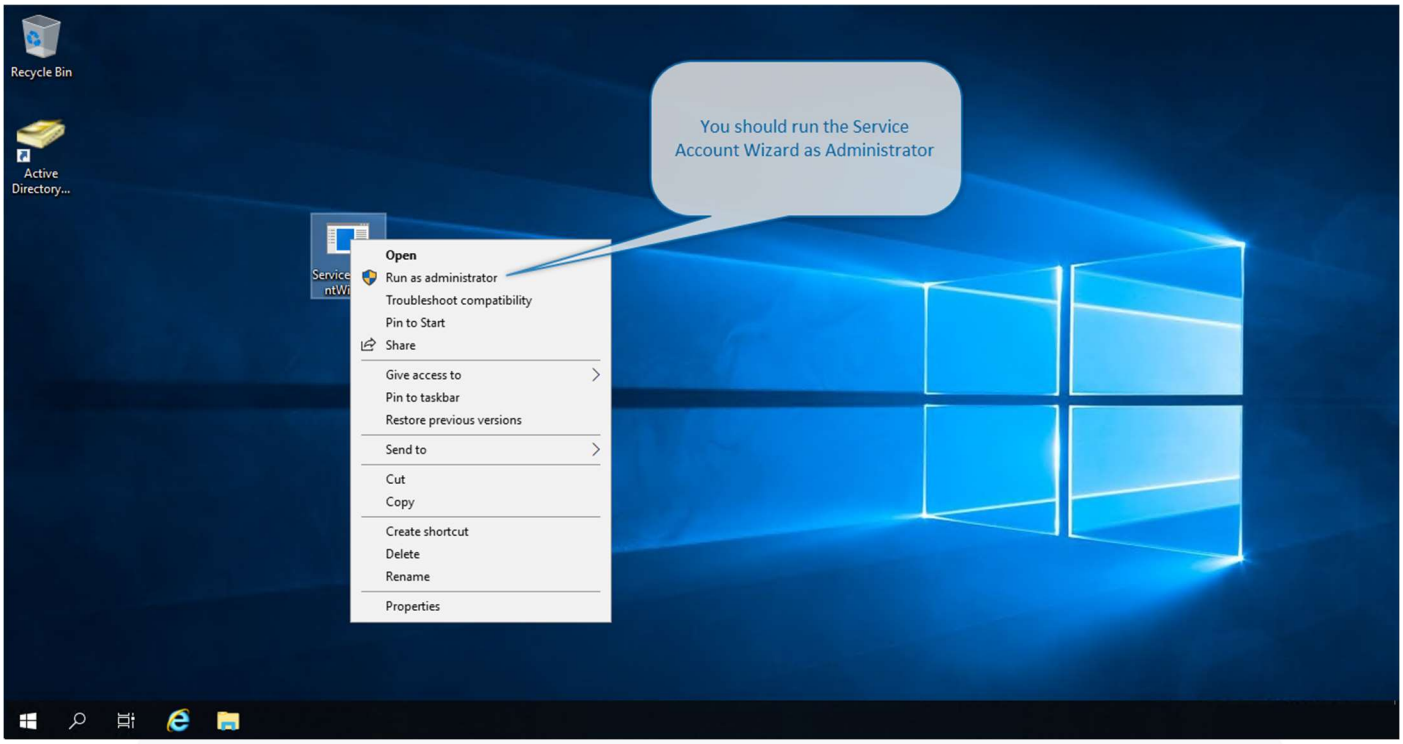
SecurEnvoy Service Permissions Account Wizard

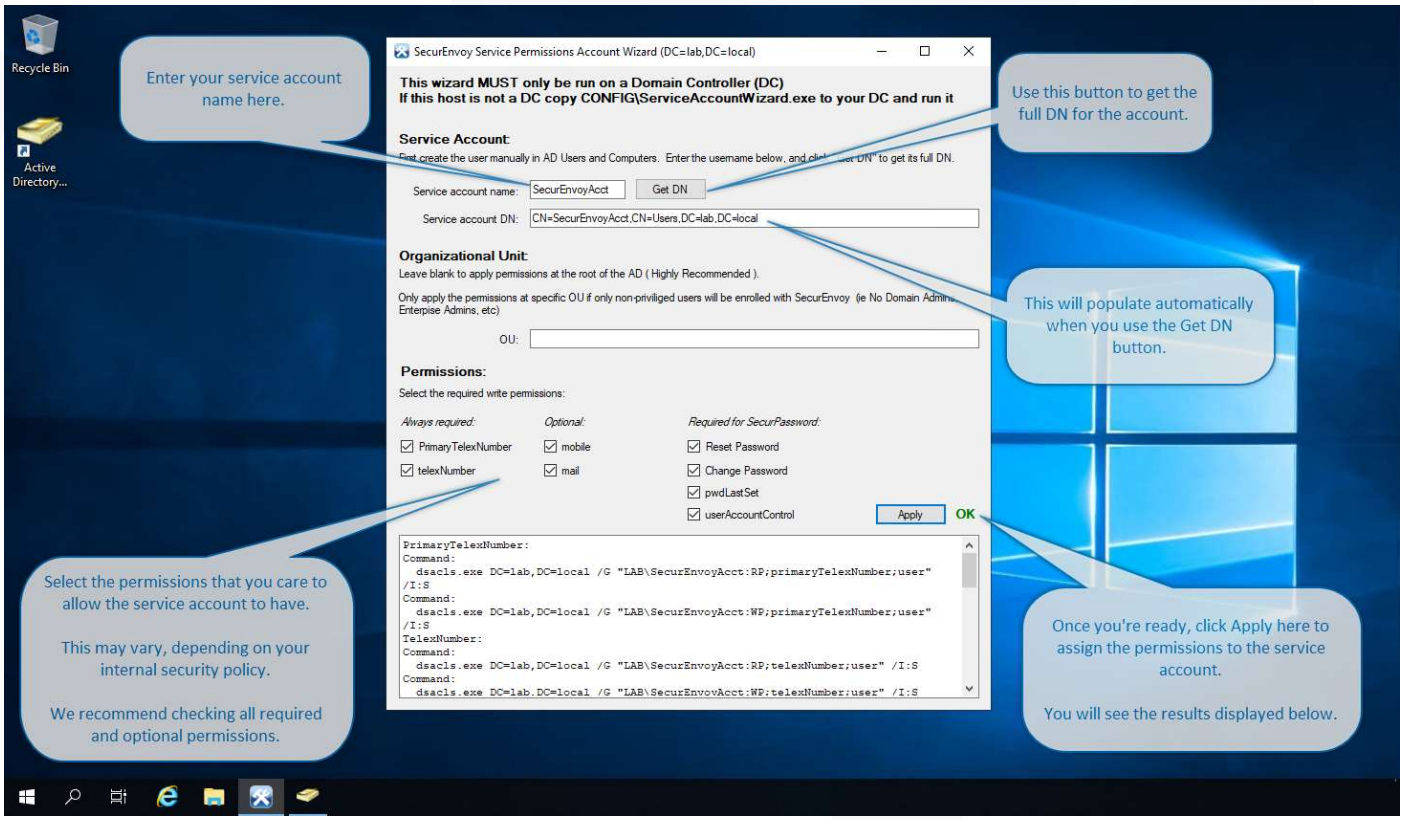
To avoid setting the service account as an administrator, its critical that the permissions for this account's access into the Active Directory be limited. As noted above, we only require access to specific fields of a users' account. Access to these fields are necessary for the system to perform functions such as adding and registering new users, adding mobile phone numbers to a user's account and updating email addresses.

- On the SecurEnvoy SecurAccess Server, navigate to C:\Program Files (x86)\SecurEnvoy\Security Server\Config
- Copy ServiceAccountWizard.exe tool to your Active Directory Domain Controller.



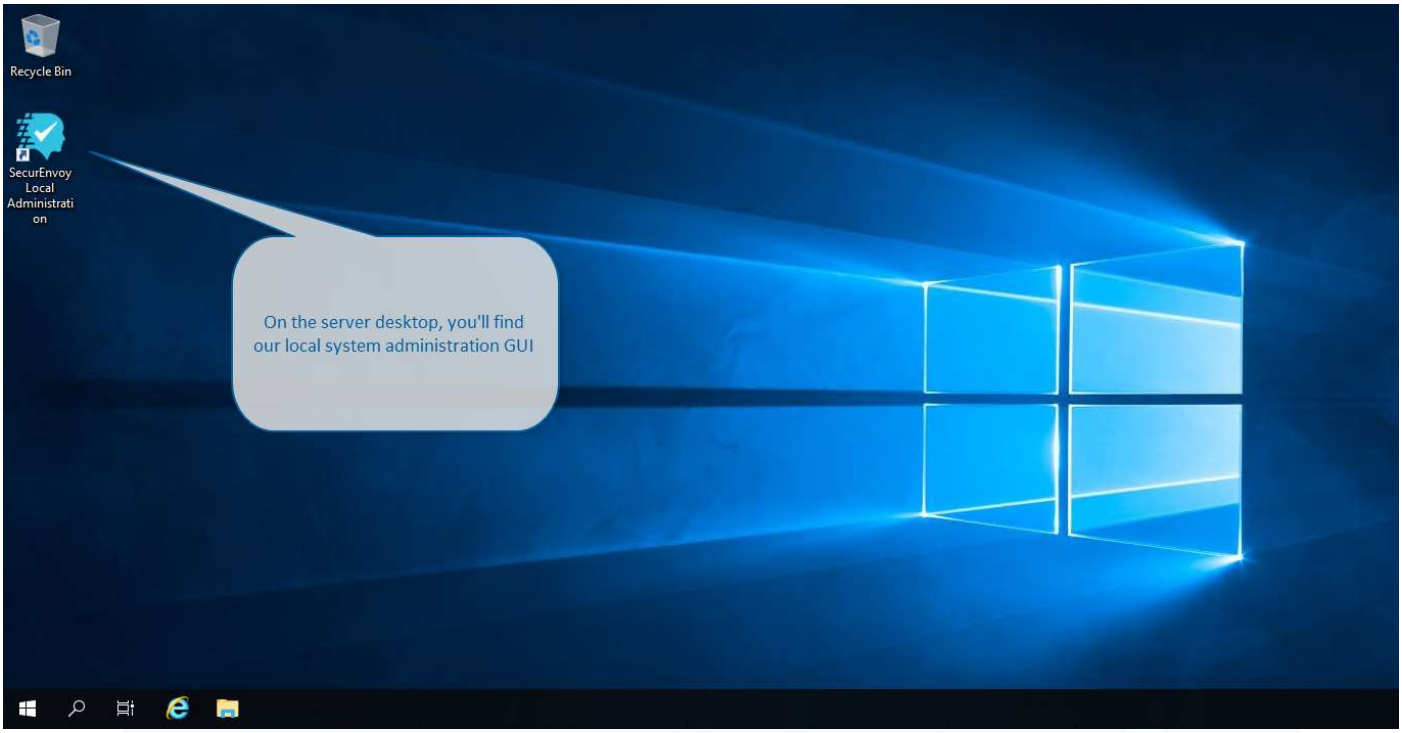
You will need to logon as a Domain Administrator and run this file with Administrative Authority.



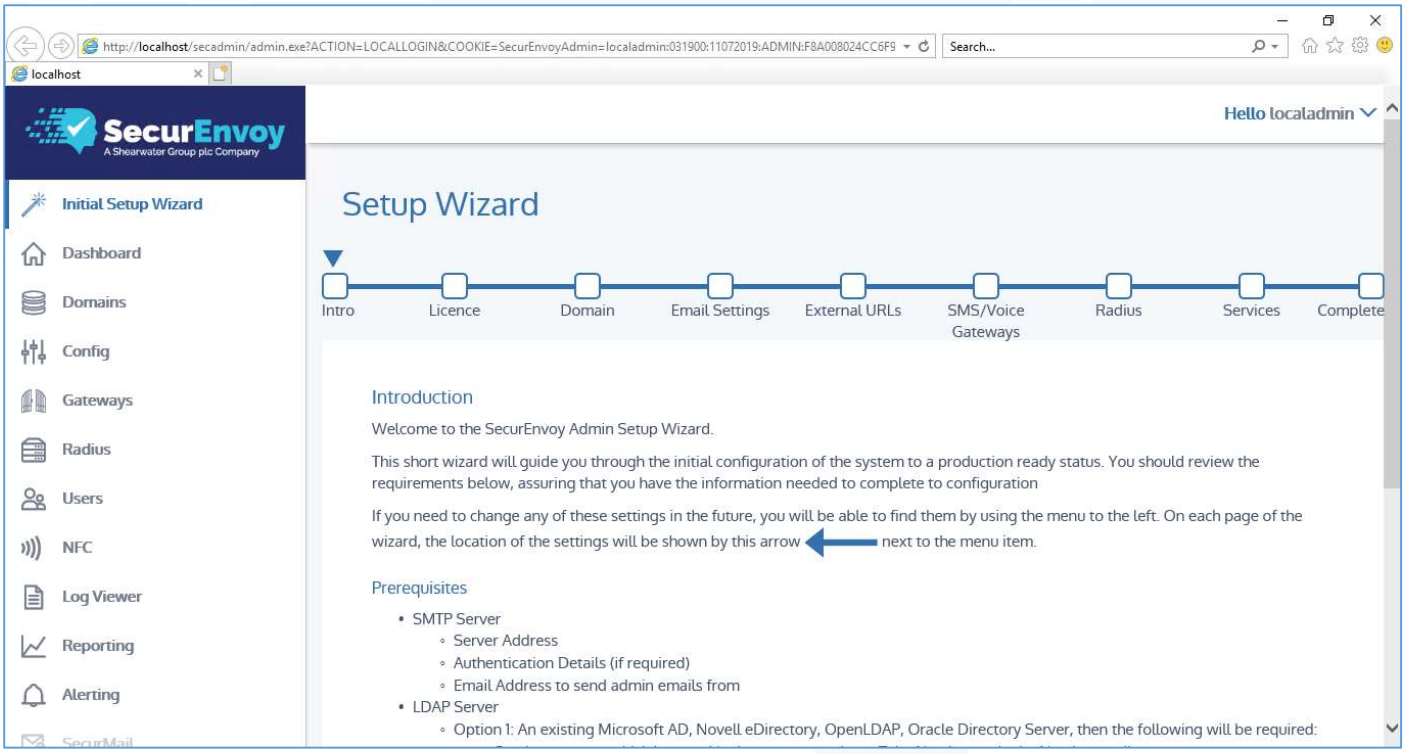


Configuring SecurEnvoy SecurAccess

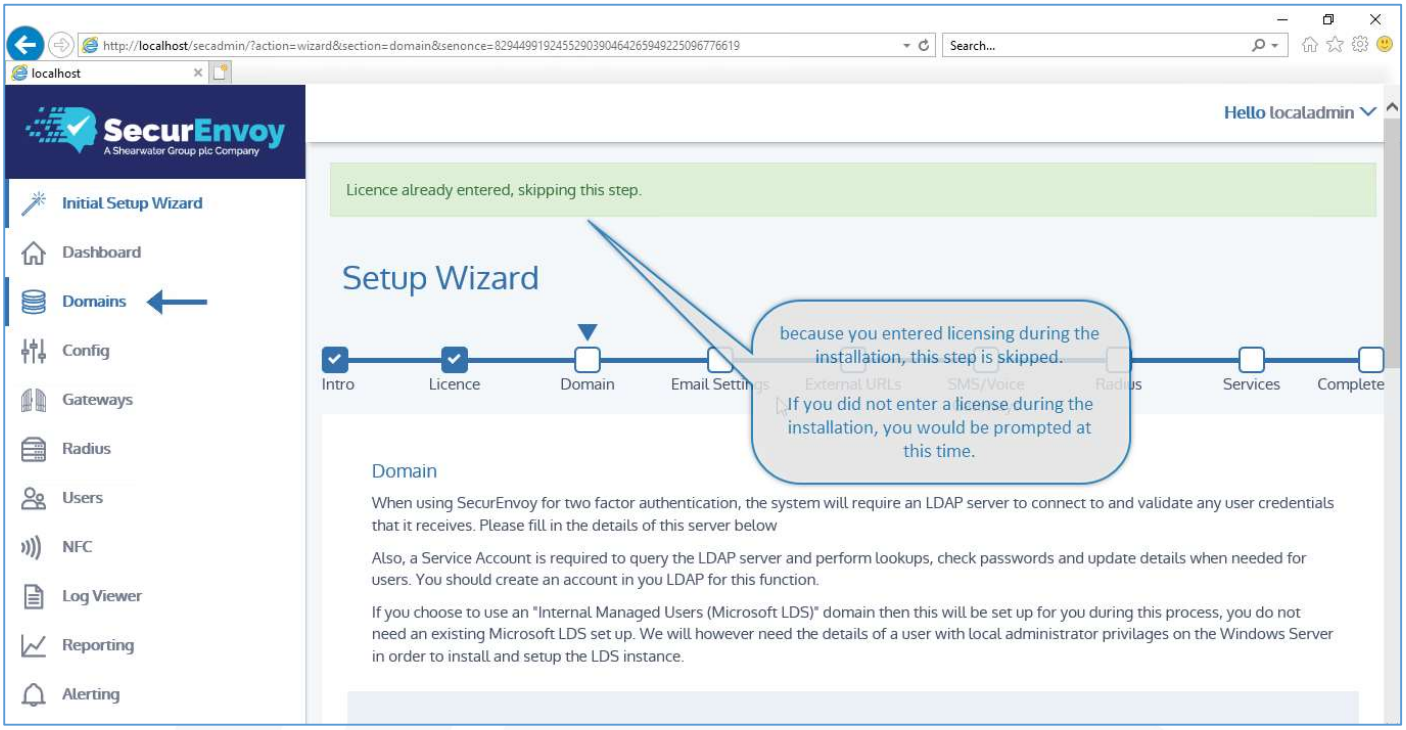
Once the installation has been completed, you will need to configure the system for use. It is required that you authenticate to the SecurEnvoy SecurAccess Security Server as a local administrator, or as a domain administrator if your system is part of an Active Directory.



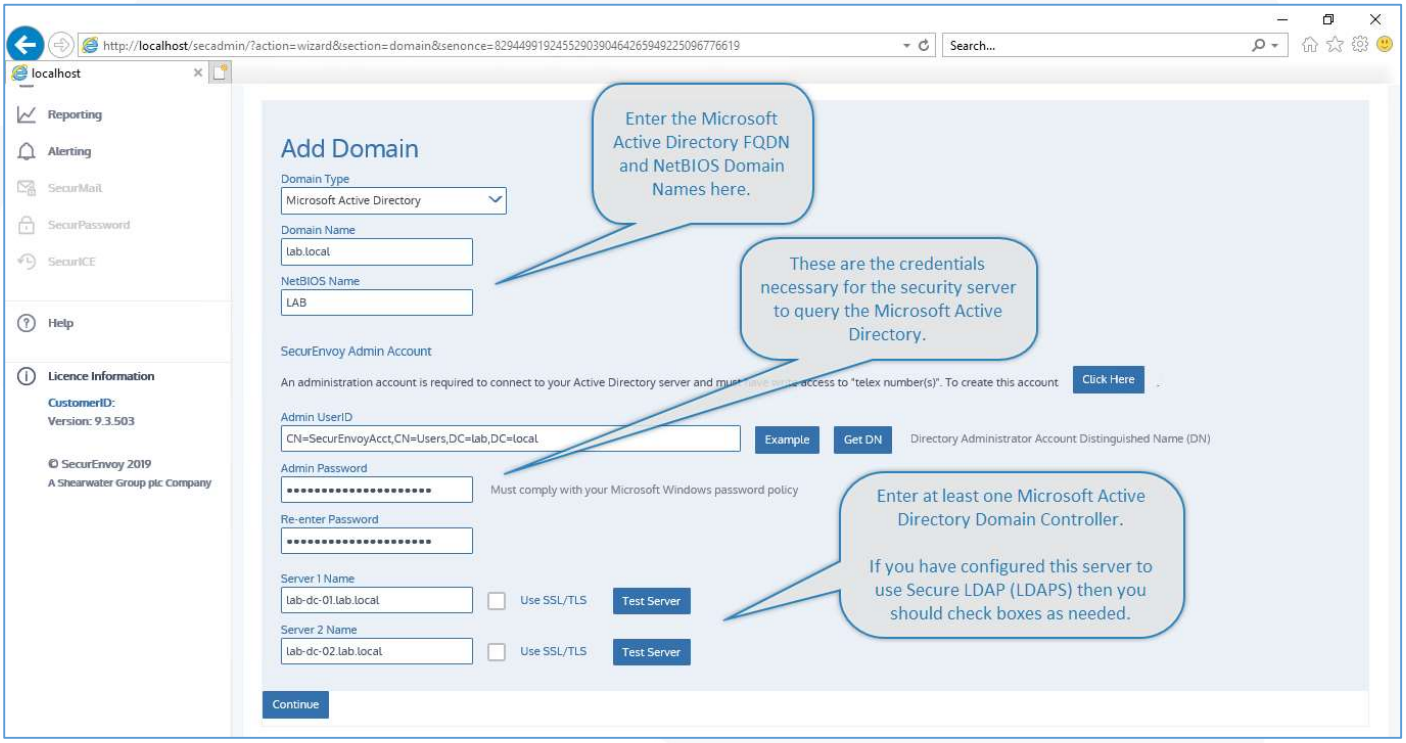
Note: The Local Administrator will run under the account context that you have authenticated to this server with.



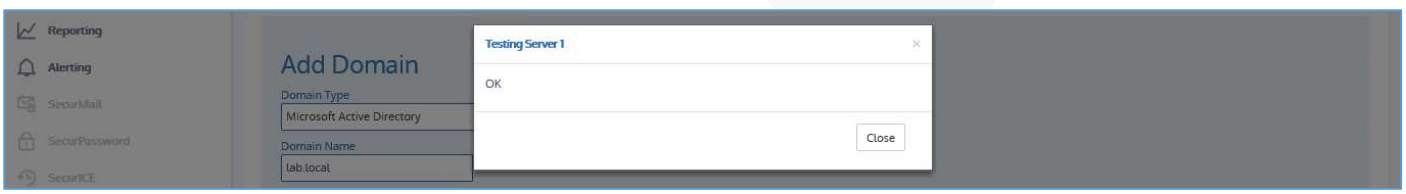
Note: As you enter details for the system, the Continue button can be located below the bottom of the screen and you'll need to scroll down.



Note: We have entered some details for you to use as a reference in these screen captures. Please assure that you are entering the correct details for your network and organization.



Note: Make sure to click the Test Server button to assure that you have established working commmunications.

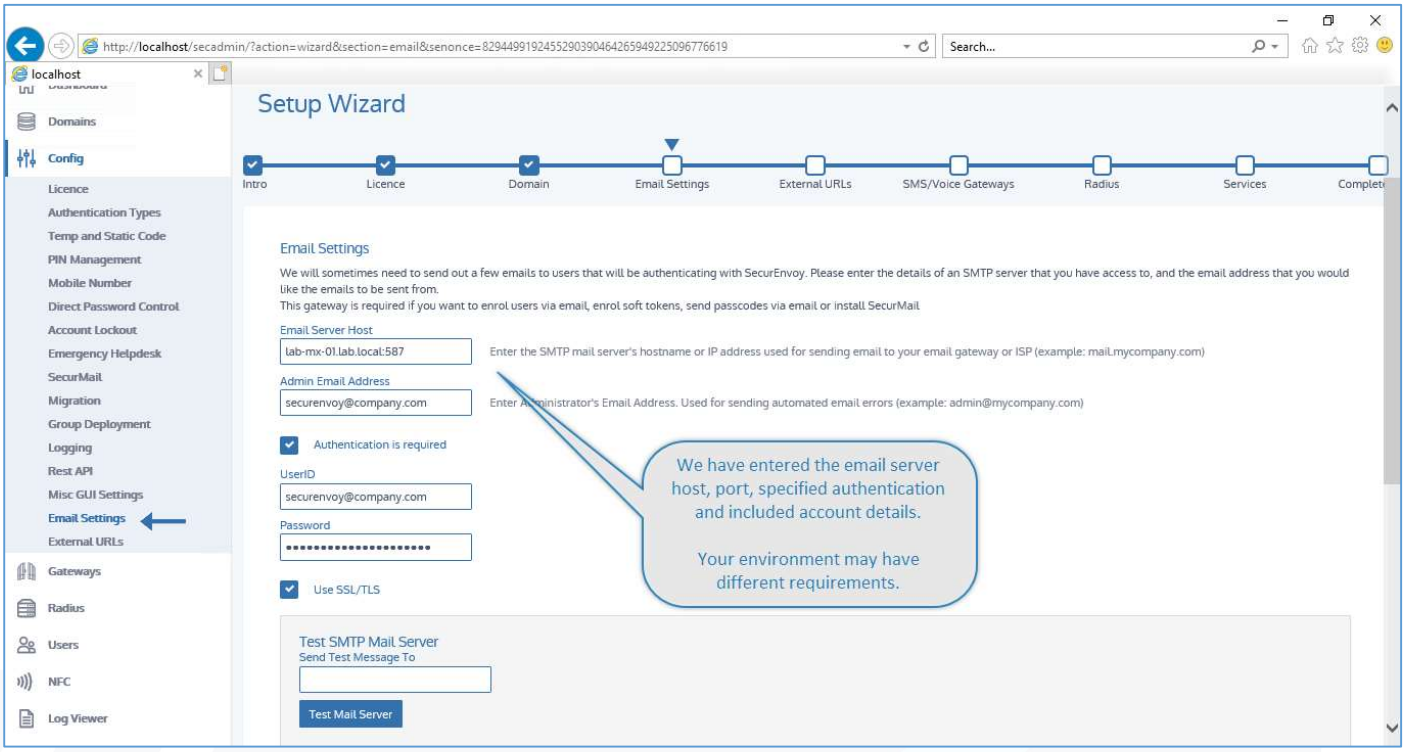


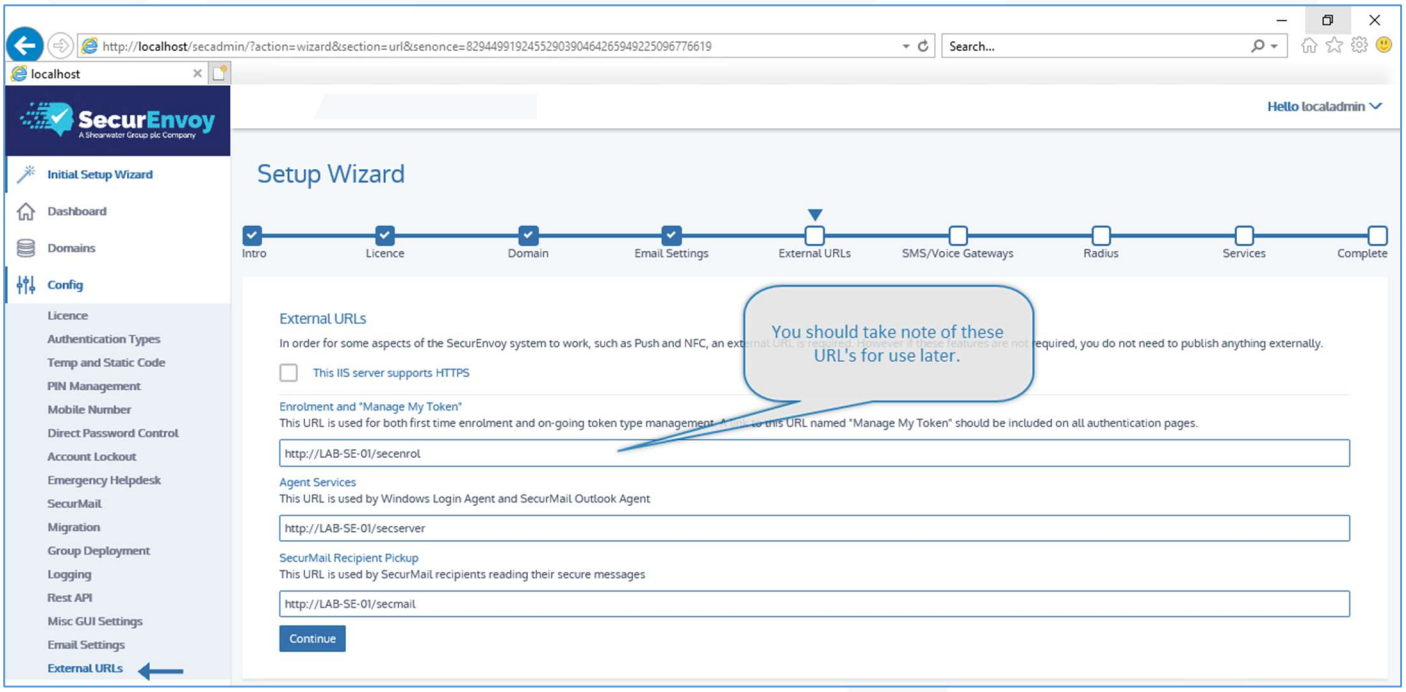
Configuring Email settings is an important part of the system. With these settings, the SecurEnvoy Security Server will be able to send welcome emails and other notifications to users and administrators of the system.

Note: The system will default to SMTP Port 25, unless you specify a different port. To specify a different port, you must add the port number to the end of your Email Server Host as follows:

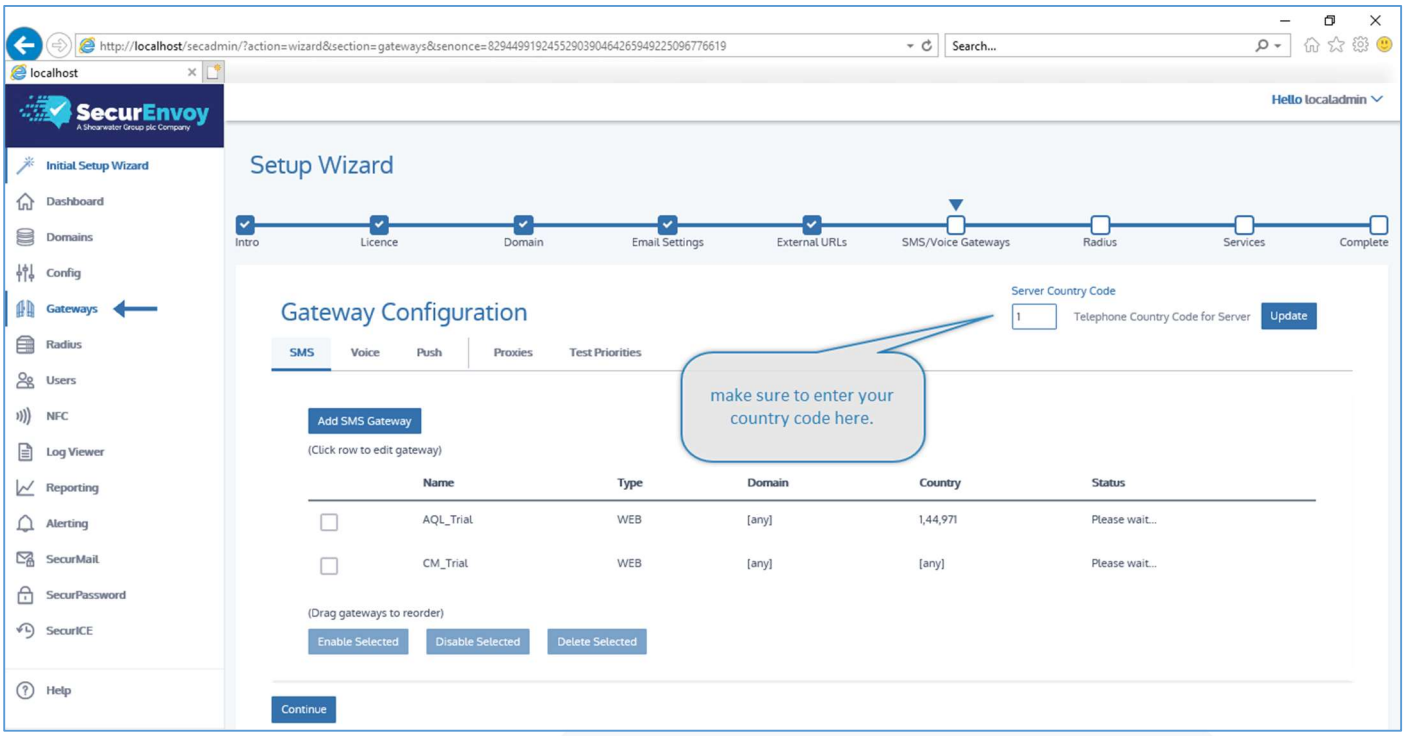
<Your Mail Server>:<Port>

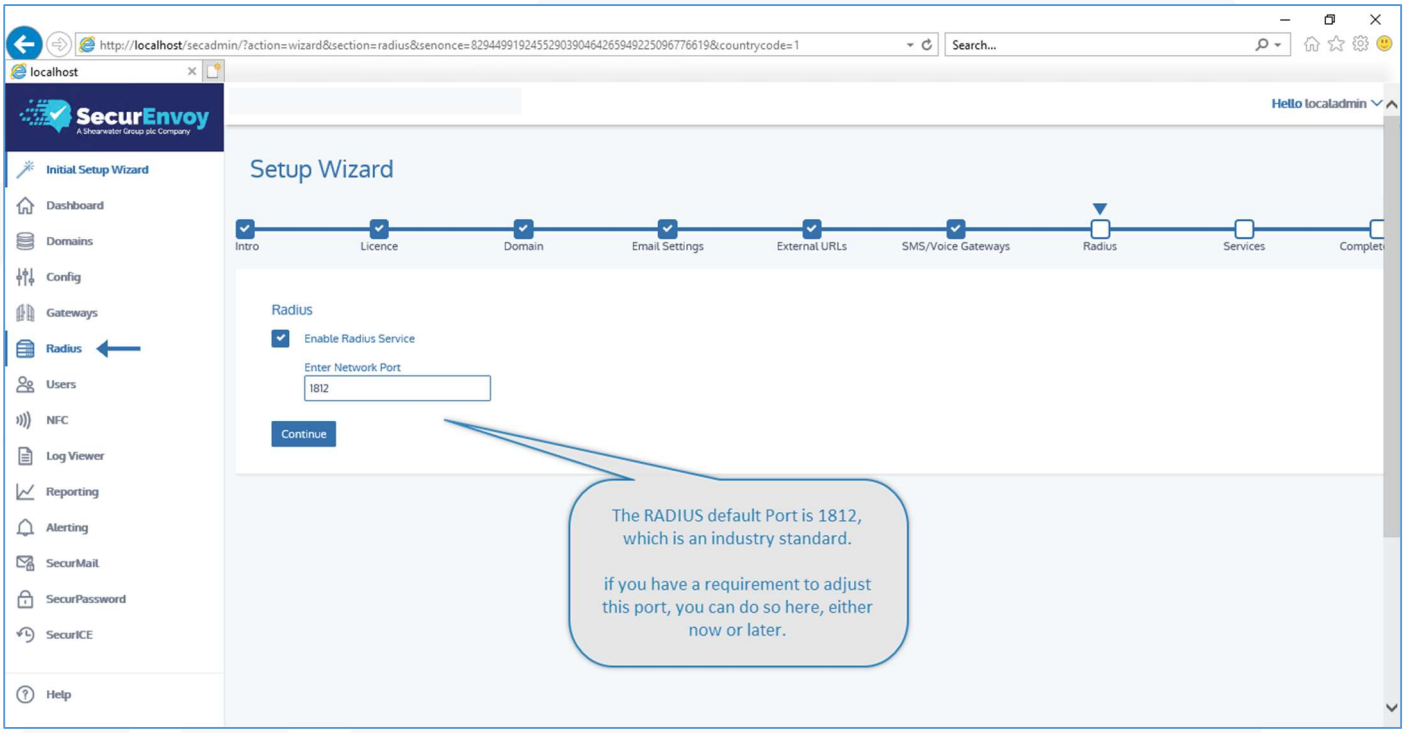
Example: smtp.gmail.com:587

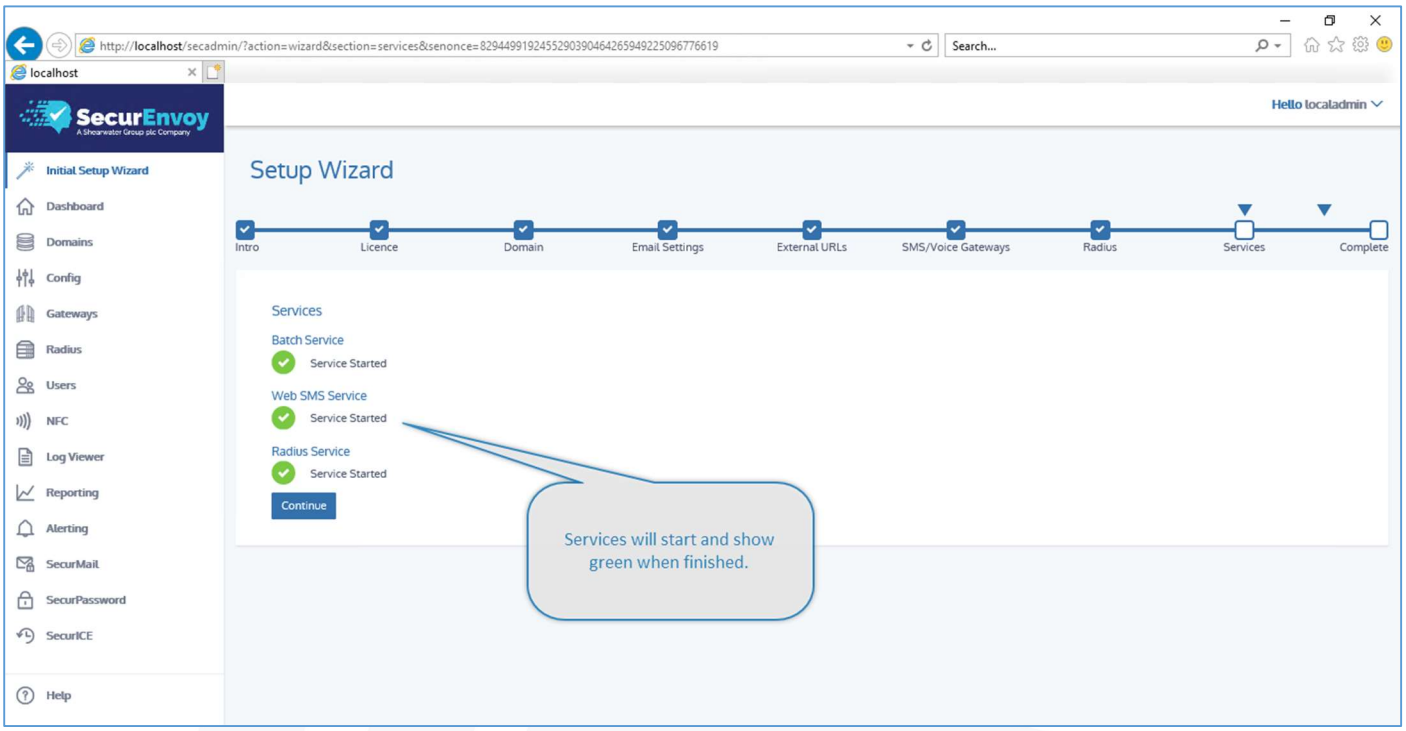


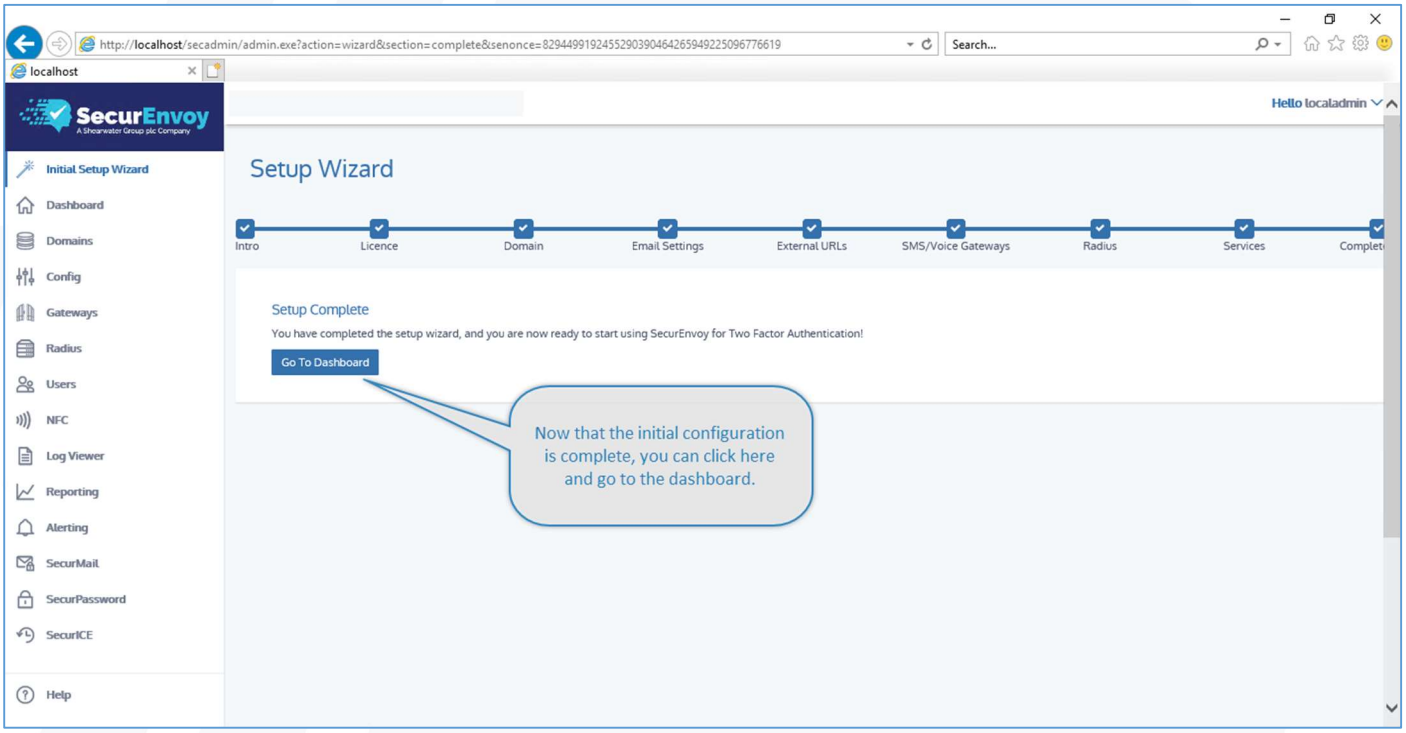


The system defaults to an unsecured URL state, since it does not initially have an SSL Certificate for IIS. Once we complete the initial setup and configuration, we cover requirements for securing the system.






http://localhost/secadmin/?action=wizard&section=services&senonce=829449919245529039046426594922509677619
Search...
localhost
SecurEnvoy
A Shearwater Group plc Company
Hello localadmin
Initial Setup Wizard
Dashboard
Domains
Config
Gateways
Radius
Users
NFC
Log Viewer
Reporting
Alerting
SecurMail
SecurPassword
SecurICE
Help
Setup Wizard
Intro
Licence
Domain
Email Settings
External URLs
SMS/Voice Gateways
Radius
Services
Complete
Services
Batch Service
Service Started
Web SMS Service
Service Started
Radius Service
Service Started
Continue
Services will start and show green when finished.


http://localhost/secadmin/admin.exe?action=wizard&section=complete&senonce=829449919245529039046426594922509677619
Search...
localhost
SecurEnvoy
A Shearwater Group plc Company
Hello localadmin
Initial Setup Wizard
Dashboard
Domains
Config
Gateways
Radius
Users
NFC
Log Viewer
Reporting
Alerting
SecurMail
SecurPassword
SecurICE
Help
Setup Wizard
Intro
Licence
Domain
Email Settings
External URLs
SMS/Voice Gateways
Radius
Services
Setup Complete
You have completed the setup wizard, and you are now ready to start using SecurEnvoy for Two Factor Authentication!
Go To Dashboard
Now that the initial configuration is complete, you can click here and go to the dashboard.

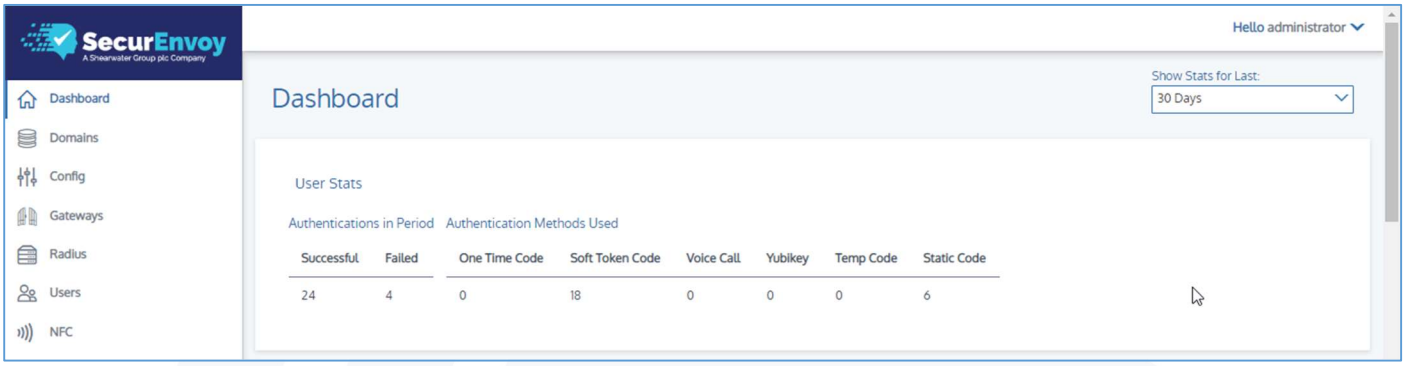
SecurEnvoy SecurAccess Dashboard

The system dashboard is a vital area for administrators to get information related to the systems health and the activities of users. The dashboard has several components which we've illustrated here.

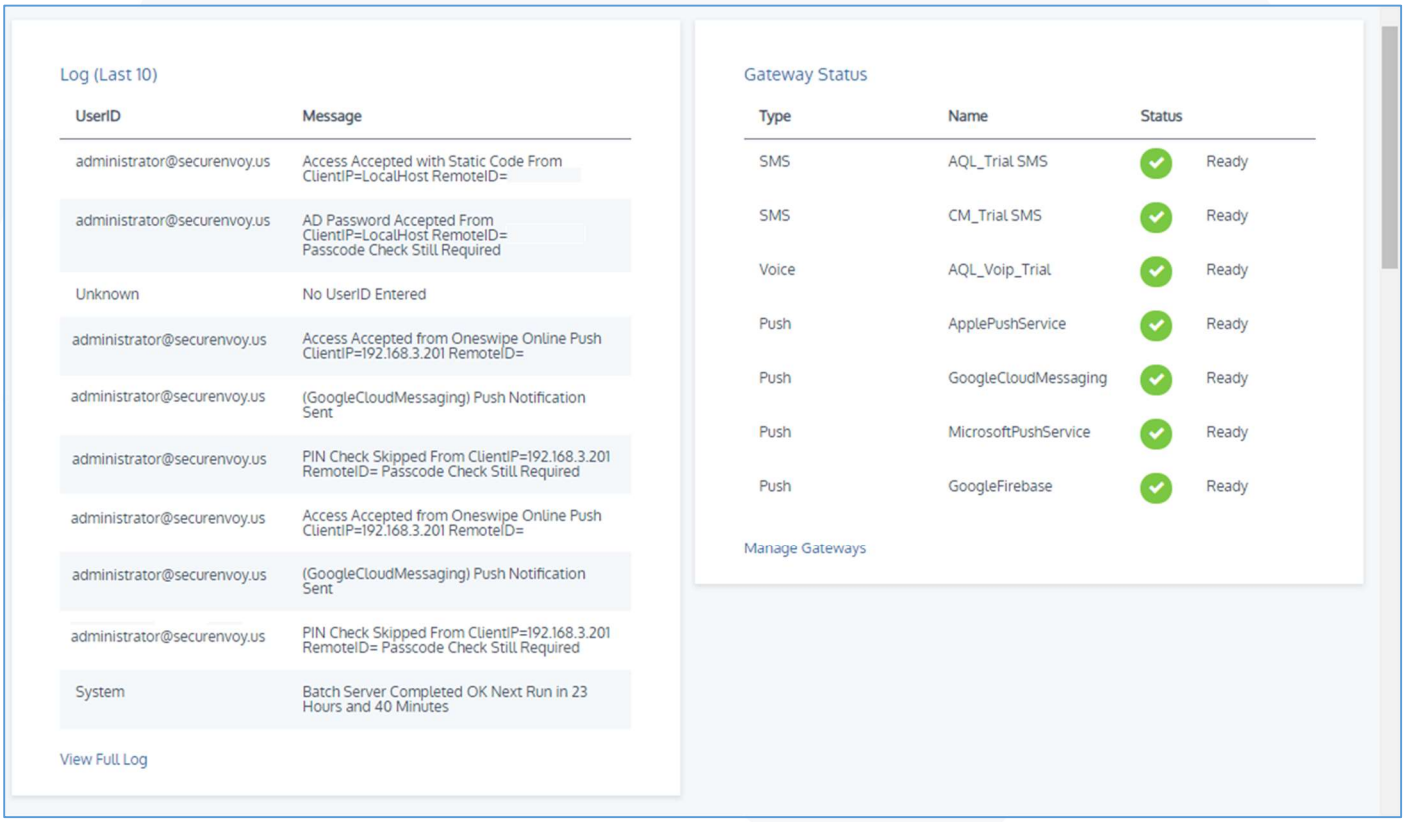
Dashboard Components

This top section of the dashboard displays current and historical data. This part is useful, providing the administrator to select the period to review, from 7, 14 or 30 days.

How users are authenticating is an important part of understanding the community. This area will also display both successful and failed authentications, so you'll be able to spot issues easily.



The middle section of the dashboard contains the most recent 10 actions from the logs and gateway status for quick reference. This section sis helpful as it provides an immediate view of system health in respect to communications and events.

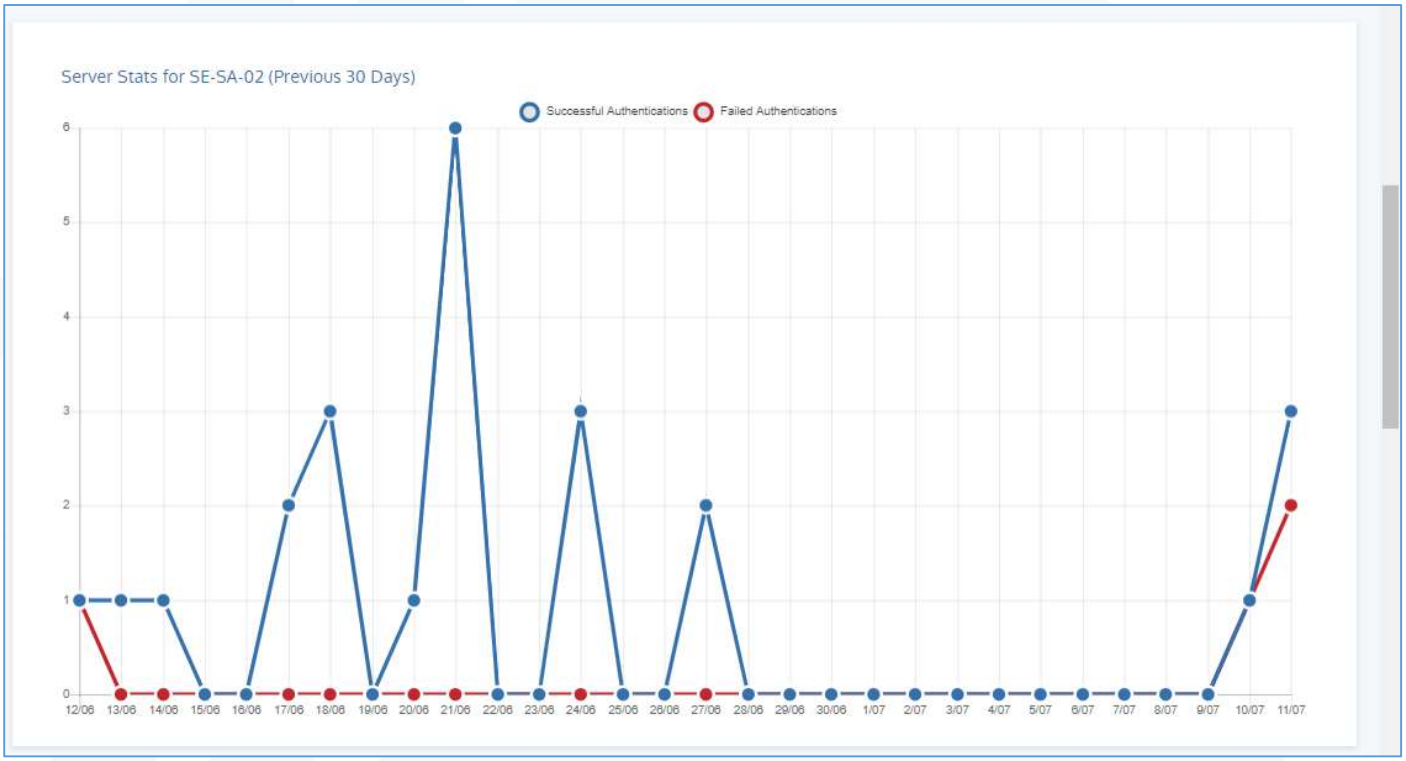


Further, this section of the dashboard provides status of services running and connectivity to LDAP environments. If you have a system that is connected to more than one LDAP environment, all of them will be displayed.

Note: You can also restart any of these services from this location.



The graph at the bottom of the dashboard illustrates trends on the system. This graph will automatically adjust it's timeframe to the same period as the rest of the dashboard.



Note: These illustrations of the dashboard includes data from our lab environment. Yours will not initially have any data.

Configure Radius Client Connections

Now that you have completed the setup and configuration of the SecurEnvoy Security Server, if you wish to use SecurAccess or SecurIce 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 (ASCII 127 Printable Characters – With some exclusions)

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.

ASCII 127 is an industry standard character code set, which is basically your keyboard. Below is a table which outlines this code set. There are a few characters that should not be used when with a Radius Shared Secret and we've highlighted these for you. We've included both the character code and the character itself, so you'll see them paired together.

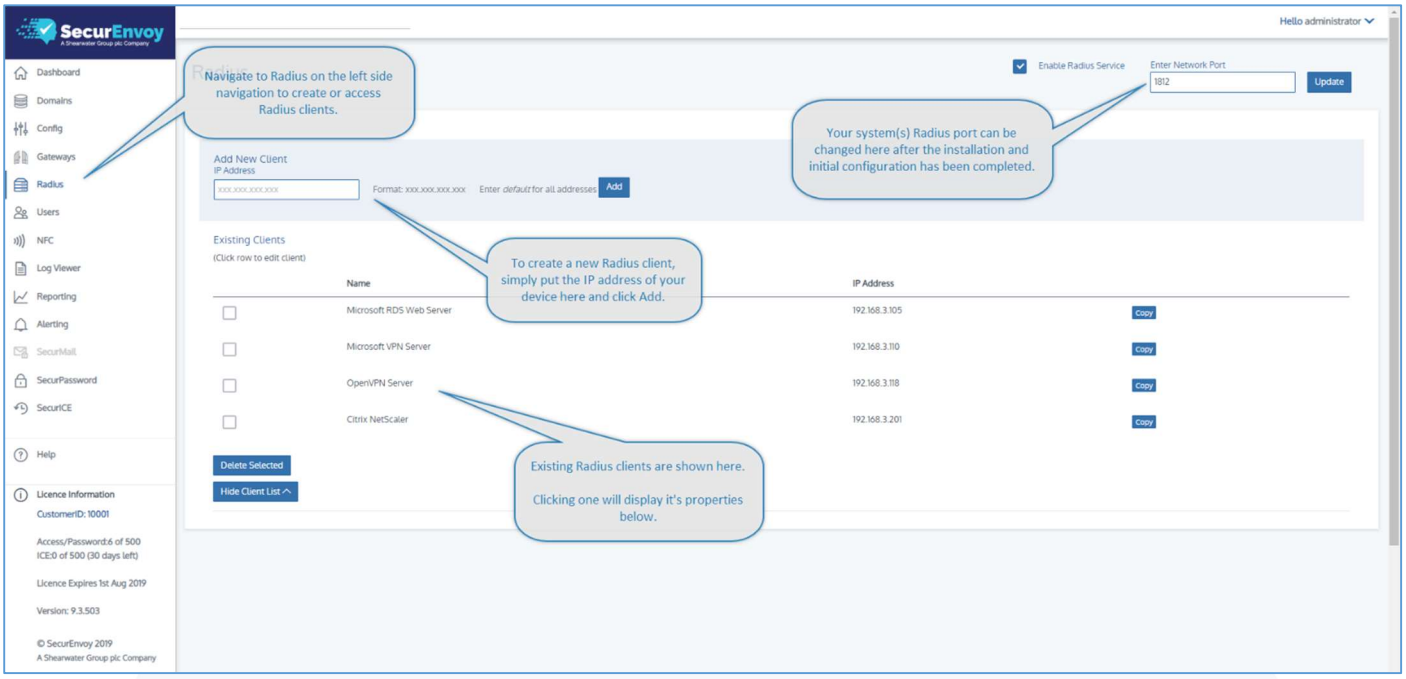
CODE	CHAR	CODE	CHAR	CODE	CHAR	CODE	CHAR	CODE	CHAR	CODE	CHAR
32	Space	48	0	64	@	80	P	96	`	112	P
33	!	49	1	65	A	81	Q	97	a	113	Q
34	"	50	2	66	B	82	R	98	b	114	R
35	#	51	3	67	C	83	S	99	c	115	S
36	$	52	4	68	D	84	T	100	D	116	T
37	%	53	5	69	E	85	U	101	e	117	U
38	&	54	6	70	F	86	V	102	f	118	V
39	'	55	7	71	G	87	W	103	g	119	W
40	(	56	8	72	H	88	X	104	h	120	X
41	)	57	9	73	I	89	Y	105	i	121	Y
42	*	58	:	74	J	90	Z	106	J	122	Z
43	+	59	;	75	K	91	[	107	K	123	{
44	,	60	<	76	L	92	\	108	l	124	|
45	-	61	=	77	M	93	]	109	m	125	}
46	.	62	>	78	N	94	^	110	N	126	~
47	/	63	?	79	O	95	_	111	o	127	Delete

All ASCII 127 codes and characters are allowable, with a few exceptions. Please try to avoid the ones highlighted in Orange.

Pro Tip: You'll notice that the first 31 are not used. These are control characters, like shift, return and line feed which are not characters you can use in text.

In order to process authentication, both devices (your VPN and this security server) need to communicate. They do this using the Radius protocol. Radius is a very popular standard for this form of communication.

There are two sides to this communication. You'll need to configure your device (Cisco VPN for example) to direct Radius traffic here and then you configure The SecurEnvoy SecurAccess Server to direct traffic back, essentially pointing the two devices to each other.





Once you click Update, your system is ready to receive Radius authentication requests from other devices within your network. If you have a requirement to configure advanced or specific settings related to the Radius configuration, you may click the Show Advanced Button.

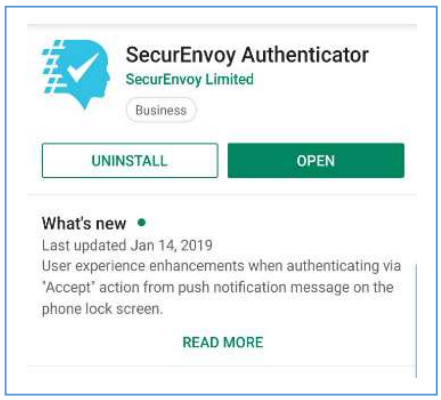
Pro Tip: Rules for Radius authentication are in the Advanced Settings. Trusted Networks, Blocked Networks, LDAP Group Based Authentication and advanced Radius Attribute configurations are located here.

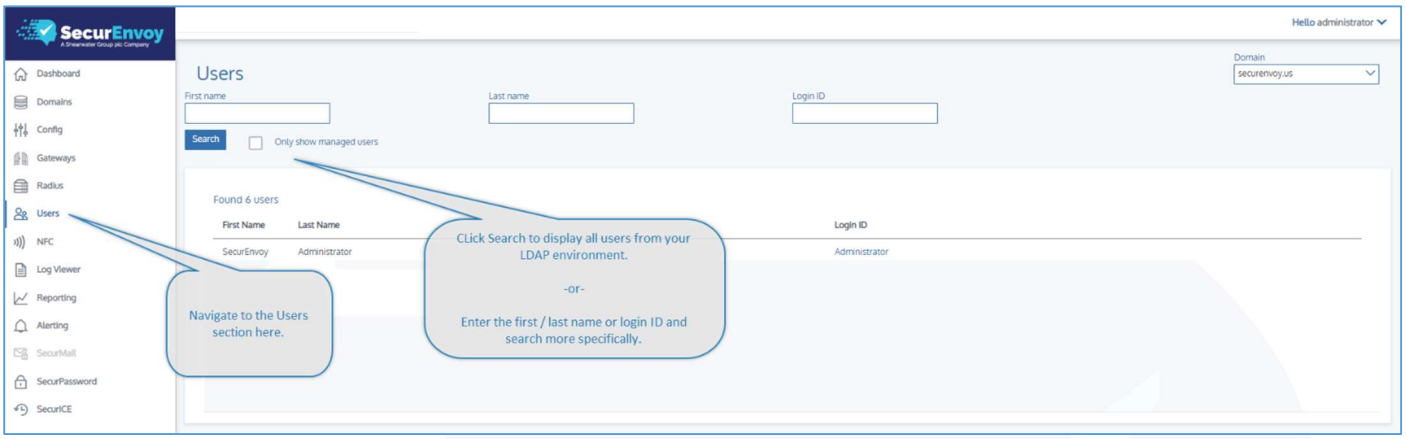
Registering Your First Device

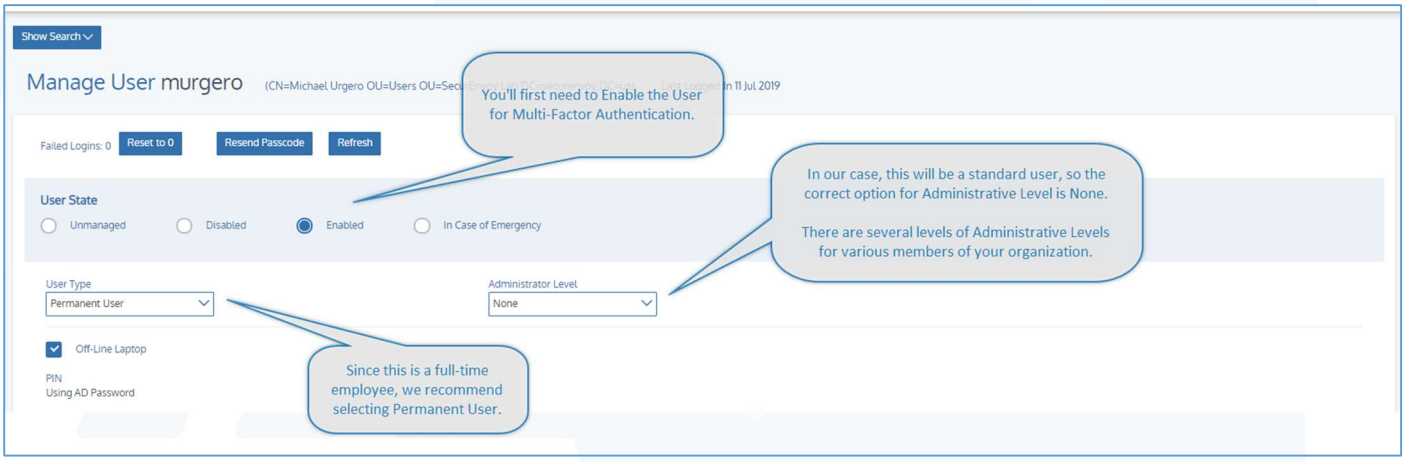
For users to have the ability to use features like push notifications and soft tokens, they'll need to download the SecurEnvoy Authenticator form the Android or Apple app store.

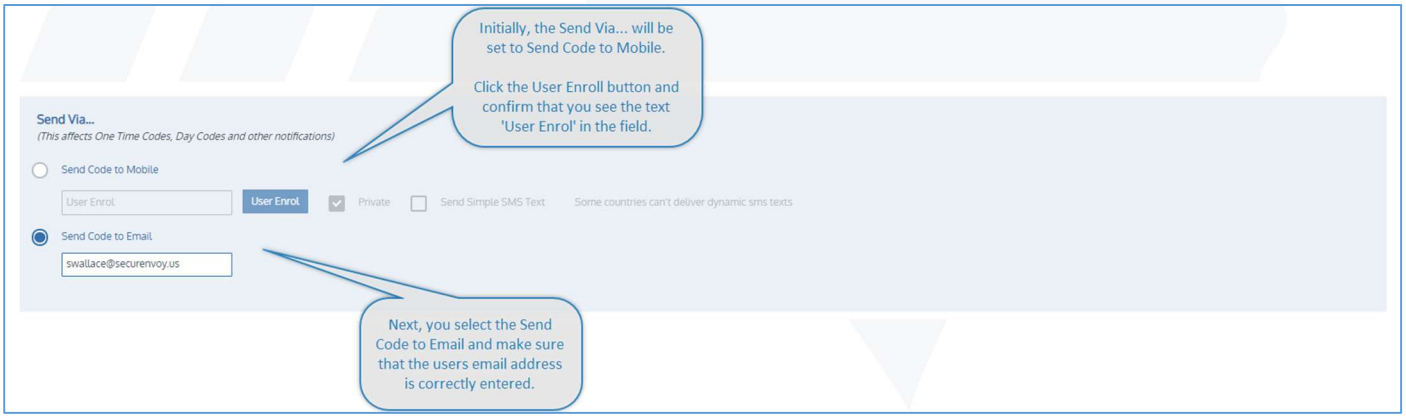
We update our SecurEnvoy Authenticator often. You'll receive notifications when there are updates available.

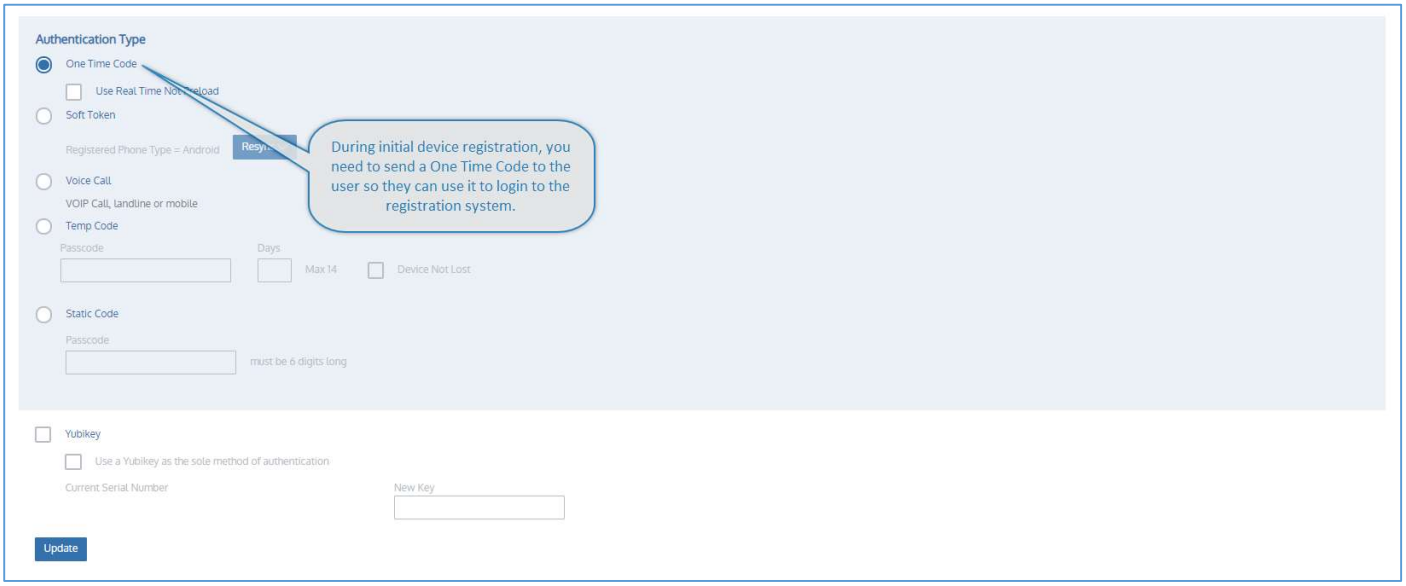
Once they have installed the app, you will need to configure their user account for use with SecurEnvoy SecurAccess.

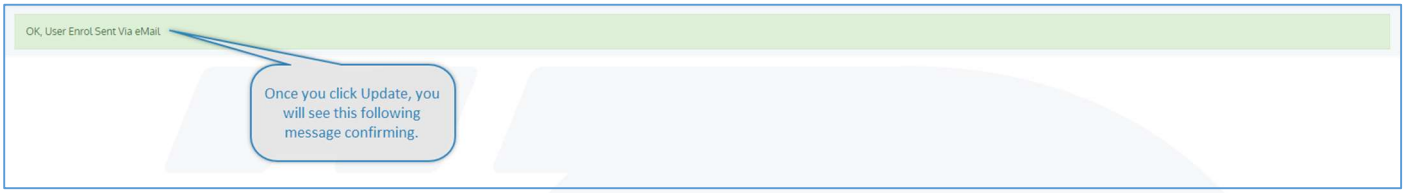












Once you click Update, the system will use the email configuration you specified earlier to deliver a message to the user. This email will contain two important components;

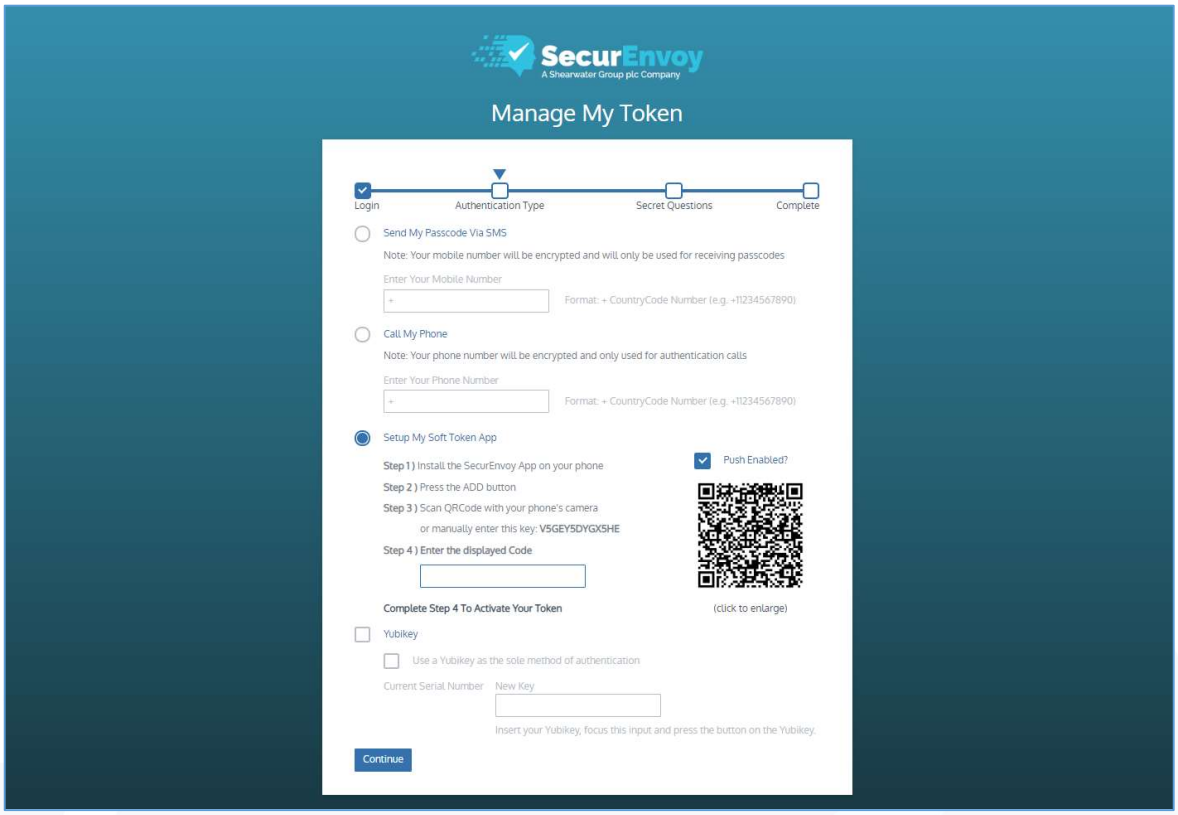
- The URL to the web site where user registers their device.
- The OTP that they'll need to get authenticated.





Once the user has authenticated, they are presented with options on how to receive and use Multi-Factor Tokens when they logon to solutions that are integrated with the system.

Note: The options presented here to users is directly related to the options made available by the system administrator. For additional details, please reference our administrators guide.

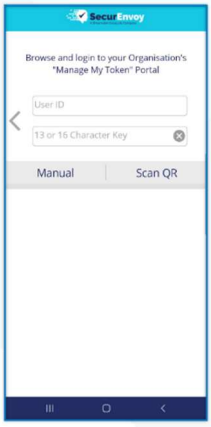


If the user is planning to use Push Authentication, the selecting this option will present them with a QR code for scanning and they should complete the following steps.

Step 1, Click the Add Icon



Step 2, Click Scan QR



Complete



Once your token is activated, you're ready to go. You will now need to configure your VPN, Citrix NetScaler, Check Point 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.

Upgrading Your Server

If a software version prior to version 9 is required to deliver a step upgrade, please contact support@securenvoy.com for access to previous software versions or download from our FTP site.

Prior to Upgrade

Before upgrading the SecurEnvoy Security Server software, please take a backup of the following item(s):

For 32 bit installations install C:\Program Files\SecurEnvoy\Security Server
For 64 bit installations install C:\Program Files(x86)\SecurEnvoy\Security Server

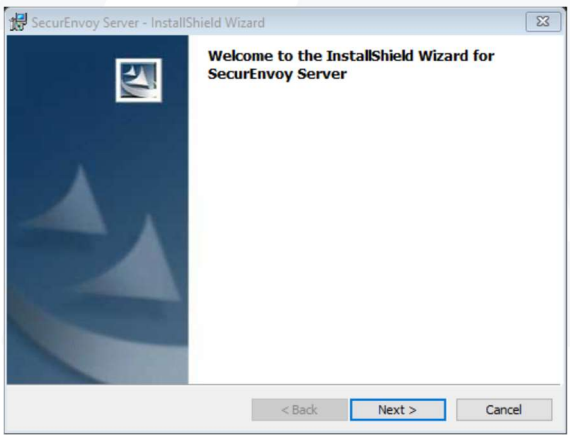
- config.db
- configpre54.db
- local.ini
- server.ini
- gateway.ini
- A full copy of the entire DATA directory
- Export the registry key HKLM\software\SecurEnvoy

Pro Tip: Please make sure that all SecurEnvoy Web Portals are closed in advance of the upgrade so that files which need to be replaced are not locked. A good method of doing this is to simply Stop IIS Web Services.

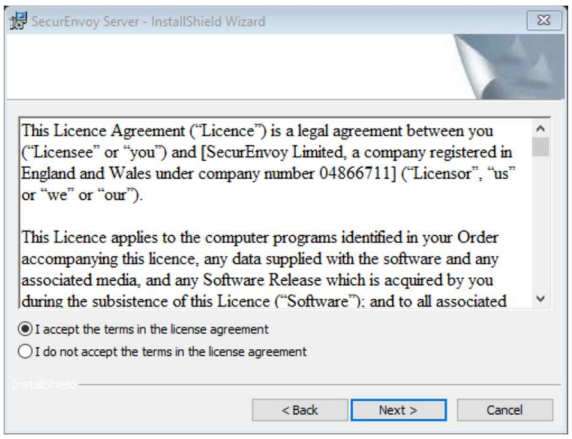
Upgrades performed are delivered directly over the existing installation.



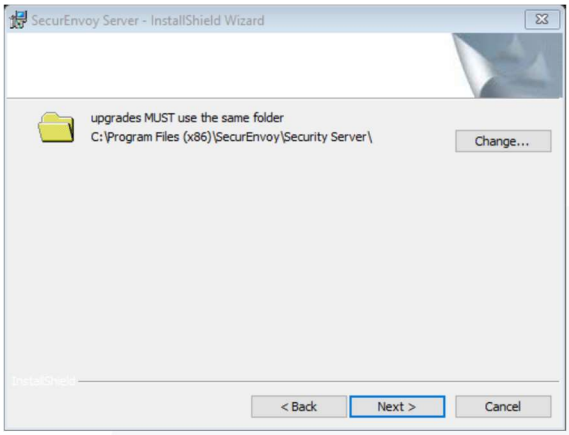
- Download the latest version of our software.
- Extract to the server.
- Run Setup.exe.
- Select Upgrade.



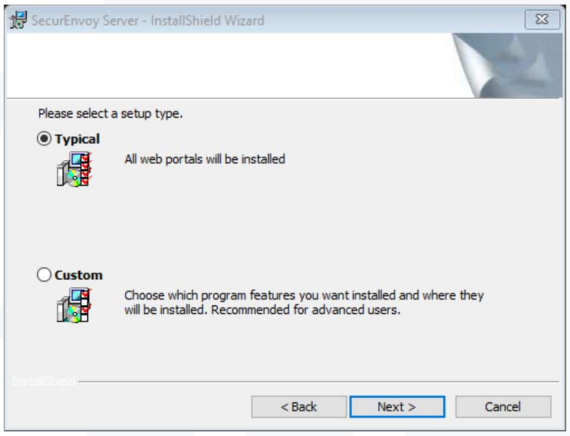
- Follow along with the on-screen prompts.



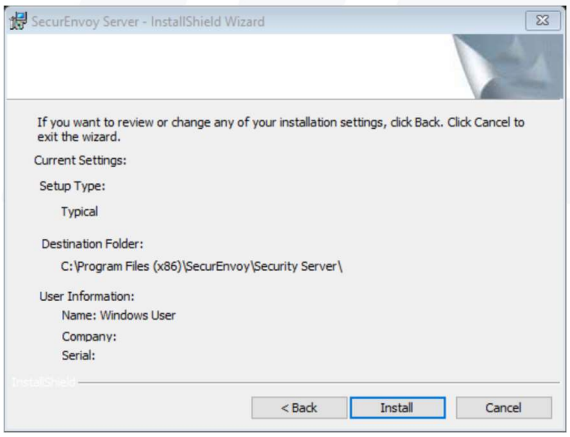
- Review and accept the licensing terms.



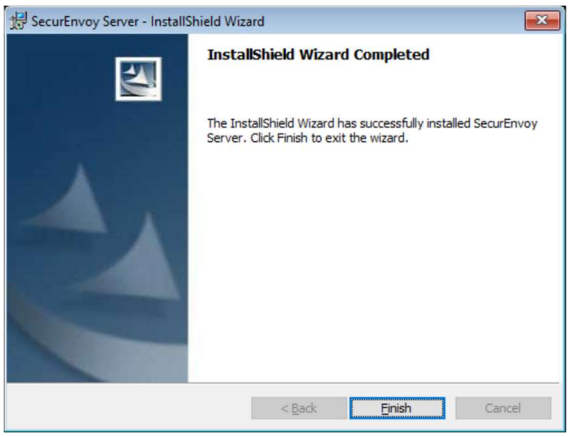
- The system installer will prompt for an install location.
- Because this is an upgrade, you need to assure that this location is the same as the original installation so files can be upgraded properly.



- Select Typical for most upgrades.
- Select Custom only if you had a custom installation previously.



- Once you click Install, the upgrade process will begin.



- When the upgrade has completed, click Finish.

Post Upgrade Tasks

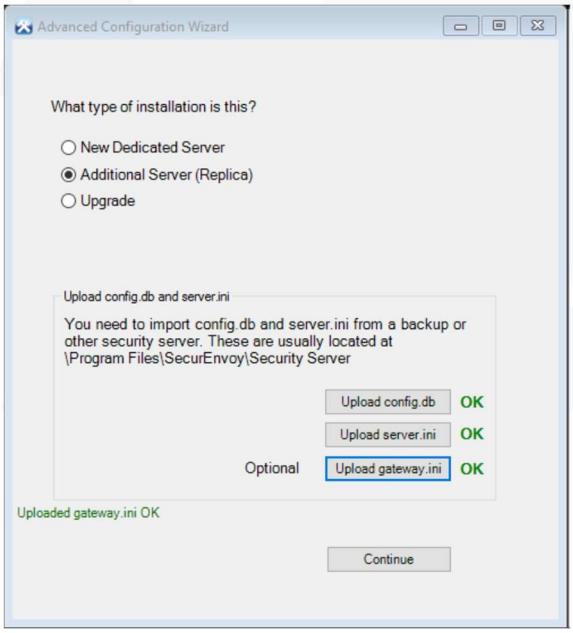
Once the upgrade has completed, you should launch the SecurEnvoy SecurAccess Admin Console. The Initial Setup Wizard will run, pre-populated with the settings from the previous installation. You have the option to change these settings or accept the existing ones as required.

Installing an Additional SecurEnvoy Server

Some organizations wish to have more than one SecurEnvoy Security Server for failover, load balancing and other redundancy. SecurEnvoy itself does not have any load balancing features integrated within it, so this process will require load balancing services from a load balancer, like a F5, Citrix NetScaler or other.

Understanding that the services within SecurEnvoy will be using an SSL Certificate, it will be important to assure that you have configured SSL Session Persistency on your load balancer so that communication between the user and this system works properly.

Adding a second server is performed in the exact same manner as a standard installation, with only one exception;



- Follow the previously described install steps, selecting Additional Server (Replica) as shown.

- Once you select Additional Server (Replic) you will be prompted for the following three files;
  - Config.db
  - Server.ini
  - Gateway.ini

These three files contain the working configuration for the first server you installed, but they do not contain everything.

- Radius Clients and settings.
- Custom templates.

Note: Additional Servers must use the same Service Account as the original.

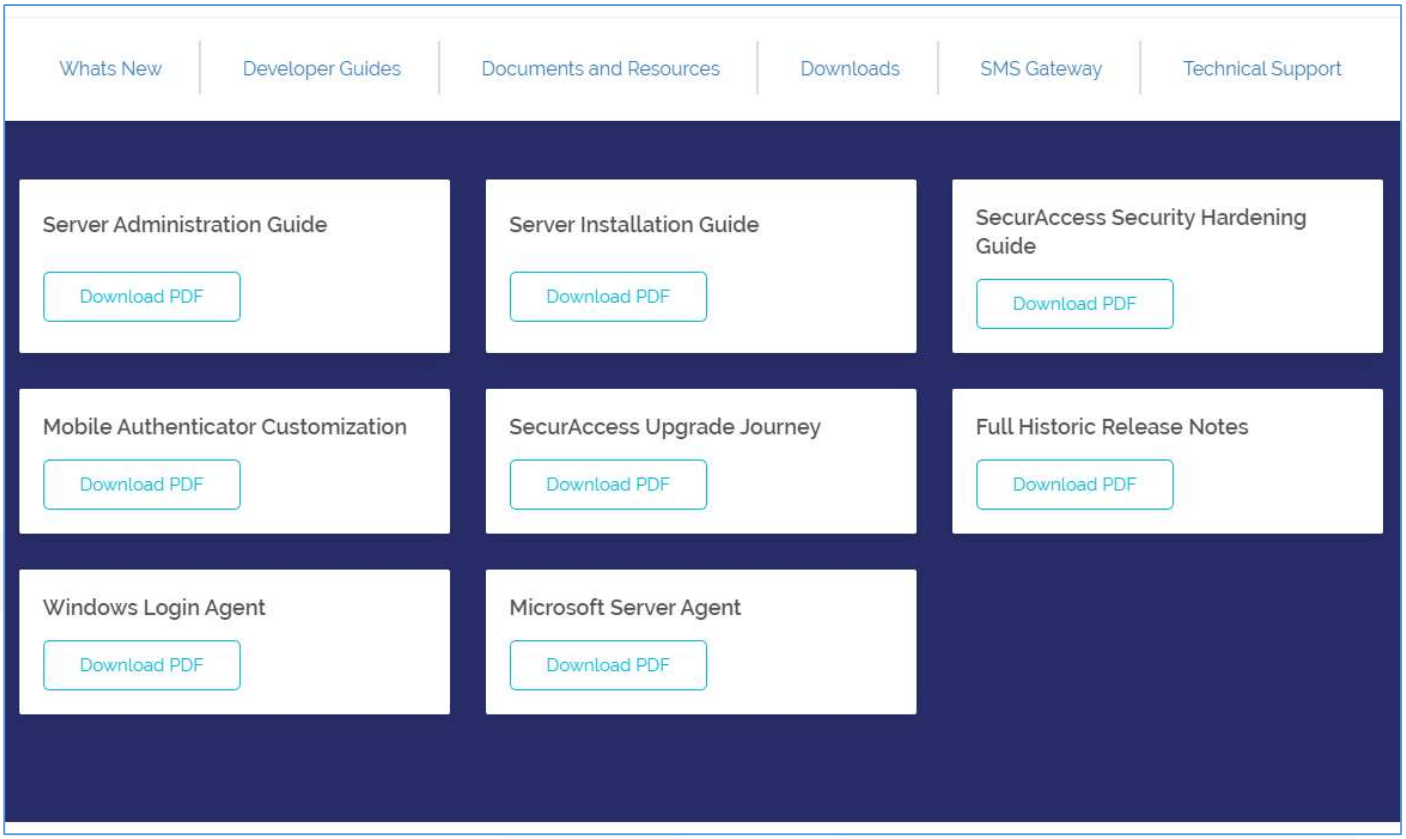
Support

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

https://www.securenvoy.com/en-us/contact-us

We have a global team of experts to assist you. You can send an email to info@securenvoy.com for an immediate response.

Our Web Site is also full of useful information, documents and how-to guides.



Appendix – Setting Service Account Permissions Manually

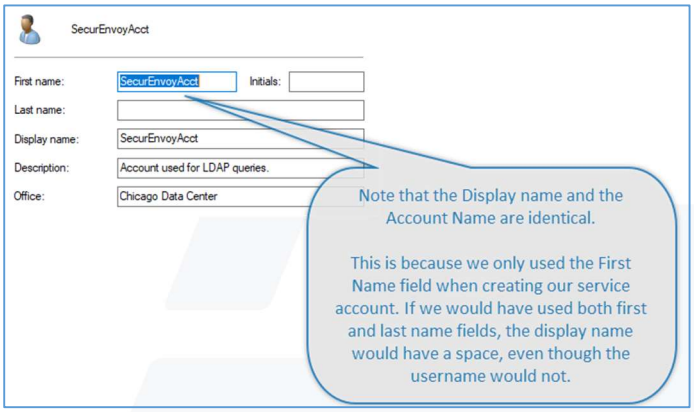
Some customers find that strict permissions on the Active Directory prevent the Service Account Wizard from assigning permissions to the SecurEnvoy Service Account properly or at all.

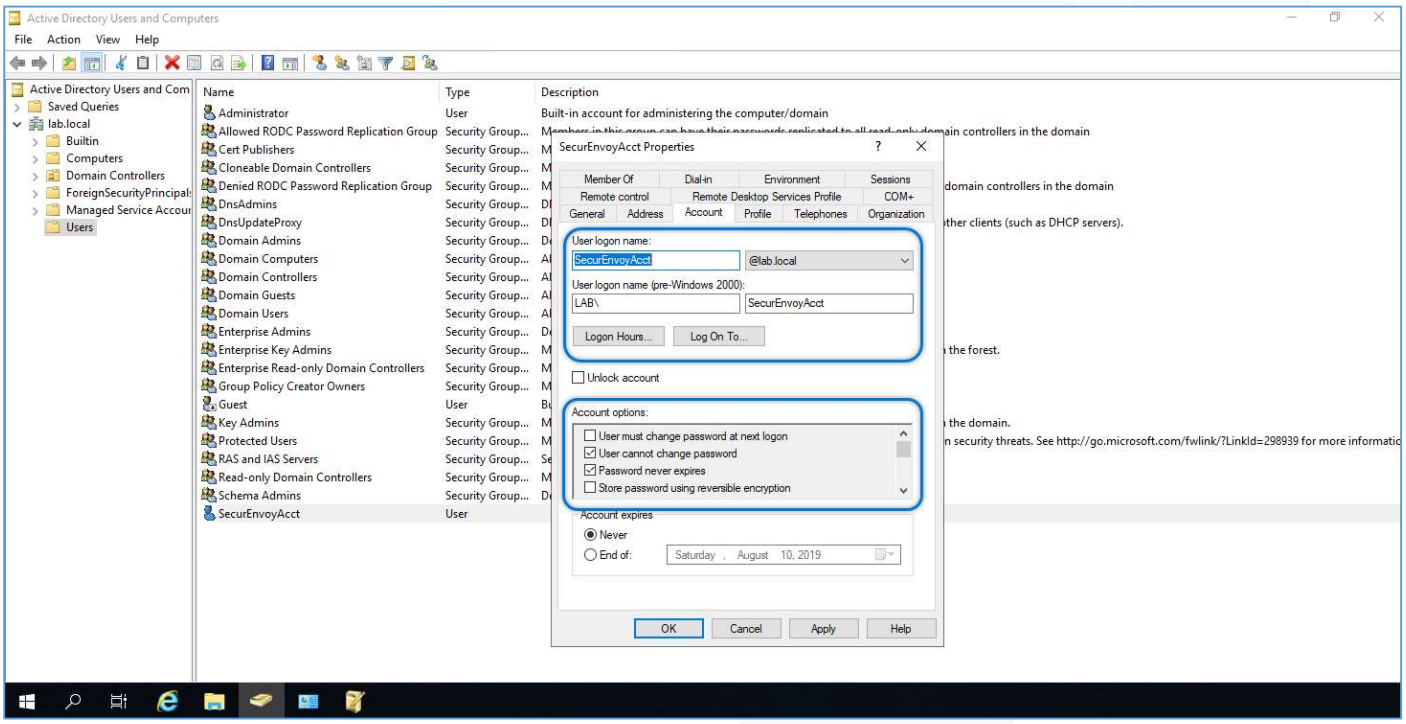
If this happens, you have two choices;

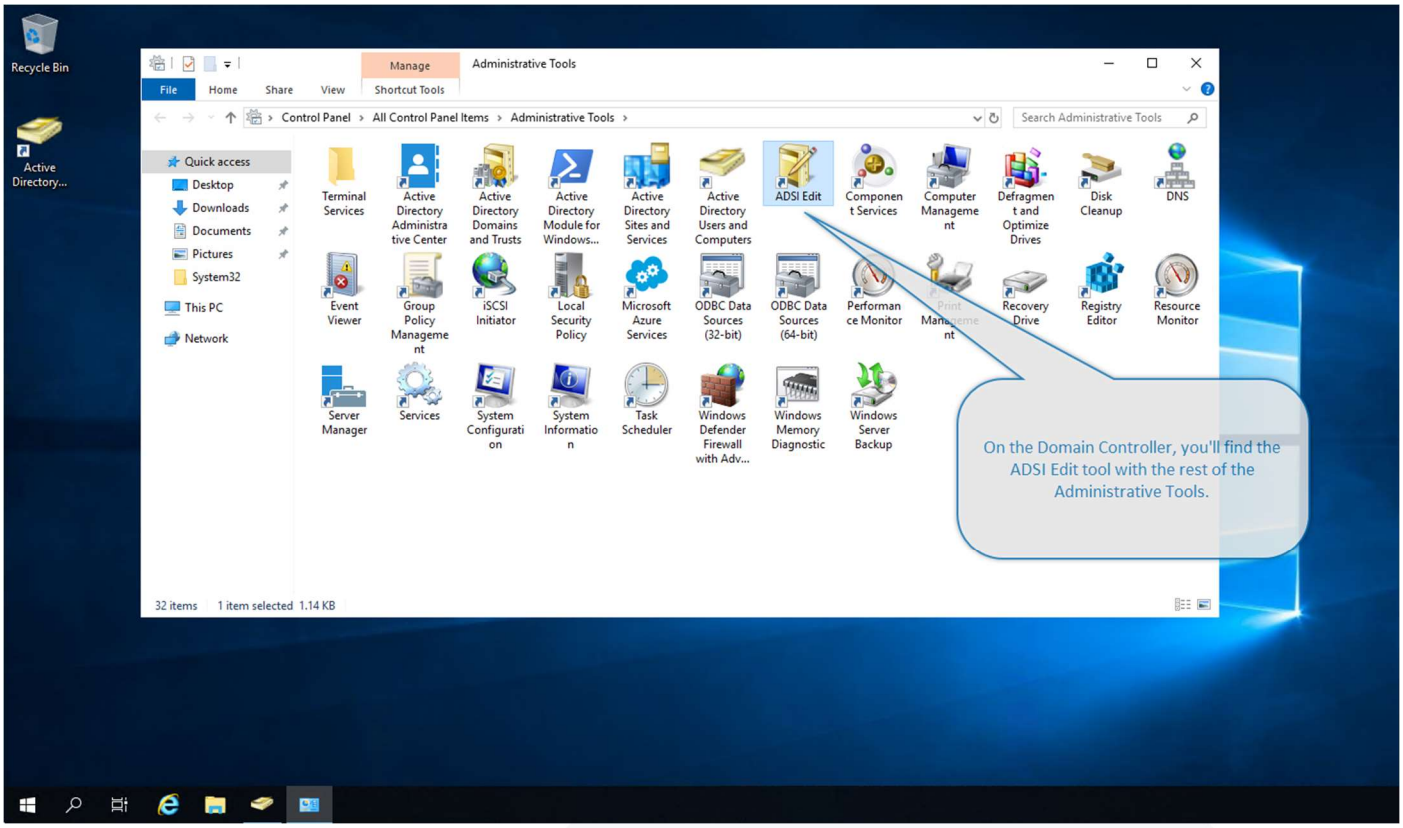
- Set the Service Account as a Domain Administrator
- Set the Permissions Manually using ADSI Edit

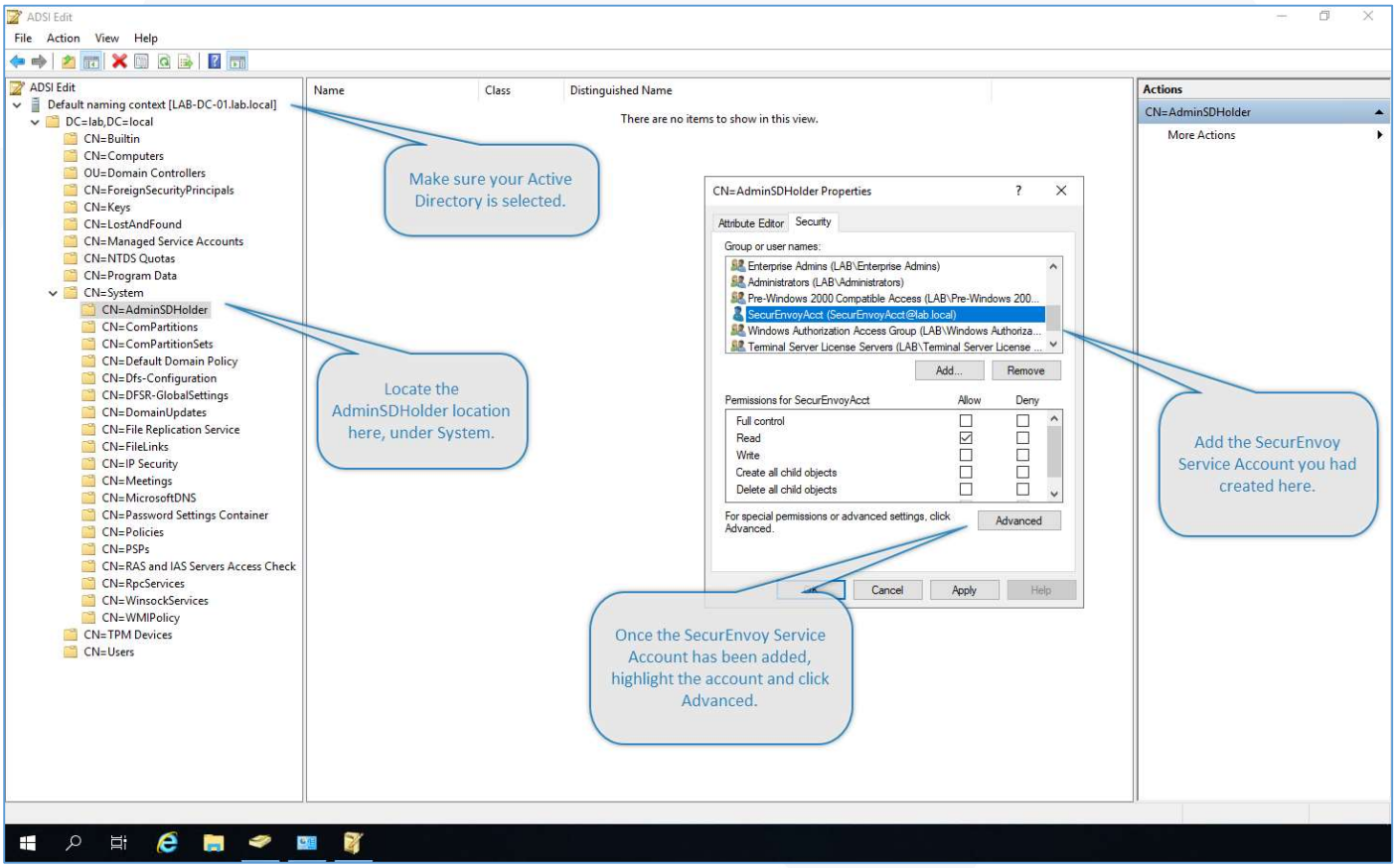
Note: We don't recommend giving the Service Account Domain Administrator permissions for a production environment.

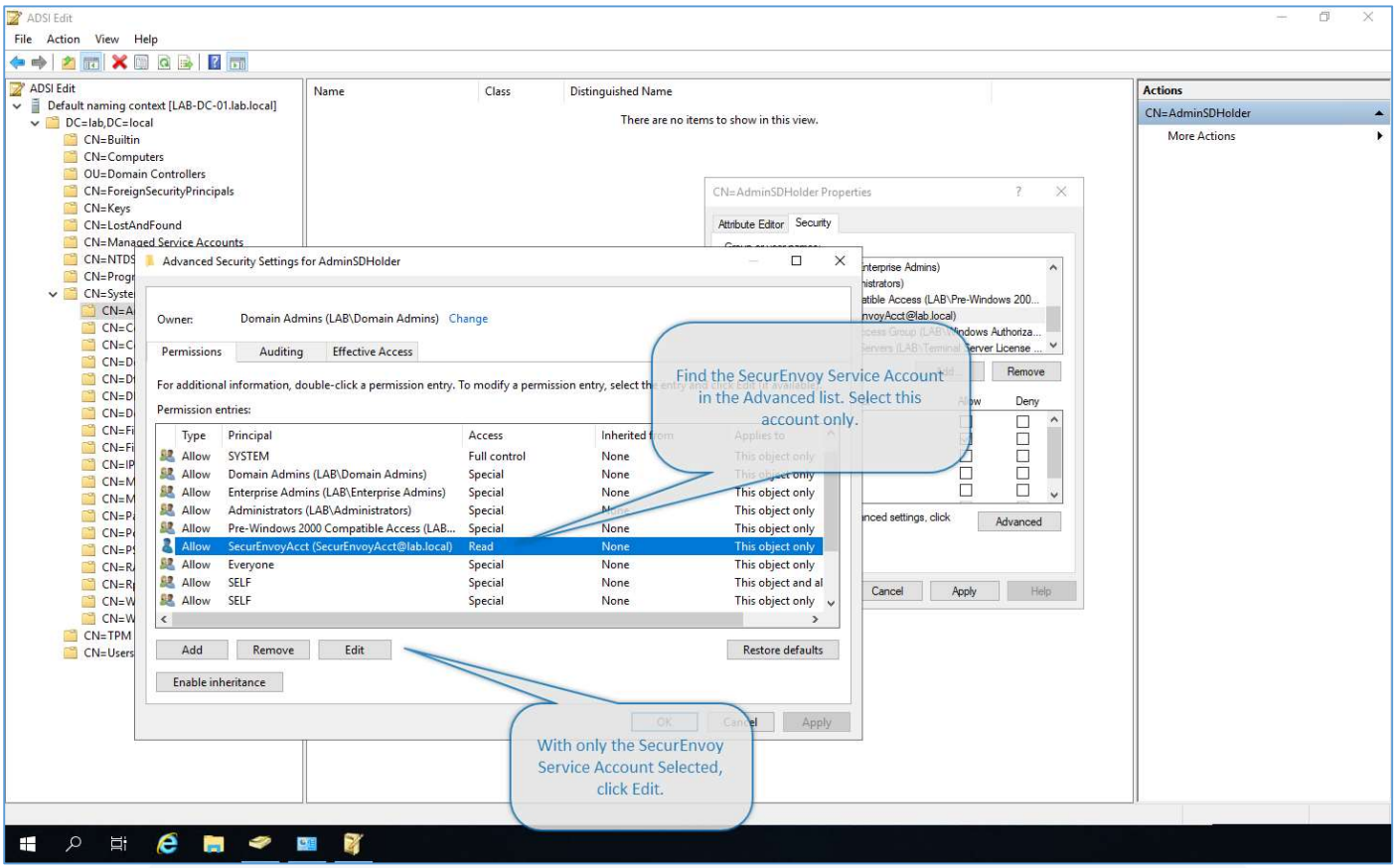
Pro Tip: When creating your service account, it's recommended that you take note of the Display Name, which can be different than the actual account name. This can become important when referencing the account's DN.






Recycle Bin
Active Directory...
Administrative Tools
Control Panel › All Control Panel Items › Administrative Tools ›
Search Administrative Tools
Quick access
Desktop
Downloads
Documents
Pictures
System32
This PC
Network
Terminal Services
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows...
Active Directory Sites and Services
Active Directory Users and Computers
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Recovery Drive
Registry Editor
Resource Monitor
Server Manager
Services
System Configuration
System Information
Task Scheduler
Windows Defender Firewall with Adv...
Windows Memory Diagnostic
Windows Server Backup
32 items
1 item selected 1.14 KB
On the Domain Controller, you'll find the ADSI Edit tool with the rest of the Administrative Tools.

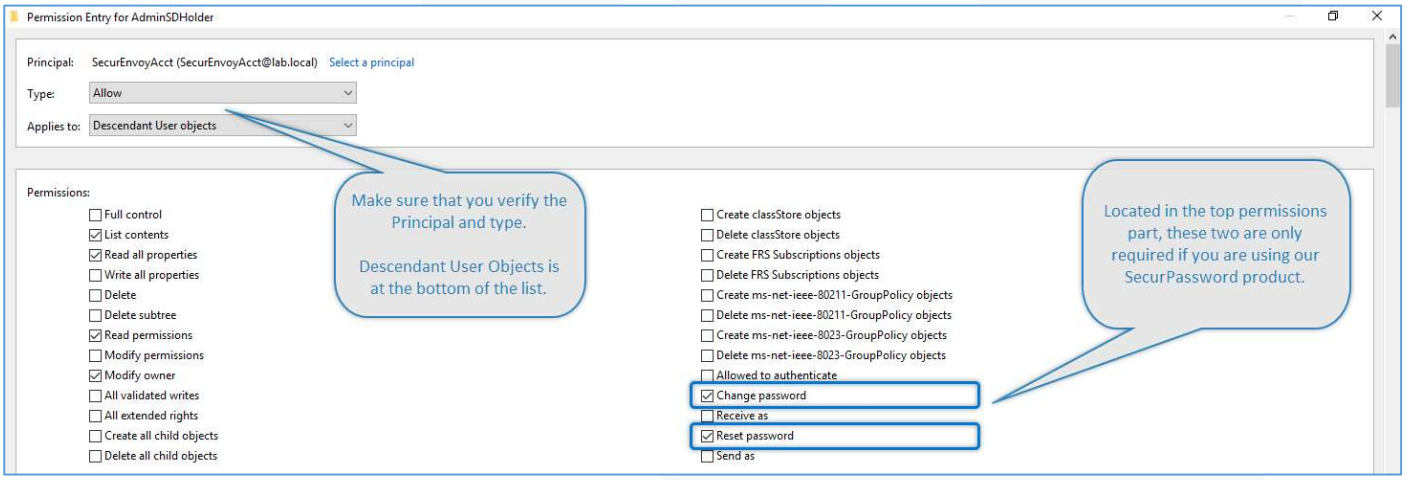

ADSI Edit
File Action View Help
ADSI Edit
Default naming context [LAB-DC-01.lab.local]
DC=lab,DC=local
CN=Builtin
CN=Computers
OU=Domain Controllers
CN=ForeignSecurityPrincipals
CN=Keys
CN=LostAndFound
CN=Managed Service Accounts
CN=NTDS Quotas
CN=Program Data
CN=System
CN=AdminSDHolder
CN=ComPartitions
CN=ComPartitionSets
CN=Default Domain Policy
CN=Dfs-Configuration
CN=DFSR-GlobalSettings
CN=DomainUpdates
CN=File Replication Service
CN=FileLinks
CN=IP Security
CN=Meetings
CN=MicrosoftDNS
CN=Password Settings Container
CN=Policies
CN=PSPs
CN=RAS and IAS Servers Access Check
CN=RpcServices
CN=WinsockServices
CN=WMIPolicy
CN=TPM Devices
CN=Users
Name
Class
Distinguished Name
There are no items to show in this view.
Actions
CN=AdminSDHolder
More Actions
Make sure your Active Directory is selected.
Locate the AdminSDHolder location here, under System.
CN=AdminSDHolder Properties
Attribute Editor
Security
Group or user names:
Enterprise Admins (LAB\Enterprise Admins)
Administrators (LAB\Administrators)
Pre-Windows 2000 Compatible Access (LAB\Pre-Windows 200...
SecurEnvoyAcct (SecurEnvoyAcct@lab.local)
Windows Authorization Access Group (LAB\Windows Authoriza...
Terminal Server License Servers (LAB\Terminal Server License ...
Add...
Remove
Permissions for SecurEnvoyAcct
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
Add the SecurEnvoy Service Account you had created here.
Once the SecurEnvoy Service Account has been added, highlight the account and click Advanced.



Once you click Edit above, you will be presented with a very detailed list of account permissions for the SecurEnvoy Service Account that you've created in the Microsoft Active Directory.

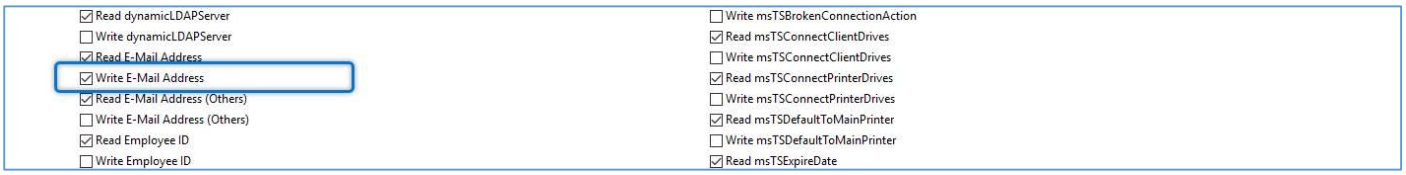
Please follow along, very specifically and exercise care to assure you are only assigning permissions required. Assigning additional or incorrect permissions may result in unusual behaviour.

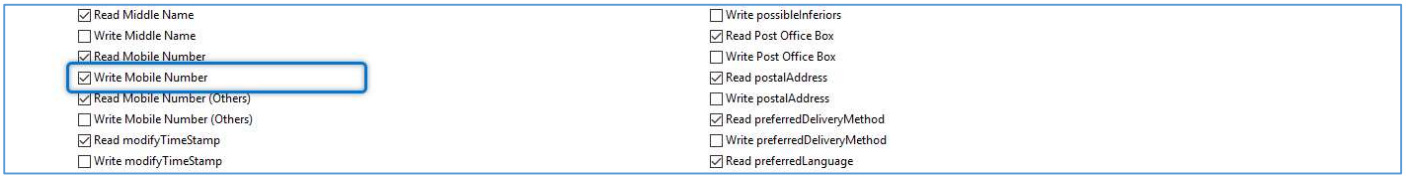
It's important to know that the following screens are large and at times and lists of permissions can be long, we may only be showing a specific part of the screen.

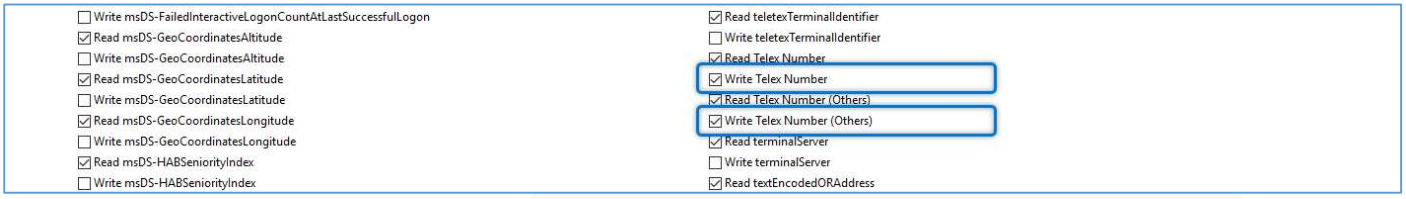


The large security permissions list is alphabetical. Here, we are showing the following specific permissions that are required.

- Allow Write E-Mail Addresses
- Allow Write Telex Number
- Allow Write Telex Number (Other)
- Allow Write Mobile Number







Note: If you have more than one SecurEnvoy SecurAccess Security Servers in your environment, they need to use the same service account to share the permissions you've set here.

Pro Tip: Once the security permissions have been applied, you can test in the SecurEnvoy Administration GUI, by looking up a user and entering a mobile number in the mobile number field.

When Successful, you'll receive a message; OK. Passcode Sent to Gateway. If you receive an error message, return here and validate your settings.

Appendix – TCP / UDP Communications / Firewall Ports

Below are all the necessary and optional port configurations for the SecurEnvoy SecurAccess Security Server. You should follow these guidelines when implementing a production system in a highly secure network.

Requirement	Description	TCP/UDP Port	Direction
User Authentication	RADIUS Client Communication (i.e FW, RAS or Application Server with SecurEnvoy Server Agent installed)	UDP/1812	Inbound to SecurAccess Server
LDAP User Lookup	Communication between SecurAccess and LDAP/AD servers	(LDAP) TCP/389 or LDAPS TCP/636	Inbound to LDAP Server from SecurAccess
Syslog	Syslog's pushed to SIEM or Log Collector Solution	UDP/514	Inbound to SIEM Server from SecurAccess
Replication	Replication connection between one or more SecurAccess Servers	TCP/443	Bidirectional
Email Enrolments	SMTP connection to mail relay server	TCP/25	Inbound to SMTP Mail Server
SMS Enrollments and tokens	HTTP connection to public SMS Gateways	TCP/443	Outbound HTTP Access to Public SMS Services
SecurAccess Portals	Client connectivity to Enrol Tokens, Change Passwords or Helpdesk	TCP/443	Inbound to SecurAccess Server
Push Authentication (Outbound)	Push Authentication to Mobile Tokens	TCP/443 Apple = TCP/2195	Outbound to gcm-http.googleapis.com Outbound to gateway.push.apple.com Outbound to a.notify.live.net
Push Authentication (Inbound)	Push Authentication Acceptance from Mobile	TCP/443	Inbound to SecurAccess SECENROL portal (Requires publishing to public Internet via Reverse Proxy)
Push (Apple Certificate)	Required to update apple.p12 cert on a yearly basis	TCP/443	Outbound to www.securenvoy.com

Please Reach Out to Your Local SecurEnvoy Team...



UK & IRELAND

Belvedere House, Basing View
Basingstoke, Hampshire
RG21 4HG, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012



EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522



ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778



USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211



USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211



USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com