# Secret Server – Training and Lab Guide

Product Version: 10.6.000026

Guide Version: 2.2

Internationaltraining@thycotic.com

www.thycotic.com

# Contents

# Before You Begin

## Purpose:

This training and lab guide is designed to accompany a Thycotic trainer lead course. During your training course the trainer will regularly reference this guide as well as demonstrating lab exercises within a shared desktop environment and discussing common use cases and real-world scenarios.

## Your training pack

Before you start this training course, ensure you have received lab details from your Thycotic trainer.

The Secret Server lab consists of the following machines:

| Machine Name | Internal lab hostname | Internal IP | Description |
|---|---|---|---|
| DC1 | DC1 | 172.31.32.10 | Domain controller – contains all active directory configuration used within the lab |
| SS | SecretServer1 | 172.31.40.114 | This machine will be used to install and host Secret Server |
| WIN | Client01 | 172.31.46.76 | Windows server, used to test a range of Secret Server functionality during the training course |
| CENTOS | | 172.31.38.35 | Centos machine – used to test a range of Secret Server functionality during the training |

You will need to initiate a remote desktop connection to the ***PUBLIC*** IP address of the Win machine. This IP address is dynamic and will change whenever the lab environment is restarted. The Win server machine serves as a jump box from which you can then RDP to the other windows machines by hostname. Lab Exercise 1 explains the process of identifying the IP address of your lab jump box and connecting to it.

The administrative credentials you will need to log into the lab machines:

**Windows Domain Admin Account**
Username: **thylab\adm-training**
Password: **Thycotic@2019!**

**Centos SSH Account**
Username: thycotic
Password thycotest12$$

## Introduction

# Module 1 - Installing Secret Server

In this module we will cover

## 1.1 Secret server components

At a high level, Secret Server consists of two components.

- Front end ASP.NET web application
- Back end SQL database

## 1.2 Pre-Requisites

### Minimum Requirements - Basic Deployments

| Web Server | Database Server |
|---|---|
| 2 CPU Cores | 2 CPU Cores |
| 4 GB RAM | 4 GB RAM |
| 25 GB Disk Space | 50 GB Disk Space |
| Windows Server 2008 R2 SP1 or newer | Windows Server 2008 R2 SP1 or newer |
| IIS 7 or newer | SQL Server 2012 or newer |
| .NET 4.5.1 or newer | |

Note: SQL Express is supported but not recommended for production environments

### Recommended Requirements - Basic Deployments

Environments budgeting for over 10,000 Secrets require a scoping call with a Thycotic engineer

| Web Server | Database Server |
|---|---|
| 4 CPU Cores | 4 CPU Cores |
| 16 GB RAM | 16 GB RAM |
| 25 GB Disk Space | 100+ GB Disk Space |
| Windows Server 2012 or newer | Windows Server 2012 or newer |
| IIS 7 or newer | SQL Server 2012 or newer |
| .NET 4.6.1 or newer | |

**Important Note – For advanced deployments where discovery, session recording or increased numbers of distributed engines are being used, please see feature specific knowledge base guides for detailed requirements.**

### 1.3 Ports used by Secret Server

The table below identifies ports and port ranges that may be required by Secret Server

| Process | Type of Traffic | Port Number |
|---|---|---|
| **Active Directory Sync** | LDAPS<br>LDAP<br>Kerberos<br>NTLM | 636<br>389<br>88<br>445 |
| **Discovery** | RPC Dynamic Port Range*<br>Microsoft DS<br>Epmap<br>SSH | 49152-65535<br>445<br>135<br>22 |
| **Remote Password Changing** | RPC Dynamic Port Range*<br>SSH<br>Telnet<br>MS SQL<br>NTLM<br>LDAP<br>LDAPS<br>Sybase<br>Oracle<br>Kerberos | 49152-65535<br>22<br>23<br>1433<br>445<br>389<br>636<br>5000<br>1521<br>464 |
| **Ports Incoming to Webserver** | HTTP<br>HTTPS | 80<br>443 |
| **Ports Incoming to Database Server** | SQL Connection TCP and UDP | 1433 |
| **Email** | SMTP | 25 |
| **RADIUS Server** | RADIUS | 1812 |

The RPC Dynamic Port ranges are a range of ports utilized by Microsoft's Remote Procedure Call (RPC) functionality. This port range varies by operating system. For Windows Server 2008 or greater, this port range is 49152 to 65535 and this entire port range must be open for RPC technology to work. The RPC range is needed to perform Remote Password Changing since Secret Server will need to connect to the computer using DCOM protocol.

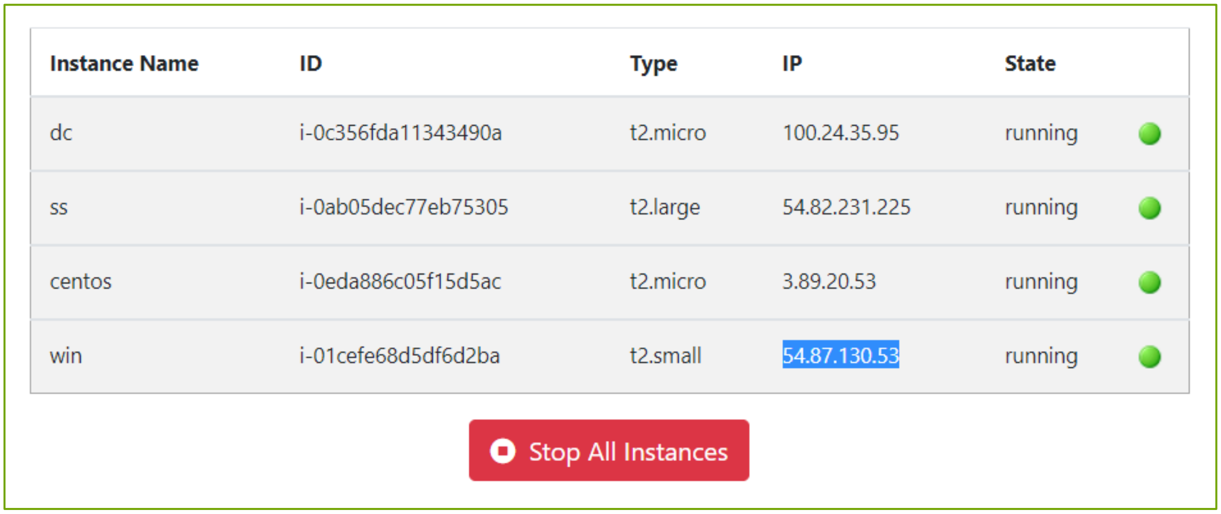
To see your ipv4 dynamic range on a given machine, type **netsh int ipv4 show dynamicport tcp** in the commandline.

To specify a specific port on your environment that Secret Server will communicate to, you can also enable WMI ports on Windows client machines

## Lab Exercise 1 – Connecting to the lab environment

In this exercise will access the Thycotic training lab environment.

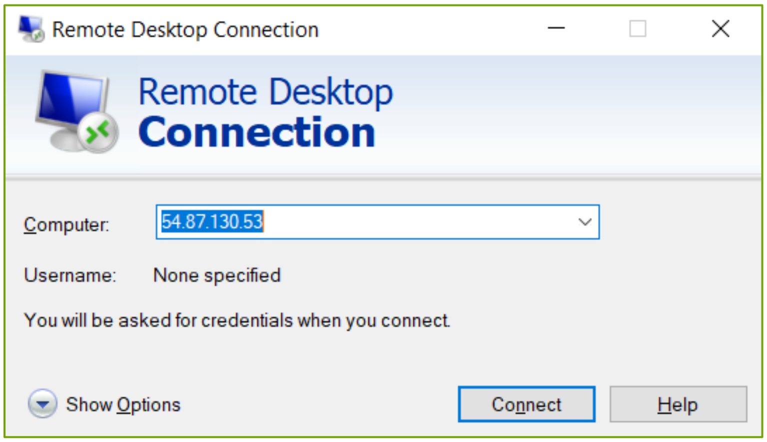
1. Navigate to the URL of the training lab environment provided by the Thycotic training team.
2. Click the power on instances button, the virtual machines within the lab environment will now be powered on. They should be available in one to two minutes
3. Select and copy in the IP address of the **win** machine as in the image below:



| Instance Name | ID | Type | IP | State | |
|---|---|---|---|---|---|
| dc | i-0c356fda11343490a | t2.micro | 100.24.35.95 | running | ● |
| ss | i-0ab05dec77eb75305 | t2.large | 54.82.231.225 | running | ● |
| centos | i-0eda886c05f15d5ac | t2.micro | 3.89.20.53 | running | ● |
| win | i-01cefe68d5df6d2ba | t2.small | 54.87.130.53 | running | ● |

Note: this IP address is dynamic and will change every time the lab environment is stopped and restarted.

4. From the start menu on your host machine, type **remote desktop connection** and open the matching application
5. In the remote desktop connection dialogue, past the IP address and click **connect**



Remote Desktop Connection

Remote Desktop **Connection**

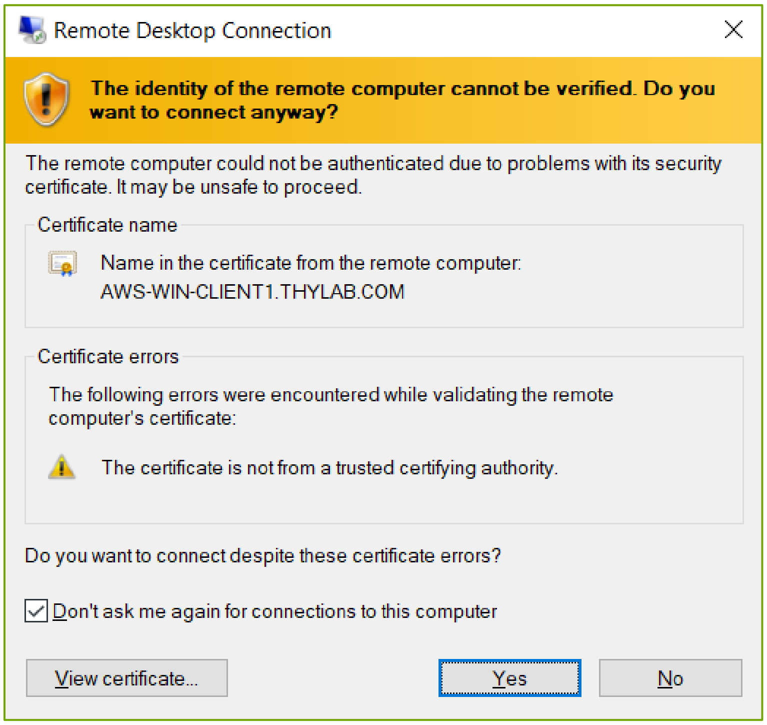
Computer: 54.87.130.53

Username: None specified

You will be asked for credentials when you connect.

6. When prompted with the windows security credentials dialogue, select **More Choices** then **Use a different account**

7. Use the following credentials to connect, username: **thylab\adm-training** / password: **Thycotic@2019!**
8. If prompted with the following certificate warning, select **don't ask me again** and click **Yes**



**The identity of the remote computer cannot be verified. Do you want to connect anyway?**

The remote computer could not be authenticated due to problems with its security certificate. It may be unsafe to proceed.

Certificate name

Name in the certificate from the remote computer:
AWS-WIN-CLIENT1.THYLAB.COM

Certificate errors

The following errors were encountered while validating the remote computer's certificate:

The certificate is not from a trusted certifying authority.

Do you want to connect despite these certificate errors?

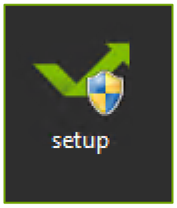
☑ Don't ask me again for connections to this computer

9. A remote desktop connection should now be initialized into the Thycotic training lab environment. From this machine you can now remote on to the other windows machines within the lab environment.

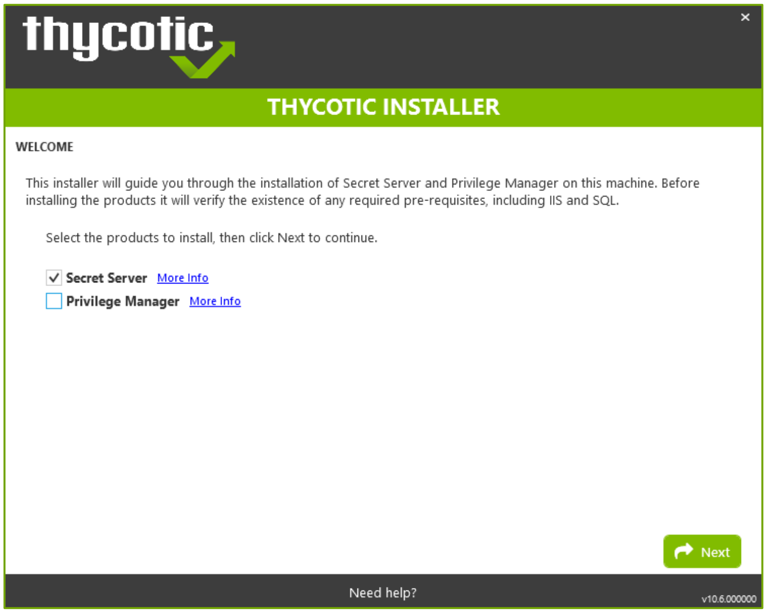
## Lab Exercise 2 – Installing Secret Server

In this exercise will power on and connect to the training lab environment before running through a complete installation of secret server.

1. In Lab exercise one we connected to the windows server that acts as a jump host. Initiate a remote desktop connection to **SECRETSERVER1** using the same credentials from lab 1 (thylab\adm-training / Thycotic@2019!)
2. On the desktop of the secretserver1 machine you will see the secret server installer executable:



3. Run the setup file, when prompted with a windows User Account Control (UAC) dialogue click **Yes**
4. The installer can install both Secret Server and Privilege Manager (Thycotic endpoint least privilege solution). In this case we only want to install Secret Server so uncheck the Privilege Manager radio button as in the image below:



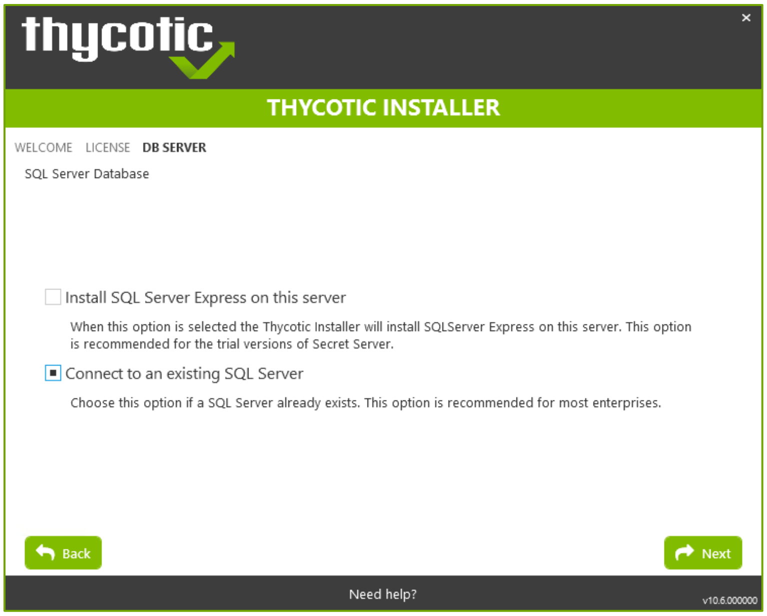
WELCOME

This installer will guide you through the installation of Secret Server and Privilege Manager on this machine. Before installing the products it will verify the existence of any required pre-requisites, including IIS and SQL.

Select the products to install, then click Next to continue.

☑ Secret Server More Info
□ Privilege Manager More Info

5. Click **Next**
6. Read and accept the license agreement
7. On the SQL Server Database screen we can either install SQL server express or connect to an existing database. In the lab environment SQL Express is already installed so select **Connect to an existing SQL server** then click **Next**



SQL Server Database

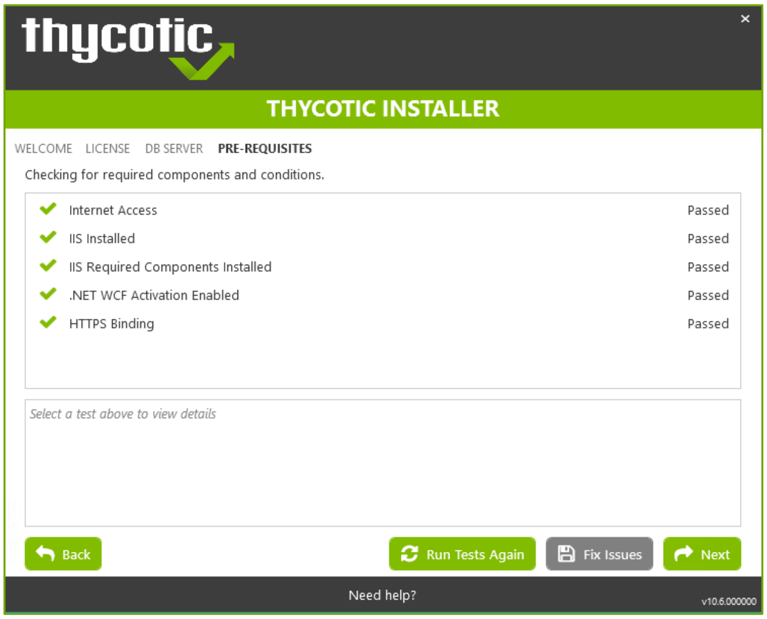
□ Install SQL Server Express on this server

When this option is selected the Thycotic Installer will install SQLServer Express on this server. This option is recommended for the trial versions of Secret Server.

▣ Connect to an existing SQL Server

Choose this option if a SQL Server already exists. This option is recommended for most enterprises.

8. The installer will now perform a range of checks to ensure pre-requisites are in place. In the lab environment all requirements should be in place, click **Next**

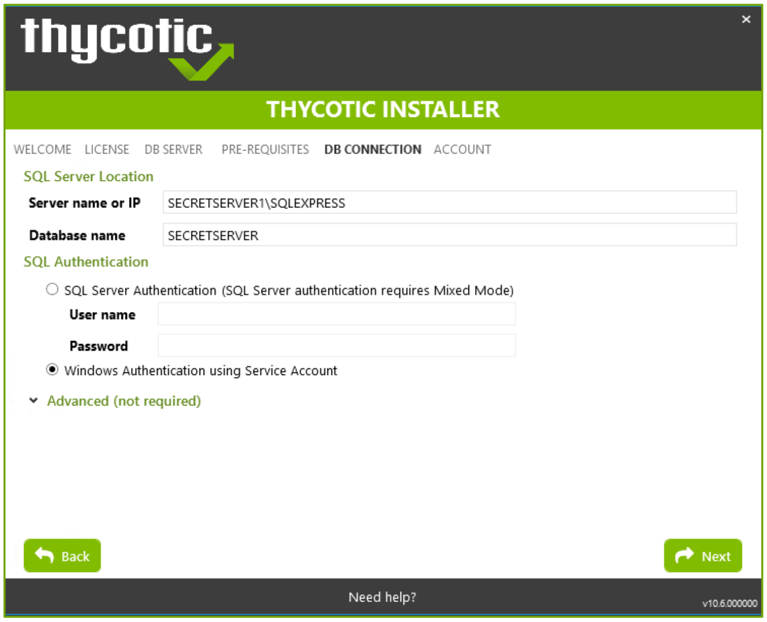


Checking for required components and conditions.

| | |
|---|---|
| ✓ Internet Access | Passed |
| ✓ IIS Installed | Passed |
| ✓ IIS Required Components Installed | Passed |
| ✓ .NET WCF Activation Enabled | Passed |
| ✓ HTTPS Binding | Passed |

*Select a test above to view details*

9. On the next screen we need to configure the database connection. As the SQL server is installed on the same machine, in the Server name or IP field enter: **secretserver1\SQLEXPRESS** in the database name field, enter: **secretserver**
10. On the same screen we now need to configure the authentication option that will be used to connect to the database. Although we can use SQL authentication or Windows authentication here, Thycotic recommend using Windows authentication. Select the **Windows Authentication using service account** radio button and click **Next**



SQL Server Location

Server name or IP: SECRETSERVER1\SQLEXPRESS

Database name: SECRETSERVER

SQL Authentication

○ SQL Server Authentication (SQL Server authentication requires Mixed Mode)

User name:

Password:

● Windows Authentication using Service Account

11. On the next screen we will be asked to configure the service account that will be used to connect to the SQL database and used to run the IIS application pools. Enter the following credentials:

username: **thylab\svc_secretserver**

password: **Thycotic@2019!**

12. To ensure the credentials are correct, click **Validate Credentials**, if they are you should see the word **success**. If not, check the credentials for any errors. Click **Next**
13. On the next screen we need to create our initial Secret Server user. At this point you can create your own user or use the following information to create the initial user:

Username: ss_admin

Display name: ss_admin

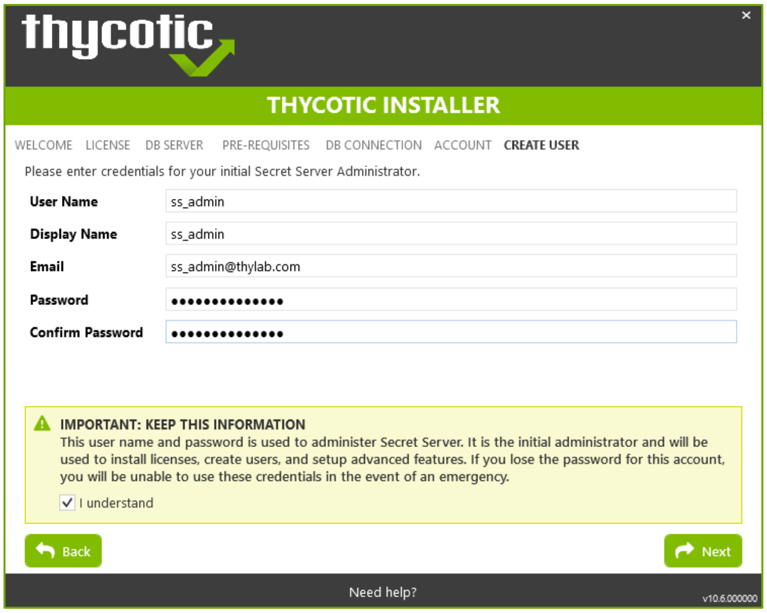
Email: ss_admin@thylab.com

Password: Thycotic@2019!

Confirm Password Thycotic@2019!

**Note: If you create your own user account at this point, ensure you remember the username and password. This account is used for the initial administration of Secret Server.**

14. Confirm you understand the importance of not loosing these credentials and click **Next**


thycotic
THYCOTIC INSTALLER
WELCOME LICENSE DB SERVER PRE-REQUISITES DB CONNECTION ACCOUNT CREATE USER
Back
Next
Need help?
v10.6.000000

Please enter credentials for your initial Secret Server Administrator.

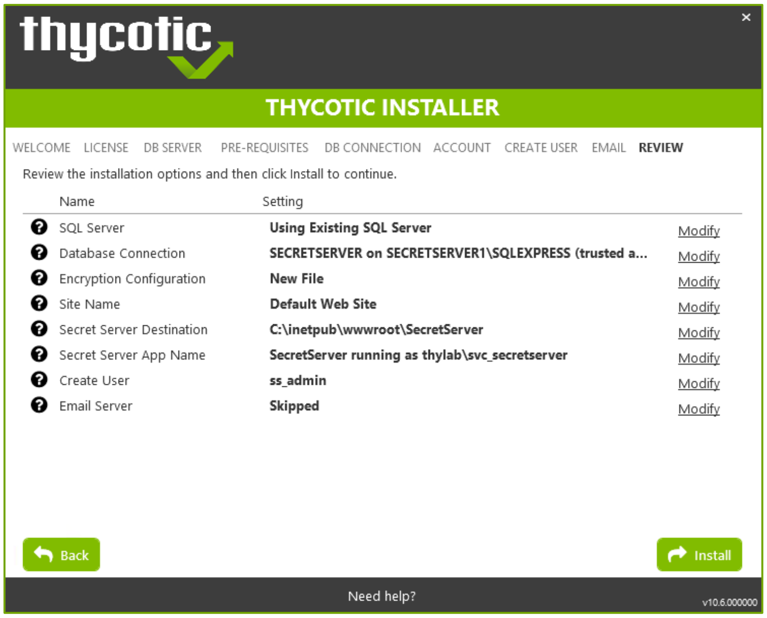
| | |
|---|---|
| User Name | ss_admin |
| Display Name | ss_admin |
| Email | ss_admin@thylab.com |
| Password | •••••••••••••• |
| Confirm Password | •••••••••••••• |

IMPORTANT: KEEP THIS INFORMATION
This user name and password is used to administer Secret Server. It is the initial administrator and will be used to install licenses, create users, and setup advanced features. If you lose the password for this account, you will be unable to use these credentials in the event of an emergency.

☑ I understand

15. On the next screen, options to configure an SMTP mail server are available. This feature will not be used during the training so click Skip Email
16. Click **Next**

17. The next screen provides a review of configured installation options and the option to modify any options if required. Click **Install**

18. 

thycotic
THYCOTIC INSTALLER
WELCOME LICENSE DB SERVER PRE-REQUISITES DB CONNECTION ACCOUNT CREATE USER EMAIL REVIEW
Back
Install
Need help?
v10.6.000000

Review the installation options and then click Install to continue.

| Name | Setting | |
|---|---|---|
| SQL Server | Using Existing SQL Server | Modify |
| Database Connection | SECRETSERVER on SECRETSERVER1\SQLEXPRESS (trusted a... | Modify |
| Encryption Configuration | New File | Modify |
| Site Name | Default Web Site | Modify |
| Secret Server Destination | C:\inetpub\wwwroot\SecretServer | Modify |
| Secret Server App Name | SecretServer running as thylab\svc_secretserver | Modify |
| Create User | ss_admin | Modify |
| Email Server | Skipped | Modify |

## 1.3 Managing the Secret Server encryption key

The Secret Server database is encrypted using a master encryption key. Each individual secret stored in the database is then encrypted with an intermediate key. When Secret Server is first installed the master encryption key is available in plain text and stored in the following location:

**C:\inetpub\wwwroot\SecretServer\encryption.conifg**

In the next module we will be protecting this encryption config file as part of the security hardening of Secret Server. At this point, Thycotic recommend taking a copy of this master encryption key and storing it in a physical vault for disaster recovery purposes. In a worst case scenario it is possible to recover the Secret Server database and all secrets with a valid database backup and the master encryption key.

**Important note:** Thycotic does not keep copies of customer encryption keys

# Module 2 – Basic Configuration

In this module we will explore a range of basic configuration tasks in Secret Server. Your trainer will also discuss best practices and common use cases

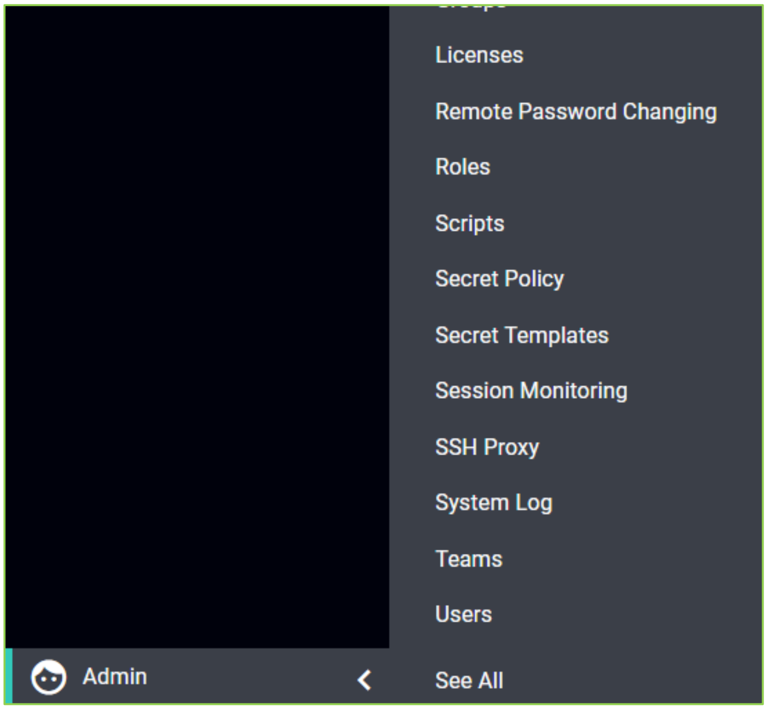
## 2.1 Installing licenses

Before any additional licenses are installed the free version of Secret Server (standard addition) allows for the creation of one user and has many feature limitations. In a production environment, additional licenses must be purchased, installed and activated for effective usage.

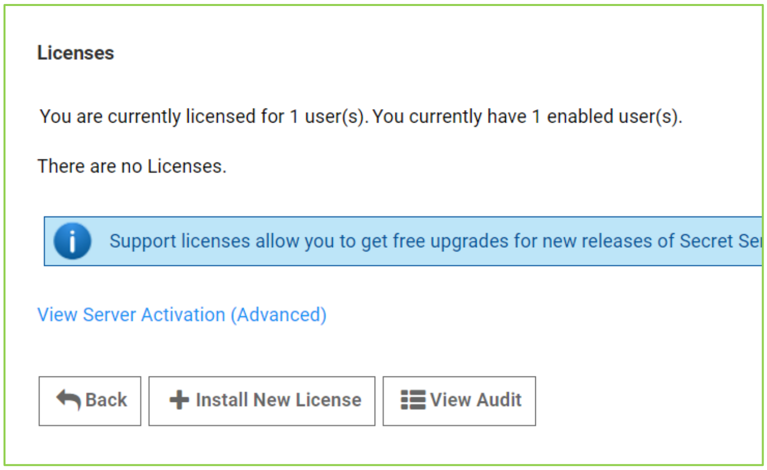
Secret server is licensed for both users and support, support licenses allow Secret Server to receive updates. The number of support licenses and user licenses must match in order to receive upgrades. Valid support licensing is required to receive any technical assistance from the Thycotic support team.

### Lab exercise 3 – Installing licenses

1. Ensure you are logged in to Secret Server with the initial account created during the installation (ss_admin / Thycotic@2019!)
2. Click the **Admin** tab from the toolbar at the bottom-right of the screen then select **Licenses**



3. From the licenses page click the **Install new license button**



**Licenses**

You are currently licensed for 1 user(s). You currently have 1 enabled user(s).

There are no Licenses.

Support licenses allow you to get free upgrades for new releases of Secret Se

View Server Activation (Advanced)

4. As we will be entering multiple license keys, select **Bulk Entry Mode**
5. In the license field paste the five license keys provided by your Trainer, they should be in the following format

```
For Evaluation Use Only    XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
For Evaluation Use Only    XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
For Evaluation Use Only    XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
For Evaluation Use Only    XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
For Evaluation Use Only    XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
```

## 2.2 License Activation

Although adding these license keys has upgraded Secret Server from standard to platinum addition, Secret Server will now be in **Limited Mode**. To remedy this the license keys, we have added need to be activated.

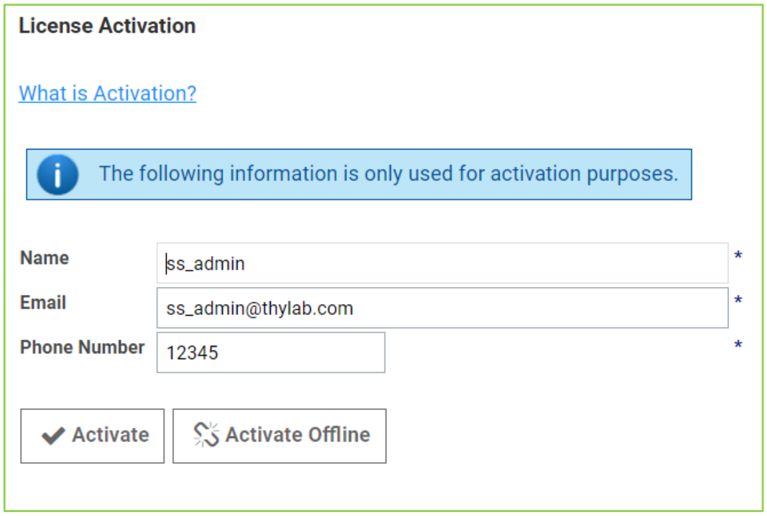
Secret Server licenses are typically activated over a secure HTTPS connection but for environments with no internet access, an offline activation process is also available

During the activation the following information is sent to Thycotic:

- Name (user entered)
- Phone Number (user entered)
- Email (user entered)
- All Licenses (license name, license key)
- Hardware Hash of each web server
  - This information is one way hashed before it is sent so it does not reveal any identifiable hardware information.
- Secret Server Version
- An Encrypted Value to identify the instance
  - This does not include any Secret data or the encryption.config file.
- The data is gathered for the purpose of contact if there is a licensing issue and Thycotic will not sell or distribute the information provided during activation. The only information available to Thycotic staff is the contact information solely for the purposes of technical support and customer service.

## Lab Exercise 4 – Activating Secret Server Licenses

1. From the licensing page, click the **License Activation button**
2. Enter the default training user details as in the image below. The phone number does not need to be valid in this training environment



License Activation

What is Activation?

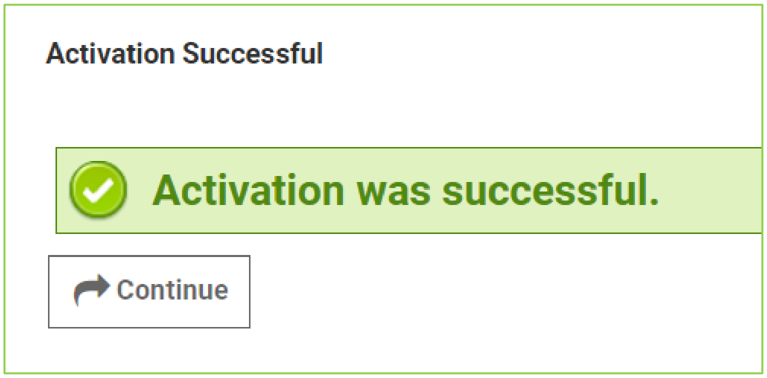
The following information is only used for activation purposes.

Name: ss_admin *

Email: ss_admin@thylab.com *

Phone Number: 12345 *

3. Select **Activate** to complete the license activation process. After a few seconds you should see the following screen:



Activation Successful

Activation was successful.

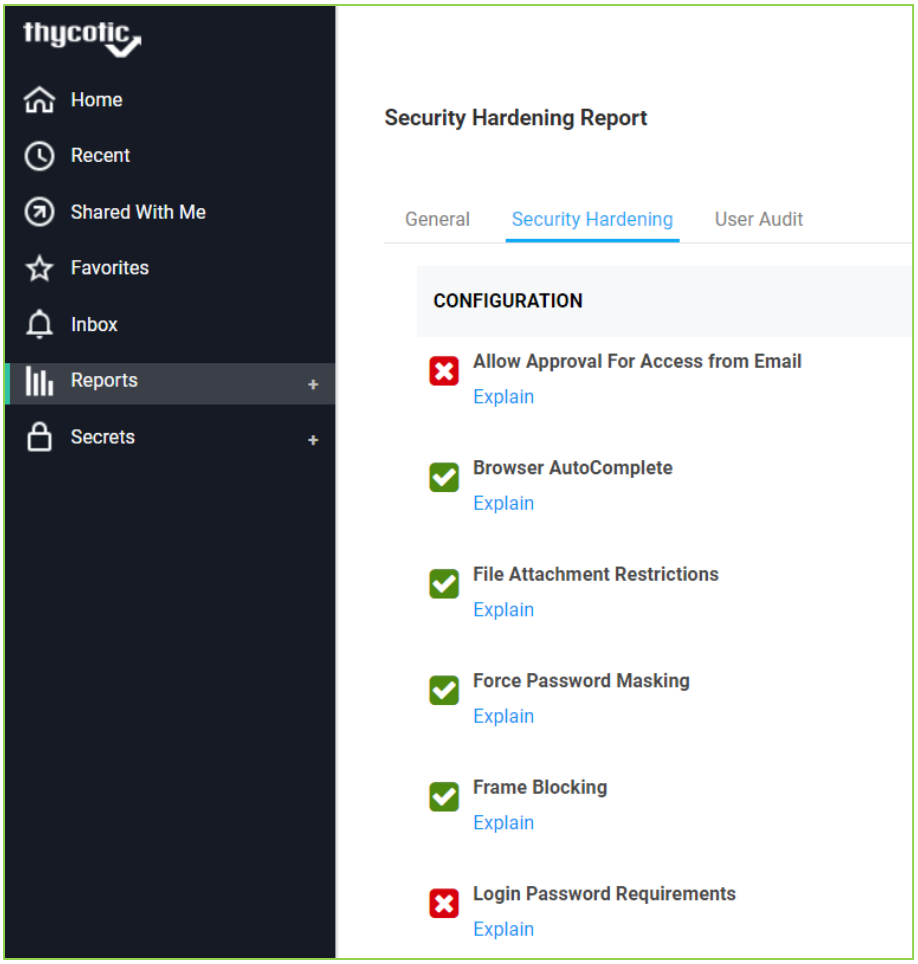
## 2.3 Security Hardening

Following the installation of Secret Server, it is important to make sure that environment and installation are as secure as possible. Secret Server makes this easy by providing a report of potential security issues and easy to follow guidance on hardening configuration to mitigate risks.

The Security Hardening report can be accessed by navigating to the **Reports** tab then selecting **Security Hardening**

In this section we will view the security hardening report and perform a number of tasks to increase the security of the installation. For a full guide on hardening a Secret Server installation visit:

https://updates.thycotic.net/secretserver/documents/SS_SecurityHardening.pdf



Security Hardening Report

CONFIGURATION

☒ Allow Approval For Access from Email

☑ Browser AutoComplete

☑ File Attachment Restrictions

☑ Force Password Masking

☑ Frame Blocking

☒ Login Password Requirements

Each item within the report represents a potential security concern that should be considered in any environment. For a detailed description of the issue and remediation actions, click **Explain**

It is important to understand that in many cases security must be balanced against user productivity. The first item in the security hardening report is a good example of this. Allow approval for access from email is a very convenient feature that allows users to approve or deny access to a secret by clicking a link in the request email. This obviously presents a security concern if the users email account is compromised. In many cases, features like this need to be considered based on the individual requirements of your organization.

## Lab Exercise 5 – Protecting the encryption config

As discussed in section 1.3 the master encryption key used to encrypt the Secret Server database is initially stored in plain text in the following location:

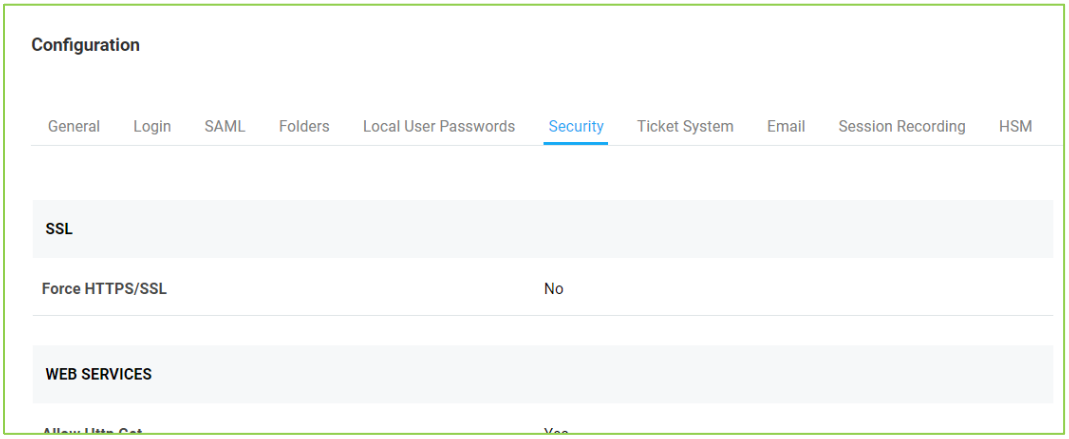
**C:\inetpub\wwwroot\SecretServer\encryption.conifg**

Thycotic strongly recommend that steps are taken to protect this file to prevent unauthorized access to the Secret Server database or individual secrets. Typically, there are three ways this can be achieved

- Protecting the encryption.comfig file with DPAPI
- Protecting the encryption.comfig file with EFS
- Protecting the encryption.config file with an integrated HSM

In this exercise we will use DPAPI to protect the encryption.config file. For more information on using EFS or a HSM please visit the Thycotic knowledge base.

1. Ensure you are logged in to Secret Server with the account created during the installation (ss_admin / thycotic@2018)
2. Open a file explorer window and navigate to C:\inetpub\wwwroot\secretserver and copy the encryption.config file to your desktop. **Note:** in a production environment Thycotic would recommend storing this in a physical vault or HSM
3. Navigate to the **Admin > Configuration** page
4. Select the security tab as in the image below:



Configuration

SSL

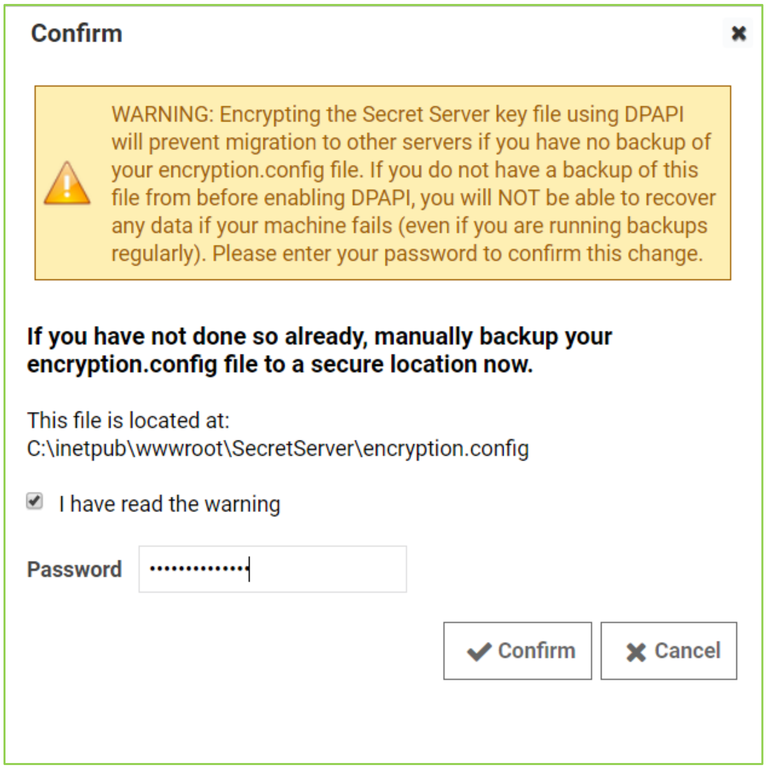
Force HTTPS/SSL: No

WEB SERVICES

Allow Http Get: Yes

5. Scroll down to the bottom of the page and click the **Encrypt key using DPAPI button** you will be presented with a confirmation dialogue.

6. Check the **I have read the warning** check box
7. Enter the password for the current user (Thycotic@2019!) and click the **Confirm button**



WARNING: Encrypting the Secret Server key file using DPAPI will prevent migration to other servers if you have no backup of your encryption.config file. If you do not have a backup of this file from before enabling DPAPI, you will NOT be able to recover any data if your machine fails (even if you are running backups regularly). Please enter your password to confirm this change.

**If you have not done so already, manually backup your encryption.config file to a secure location now.**

This file is located at:
C:\inetpub\wwwroot\SecretServer\encryption.config

☑ I have read the warning

Password ••••••••••••••

8. In notepad, open the version of encryption.config exported in step 2 and the newly encrypted version side by side. They should now look different.

# Module 3 - Users, Groups and Roles

In this module we will be covering how users are created and managed within Secret Server and how role-based access control (RBAC) can be used to ensure users only have access to the areas of the application required in their specific job role.

## 3.1 Creating Secret Server Users

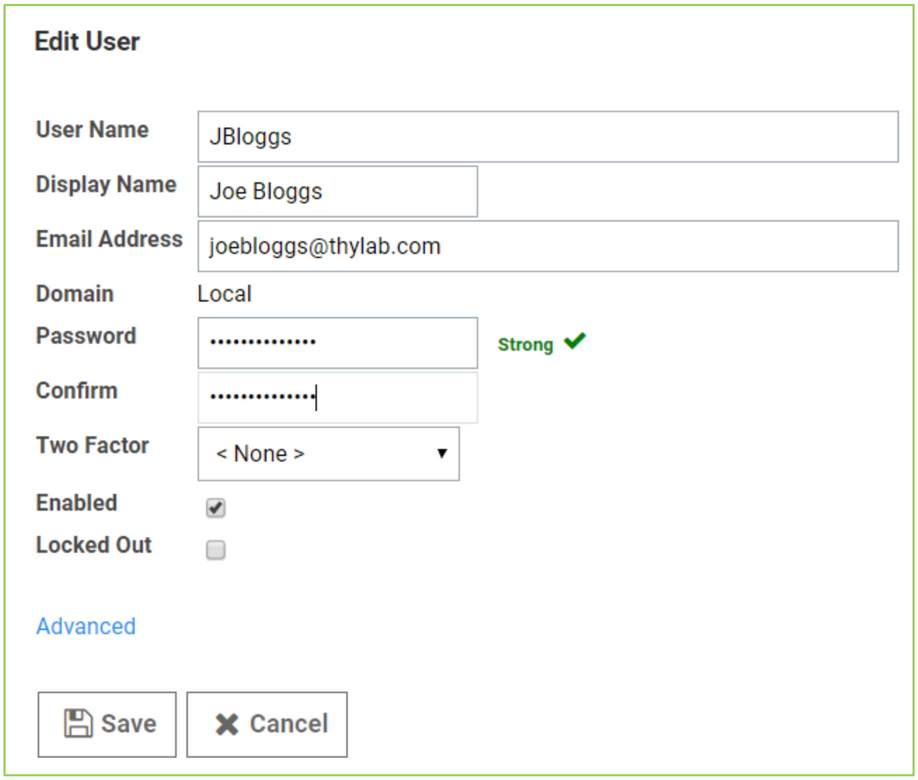
The initial configuration we have completed so far has been performed using the initial account created during the installation of Secret Server. We now need to consider how we will provide access to other users. There are three main ways in which user access can be provided within secret server

- **Creating local users** – User accounts can be created within secret server
- **Active Directory Sync** – Specific users or groups of users will be able to log in to secret server using the active directory domain credentials
- **SSO Integration** – Secret server can integrate with many single sign on providers using SAML

In this section we will create a new local user as an example and then configure Active Directory synchronization to allow existing AD users to log into Secret Server with their domain credentials.

### Lab Exercise 6 – Creating a local user

1. Ensure you are logged in to Secret Server with the account created during the installation (ss_admin / thycotic@2018)
2. Navigate to the **Admin > Users** page
3. At the bottom of the page, click the **Create New button, the new user page will appear**
4. Create a new user account using the settings from the image below (feel free to change the username)



## Edit User

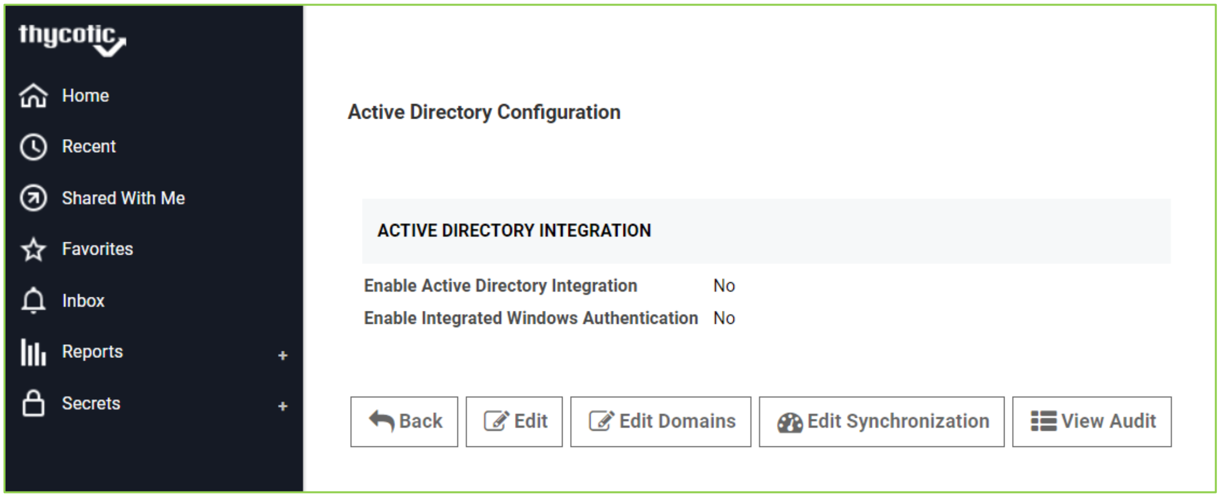
| | |
|---|---|
| User Name | JBloggs |
| Display Name | Joe Bloggs |
| Email Address | joebloggs@thylab.com |
| Domain | Local |
| Password | •••••••••••••• Strong ✓ |
| Confirm | •••••••••••••• |
| Two Factor | < None > ▾ |
| Enabled | ☑ |
| Locked Out | ☐ |

5. Click **Save** to create the new user account

## Lab Exercise 7 – Configuring Active Directory Synchronization

In this exercise will set up synchronization between secret server and an Active Directory domain. This will allow specific users or groups users access to Secret Server using their Domain credentials.

1. Ensure you are logged in to Secret Server with the account created during the installation (ss_admin / thycotic@2018)
2. Navigate to the **Admin > Active Directory page**



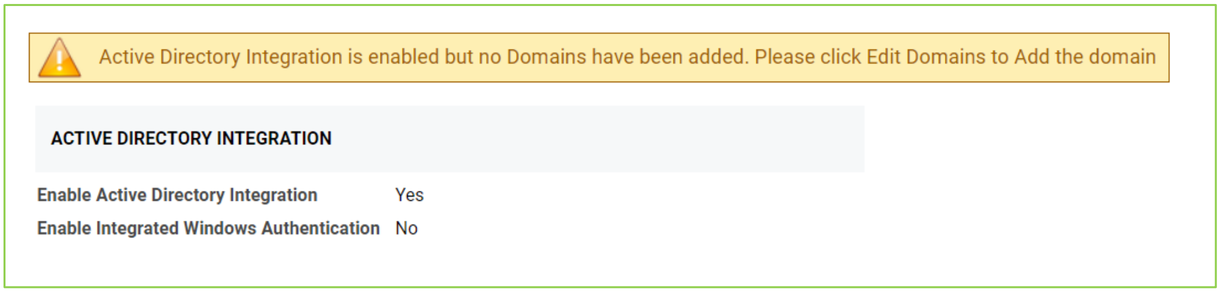
Active Directory Configuration

ACTIVE DIRECTORY INTEGRATION

| | |
|---|---|
| Enable Active Directory Integration | No |
| Enable Integrated Windows Authentication | No |

3. As you can see from the image above, Active Directory integration is not currently enabled. To enable AD Sync, click the **Edit button**
4. On the Edit Active Directory configuration change the following settings:
5. **Enable Active Directory Integration**
6. **Do NOT Enable Integrated Windows Authentication.** This feature automatedly logs users in to Secret Server using their current Windows credentials. Although convenient, Thycotic does not recommend using this feature as it introduces a number of potential security issues such as users leaving their machines unlocked and unauthorized users gaining access to Secret Server.
7. **Enable Synchronization of Active Directory** by checking the relevant box. This allows Secret Server to regularly synchronize against specified AD security group/s. For example, if a user is added to a group in AD that is synced, the account will automatically be created in Secret Server.
8. Leave the synchronization interval with the default setting of **1 hour**
9. Change the User Account Option field to **User Status Mirrors Active Directory (automatic).** This ensures that when a user account is enabled or disabled in Active Directory, the change will be mirrored in Secret Server at the next synchronization interval.
10. Click **Save**

As we have enabled Active Directory Integration but not yet configured any domains to integrate with you will see the following warning:

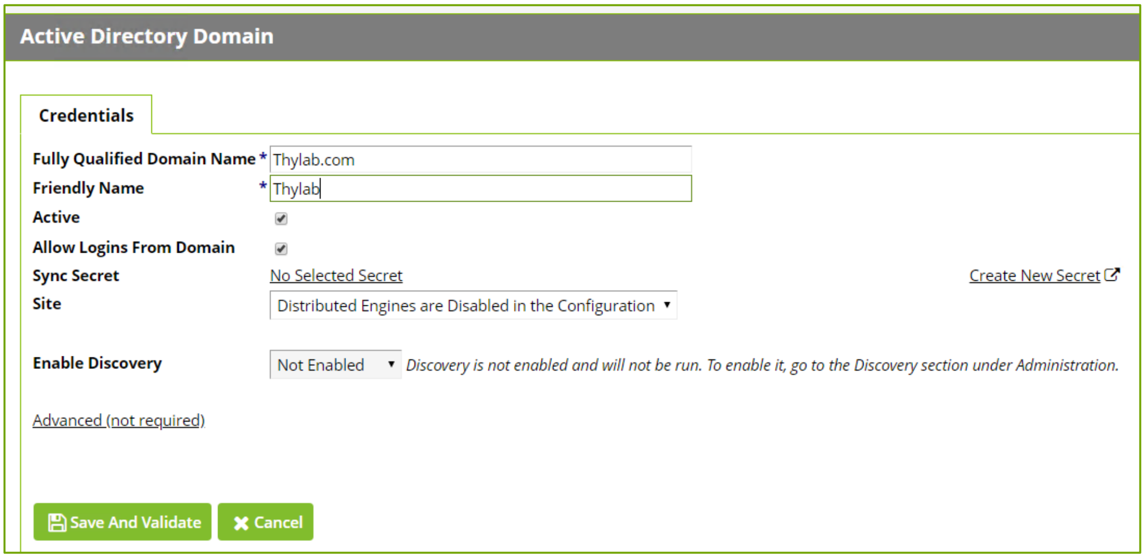


Active Directory Integration is enabled but no Domains have been added. Please click Edit Domains to Add the domain

ACTIVE DIRECTORY INTEGRATION

| | |
|---|---|
| Enable Active Directory Integration | Yes |
| Enable Integrated Windows Authentication | No |

11. To configure domain/s to integrate with, click the **Edit Domains button,** The Active Directory Domains page will be displayed:
12. Click the **Create New button**
13. Set the set the Fully Qualified Domain Name field to **Thylab.com**
14. Set the friendly name to **Thylab**
15. Check **Active**
16. Check **Allow Logins From Domain**
17. For the Sync Secret, we will need to create a new secret in secret server for the credentials of an account that has read access to Active Directory. Click **Create New Secret** on the right-hand side of the screen



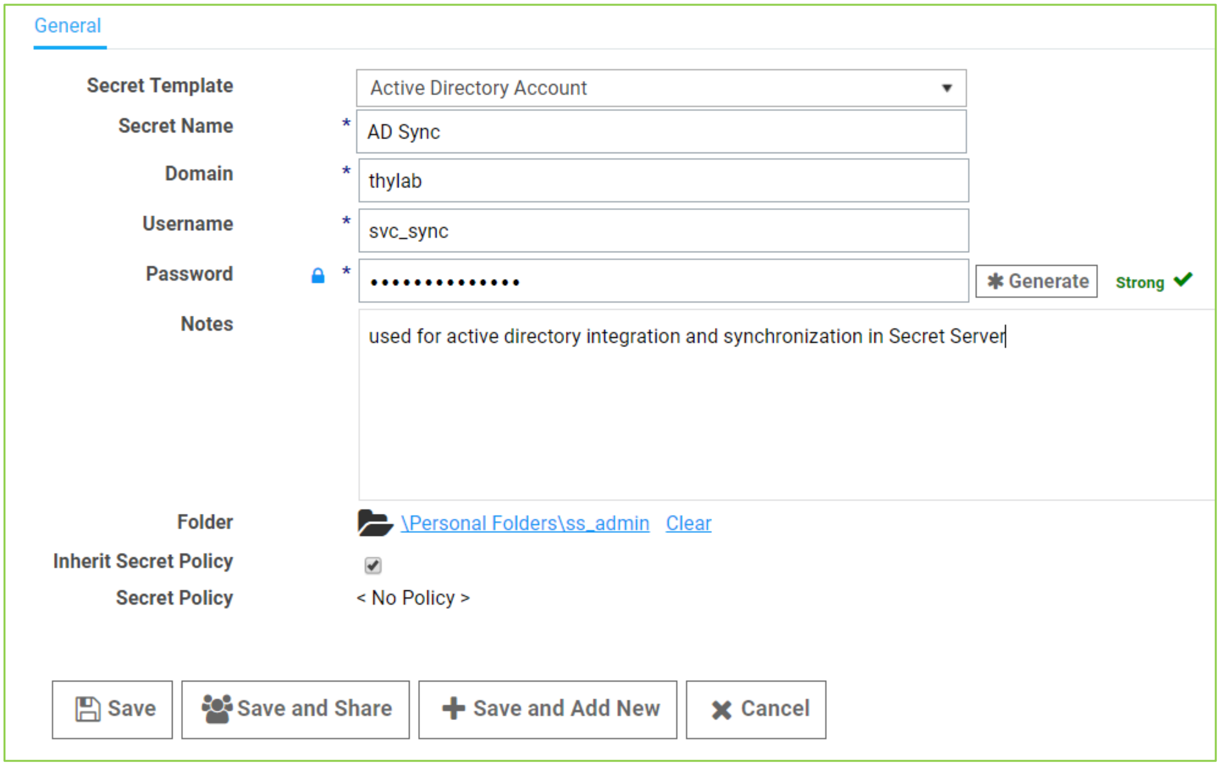
Active Directory Domain

Credentials

| | |
|---|---|
| Fully Qualified Domain Name * | Thylab.com |
| Friendly Name * | Thylab |
| Active | ☑ |
| Allow Logins From Domain | ☑ |
| Sync Secret | No Selected Secret |
| Site | Distributed Engines are Disabled in the Configuration |
| Enable Discovery | Not Enabled *Discovery is not enabled and will not be run. To enable it, go to the Discovery section under Administration.* |

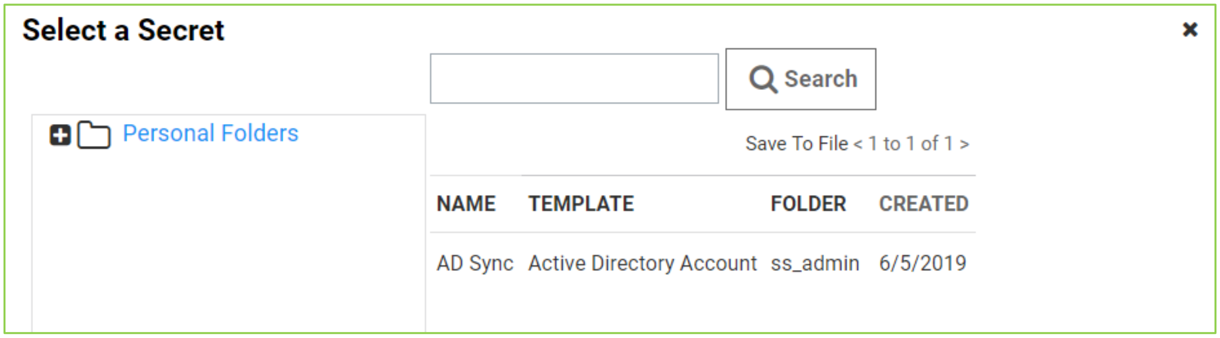
18. The new secret page should now be opened in a new tab, configure the new secret with the following information:
19. Ensure secret template is set to **Active Directory Account**
20. Set Secret Name to **AD Sync**
21. Set Domain to **Thylab.com**
22. Set Username to **svc_sync**
23. Set Password to **Thycotic@2019!**
24. In the notes field, type **used for active directory integration and synchronization in Secret Server**

25. Leave the Folder, Inherit Security Policy and Secret Policy fields with the default values, your configuration should match the image below:



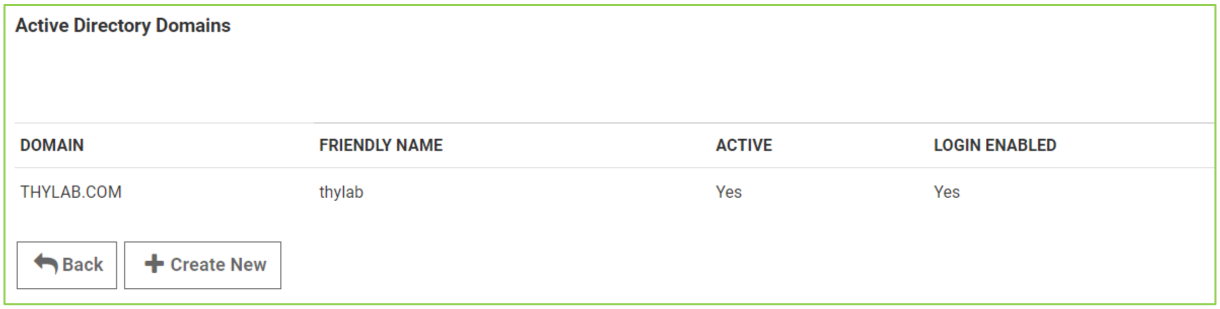
|  |  |
|---|---|
| Secret Template | Active Directory Account |
| Secret Name * | AD Sync |
| Domain * | thylab |
| Username * | svc_sync |
| Password * | •••••••••••••• |
| Notes | used for active directory integration and synchronization in Secret Server |
| Folder | \Personal Folders\ss_admin Clear |
| Inherit Secret Policy | ☑ |
| Secret Policy | < No Policy > |

26. Click **Save**
27. Go back to the original **Secret Server tab** to finish adding the domain configuration
28. In the Sync Secret field, click **No Selected Secret** , the select a Select a Secret dialogue will be displayed as per the below image:



| NAME | TEMPLATE | FOLDER | CREATED |
|---|---|---|---|
| AD Sync | Active Directory Account | ss_admin | 6/5/2019 |

29. Select the AD Sync secret created earlier
30. Leave the Site, Enable Discovery and Advanced settings with default configuration and click **Save and Validate**
31. Secret Server will check tha the Domain can be contacted, you should now see the Thylab.com domain in the Active Directory Domains page:



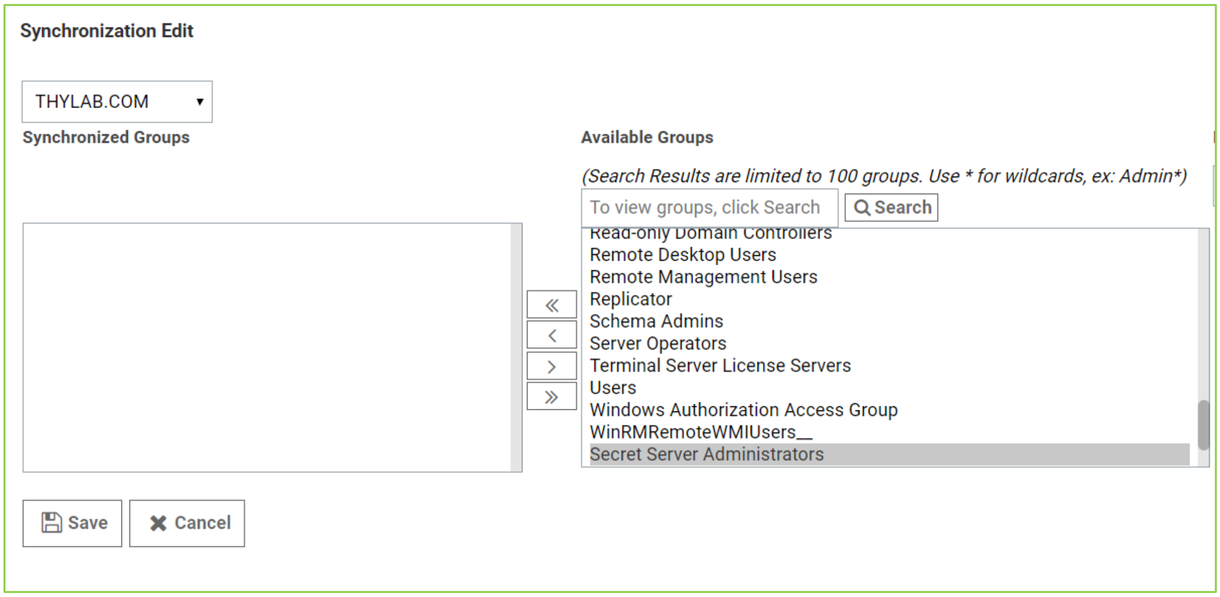
Active Directory Domains

| DOMAIN | FRIENDLY NAME | ACTIVE | LOGIN ENABLED |
|---|---|---|---|
| THYLAB.COM | thylab | Yes | Yes |

32. Click **Back**

Now that the Domain has been configured, we need to identify which users or groups of users from Active Directory we want to synchronize into Secret Server.

33. From the Active Directory Configuration page, click **Edit Synchronization**
34. Drop the Select Domain field down and select **Thylab.com,** The synchronized groups page will now appear:



Synchronization Edit

THYLAB.COM

Synchronized Groups

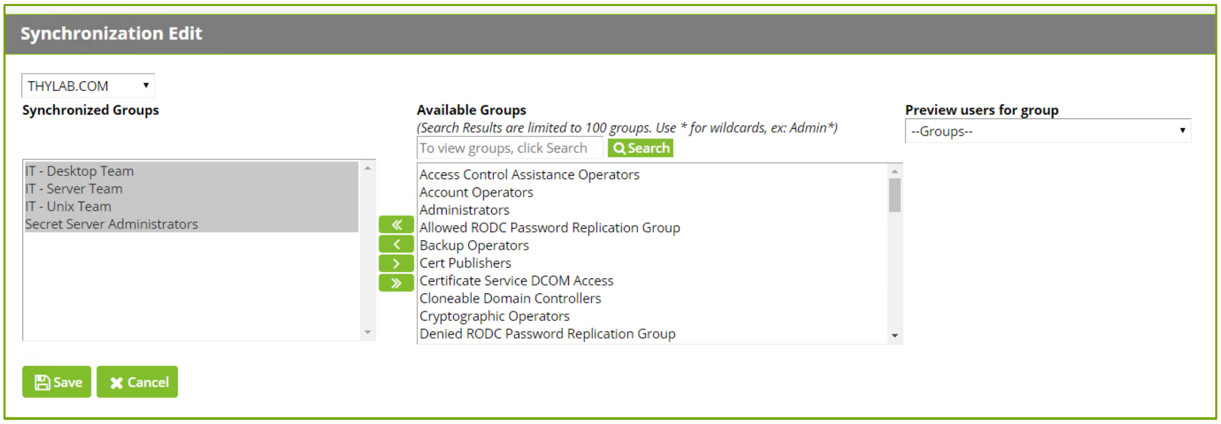
Available Groups

*(Search Results are limited to 100 groups. Use * for wildcards, ex: Admin*)*

To view groups, click Search

Read-only Domain Controllers
Remote Desktop Users
Remote Management Users
Replicator
Schema Admins
Server Operators
Terminal Server License Servers
Users
Windows Authorization Access Group
WinRMRemoteWMIUsers__
Secret Server Administrators

35. Click the **Search button** to display a list of all groups present in the specified domain
36. Select the following groups in the available groups field by hold the CTRL key while selecting:
    a. Secret Server Administrators
    b. IT – Desktop Team
    c. IT – Server Team
    d. IT – Unix Team
37. Click the **single left arrow** button to move the selected groups to the Synchronized groups field:


Synchronization Edit

THYLAB.COM

Synchronized Groups

- IT - Desktop Team
- IT - Server Team
- IT - Unix Team
- Secret Server Administrators

Available Groups

*(Search Results are limited to 100 groups. Use * for wildcards, ex: Admin*)*

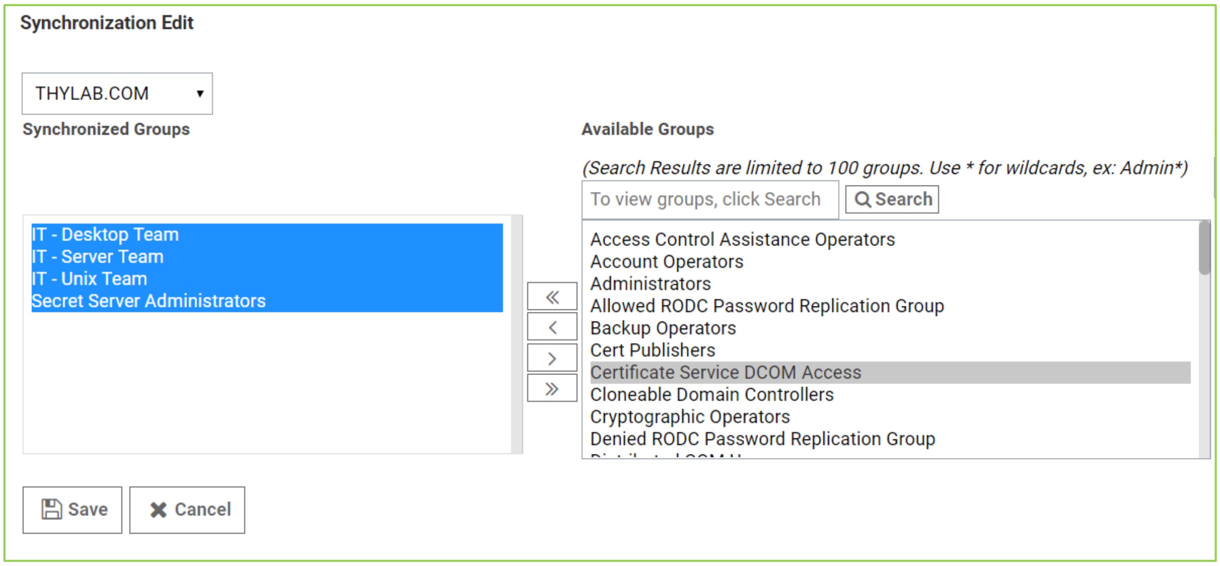
To view groups, click Search

- Access Control Assistance Operators
- Account Operators
- Administrators
- Allowed RODC Password Replication Group
- Backup Operators
- Cert Publishers
- Certificate Service DCOM Access
- Cloneable Domain Controllers
- Cryptographic Operators
- Denied RODC Password Replication Group

Preview users for group

--Groups--

38. Click **Save,** you will be taken back to the Active Directory Configuration page
39. To perform the first synchronization manually without having to wait for the first scheduled run, Click the S**ynchronize Now button**
40. Wait a few seconds then click the **refresh icon** (highlighted below), You should now have added the targeted users into Secret Server:


Synchronization Edit

THYLAB.COM

Synchronized Groups

- IT - Desktop Team
- IT - Server Team
- IT - Unix Team
- Secret Server Administrators

Available Groups

*(Search Results are limited to 100 groups. Use * for wildcards, ex: Admin*)*

To view groups, click Search

- Access Control Assistance Operators
- Account Operators
- Administrators
- Allowed RODC Password Replication Group
- Backup Operators
- Cert Publishers
- Certificate Service DCOM Access
- Cloneable Domain Controllers
- Cryptographic Operators
- Denied RODC Password Replication Group

41. To verify navigate the **Admin > Users page**
42. Finally, navigate back to the **Admin > Active Directory page** and select Synchronize now to perform a manual sync of all groups

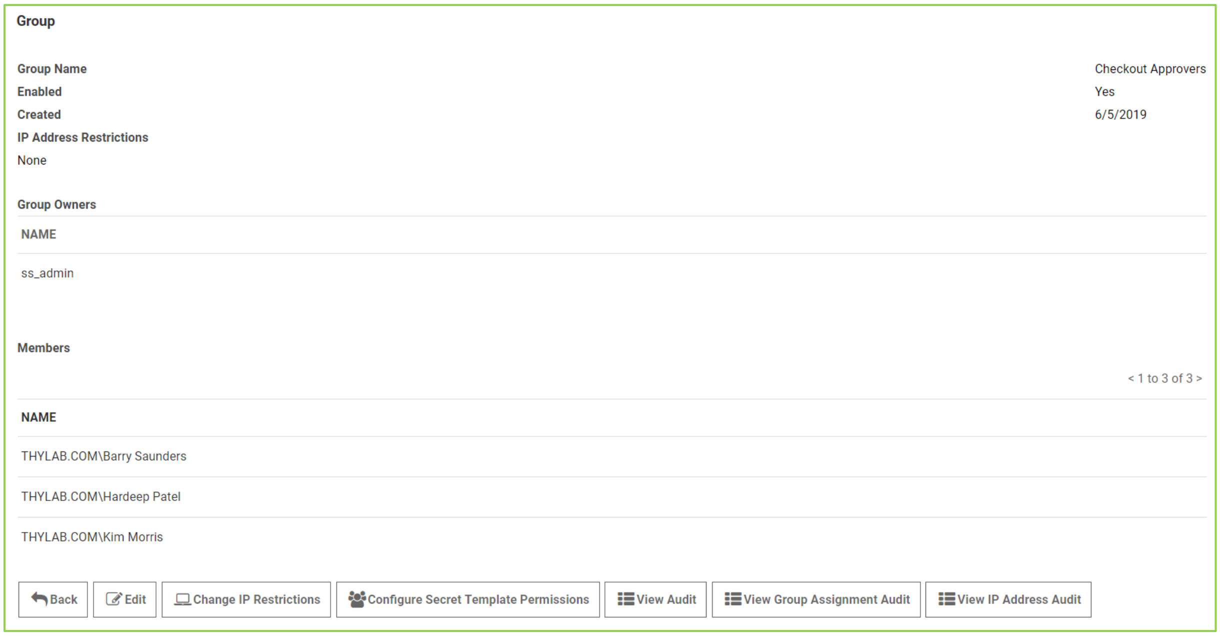
## 3.2 Groups

Within Secret Server groups are an important organizational container for user accounts. Although Roles (discussed in the next section) permissions and access to secrets can be determined at the individual user level, this approach can be highly complex, time consuming and difficult to manage. Adding users to groups means that configuration can then easily be applied to all users within the group while still providing the option for exceptions at the individual user level.

If Active Directory integration and synchronization have been configured, then any selected groups and group memberships from Active Directory will be replicated within Secret Server. If these groups do not provide the level of granularity required in Secret Server, local groups can also be created.

## Lab Exercise 8 – Creating a local group

1. Navigate to the **Admin > Groups** page, you should see the four groups that were synced from Active Directory plus a default local group called **Everyone**
2. To create a new group, click the **Create New** button
3. Create a new group with the following details:
4. Set Group name to **Checkout Approvers**
5. Ensure Enabled is **checked**
6. Leave the Managed By field set to **Group Administrators**
7. Hold down the CTRL and select **Barry Saunders**, **Hardeep Patel** and **Kim Morris**
8. Click the **single left arrow button** to add these users to the members field, your configuration should match the image below



**Group**

| | |
|---|---|
| **Group Name** | Checkout Approvers |
| **Enabled** | Yes |
| **Created** | 6/5/2019 |

**IP Address Restrictions**

None

**Group Owners**

| NAME |
|---|
| ss_admin |

**Members**

< 1 to 3 of 3 >

| NAME |
|---|
| THYLAB.COM\Barry Saunders |
| THYLAB.COM\Hardeep Patel |
| THYLAB.COM\Kim Morris |

Back
Edit
Change IP Restrictions
Configure Secret Template Permissions
View Audit
View Group Assignment Audit
View IP Address Audit

9. Click **Save,** this group will be used in later lab exercises

## 3.3 Roles

When users are created or synchronized into Secret Server they must be assigned to a role. This ensures that a strict role-based access (RBAC) approach can applied within secret server.

A role in Secret Server is basically a permission set. There are 117 set highly granular permissions that can be included or excluded from a role to ensure that your organization can provide each user with the specific permissions they require without creating over privileged users.

In this section we will cover the default roles available in Secret Server and how to apply roles to users or groups of users. We will also introduce several scenarios where you may want to create custom roles.

The three key default role sin Secret Server:

| Administrator | User | Basic User |
|---|---|---|
| **All permissions apart from the following**:<br>Access Offline Secrets on Mobile<br>Allow Access Challenge<br>Privilege Manager MacOS Admin<br>Privilege Manager User<br>Privilege Manager Windows Admin<br>Web Services impersonate | Add Secret<br>Allow Access Challenge<br>Assign Secret Policy<br>Copy Secret<br>Delete Secret<br>Delete Secrets from Reports<br>Edit Secret<br>Own Secret<br>Personal Folders<br>Unrestricted by Teams<br>User Audit Expire Secrets<br>View About<br>View Advanced Dashboard<br>View Advanced Secret Options<br>View Launcher Password<br>View Password Requirements<br>View Secret<br>View Secret Audit<br>View User Audit Report | Add Secret<br>Allow Access Challenge<br>Copy Secret<br>Delete Secret<br>Delete Secrets from Reports<br>Edit Secret<br>Own Secret<br>Personal Folders<br>Unrestricted by Teams<br>View Launcher Password<br>View Password Requirements<br>View Secret<br>View Secret Audit |

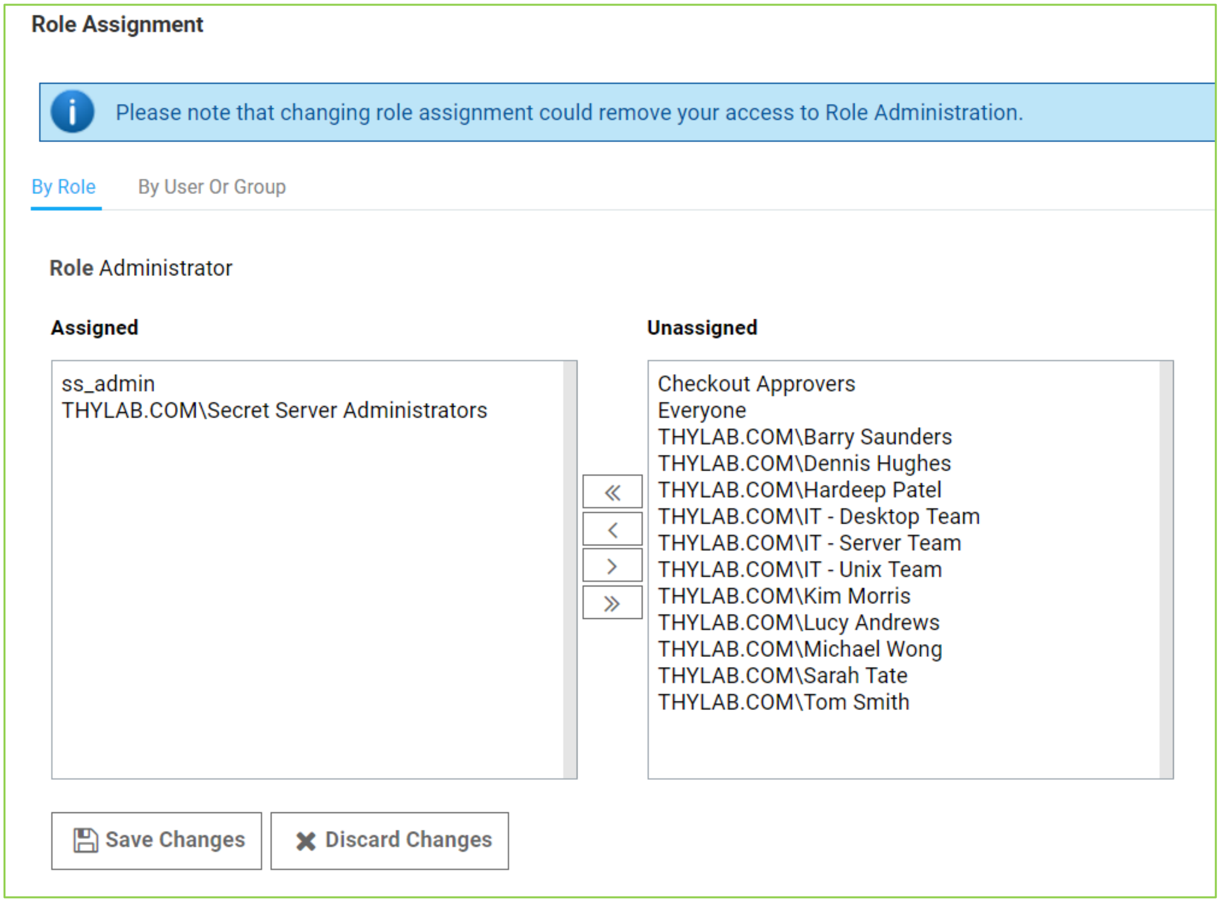
**Note:** By default, when users are first created or synchronized into secret server, they are assigned the **user role**. This can be changed by navigating to the **Admin > Configuration page**. Under the **User Experience section,** you will find the **Default New User Role field**. You can change this to any available role.

## Lab exercise 9 – Applying Roles

Roles can be applied to individual user accounts or to groups. As a best practice, users should be added to groups and then roles applied at the group level. This provides a more scalable, manageable approach to role-based access control (RBAC).

We will now apply the built in Administrators role to the Secret Server Administrators group we have previously synced from Active Directory

1. Navigate to the **Admin > Roles page**
2. Click the **Assign Roles button**
3. At this point, roles can be assigned by role (role is selected first then users added to the role) or by user or group (user or group is selected first then role added to the user or group). We will apply **By Role**
4. Ensure the Administrator role is selected in the drop-down role field
5. Find and select the **thylab\secret server administrators group**
6. Click the single left arrow button to move the group into the assigned field
7. Your configuration should match the image below:



**Role Assignment**

Please note that changing role assignment could remove your access to Role Administration.

**Role** Administrator

**Assigned**

ss_admin
THYLAB.COM\Secret Server Administrators

**Unassigned**

Checkout Approvers
Everyone
THYLAB.COM\Barry Saunders
THYLAB.COM\Dennis Hughes
THYLAB.COM\Hardeep Patel
THYLAB.COM\IT - Desktop Team
THYLAB.COM\IT - Server Team
THYLAB.COM\IT - Unix Team
THYLAB.COM\Kim Morris
THYLAB.COM\Lucy Andrews
THYLAB.COM\Michael Wong
THYLAB.COM\Sarah Tate
THYLAB.COM\Tom Smith

8. Click **Save Change**

## Lab exercise 10 – Creating custom roles

Out of the box, Secret Server provides a range of Roles that satisfy many common use cases. Thycotic does recommend that each customer creates custom roles based the needs of their organization

In this lab exercise we will explore a common scenario where more granular permission sets may be required.

Secret Server provides an important break glass mechanism called **Unlimited Administration Mode.** If this administration mode is enabled, any user with a specified permission will automatically gain access to **all** secrets stored in secret server, regardless of any permissions applied at the folder or individual secret level.

There are three role permissions relevant to Unlimited Administration:

- **Administer Configuration Unlimited Access** – Users with this role permission can enable or disable unlimited administration mode
- **Unlimited Administrator** – Users with this role permission receive unlimited secret access if unlimited administration mode is enabled
- **View Configuration Unlimited Administrator** – Users with this role permission can view the current administration mode configuration

As a best practice, Thycotic recommends splitting the Administrator role out to ensure a least privilege approach

| | |
|---|---|
| **User** | Administrator (Super User) |
| **Description** | Can configure and receive unlimited administration |
| **Permissions** | • Administer Configuration Unlimited Access<br>• Unlimited Administrator<br>• View Configuration Unlimited Administrator |

| | |
|---|---|
| **User** | Administrator (Unlimited Admin Configure) |
| **Description** | Can configure **but NOT** receive unlimited administration |
| **Permissions** | • View Configuration Unlimited Administrator |

| | |
|---|---|
| **User** | Administrator (Unlimited Admin User) |
| **Description** | Can receive **but NOT** configure unlimited administration |
| **Permissions** | • Unlimited Administrator<br>• View Configuration Unlimited Administrator |

1. Navigate to the **Admin > Roles page**
2. Select the **Administrato**r role

3. Scroll to the bottom of the page and click **Edit**
4. Scroll back to the top of the page and change the Role Name field to **Administrator (Super User)**
5. Click **Save**
6. Go back to the **Admin > Roles page**
7. Click the **Create New button**
8. Enter a role name of **Administrator (Unlimited Admin Configure)**
9. Click the double left arrow to move all permissions from the Permissions Unassigned field to Permissions Assigned
10. Move the following permissions back to the unassigned field:

| |
|---|
| Access Offline Secrets on Mobile |
| Allow Access Challenge |
| Privilege Manager MacOS Admin |
| Privilege Manager User |
| Privilege Manager Windows Admin |
| Web Services impersonate |
| **Unlimited Administrator** |

11. Click **Save**
12. Repeat steps 6-11 for the Administrator (Unlimited Admin User) where all permissions are included apart from the following:

| |
|---|
| Access Offline Secrets on Mobile |
| Allow Access Challenge |
| Privilege Manager MacOS Admin |
| Privilege Manager User |
| Privilege Manager Windows Admin |
| Web Services impersonate |
| **Administer Configuration Unlimited Access** |

13. Now unassign the Administrator (Super User) role from the Secret Server Administrators AD group
14. Assign the new Administrator (Unlimited Admin Configure) role to Sarah Tate
15. Assign the new Administrator (Unlimited Admin User) role to Tom Smith

# Module 4 – Folders and Policies

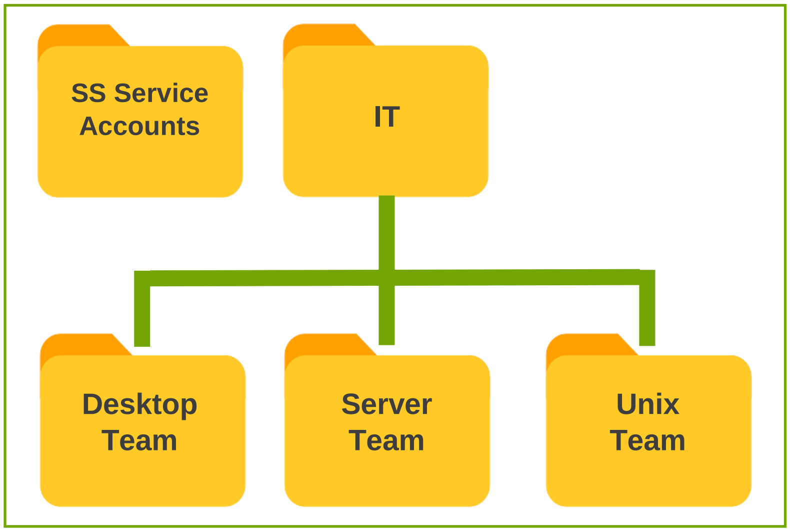
## 4.1 Secret Folder Structure

Before starting to add Secrets into Secret Server, it is essential that that a well-planned folder structure is created. A well planned, effective folder structure not only provides the ability to keep all secrets organized but it also allows for the effective use of security policies.

Security settings can be applied to individual secrets but with hundreds or thousands of secrets managing security on each secret does not scale. The way folder structures work in Secret Server is very similar to NTFS folder and file permissions in the Microsoft Windows world

**Discussion Point:** At this point your trainer will discuss common approaches to planning your folder structure.

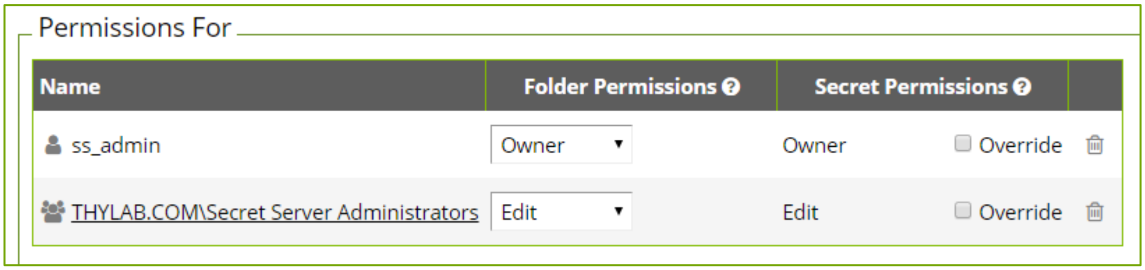
In this module we will be creating a basic folder structure for the IT team and applying netfsecret policies to the folder to ensure users only have access to Secrets they require in their role.



## Lab Exercise 11 – Creating Secret Folders

To create a new root folder:

1. Navigate to the **Admin > Folders page**
2. Ensure that no other folders are selected then click the **New button**
3. Create a new folder with the following details:
4. Folder name: **SS Service Accounts**
5. Folder Icon: **Folder**
6. Inherit Secret Policy: **Unchecked**
7. Secret Policy: **No Policy**
8. Inherit Permissions from Parent: **Unchecked**
9. Add permissions for the following groups:



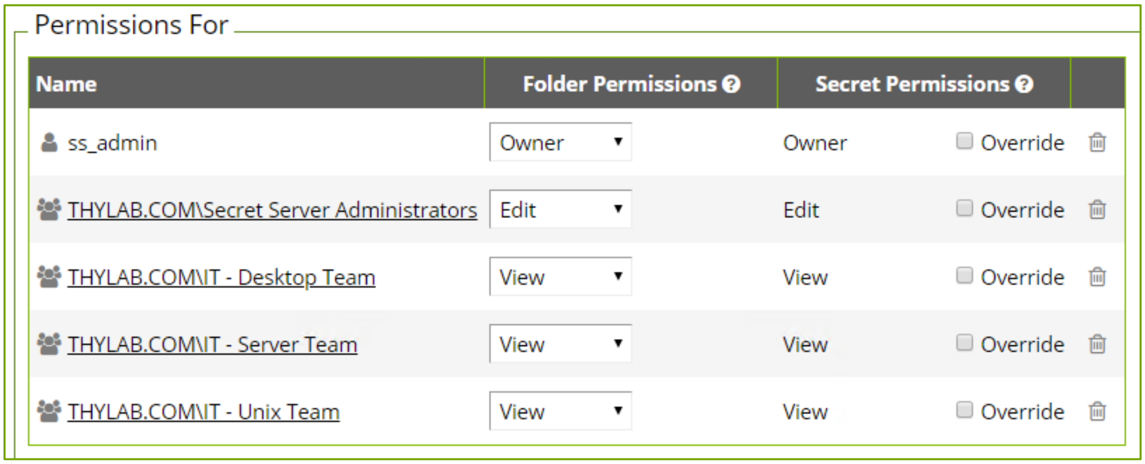
Permissions For

| Name | Folder Permissions | Secret Permissions | | |
|---|---|---|---|---|
| ss_admin | Owner ▾ | Owner | ☐ Override | 🗑 |
| THYLAB.COM\Secret Server Administrators | Edit ▾ | Edit | ☐ Override | 🗑 |

10. Click Save

Next, we will create the root IT Folder

1. Create a new folder with the following details:
2. Folder name: **IT**
3. Folder Icon: **Folder**
4. Inherit Secret Policy: **Unchecked**
5. Secret Policy: **No Policy**
6. Inherit Permissions from Parent: **Unchecked**
7. Add permissions for the following groups:



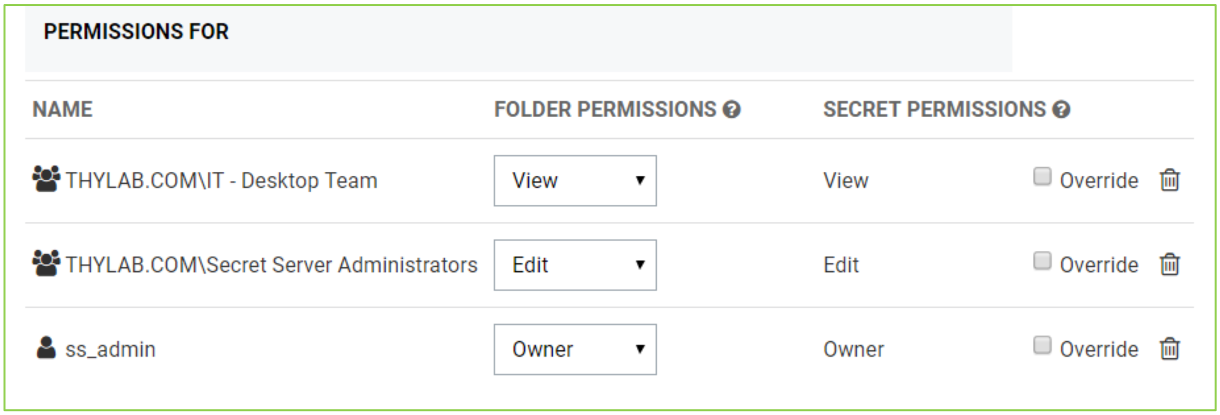
Permissions For

| Name | Folder Permissions | Secret Permissions | | |
|---|---|---|---|---|
| ss_admin | Owner ▾ | Owner | ☐ Override | 🗑 |
| THYLAB.COM\Secret Server Administrators | Edit ▾ | Edit | ☐ Override | 🗑 |
| THYLAB.COM\IT - Desktop Team | View ▾ | View | ☐ Override | 🗑 |
| THYLAB.COM\IT - Server Team | View ▾ | View | ☐ Override | 🗑 |
| THYLAB.COM\IT - Unix Team | View ▾ | View | ☐ Override | 🗑 |

8. Click Save

Now we will create three sub folders in **\IT**

1. From the Admin > Folders page, select the IT folder
2. Click the **New button**
3. Create a new folder with the following details:
4. Folder name: **IT – Desktop Team**
5. Folder Icon: **Folder**
6. Inherit Secret Policy: **Checked**
7. Secret Policy: **No Policy**
8. **Uncheck** Inherit Permissions from Parent
9. Remove permissions for server team and unix team groups, your permission configuration should match the image below:

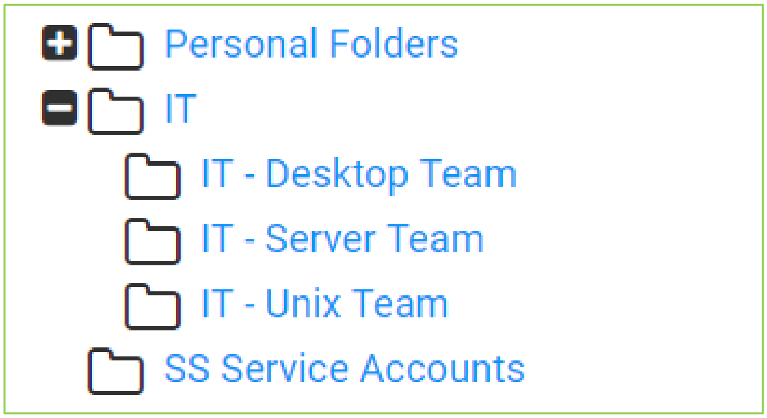


PERMISSIONS FOR

| NAME | FOLDER PERMISSIONS | SECRET PERMISSIONS | | |
|---|---|---|---|---|
| THYLAB.COM\IT - Desktop Team | View ▾ | View | □ Override | 🗑 |
| THYLAB.COM\Secret Server Administrators | Edit ▾ | Edit | □ Override | 🗑 |
| ss_admin | Owner ▾ | Owner | □ Override | 🗑 |

10. Click Save

Repeat the above steps to create additional sub-folders: IT – Server Team and IT – UNIX Team. Ensure only the relevant team can view secrets. Your folder structure should match the image below:



- Personal Folders
- IT
  - IT - Desktop Team
  - IT - Server Team
  - IT - Unix Team
- SS Service Accounts

## 4.2 Secret Policy

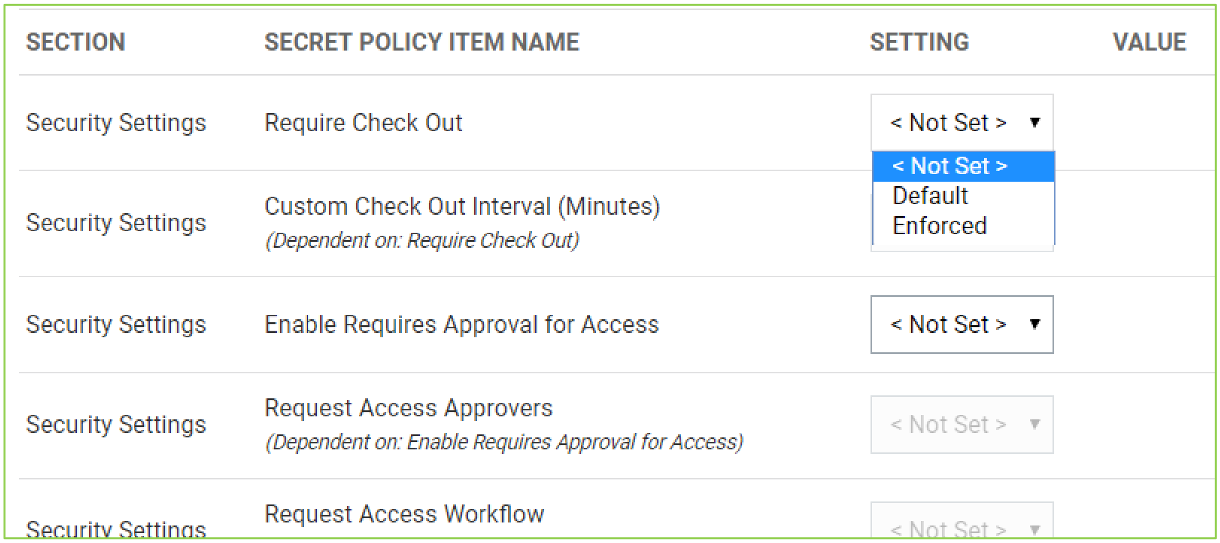
It is important to apply security settings to the secrets created or imported in Secret Server. Although it is possible to configure security settings on each and every individual secret stored, this approach simply does not scale when managing large numbers of secrets. For this reason, it is possible to create Secret Policies which define a range of security settings. Once created Policies can be applied at the folder or secret level allowing consistent security standards to be applied to different types of secret within your organization.

The following table defines the settings that can be controlled within a Secret Template:

| Setting | Description |
|---|---|
| Site | If Secret Server is configured with multiple sites, which site should secrets be associated with |
| Require Check Out | If enabled, secrets will require check out |
| Custom Check Out Interval (Minutes) | (Dependent on: Require Check Out). If checkout is enabled, the secret will be available to the user for a default period of 30 minutes. Use this setting to configure a custom check out duration |
| Enable Requires Approval for Access | If enabled, users will need to request approval to access secrets |
| Request Access Approvers | Defines which users or groups of users are able to approve access requests |
| Request Access Workflow | Defines the access approval workflow users for Secrets |
| Editors also Require Approval | If enabled, users with edit permissions to secrets will also need to submit approval requests for secret access |
| Owners and Approvers also Require Approval | If enabled, users with owner or approver permissions to secrets will also need to submit approval requests for secret access |
| Require Comment | If enabled, users will need to provide a comment when accessing secrets |
| Enable Session Recording | If enabled, any sessions launched from secrets will be recorded |
| Hide Launcher Password | If enabled, the password field will not be visible to users accessing secrets |
| Enable SSH Command Restrictions | Can be used to create lists of approved SSH commands. |
| Allow Owners Unrestricted SSH Commands | If this is enabled, secret owners would not be subject to SSH command restrictions |

| | |
|---|---|
| SSH Command Menu Groups | Used to define which users or groups have access to SSH command menus |

You will notice that for each of the above settings, the following options are available:



| SECTION | SECRET POLICY ITEM NAME | SETTING | VALUE |
|---|---|---|---|
| Security Settings | Require Check Out | < Not Set > | |
| Security Settings | Custom Check Out Interval (Minutes)<br>*(Dependent on: Require Check Out)* | | |
| Security Settings | Enable Requires Approval for Access | < Not Set > | |
| Security Settings | Request Access Approvers<br>*(Dependent on: Enable Requires Approval for Access)* | < Not Set > | |
| Security Settings | Request Access Workflow | < Not Set > | |

- Default - Any items selected as 'Default' will be applied on the creation of any Secret that has this Secret Policy applied to it.
- Enforced Any items selected as 'Enforced' will be applied to all Secrets that have this Secret Policy applied to it.

**It is important to note that users with edit or owner permissions on a secret would be able to change settings if the applied policy setting is Default. Enforced settings cannot be changed on the Secret.**

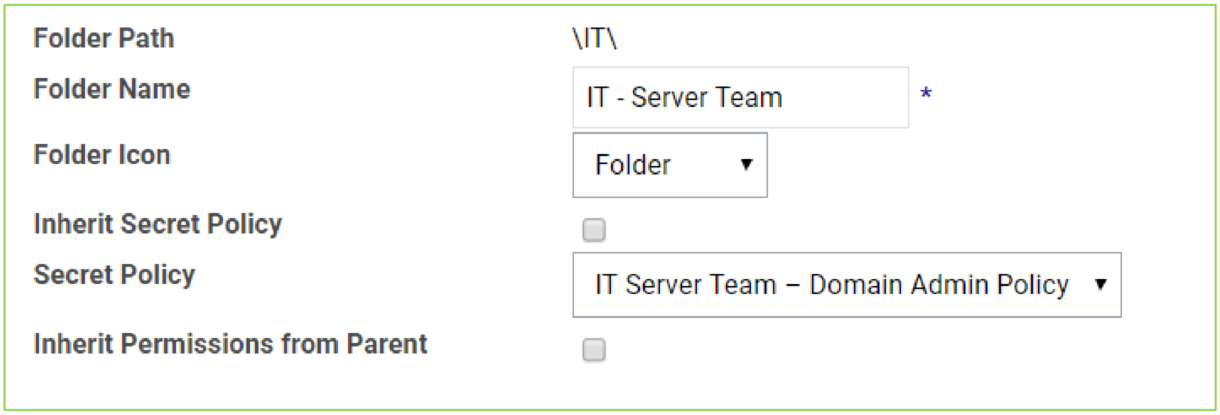
## Lab Exercise 12 - Creating a Secret Policy

In this exercise we will create a policy to define settings for secrets within the IT - Server Team folder

1. Navigate to the **Admin > Secret Policy page**
2. Click **Create New**
3. Create the policy with the following configuration:
4. Secret Policy Name: **IT Server Team – Domain Admin Policy**
5. Description:  **Defines secret security settings for secrets within the IT Server Team folder**
6. Active: **Checked**
7. Require Checkout: Setting: **Default / Value: Checked**
8. Custom Checkout Interval: **Setting: Default / Value: 120**
9. Enable Requires Approval for Access: **Not set**
10. Require Comment: Setting: **Default / Value: Checked**
11. Hide Launcher Password: **Setting: Enforced / Value Checked**
12. Enable SSH Command Restrictions: **Not Set**
13. Click **Save**

Now we will apply this policy to the IT – Server Team Folder

1. Navigate to the **Admin > Folders page**
2. Expand the **IT Folder**
3. Select the **IT – Server Team folder**
4. Click **Edit**
5. **Uncheck** Inherit Secret Policy
6. In the Secret Policy drop down select the new **IT Server Team – Domain Admin Policy**
7. Your configuration should match the image below



| | |
|---|---|
| Folder Path | \IT\ |
| Folder Name | IT - Server Team * |
| Folder Icon | Folder ▾ |
| Inherit Secret Policy | □ |
| Secret Policy | IT Server Team – Domain Admin Policy ▾ |
| Inherit Permissions from Parent | □ |

8. Click Save

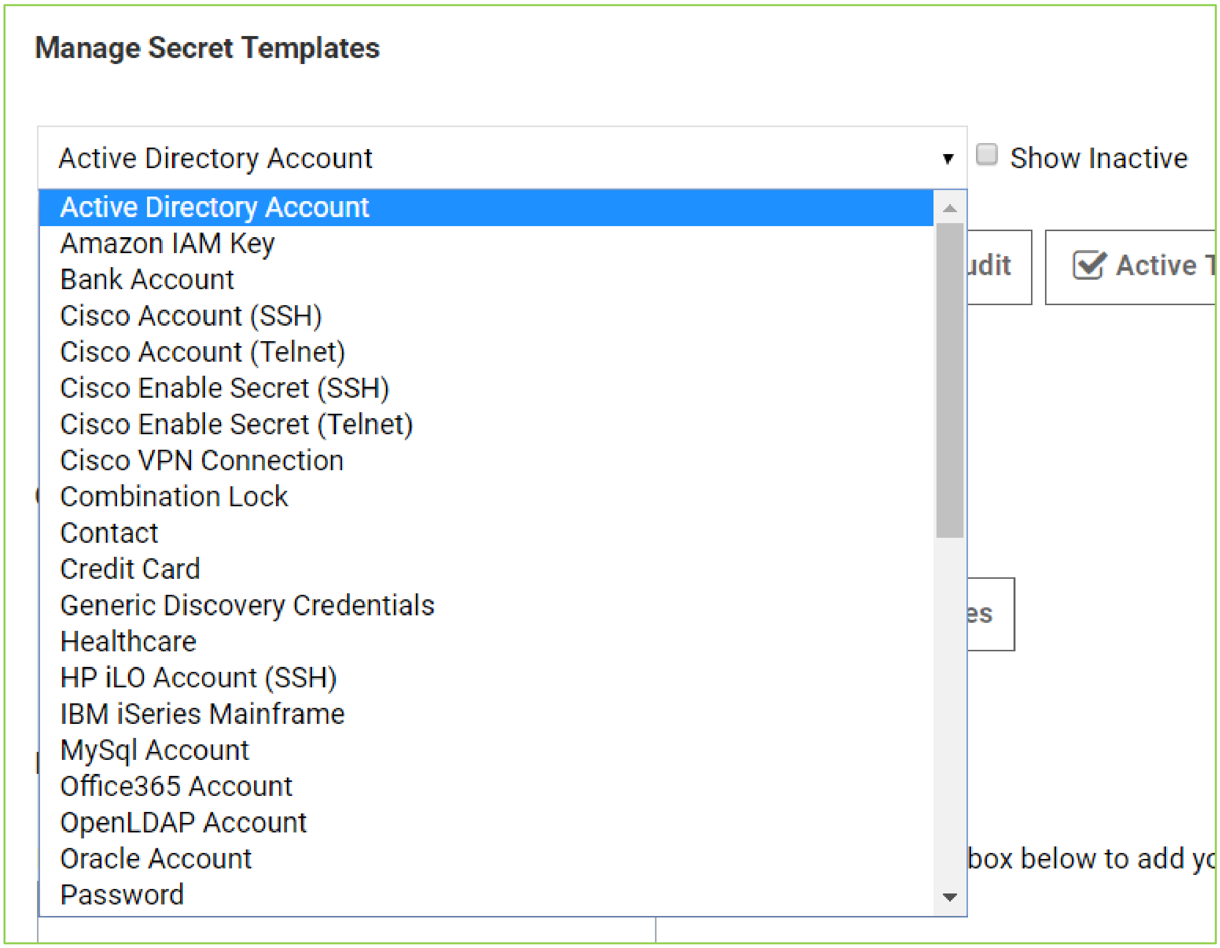
Any new Secrets created in the IT – Server Team folder will now have these security settings applied.

# Module 5 – Secret Templates

## 5.1 Built-In Secret Templates

When creating new secrets, a template is used to determine what information the secret should hold, password complexity requirements, launcher configuration and many other secret settings

Secret Server comes with a range of built-in secret templates. These templates can be viewed and edited by navigating to Admin>Secret Template and selecting the relevant template:



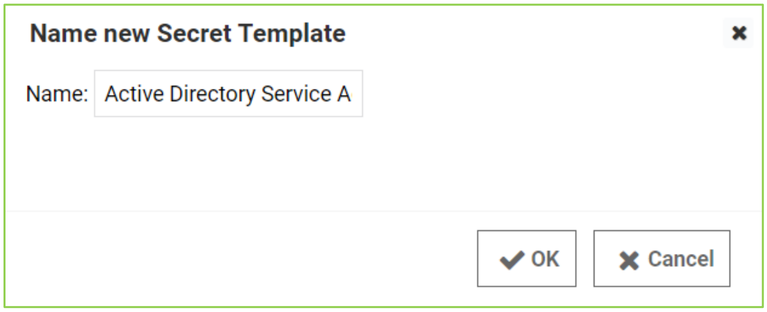
**Demo: At this point your trainer will demonstrate and explain the available configuration options within a Secret Template**

## Lab Exercise 13 - Creating a Secret Template for Active Directory service accounts

In this exercise we will be creating a Secret template that can be used for Active Directory service accounts. This template will be the same as the regular AD template, but we will remove the launcher. Because service accounts are used to provide a security context to an application, users should not be able to use the account interactively with a launcher.

As, in this case the Secret Template we are creating is very similar to the existing Active Directory account template we will create a copy rather than starting from scratch.

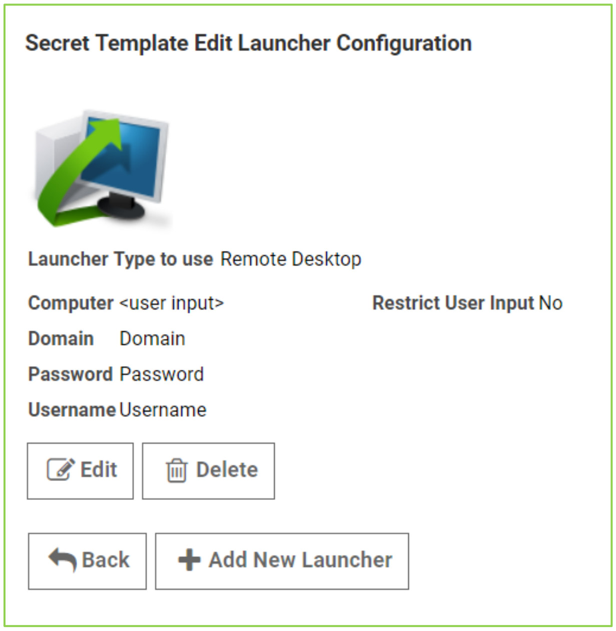
14. Navigate to the **Admin > Secret Templates** page
15. Make sure Active Directory Account is selected in the template drop-down menu
16. Click Edit
17. Click the **Copy Secret Template button**,
18. In the name new secret dialogue type: **Active Directory Service Account** as in the image below;



Name new Secret Template

Name: Active Directory Service A

19. Click **OK and continue**
20. In the new template select Configure Launcher



Secret Template Edit Launcher Configuration

Launcher Type to use Remote Desktop

Computer <user input>

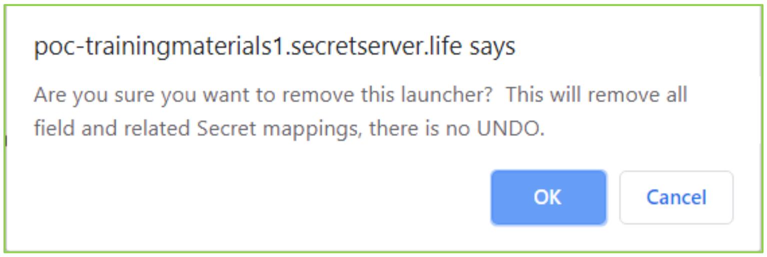
Restrict User Input No

Domain Domain

Password Password

Username Username

21. Click Delete and accept the following warning prompt:

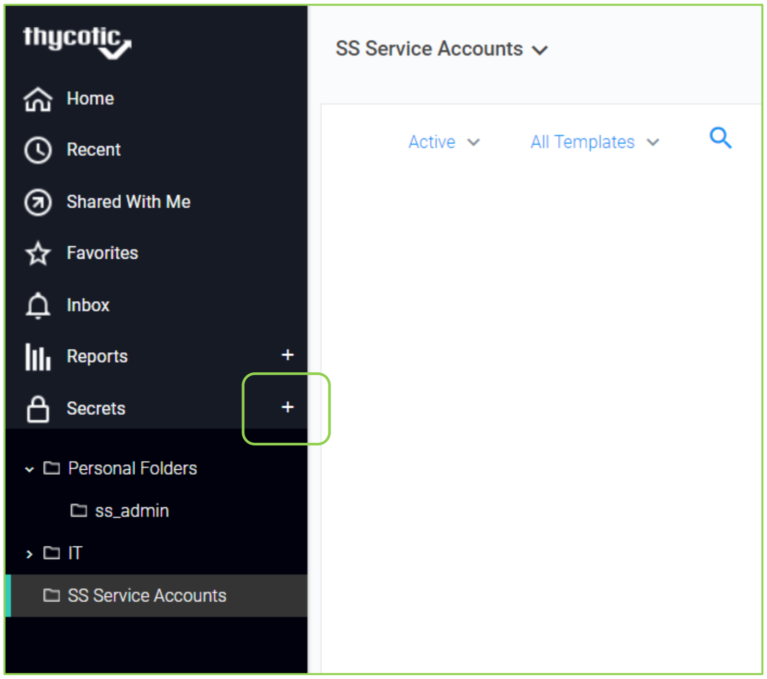


poc-trainingmaterials1.secretserver.life says

Are you sure you want to remove this launcher? This will remove all field and related Secret mappings, there is no UNDO.

We will now use this template to recreate the secret used Active Directory integration.

1. Navigate to the Home screen
2. Select the SS Service Accounts folder
3. Click the + Icon next Secrets (highlighted in the image below:

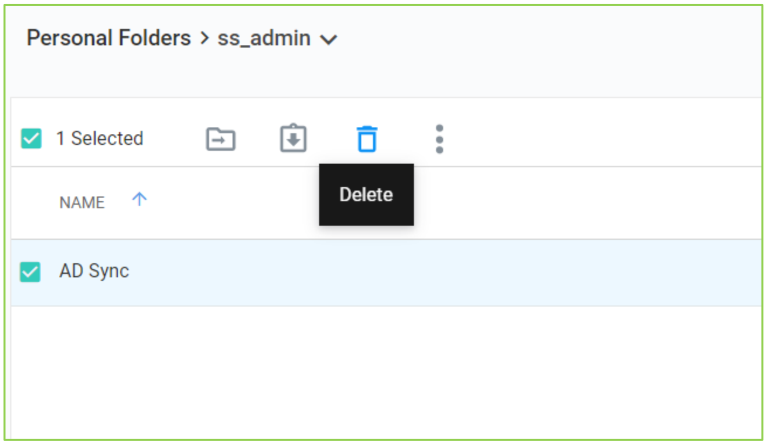


4. The new secret dialogue appears, select the newly created Active Directory Service Account template
5. Add the following detail into the secret:
6. Set Secret Name to **AD Sync**
7. Set Domain to **Thylab.com**
8. Set Username to **svc_sync**
9. Set Password to **Thycotic@2019!**
10. In the notes field, type **used for active directory integration and synchronization in Secret Server**
11. Leave the Folder, Inherit Security Policy and Secret Policy fields with the default values
12. Click **Create Secret**

Note: The new secret we have created does not have an RDP launcher so users cannot interactively use the credential from Secret Server.

We can now delete the first AD Sync secret from the SS_Admin personal folder

1. From the home screen, expand personal folders
2. Select SS_Admin
3. Check the box next to the AD Sync secret
4. Click the trashcan icon do delete

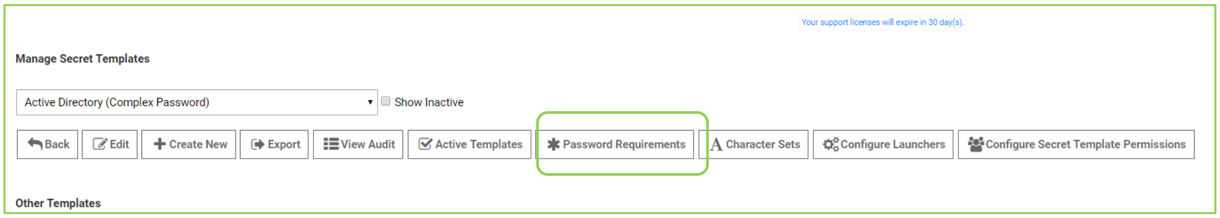


5. Now navigate to **Admin > Active Directory**
6. Click **Edit Domains**
7. Select the Thylab.com domain
8. Next to Sync Secret, click **Clear** to remove the secret we previously deleted
9. Click No Selected Secret and select the new AD Sync secret
10. Click **Save and Validate** to complete

## Lab Exercise 14 - Creating a Secret Template with custom password complexity requirements

In this exercise we will modify the Active Directory Service Account template created in exercise 13 with a more stringent password complexity requirement. This configuration can then be used to ensure that all secrets based on this template must have a customized password complexity requirement.

1. Navigate to the **Admin > Secret Templates** page
2. Click the **Password Requirements button**

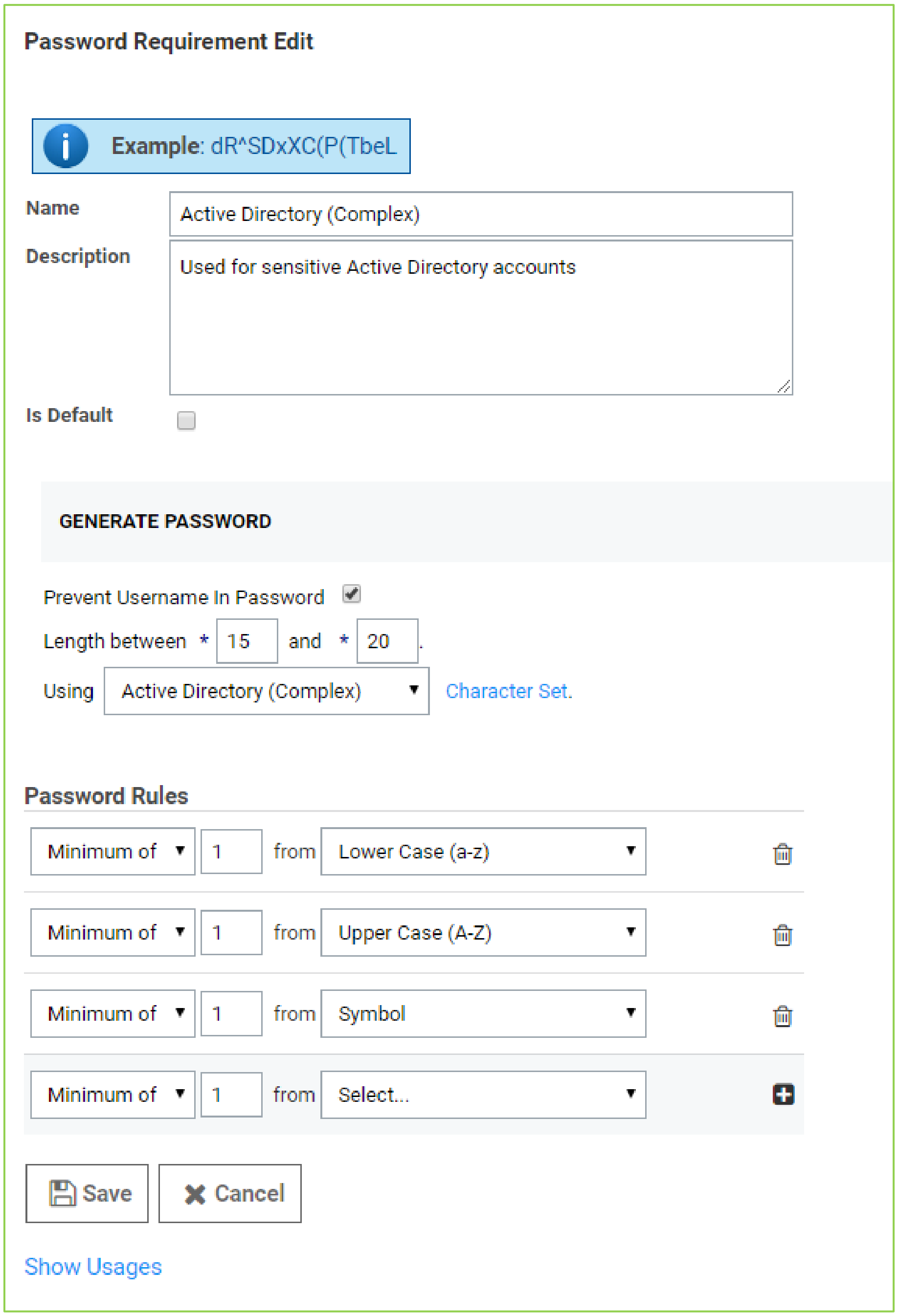


3. Click **Create New**
4. In the name new secret dialogue type: **Active Directory (Complex Password)** as
5. You will notice, only the Default, SAP and Mainframe password requirements exist
6. Click **Create New**

At this point we will create a custom character set to be used in the password requirement configuration:

7. Click the blue **Character Set text**, a new tab will open on the character set page
8. In the open row at the bottom of the page create a new character Set called **Active Directory (Complex)**
9. In the Character Set field copy the existing set from the **SAP character set.** This contains standard alphabetic characters in lower and upper case and a range of common symbols. Feel free to customize your own character set here.
10. Click the + symbol to the right of the new character set
11. Close the character set tab
12. Refresh the original password requirement page so that the new character set is displayed in the drop down
13. Create a new Password Requirement with the following configuration
    a. Name: Active Directory (Complex)
    b. Description: Used for sensitive Active Directory accounts
    c. Is Default: Unchecked
    d. Prevent username in password: Checked
    e. Length Between: 15 and 20
    f. Using: Active Directory (complex)
    g. Password Rule 1: Minimum of 1 from Lower Case
    h. Password Rule 2: Minimum of 2 from Upper Case
    i. Password Rule 3: Minimum of 3 from Symbol

14. Your configuration should match the image below:



**Password Requirement Edit**

**Example**: dR^SDxXC(P(TbeL

Name: Active Directory (Complex)

Description: Used for sensitive Active Directory accounts

Is Default: □

**GENERATE PASSWORD**

Prevent Username In Password ☑

Length between * 15 and * 20.

Using Active Directory (Complex) Character Set.

**Password Rules**

| | | | |
|---|---|---|---|
| Minimum of | 1 | from | Lower Case (a-z) |
| Minimum of | 1 | from | Upper Case (A-Z) |
| Minimum of | 1 | from | Symbol |
| Minimum of | 1 | from | Select... |

15. Click **Save**

Now we will assign the new password requirement to the Active Directory Service account template:

16. Navigate to the **Admin > Secret Templates** page
17. Select Active Directory Service Account from the dropdown
18. Click **Edit**

19. Click **Assign Password Requirement**
20. The default requirement is currently configured, to change click the edit button on the right of the screen
21. Select the new Active Directory (Complex) requirement from the dropdown
22. Click the Save icon on right of the screen

When any passwords are rotated for Secrets using this template, the new password requirement will be enforced.

**Demo: Your trainer will now demonstrate how to run a report of secrets that do not meet password complexity requirements.**

# Module 6 – Launchers

## 6.1 Launchers overview

Secret Server provides the ability to launch remote desktop or SSH sessions, run applications or log into web pages directly, using the credentials from a secret. This provides users with a ‘single pane of glass’ where they not only have access to all credentials required for a role but also all the tools necessary to perform tasks using the credentials.

The biggest benefit of launchers aside from this efficiency gain is that because Secret Server can seamlessly inject the credentials into the session, application or website, the user never needs visibility of the username and password. This means that passwords can be hidden from users, which, in turn provides a whole range of benefits:

- Prevents users from circumnavigating audit trails or monitoring from Secret Server or other security tools
- Prevents users from sharing credentials with non-authorized parties
- Allows for highly complex passwords as users don’t need to remember or input them
- Allows for regular password rotation

Out of the box, Secret Server provides the following launchers:

- Remote Desktop
- PuTTy
- Website Login
- Powershell Launcher
- SQL Server Management Studio Launcher
- Sybase isql Launcher
- z/OS Launcher
- IBM iSeries Launcher

In addition to these ‘out of the box’ launchers, custom launchers can be created to execute any process that can be executed from the command line. Secret Server can pass secret text fields such to seamlessly run applications with a range of command line arguments.

**Demo: Your trainer will now demonstrate a number of built in launchers and explain their functionality**

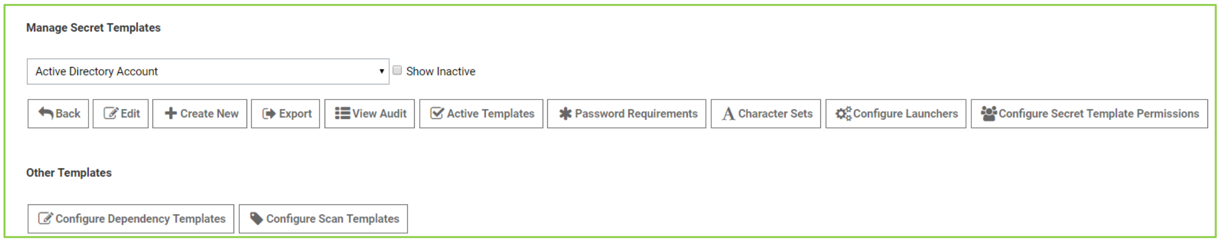
## Lab Exercise 15 - Creating a ‘restricted launch’ RDP launcher

The built-in remote desktop launcher allows the user to enter the hostname, fully qualified domain name (FQDN) or IP address of a target machine they want to connect to. In some scenario’s users may not know this information or we may only want them to able to connect to a defined list of endpoints. In this scenario a modified RDP launcher can be created with a defined list of target endpoints.

As launchers are linked to a secret template, the first step is to create a new template to contain the launcher

**Note: This lab exercise should be performed from the client lab machine (AWS-WIN-CLIENT1)**

1. Navigate to the **Admin > Secret Templates**



2. Make sure **Active Directory Account** is selected in the drop-down
3. Click **Edit**
4. Select **Copy Secret Template**
5. Name the new template: **Active Directory Account (Restricted Launch)**
6. Click **Continue**

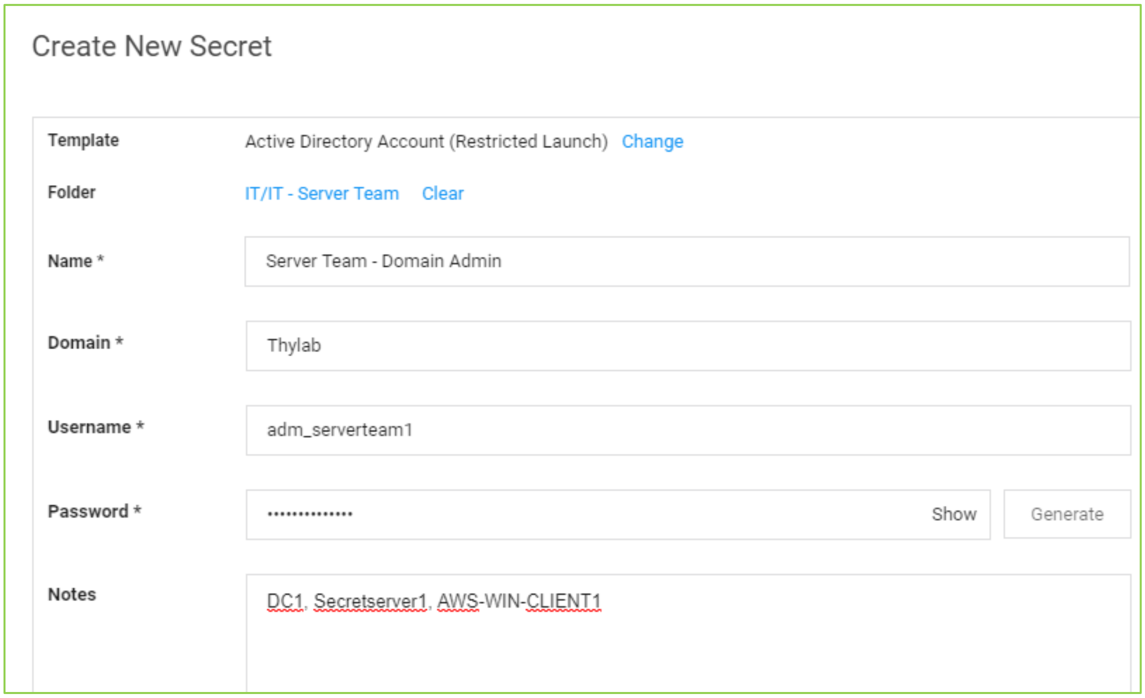
Now we can configure a modified RDP launcher for the new template

7. Select **Configure Launcher**
8. Click Edit
9. Leave all basic settings as they are
10. Under Advanced Settings, check **Restrict User Input**
11. Ensure the following settings are configured:
    a. Restrict as: **Whitelist**
    b. Restrict by Secret Field: **Notes**
    c. Include machines from dependencies: **Unchecked**
12. Click **Save**

This configuration means that the user will be presented with a list of endpoints to connect to that will be held in the Notes field of the secret. To test the new template and launcher we will create a secret to launch from.

13. From the **Home screen** expand the secret folder structure
14. Navigate to **IT > IT – Server Team**

15. Click the **+** icon next to Secrets to create a new secret in this folder
16. The **Create New Secret** Dialogue appears
17. Select **Active Directory Account (Restricted Launch)**
18. Configure the secret with the following settings:
    a. Name: **Server Team - Domain Admin**
    b. Domain: **Thylab**
    c. Username **adm_serverteam1**
    d. Password: **Thycotic@2019!**
    e. Notes: **DC1,Secretserver1,AWS-WIN-CLIENT1**
19. Your configuration should match the image below:

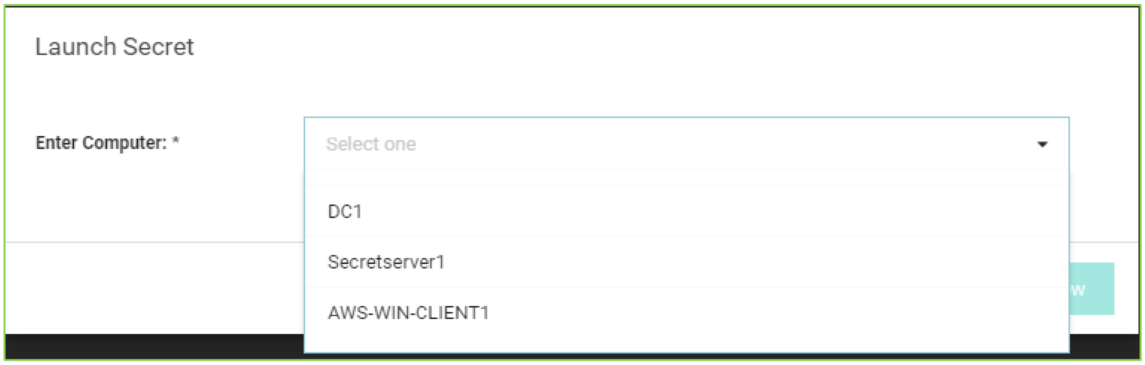


Create New Secret

| | |
|---|---|
| Template | Active Directory Account (Restricted Launch) Change |
| Folder | IT/IT - Server Team Clear |
| Name * | Server Team - Domain Admin |
| Domain * | Thylab |
| Username * | adm_serverteam1 |
| Password * | •••••••••••••• Show Generate |
| Notes | DC1, Secretserver1, AWS-WIN-CLIENT1 |

20. Click **Create Secret**
21. To test our configuration, open the secret (note: Because of the Secret Policy configured earlier, this secret will require checkout and comment) and select the launcher.

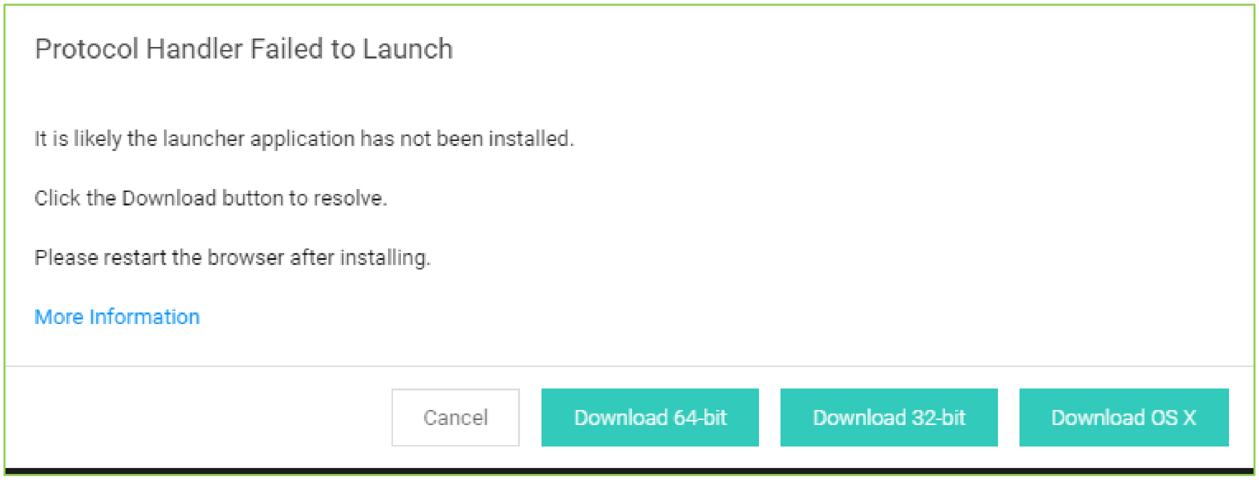
The user can only connect to the endpoints listed in the drop-down menu:



Launch Secret

Enter Computer: *

22. Select one of the endpoints, and click **Launch Now**
23. Note: if this is the first time the user has opened a Secret Server launcher they will prompted to download and install the Thycotic Protocol Handler:



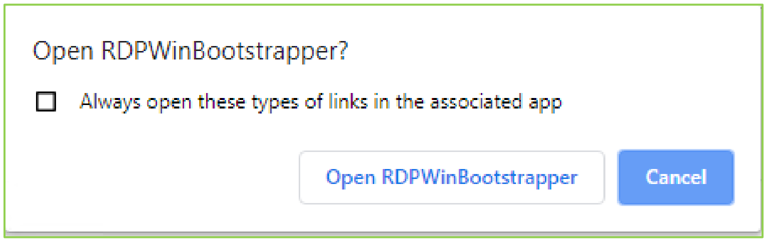
Protocol Handler Failed to Launch

It is likely the launcher application has not been installed.

Click the Download button to resolve.

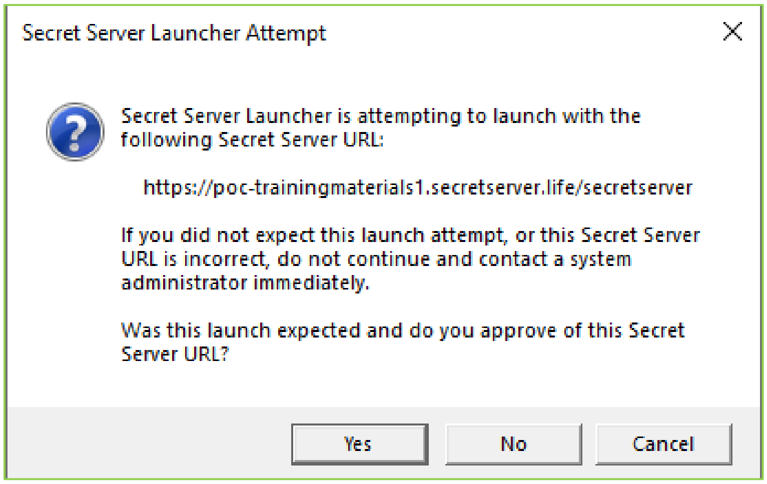
Please restart the browser after installing.

24. Download and install the 64bit version
25. Once installed, close the browser, reopen and navigate back to the secret
26. Relaunch the same launcher
27. Windows will now prompt the following warning messages



Open RDPWinBootstrapper?

□ Always open these types of links in the associated app



Secret Server Launcher Attempt

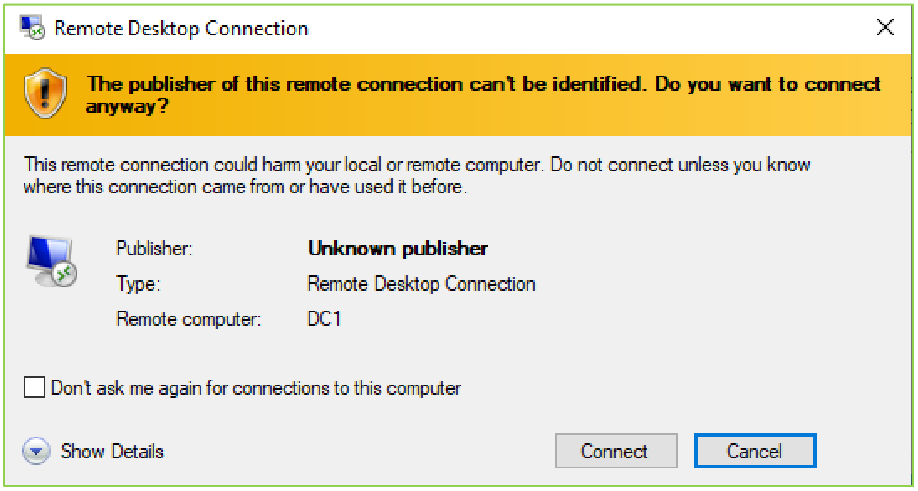
Secret Server Launcher is attempting to launch with the following Secret Server URL:

https://poc-trainingmaterials1.secretserver.life/secretserver

If you did not expect this launch attempt, or this Secret Server URL is incorrect, do not continue and contact a system administrator immediately.

Was this launch expected and do you approve of this Secret Server URL?

28. If you receive the following certificate warning in the lab, click **Connect** to proceed:



Remote Desktop Connection

**The publisher of this remote connection can't be identified. Do you want to connect anyway?**

This remote connection could harm your local or remote computer. Do not connect unless you know where this connection came from or have used it before.

Publisher: **Unknown publisher**
Type: Remote Desktop Connection
Remote computer: DC1

□ Don't ask me again for connections to this computer

29. Your RDP session should now be launched.

# Module 7 – Remote Password Changers

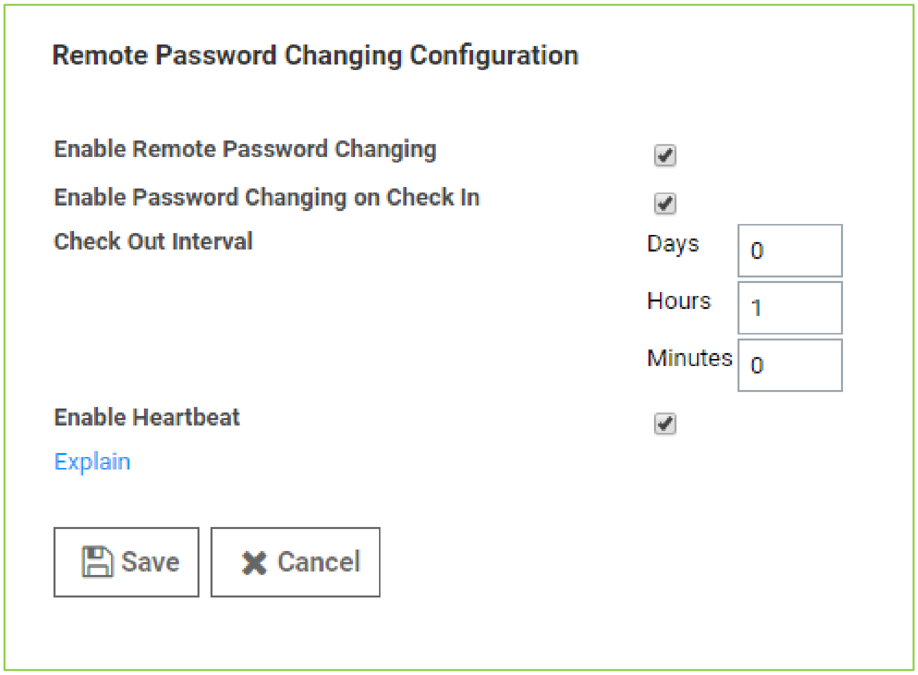
## 7.1 Remote password changing overview

As well as storing the credentials of privileged accounts, Secret Server provides the ability to rotate or change passwords for corresponding accounts in Active Directory, local machines, Unix/Linux machines or other devices manually or via an automated schedule. This functionality ensures you that all accounts can be configured to meet your internal password expiration or rotation policy or external compliance rules that you need to adhere to.

## Lab Exercise 16 – Enabling RPC

The first step to configuring remote password changing is to enable the feature in configuration:

1. Navigate to **Admin > Remote Password Changing**
2. Click Edit
3. Check **Enable Remote Password changing**
4. Check **Enable Password Changing on Check In**
5. Set the **Check Out Interval** to **1 hour**
6. Check **Enable Heartbeat**
7. Your configuration should match the image below:



Remote Password Changing Configuration

Enable Remote Password Changing ☑

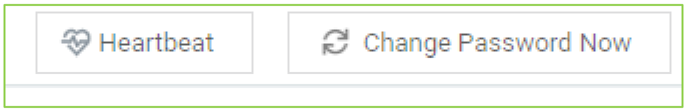
Enable Password Changing on Check In ☑

Check Out Interval Days 0 Hours 1 Minutes 0

Enable Heartbeat ☑

8. Click **Save**

9. To test the configuration, navigate to the **server team - domain admin secret** crated earlier
10. You will now see two new options in the top-right of the secret view:

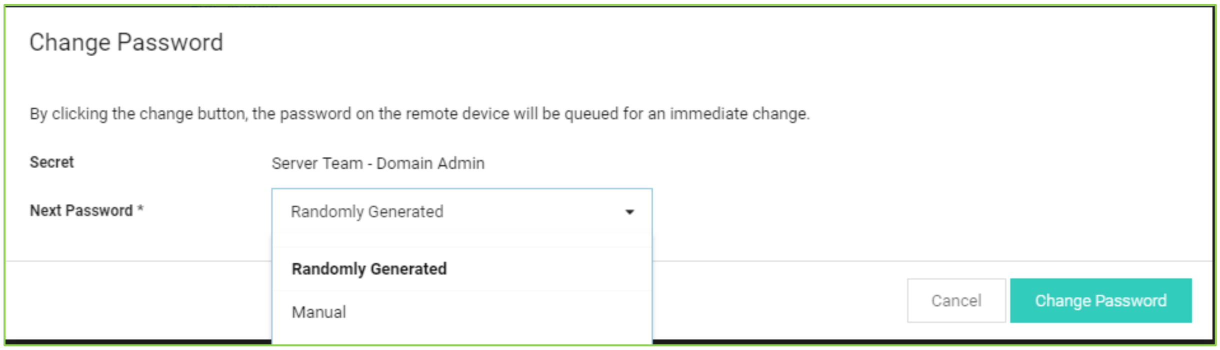


## Lab Exercise 17 – Manually changing a password

Now that RPC has been enabled, all secrets will have a Change Password Now and Heartbeat option visible in the secret view. This allows a user with the relevant permission to change a password at any time.

To change a password:

1. Within the Secret View select the **Change Password Now** option, the change password dialogue is displayed:

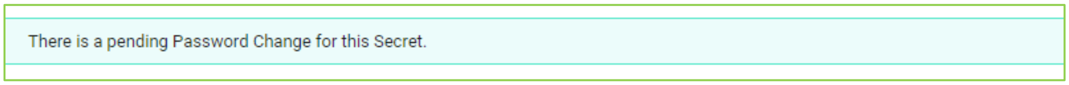

Change Password

By clicking the change button, the password on the remote device will be queued for an immediate change.

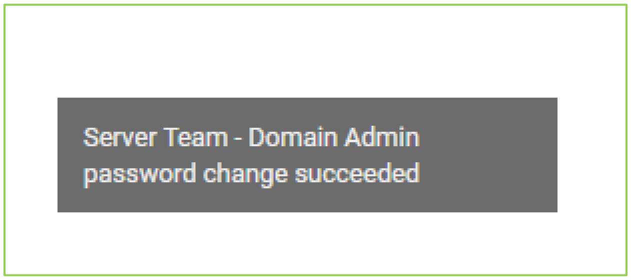
Secret: Server Team - Domain Admin

Next Password *: Randomly Generated

2. Choose either option (change using a generated password or define a new password manually)
3. Click Change Password
4. At the top of the secret the following message is displayed:


There is a pending Password Change for this Secret.

5. Once successful the following message is displayed:

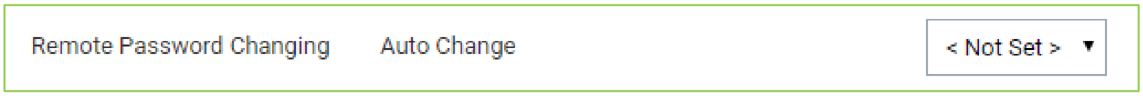

Server Team - Domain Admin password change succeeded

## 7.2 RPC Auto Change

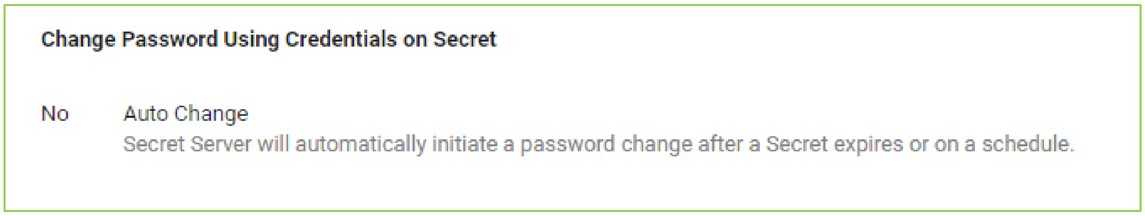
As we have previously seen, once RPC is configured users within sufficient permissions can manually rotate and validate passwords whenever required. For many secrets we will want to ensure that passwords are rotated on a regular schedule without the need for user intervention.

For automatic password changing there are a number of configuration options to consider:

- The Secret Template used to configure the secret must have password changing enabled
- The Expiration Days field on the secret template or secret itself (Once the secret has expired, remote password configuration will apply)
- Is Remote Password Changing configured within the applied secret policy?


Remote Password Changing Auto Change < Not Set >

- Is remote password changing configured on the secret itself?


Change Password Using Credentials on Secret

No Auto Change
Secret Server will automatically initiate a password change after a Secret expires or on a schedule.

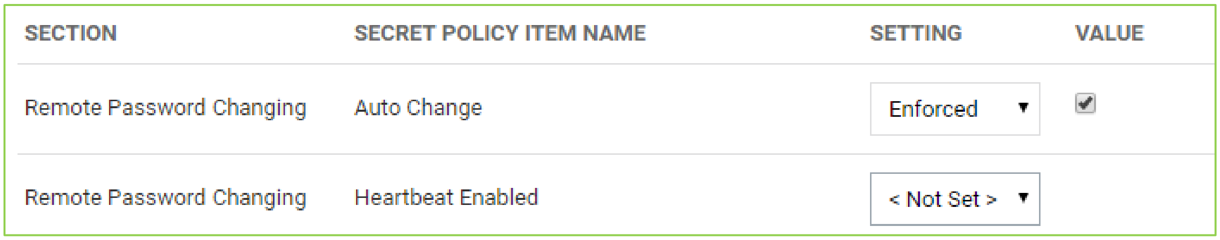
**Note: The fact that RPC can be configured (and enforced) provides a high level of granularity.**

If ALL secrets with a specific policy require RPC can then this should be enforced. Otherwise the RPC option in the secret policy can be left unset and RPC configured on individual secrets.

## Lab Exercise 18 – Configuring RPC auto change

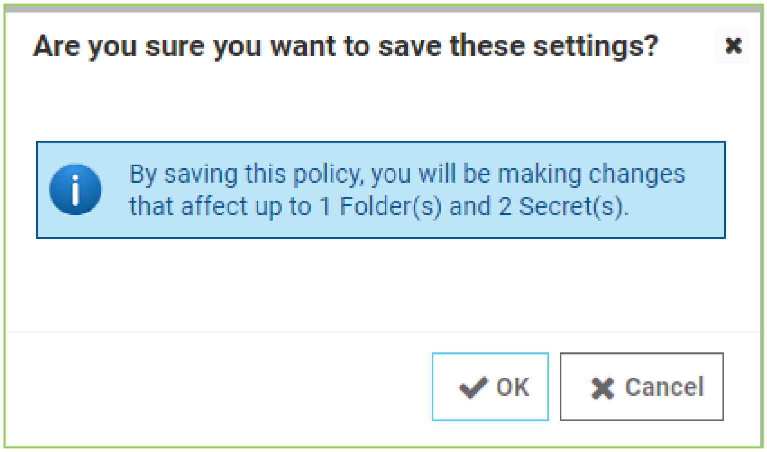
In this exercise we will assume that all secrets with the **IT Server Team – Domain Admin** Policy applied should be configured for RPC auto change.

1. Navigate to **Admin > Secret Policy**
2. Select **IT Server Team – Domain Admin**
3. Click **Edit**
4. Find the Remote **Password Changing – Auto Change** option and set to **Enforced** and ensure the Value is **checked**



| SECTION | SECRET POLICY ITEM NAME | SETTING | VALUE |
|---|---|---|---|
| Remote Password Changing | Auto Change | Enforced ▾ | ☑ |
| Remote Password Changing | Heartbeat Enabled | < Not Set > ▾ | |

5. Scroll to the bottom of the screen and click **Save**
6. As the Enforced option will actively change settings on existing secrets, the following warning is shown:



Are you sure you want to save these settings?

By saving this policy, you will be making changes that affect up to 1 Folder(s) and 2 Secret(s).

7. Click **OK**

To validate, open a secret with the IT Server Team – Doman Admin Policy applied and navigate to the RPC tab. The secret should now be configured for automatic password changing.

# Module 8 – Discovery

## 8.1 Discovery overview

Once basic configuration tasks have been completed such as the creation of folders, templates and policies, secrets can now be added to Secret Server. Although secrets can be added manually this can be time consuming in large environments. Secret Server provides the Discovery functionality to automatically find the following accounts:

- Active Directory user accounts
- Active Directory service accounts
- Local Windows accounts
- Unix / Linux accounts
- VMware ESX/ESXi accounts
- Many more with extensible discovery

Once found, accounts can then automatically be pulled into Secret Server. The configured secret templates, folder structure and policies will ensure that secrets have all relevant settings automatically applied.

## Exercise 19 – Enabling Discovery

To enable discovery in Secret Server:

1. Navigate to **Admin > Discovery**
2. Click **Edit**
3. Select the **Enable Discovery checkbox**
4. Leave the **Default Synchronization Interval for Discovery at 1 Day**
5. Click **Save**

Now that discovery is enabled, we can start to create discovery sources to look for accounts in different locations:

In this section we will perform discovery in the following areas:

- Active Directory
- Local Windows Accounts
- Linux / Unix Accounts

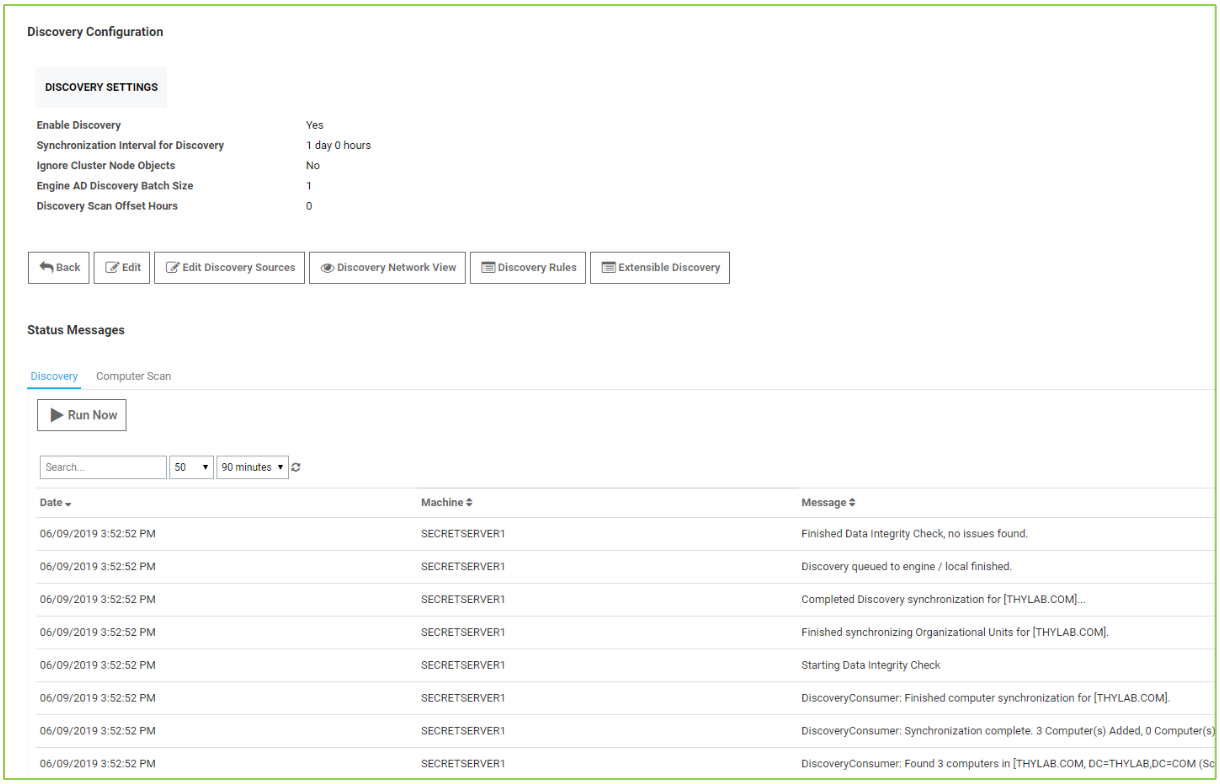
## Exercise 20 – Configuring Active User Account Directory Discovery

1. Navigate to the **Admin > Discovery page**
2. Click **Edit Discovery Sources**
3. Click **Show Inactive and Disabled**, the Thylab.com domain will appear as we did not configure discovery when the domain was added earlier
4. Select the Thylab.com domain
5. Change the **Enable Discovery field** to **Entire Domain**
6. Set Credential Secrets to **Use Sync Credentials**

**Note: For more information on the permissions required by accounts used for discovery purposes check the following KB article:**

https://thycotic.force.com/support/s/article/Account-Permissions-for-Discovery?topicName=Secret+Server&topicId=0TO370000008fpDGAQ

7. Switch to the **Scanner Settings** Tab
8. Under Find Accounts notice that only **Windows Local Accounts** are listed. Click **Add New Account Scanner**
9. Select **Active Directory User Accounts**, leave the group filter blank
10. Click **OK**
11. Click **Back**
12. Click **Save and Validate**
13. Click **Back** to return to the Discovery page
14. To discover computers within the Thylab.com domain, click **Run Now**



Discovery Configuration

DISCOVERY SETTINGS

| | |
|---|---|
| Enable Discovery | Yes |
| Synchronization Interval for Discovery | 1 day 0 hours |
| Ignore Cluster Node Objects | No |
| Engine AD Discovery Batch Size | 1 |
| Discovery Scan Offset Hours | 0 |

Status Messages

| Date | Machine | Message |
|---|---|---|
| 06/09/2019 3:52:52 PM | SECRETSERVER1 | Finished Data Integrity Check, no issues found. |
| 06/09/2019 3:52:52 PM | SECRETSERVER1 | Discovery queued to engine / local finished. |
| 06/09/2019 3:52:52 PM | SECRETSERVER1 | Completed Discovery synchronization for [THYLAB.COM]... |
| 06/09/2019 3:52:52 PM | SECRETSERVER1 | Finished synchronizing Organizational Units for [THYLAB.COM]. |
| 06/09/2019 3:52:52 PM | SECRETSERVER1 | Starting Data Integrity Check |
| 06/09/2019 3:52:52 PM | SECRETSERVER1 | DiscoveryConsumer: Finished computer synchronization for [THYLAB.COM]. |
| 06/09/2019 3:52:52 PM | SECRETSERVER1 | DiscoveryConsumer: Synchronization complete. 3 Computer(s) Added, 0 Computer(s) |
| 06/09/2019 3:52:52 PM | SECRETSERVER1 | DiscoveryConsumer: Found 3 computers in [THYLAB.COM, DC=THYLAB,DC=COM (Sc |

15. Click the refresh wheel under Run Now to see an updated audit of discovery activity
16. To view and explore the results, click the **Discovery Network View**

**Demo: Your trainer will now demo several options around importing secrets from Discovery and creating automated discovery rules**

# Module 9 – Auditing and Security

## 9.1 Auditing and Security Overview

In this module we will explore a range of auditing and security functionality within Secret Server. This area is of particular importance as most Thycotic Secret Server customers use this functionality to ensure they adhere to various internal and external compliance regulations.

## 9.2 Secret Server Reporting

Secret Server provides a comprehensive range of audit reports out of the box. The available reports are designed to help users answer questions about secrets, users, compliance and administrative behavior.

To view reports, select the Reports button from the left-hand column. On the reporting page there are three tabs, General, Security Hardening, User Audit.

General – Contains a range of reports separated into different areas such as Activity, Secrets, Password compliance etc.

Security Hardening – Contains the security hardening report which we have previously used to identify and configure security configuration to harden the Secret Server installation

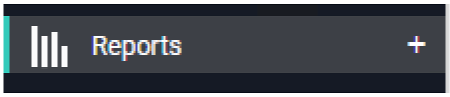
User Audit – Contains a report to monitor specific user activity and expire and secrets a targeted user has interacted with.

Although the out of the box reports provide most customers with all the visibility and intelligence they typically need, it is possible to create custom reports within the Secret Server interface. In the next lab exercise we will configure a custom report.

## Lab Exercise 21 – Configuring a Custom Report

In this exercise we will configure a custom report to show the start date and end date details for all remote sessions.

1. Click the + icon next to Reports in the right-hand column



2. Configure the report with the following detail:
    a. Report Name: **Remote Sessions – Start and End date**
    b. Report Description: **Shows the start and end date detail of all remote sessions launched from Secret Server**
    c. Report Category: **User**

d. Chart Type: **None**
e. Page Size: **15**
f. Report SQL: Paste the following

```
SELECT
        u.userid
        ,u.username
        ,u.displayname
        ,s.SecretId
        ,s.SecretName
        ,CAST(ls.[SessionGuid] AS VARCHAR(40)) as SessionGuid
        ,ls.[StartDate]
        ,ls.[EndDate]
        ,ls.[Status]
        ,ls.[Duration]
     FROM dbo.tbLauncherSession ls
     INNER JOIN tbSecretSession ss ON ls.SessionGuid =
ss.LauncherSessionGuid
     INNER JOIN tbSecret s ON ss.SecretId = s.SecretID
     INNER JOIN tbfolder f ON f.FolderID = s.FolderId
     INNER JOIN tbUser u ON u.UserId = f.UserId
     WHERE
        ls.StartDate >= DATEADD(day, -7, GETUTCDATE()) AND --in the last 7 days
        ls.[Duration] > 5 --duration is more than 5 seconds
```

3. Click Save
4. If any sessions have been launched that match the criteria, they should now be visible in the custom report

## 9.3 Event Subscriptions

Secret Server can be configured to generate an Event Subscription or alert for virtually any action that is carried out within the system. This functionality means that whenever a particular action is performed, a defined list of users (or email distribution groups) can be notified automatically

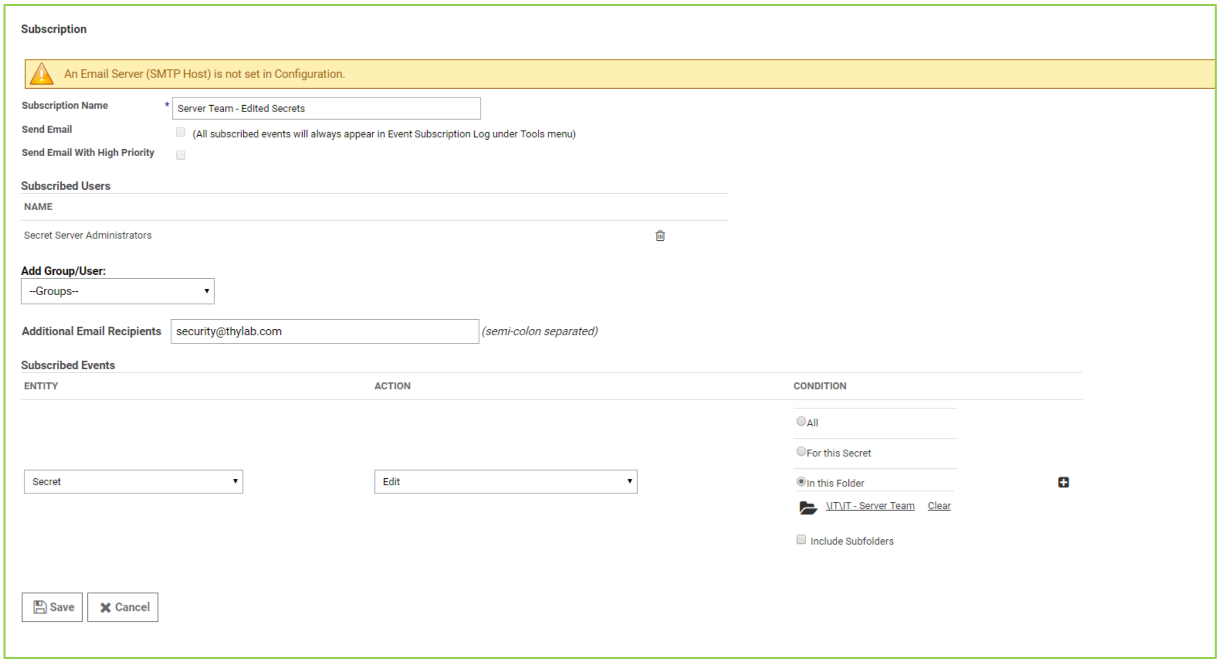
**Important: Thycotic recommends using Event Subscriptions sparingly, if users are bombarded with too many alerts they can quickly be perceived as spam and loose importance.**

### Lab Exercise 22 – Configuring an Event Subscription

In this exercise we will configure an event subscription that will alert specific users if any secret in the IT – Server Team folder is edited.

Note: The training lab does not currently contain an SMTP server so this event subscription can be configured but will not generate any email alerts.

1. Navigate to the **Admin > See All page**
2. Select **Event Subscriptions**
3. Click the **New Button**
4. Create a new subscription with the following configuration
   - **4.1.** Subscription Name: **Server Team – Edited Secrets**
   - 4.2. Send Email: **Unchecked (this cannot be checked in the lab due to the lack of SMTP Server)**
   - 4.3. Send Email with High Priority: **Unchecked**
   - 4.4. Add Group/User: **Thylab\Secret Server Administrators**
   - 4.5. Additional Email Recipients: security@thylab.com
   - 4.6. Subscribed Events Entity: **Secret**
   - 4.7. Subscribed Events Action: **Edit**
   - **4.8.** Condition: **In this folder (Select IT – Server Team)**
5. Your configuration should match the image below:



Subscription

⚠ An Email Server (SMTP Host) is not set in Configuration.

Subscription Name * Server Team - Edited Secrets

Send Email □ (All subscribed events will always appear in Event Subscription Log under Tools menu)

Send Email With High Priority □

Subscribed Users

| NAME |
|---|
| Secret Server Administrators |

Add Group/User: --Groups--

Additional Email Recipients security@thylab.com *(semi-colon separated)*

Subscribed Events

| ENTITY | ACTION | CONDITION |
|---|---|---|
| Secret | Edit | ○ All<br>○ For this Secret<br>● In this Folder<br>\IT\IT - Server Team Clear<br>□ Include Subfolders |

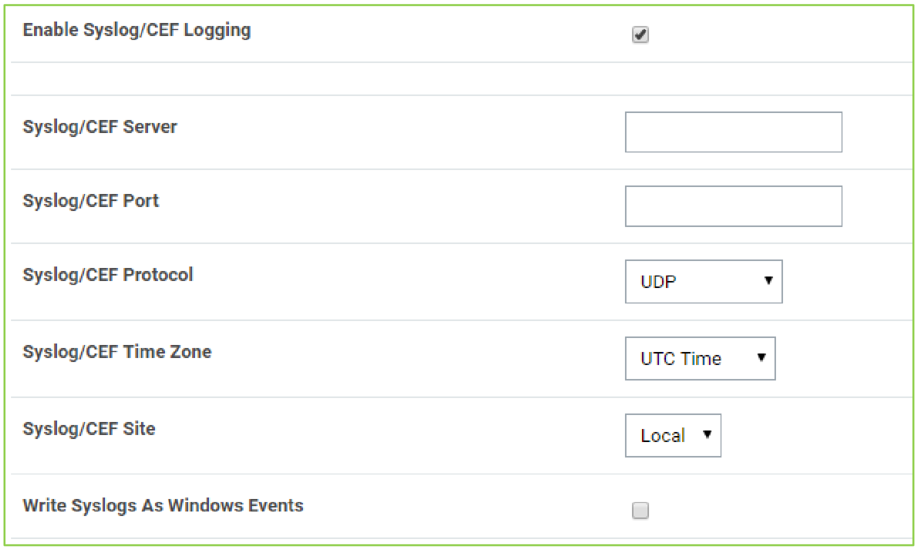
6. Click **Save**
7. To test the subscription, edit a secret in the IT – Server Team folder in some way. The email will not be generated but the event should be visible in the **Event Subscription Log under the Tools menu**

## 9.4 SIEM integration

Secret Server can easily be configured to forward all auditing information to SIEM solution. This is typically achieved using Syslog/CEF output.

To configure SIEM integration:

1. Navigate to Admin > Configuration
2. Enable Syslog/CEF logging and specify the Syslog/CEF server
3. The available configuration options are visible in the image below:



| | |
|---|---|
| Enable Syslog/CEF Logging | ☑ |
| Syslog/CEF Server | |
| Syslog/CEF Port | |
| Syslog/CEF Protocol | UDP |
| Syslog/CEF Time Zone | UTC Time |
| Syslog/CEF Site | Local |
| Write Syslogs As Windows Events | ☐ |

## 9.4 Privileged Behavior Analytics (PBA)

Privileged Behavior Analytics can help IT and Security administrators quickly detect breaches before they happen, analyze distribution of privileged accounts and access across your organization, and add a layer of security to your Secret Server deployment. Free up the time of Secret Server administrators to focus on discovering, managing, and protecting your privileged account credentials.

PBA is a cloud-based solution that can be used with both Secret Server on premise and Secret Server cloud. PBA is not currently available in the training lab environment, but your trainer will now demonstrate PBA and discuss common use cases and configuration.

**Demo: Your trainer will now demonstrate Privileged Behavior Analytics**

## 9.5 Session Recording and Monitoring

As previously discussed, Secret Server audits all user activity, including secret and launcher access. In many scenarios, as well as being able to audit the fact that a user accessed a secret and launched a session, organizations may need to record the content of launched sessions. Secret Sever session monitoring allows for the recording of any RDP or Putty session launched via Secret Server or from external sessions.

Within Secret Server there are, effectively two types of session recording. Basic session recording provides a video of a launched RDP or SSH session. Advanced session recording provides the video recording and additional session metadata such as launched process detail, keystroke logging. When advanced session recording is configured, users can search for keystrokes or applications across sessions, and the session playback interface shows additional activity information mapped to the video.

There are some important considerations about the different types of session recording available:

- Basic RDP/SSH session recording relies on the locally installed protocol handler to record video.
- RDP metadata collection relies on the configuration of advanced session recording and the installation of the Advanced Session Recording Agent (ASRA) on the target endpoint
- SSH metadata collection relies on the Secret Server SSH proxy (this will be discussed in a later module)

### Lab Exercise 23 – Configuring session recording

In this exercise we will configure basic session recording so that RDP sessions and SSH (Putty) sessions launched from Secret Server are recorded and can be viewed within the console

We will first enable session recording, then configure specific secrets to be recorded.

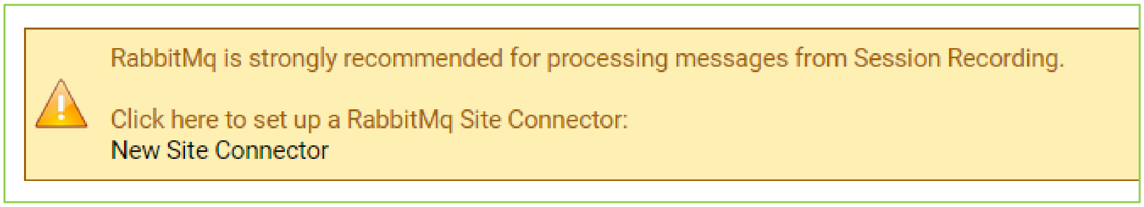
1. Navigate to **Admin > Configuration**
2. Select the **Session Recording Tab**, session recording is currently not configured
3. Click **Edit**
4. Check the **Enable Session Recording box,** several additional options will now appear
5. Configure the session recording options as follows:
   5.1. Hide recording indicator: leave unchecked (users will know the session is being recorded)
   5.2. Enable on demand video processing: **Checked** (Enable On-Demand Video Processing” option in SS which leaves the recordings in WEBM format, which Chrome and Firefox can playback without any further processing, saving server

processing time. If an on-demand recording is viewed with Internet Explorer or Edge (which do not support WEBM playback), you can click a “Request Video Processing” button and the video will be converted to H.264/MP4, which they can then play. If “Enable On-Demand Video Processing” is not checked, then all sessions recorded by the Windows protocol handler will be automatically converted to H.264/MP4.)

5.3. Enable inactivity timeout: Checked (Default)
5.4. Inactivity Timeout (Minutes): 120 (Default)
5.5. Max session length (hours): 24 (Default)
5.6. Use Hardware Acceleration: Checked (Default)
5.7. Save Videos To: Database (Default)

6. Click Save

Note: You will see a warning at the top of the page (image below):



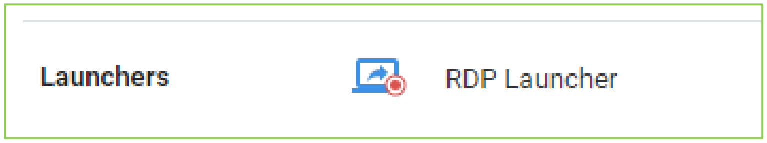
RabbitMq is strongly recommended for processing messages from Session Recording.

Click here to set up a RabbitMq Site Connector:
New Site Connector

For testing and proof of concept deployments, SS's Internal Site Connector is sufficient for session recording. For production deployments we strongly recommend RabbitMQ for a more-robust message queue.

Now that session recording has been configured, we can enable session recording on a secret.

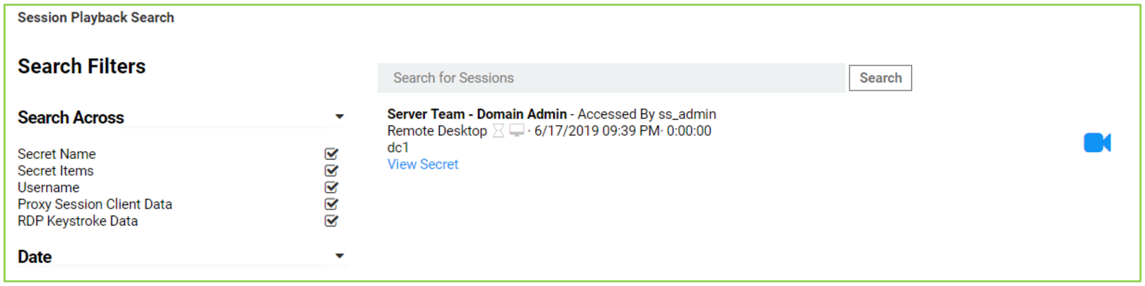
1. Navigate to the **Server Team – Domain Admin Secret**
2. Select the **Security tab** from the secret view
3. Click **Edit** next to the **Other Security section**
4. Set **Session Recording Enabled** to **checked**
5. Click **Save**
6. Select the General tab, notice that the Launcher icon has changed to reflect the configuration change (image below:



Launchers RDP Launcher

7. To test, ensure you are logged on to the **AWS-WIN-CLIENT1** machine and launch from the **Server Team – Domain Admin secret** to **DC1**
8. Perform a test action such as adding a user to Active Directory, then end your RDP session.
9. Go to the Audit tab of the secret, you should see the launch action, under session recording the message Waiting to process Movie should be displayed

10. After a minute or so, the Recording will be visible in the Session Monitoring console. Navigate to **Admin > Session Recording**



Session Playback Search

**Search Filters**

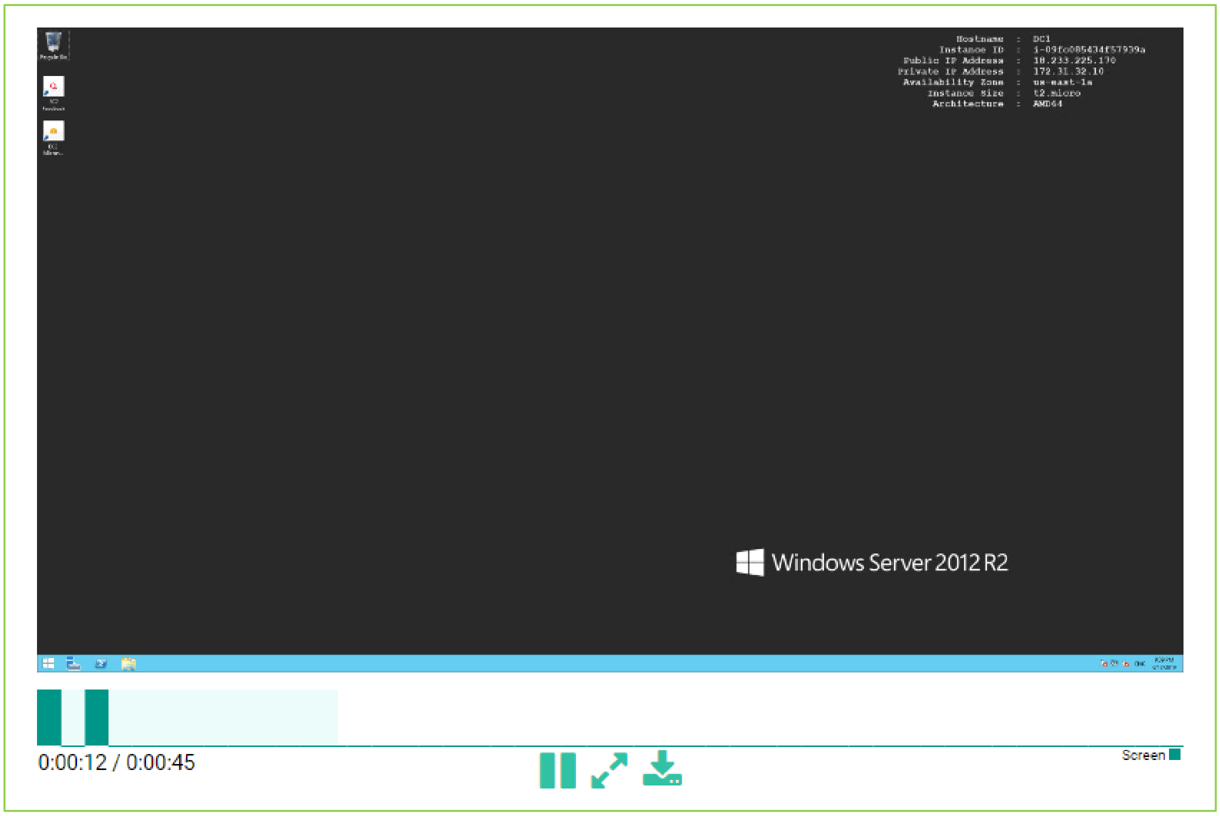
**Search Across**

Secret Name ☑
Secret Items ☑
Username ☑
Proxy Session Client Data ☑
RDP Keystroke Data ☑

**Date**

**Server Team - Domain Admin** - Accessed By ss_admin
Remote Desktop · 6/17/2019 09:39 PM· 0:00:00
dc1
View Secret

11. Select the recording and press play to watch it:



```
        Hostname  :  DC1
     Instance ID  :  i-09fc085434f57939a
Public IP Address  :  18.233.225.170
Private IP Address  :  172.31.32.10
Availability Zone  :  us-east-1a
   Instance Size  :  t2.micro
    Architecture  :  AMD64
```

0:00:12 / 0:00:45

**Note: At this point your trainer will discuss the configuration of Advanced Session Recording which cannot be completed yet as an additional site is required**