

# IBM Security Secret Server

Version 10.7

## *Administration Guide*

IBM

# Table of Contents

<b>Introduction .....</b>	<b>1</b>
Purpose.....	1
Terms and Definitions .....	1
Document Conventions .....	4
Additional Resources.....	5
Secret Server Redesign Onboarding Wizard .....	6
<b>Getting Started with Secret Server.....</b>	<b>7</b>
Topic 1: Trial Installation and Proof-of-Concept Prerequisites .....	7
System Requirements .....	7
Hardware Requirements .....	7
Software Requirements.....	7
Application Configuration.....	8
Topic 2: Installing Secret Server .....	9
Process .....	9
Licenses .....	9
Topic 3: The Secret Server Dashboard.....	10
Topic 4: Applying Security Best Practices .....	10
Local Admin Account Best Practices .....	11
SSL (HTTPS) Best Practice .....	11
Topic 5: Configuring Backups.....	11
Topic 6: Integrating with Active Directory .....	12
Setting up Active Directory.....	12
Enabling Active Directory Users.....	12
Managing Active Directory Users via a Distributed Engine.....	12
Topic 7: Creating Secret Server Infrastructure and Secrets .....	12
Topic 8: Running Discovery .....	12
Topic 9: Configuring Remote Password Changing.....	13
Enabling Remote Password Changing .....	13
Performing a Manual RPC.....	13
Common RPC Error Codes.....	13

Topic 10: Configuring Heartbeat .....	13
Enabling Heartbeat .....	13
Running Heartbeat.....	13
Topic 11: Running Audits and Reports .....	13
Topic 12: Controlling Secret Access and Workflow.....	14
Topic 13: Accessing Remote Machines with Secret Launchers.....	14
Topic 14: Recording Sessions .....	15
Topic 15: Accessing Secret Server with APIs and the CLI .....	15
Topic 16: Finding Additional Resources for Secret Server .....	17
<b>Secret Server Dashboard.....</b>	<b>18</b>
Overview .....	18
Dashboard Widgets .....	18
Managing Widgets .....	19
Customizing Dashboard Tabs.....	19
Overview Tab .....	19
Running Dashboard Bulk Operations .....	20
Secrets .....	21
Introduction.....	21
Secret Tabs .....	21
Secret Configuration Options .....	24
Managing Secrets .....	24
Secret Folders.....	33
Introduction.....	33
Managing Folders .....	35
Secret Templates.....	50
Secret Template Settings .....	50
Template Character Sets.....	51
Template Password Requirements.....	52
Template Naming Patterns .....	58
SSH Authentication Templates .....	58
Managing Secret Templates.....	59
Searching Secrets.....	67
Search Indexer .....	68

Importing Secrets .....	70
Introduction .....	70
Configuring Data for Importation .....	71
Importing Secrets with the Secret-Server Migration Tool.....	73
Importing Secrets with Advanced XML Importation .....	73
Secret Launchers .....	74
Introduction .....	74
Built-In Launcher Types .....	74
Enabling Launchers .....	74
Launching Sessions .....	76
Remote Desktop Launchers .....	76
Web Launchers .....	77
Launcher Configuration and Support .....	87
Secret Expiration .....	95
Secret DoubleLocks .....	97
Introduction .....	97
Using a DoubleLock .....	98
Creating a DoubleLock and a DoubleLock Password.....	99
Assigning a User a DoubleLock Password .....	101
Assigning a DoubleLock to a Secret .....	102
Assigning Users to Existing DoubleLocks .....	105
Resetting a DoubleLock Password.....	108
Secret Check-Outs.....	110
Introduction .....	110
Configuring Password Changing on Check in.....	110
Checking Out Secrets .....	110
Configuring a Secret for Check Out .....	111
Exclusive Access.....	111
Check-Out Hooks.....	111
Secret Access Requests .....	112
Basic Secret-Access Requests.....	112
Advanced Secret-Access Requests with Workflow Templates .....	115
Remote Password Changing (RPC) .....	135

Introduction .....	135
Remote Accounts Supported .....	135
Enabling RPC.....	135
Automatic RPC (AutoChange) .....	135
Privileged Accounts and Reset Secrets .....	136
Run a Manual RPC.....	136
Mapping Account Fields for RPC .....	137
RPC Ports .....	138
RPC Logs .....	139
RPC Error Codes .....	139
RPC for Service Accounts and SSH Keys.....	139
Configuring Secret Dependencies for RPC.....	140
Custom Password Changers.....	143
Distributed Engines and RPC.....	148
Password Changing Scripts .....	148
Heartbeats: Automatically Testing Secret Credentials .....	149
Introduction .....	149
Remote Accounts Supported .....	149
Enabling Heartbeat in RPC .....	150
Configuring Heartbeat .....	150
Running Heartbeat for a Secret.....	150
Heartbeat Logs .....	151
Heartbeat Status Codes .....	151
Alerts on Heartbeat Failure .....	151
Automatic Secret Discovery .....	151
Introduction.....	151
Enabling Discovery for Secret Server .....	152
Enabling Discovery for an Active Directory Domain .....	152
Enabling Discovery for Specific Organization Units of a Domain .....	152
AWS Account Discovery .....	153
Session Recording .....	155
Overview .....	155
Improvements for Secret Server 10.6 SP2.....	158

Session Recording Requirements .....	160
System Capacity Specifications .....	160
Caveats and Recommendations.....	161
Web services.....	163
Enabling Web services.....	163
Windows Integrated Authentication Webservice .....	163
Using the Java Console API Access Secret Values.....	164
Folder Synchronization.....	164
Synchronizing with the ConnectWise API.....	164
Synchronizing with a Database (Advanced).....	167
Users .....	168
Creating Users .....	168
User Groups .....	174
Creating User Groups .....	174
Adding Users to Groups.....	174
Assigning Group Assignment .....	175
Group Owners.....	176
Active Directory Synchronization .....	177
Configuring Active Directory.....	177
Enabling and Disabling Active Directory Users.....	179
Unlocking Local Accounts .....	180
Syncing and Authenticating AD Users via a Distributed Engine .....	180
Active Directory Configuration Parameters .....	181
Creating Active Directory Users .....	182
Teams .....	183
Overview .....	183
Team Management.....	183
Roles .....	201
Creating Roles.....	201
Editing Role Permissions.....	201
Assigning Roles to a User .....	202
Creating Synchronization Secrets .....	202
Adding Domains.....	202

Local Sites Versus Distributed Engine Sites .....	202
Setting Up Synchronization Groups .....	202
Advanced Authentication .....	203
Integrated Windows Authentication .....	203
Enabling Integrated Windows Authentication .....	203
Configuring IIS.....	203
Logging on As a Local Account .....	203
SAML .....	204
IP Address Restrictions .....	204
Creating IP Address Ranges.....	204
Editing and Deleting IP Address Ranges.....	204
Assigning an IP Address Range.....	205
<b>Administration Tabs.....</b>	<b>206</b>
General Tab.....	206
Login Tab.....	207
Folders Tab .....	208
Local User Passwords Tab.....	209
Security Tab .....	209
Ticket System Tab .....	210
Ticket Number Validation.....	210
BMC Remedy Integration .....	211
ServiceNow Integration.....	213
PowerShell Integration.....	215
Email Tab .....	216
Session Recording Tab .....	216
HSM Tab.....	217
<b>Administration Auditing .....</b>	<b>218</b>
Viewing a User Audit Report.....	218
Secret Audit Log.....	218
Report Auditing.....	219
<b>Backup and Disaster Recovery .....</b>	<b>220</b>
Backup Settings .....	220
Folder Permissions .....	220

Manual Backups .....	220
Scheduled Backups .....	220
File Attachment Backups .....	221
Exporting Secrets .....	221
Exported File Format .....	221
Recovery .....	221
Unlimited Administration Mode .....	221
<b>Events and Alerts.....</b>	<b>223</b>
System Log.....	223
Event Subscription Page.....	223
Creating Event Subscriptions .....	223
Editing a Subscription.....	224
Deleting a Subscription .....	224
Viewing Event Subscription Logs .....	224
Alert Notification Center (Inbox).....	225
CEF and SIEM Integration .....	225
Configuring CEF .....	225
Testing CEF .....	226
<b>Customizing Secret Server's Appearance .....</b>	<b>227</b>
Creating Themes.....	227
Embedded Mode.....	227
<b>Secret Server Reports .....</b>	<b>228</b>
Reports General Tab.....	229
Modifying Report Categories .....	229
Creating and Editing Reports.....	229
Report Page .....	230
Viewing Reports.....	230
Deleting or Undeleting Reports .....	230
Viewing Auditing for a Report.....	231
Saving Reports to File.....	231
Scheduled Reports .....	234
Creating New Schedules for Reports .....	234
Viewing Existing Report Schedules.....	234



Editing Schedule Settings.....	234
Reports Security Hardening Tab .....	235
Reports User Audit Tab .....	237
Reporting and Dual Controls .....	237
<b>Server Clustering .....</b>	<b>238</b>
<b>General Encryption and Security.....</b>	<b>239</b>
Advanced Encryption Standard.....	239
SSL Certificates.....	239
Security Compliance Standards .....	239
FIPS Compliance .....	239
PCI Datacenter Compliance .....	239
HSM Integration.....	240
Key Rotation.....	240
<b>Two-Factor Authentication .....</b>	<b>242</b>
Email Two-Factor Authentication .....	242
RADIUS Authentication .....	242
Configuring RADIUS.....	243
Enabling RADIUS for a User .....	243
TOTP Two-Factor Authentication.....	243
Enabling TOTP Two-Factor Authentication .....	243
Disabling TOTP Two-Factor Authentication.....	244
Resetting TOTP Two-Factor Authentication .....	244
Setting up TOTP Two-Factor Authentication (User) .....	244
Duo Security Authentication .....	244
Enabling Duo (Admin).....	244
Setting up Duo (User) .....	245
FIDO2 (YubiKey) Two-Factor Authentication Configuration .....	245
Overview .....	245
Configuration .....	245
SMTP Configuration for Two-Factor Authentication.....	245
<b>Upgrading Secret Server.....</b>	<b>247</b>
<b>Licensing.....</b>	<b>248</b>
Installing New Licenses.....	248

Converting from Trial Licenses .....	248
Activating Licenses .....	248
Licensing Limited Mode .....	248

31 January 2020



# Introduction

## PURPOSE

This document is a guide to IBM Security Secret Server for administrators and advanced users.

**Installation:** Secret Server is distributed as an .msi (setup.exe) which installs the Web application. A .zip file option is also available but is not recommended as using setup.exe is much easier. To install Secret Server, run setup.exe. For more detailed information on setting up the prerequisites (IIS, ASP.NET, and connecting to Microsoft SQL Server), please see the [Secret Server Installation Guide](#).

## TERMS AND DEFINITIONS

**Table: Terms and Definitions**

Term	Definition
2FA	<i>Two-Factor Authentication</i>
AD	<i>Active Directory</i>
Administrator	Administrator (uppercase) is a default role that comes preconfigured with Secret Server. Roles control access to features within Secret Server. This role can be customized to have different permissions. In this guide, administrator (lowercase) is used when referring to users who manage the system and have control over global security and configuration settings. Note that administrators in Secret Server do not automatically have access to all data stored in the system--access to data is still controlled by explicit permissions on that data.
AES	<i>Advanced Encryption Standard</i>
API	<i>Application Programming Interface</i>
ASCII	<i>American Standard Code for Information Interchange</i>
ASP	<i>Advanced Server Pages</i>
AWS	<i>Amazon Web Services</i>
CEF	<i>Common Event Format</i>
CHG	<i>Change</i>
CIDR	<i>Classless Inter-Domain Routing</i>
CRM	<i>Customer Relationship Management</i>
CSV	<i>Comma-Separated Values</i>
DBA	<i>Database Administrator</i>
DE	Distributed Engine (Secret Server)
DES	<i>Data Encryption Standard</i>

DPAPI	<i>Data Protection Application Programming Interface</i>
DSS	<i>Data Security Standard</i>
EC2	<i>Elastic Compute Cloud</i>
ESX	<i>Elastic Sky X</i>
FIPS	<i>Federal Information Processing Standard</i>
FQDN	<i>Fully Qualified Domain Name</i>
HSM	<i>Hardware Security Module</i>
HSTS	<i>HTTP Strict Transport Security</i>
IAM	<i>Identity and Access Management</i>
IIS	<i>Internet Information Services</i>
IP	<i>Internet Protocol</i>
ITSM	<i>Information Technology Service Management</i>
KB	<i>Kilobyte or Knowledge Base</i>
LDAP	<i>Lightweight Directory Access Protocol</i>
NAT	<i>Network Address Translation</i>
NATO	<i>North Atlantic Treaty Organization</i>
NIST	<i>National Institute of Standards and Technology</i>
NSA	<i>National Security Agency</i>
NTLM	<i>NT LAN Manager</i>
OATH	<i>Open Authentication</i>
OS	<i>Operating System</i>
OTP	<i>One-Time Password</i>
OU	<i>Organizational Unit</i>
PCI	<i>Payment Card Industry</i>
PDF	<i>Portable Document Format</i>
PuTTY	<i>Popular SSH and Telnet Client</i>
QR	<i>Quick Response (code)</i>
RADIUS	<i>Remote Authentication Dial-In User Service</i>
RBAC	<i>Role-Based Access Control</i>
RBS	<i>Role-Based-Security</i>
RD	<i>Remote Desktop</i>
RDP	<i>Remote Desktop Protocol</i>
Remote Password Changing	Secret Server can automatically change passwords on remote devices and various platforms, including the following: Windows accounts, database logins, Active Directory accounts, Unix and Unix-like accounts (including root passwords), network appliances or devices and more.

REST	<i>Representational State Transfer</i>
Role-based Security	Secret Server uses role-based access control, which provides the ability to set strict, granular permissions for each user. All features in Secret Server are available to users based on permissions, which collectively make up roles.
RPC	<i>See Remote Password Changing</i>
SAML	<i>Security Assertions Markup Language</i>
SEC	<i>Security and Exchange Commission</i>
Secret	A piece of information that is stored and managed within Secret Server is referred to as a secret. Secrets are derived from Secret templates. Typical secrets include, but are not limited to, privileged passwords on routers, servers, applications, and devices. Files can also be stored in secrets, allowing for storage of private key files, SSL certificates, license keys, network documentation, Microsoft Word or Excel documents and more.
Secret Template	Secret templates are used to create secrets and allow customization of the format and content of secrets to meet company needs and standards. Examples include: Local Administrator Account, SQL Server Account, Oracle Account, Credit Card and Web Password. Templates can contain passwords, usernames, notes, uploaded files, and drop-down list values. New Secret templates can be created, and all existing templates can be modified.
SHA1	<i>Secure Hashing Algorithm 1</i>
SIEM	<i>Security Information Event Management</i>
SMS	<i>Short Message Service</i>
SMTP	<i>Simple Mail Transfer Protocol</i>
SOAP	<i>Simple Object Access Protocol</i>
SP	<i>Service Pack</i>
SQL	<i>Structured Query Language</i>
Secret Server	<i>Secret Server</i>
SSH	<i>Secure SHell</i>
SSL	<i>Secure Socket Layer</i>
TCP	<i>Transmission Control Protocol</i>
TOTP	<i>Time-Based One-Time Password</i>
UDP	<i>User Datagram Protocol</i>
UI	<i>User Interface</i>
UNC	<i>Universal Naming Convention</i>

Unlimited Administration Mode	An emergency, break-the-glass mode that gives administrators access to all content within the system, regardless of explicit permissions. Access to Unlimited Administration Mode is controlled using role permissions.
URL	<i>Uniform Resource Locator</i>
VM	Virtual Machine
VPN	Virtual Private Network
WS	<i>Web Services</i>
XML	eXtensible Markup Language

## DOCUMENT CONVENTIONS

These conventions are used throughout this guide:

**Note:** Many of the actions depicted in this guide can be accomplished in other ways, such as keyboard shortcuts. For consistency, this guide adheres to a visual, mouse-oriented approach.

**Note:** IP addresses, machine names, screen grabs, and the like are generic examples unless otherwise noted.

### Screen Components and Attentional Targets

- Mouse-click, keyboard, and other attentional targets (anything a looks for) are denoted by bold type: **OK** button or **Login** link.
- Attentional Targets and screen component names in system *responses* are not in bold: "The OK button appears" verses "Click the **OK** button."
- Names of screen components, such as tabs, buttons, and text boxes, are corrected for spelling and capitalization. The component type appears in lowercase. Example: **Server configuration** window becomes **Server Configuration** window.

### Notes

There are three types of notes: *regular*, *important* and *warning*.

**Note:** Regular notes have a title, either "Note" or something custom, which appears as a phrase followed by a colon at the beginning of the note. A note contains tangential (an aside) or supplemental information (a tip or clarification).

**Important:** Important notes contain substantive information that should be heeded, or negative consequences can occur, involving frustration, wasted time, or minor data loss.

**Warning:** Warning notes contain substantive information that should be heeded, or negative consequences can occur, involving injury, major data loss, or equipment damage.

### Keyboard Shortcuts

- Keyboard keys are bolded and surrounded with square brackets: **[Enter]**

- Concurrent key presses are denoted with plus signs: **[Ctrl]+[Alt]+[Del]**
- Sequential key presses are denoted by commas: **[Page Down], [Enter]**

### Other Special Text

- Email addresses and URLs are usually denoted by a colored underline: [support@example.com](mailto:support@example.com).
- When URLs are part of the instruction, as opposed to clickable link, they appear in monospaced text: Type `https://www.example.com` or click `https://www.example.com`.
- Cross-references to headings are hyperlinks: See [Booting a Server](#).
- Document or article names (not sections) appear in italics: See the *Server Administration Guide*. They may or may not be hyperlinks.
- All file and folder paths appear in monospaced text: `app\bin\web_config.xml`
- File names by themselves do *not* appear in monospaced text: `web_config.xml`. If the file name contains spaces, the name is surrounded by quotation marks: `"web config.xml"`.

**Note:** Ending punctuation may be omitted for clarity when following typed-in text, including URLs.

### Code and Command Line Text

Variable text in literal typed-in text and command-line parameters follow these industry-wide standards:

- All code and command-line interface text appear in monospaced text.
- Required parameters appear in angle brackets: `ping <hostname>`
- Optional parameters appear in square brackets: `mkdir [-p] <dirname>`
- Repeated parameters are followed by ellipses: `cp <source1> [source2...] <dest>`
- Multiple choice items are separated by vertical bars and grouped by curly brackets: `netstat {-t|-u}`

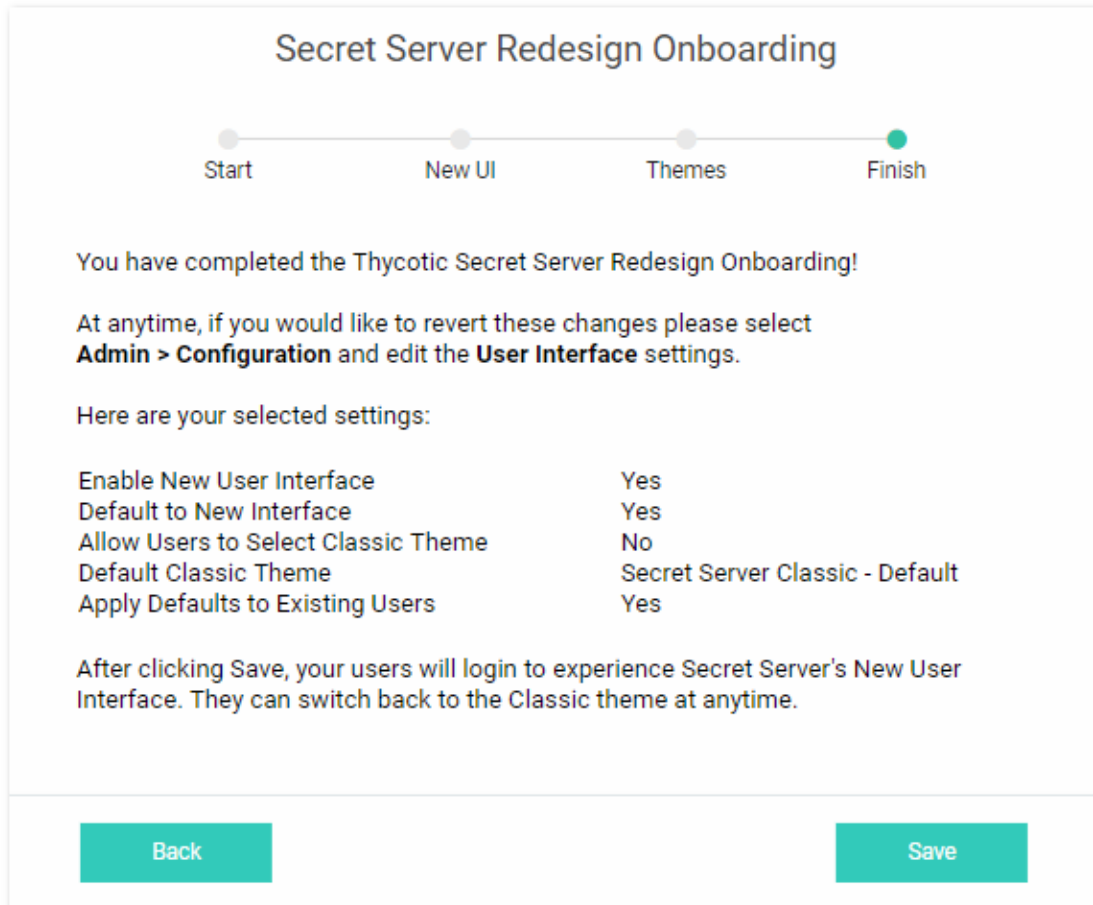
## ADDITIONAL RESOURCES

- [Best Practices Guide](#)
- [Installation Guide](#)
- [Secret Server Support Page](#)
- [System Requirements](#)



## SECRET SERVER REDESIGN ONBOARDING WIZARD

Secret Server has a new user interface (UI). A new UI can be burdensome for users. To ease this, we provide a wizard to walk the first admin who logs on through a series of choices related to the new UI. After completing the wizard, your choices are listed in the final page prior to committing to them:



The screenshot shows the 'Secret Server Redesign Onboarding' wizard completion screen. At the top, a progress bar indicates four steps: 'Start', 'New UI', 'Themes', and 'Finish'. The 'Finish' step is highlighted with a green dot. Below the progress bar, the text reads: 'You have completed the Thycotic Secret Server Redesign Onboarding!'. It then provides instructions on how to revert changes: 'At anytime, if you would like to revert these changes please select **Admin > Configuration** and edit the **User Interface** settings.' A section titled 'Here are your selected settings:' lists five settings with their values: 'Enable New User Interface' (Yes), 'Default to New Interface' (Yes), 'Allow Users to Select Classic Theme' (No), 'Default Classic Theme' (Secret Server Classic - Default), and 'Apply Defaults to Existing Users' (Yes). At the bottom, there are two teal buttons: 'Back' on the left and 'Save' on the right.

Secret Server Redesign Onboarding

Start New UI Themes Finish

You have completed the Thycotic Secret Server Redesign Onboarding!

At anytime, if you would like to revert these changes please select **Admin > Configuration** and edit the **User Interface** settings.

Here are your selected settings:

Enable New User Interface	Yes
Default to New Interface	Yes
Allow Users to Select Classic Theme	No
Default Classic Theme	Secret Server Classic - Default
Apply Defaults to Existing Users	Yes

After clicking Save, your users will login to experience Secret Server's New User Interface. They can switch back to the Classic theme at anytime.

Back Save

**Note:** At any time, if you want to change your selections, please select **Admin > Configuration** and edit the **User Interface** settings.

# Getting Started with Secret Server

The introductory guided tutorial, for new users, helps you learn to use the product.

## TOPIC 1: TRIAL INSTALLATION AND PROOF-OF-CONCEPT

### PREREQUISITES

The following suggested guidelines describe how to prepare to run a trial or proof-of-concept (POC) of Secret Server.

### System Requirements

Review the detailed [System and Memory Requirements for Secret Server](#) (KB). The *Minimum Requirements* are for trial, sandbox, and POC environments. The *Recommended Requirements* are for production deployments.

### Hardware Requirements

You can install Secret Server on a physical server or virtual machine.

If you want to set up front-end (application) clustering, you must have two or more servers available.

For testing of high availability for the SQL Server, you can use either existing Microsoft AlwaysOn infrastructure or database mirroring. If you choose to test this model, your database team must prepare in advance.

### Software Requirements

#### Checklist

- Windows Server 2012 or newer (recommended) (one server, minimum)
- SQL Server (one instance, minimum)
- Application server prerequisites
- SSL certificate

#### SQL Server

You can create the SQL database in an existing SQL instance, or a new installation of SQL Server. For high availability, this must be a paid edition of SQL Server (not SQL Express). If you are using a new installation of SQL Server, please have this installed beforehand.

Detailed instructions for installation and configuration of SQL Server are included in one of the installation guides below (choose the guide matching the OS that SQL server will be installed on).

## Application Server

It is suggested that you install Secret Server on Windows Server 2012 or greater. Include IIS, ASP.NET and .NET Framework. Refer to the System Requirements KB to view the prerequisites.

## Application Configuration

### Service Account

Set up a service account:

1. Log on as a batch job (on the server that Secret Server runs on)
2. Modify permissions to the Secret Server application directory (typically C:\inetpub\wwwroot) and C:\Windows\temp.
3. Provide access to your SQL Server instance by adding the db\_owner permission to the Secret Server database.

For detailed instructions on how to configure the permissions for the service account, see [Running Secret Server IIS Application Pool with a Service Account](#) (KB). The installation guides includes instructions for assigning **db\_owner** permission to the service account in SQL Server.

If you would like to test features that rely on Active Directory, such as AD group sync or discovery, you should also have accounts available with the appropriate permissions (described below). One option is to use the same account for both features.

### Active Directory Group Sync

Active Directory group synchronization means that Secret Server can automatically add users and enable or disable them to log into Secret Server based off of their Active Directory group membership. You can choose which groups to sync. When configuring AD group sync in Secret Server, you are required to specify an account that can read the properties of users and groups. See [Active Directory Synchronization Rights for Synchronization Account](#) (KB) for a detailed list of required permissions.

### Discovery

To test discovery, please have some machines available for Secret Server to connect to for discovering accounts. An account is required to sync with AD and also scan the machines found for Windows local account and service account discovery. [Account Permissions for Discovery](#) (KB) describes the permissions required for an AD account to be used for discovery.

### Test Accounts

We recommend having a few test accounts available to represent the types of accounts you want to manage using Secret Server. These could be local Windows accounts, service accounts running scheduled tasks or services, SQL server accounts, and others.

## Email Notifications

To test email notifications, which can be used for event subscription notifications or requests for approval to passwords, you need configuration information for the company SMTP server:

- Service account to run the application and connect to SQL
- Domain (test or production)
- Domain account to be used for AD sync and discovery
- Test machines (if testing discovery)
- Test accounts
- SMTP server settings

## SSL Certificate

It is suggested that you set up SSL (or https) for access to Secret Server. To do so, you will need an SSL certificate. You may use an existing wildcard certificate, create your own domain certificate, or purchase a third-party SSL certificate for the Secret Server.

## Firewalls and Ports

Secret Server must connect directly to a target system to change its password. For devices that are firewalled off from Secret Server, remote agent can provide connectivity to them, but they also require connectivity from them to the target systems for password changing.

Please see [Ports used by Secret Server](#) (KB) for a list of ports needed by Secret Server for password changing, discovery, and other features.

## TOPIC 2: INSTALLING SECRET SERVER

### Process

Run the Installer: Secret Server comes with an installer that walks you through the entire process from start to finish. Once you have the prerequisites ready to go, download and run your installer, and the wizard will take you through the installation process. Please see our [installation guide](#).

### Licenses

#### Understanding Licenses

After installation, enter your licenses. You can do this in the Getting Started Wizard or from the Licenses Administration page (instructions below). This not only allows you to add more users but also enables additional features in Secret Server.

For the Express edition, you have one license to enter. For Professional edition and higher, you have, at minimum:

- An edition license
- A user license
- A support license.

If you purchased additional licenses for sites or distributed engines, you may have more licenses to add.

**Note:** You will not have a support license if you have purchased the installed edition of Secret Server but did not purchase support or upgrade protection.

### Activating Licenses

1. Go to **Admin > Licenses**.
2. Click the **Install New License** button.
3. Type the **License Name** and **License Key** for one of the licenses that you received from your account manager.
4. Click **Save**.
5. If you have another license to add, click **Add Another License**.
6. When you have added all licenses, click **License Activation**.
7. Enter your name, email address, and phone number, then click the **Activate** button. If your server does not have outbound network access, click **Activate Offline** instead.

**Note:** For more information about license activation, see [License Activation](#) (KB).

## TOPIC 3: THE SECRET SERVER DASHBOARD

The Secret Server Dashboard is the main page for searching and viewing secrets. Everything you do in Secret Server starts with the Dashboard. See [Secret Server Dashboard](#) for details.

**Note:** For a visual demonstration of the Dashboard, see the video at <http://my.thycotic.com/movies/secretserver/welcome/>.

## TOPIC 4: APPLYING SECURITY BEST PRACTICES

As you start using Secret Server, consider configuring the following security settings. While these are optional, setting them is a best practice.

## Local Admin Account Best Practices

Even if you plan to [integrate with Active Directory](#) to log into Secret Server, chances are you will must use this account again. This is the first account you created during the installation process. Keep this account secure and avoid being locked out of Secret Server by following these suggestions:

- Store the credentials in a secure location that you can access if you lose all access to Secret Server.
- Enable the **Allow Users to Reset Forgotten Passwords** setting to provide a way of resetting the password if account is locked out or if the password is forgotten:
  1. Select **Admin > Configuration**. The Configuration page appears.
  2. Click the **Local User Passwords** tab to locate the setting.
  3. Click **Edit** to edit the setting.
  4. Click **Save** when finished.

**Note:** This requires an [SMTP server configured](#). (KB).

- Configure the other **Local User Passwords** settings to enforce your password requirements, expiration, password history, and other password policies.

## SSL (HTTPS) Best Practice

We recommend requiring SSL access to Secret Server. This requires setting up an SSL certificate for the website, preferably with a domain certificate. However, if you don't have a certificate, see [Installing a Self-Signed Certificate](#) (KB). Once you have your certificate:

1. Configure the HTTPS binding for your Secret Server website using the certificate you choose.
2. Ensure your certificate is trusted on the Secret Server users' machines. See [Trusting an SSL Certificate on a Client Machine](#) (KB) for instructions.
3. Enable **Force HTTPS/SSL** on the **Security** tab of the Secret Server **Configuration** settings.

## TOPIC 5: CONFIGURING BACKUPS

Configure backups to avoid losing your data. Secret Server provides the option to automatically take a backup on the interval you specify, sending the backups to a local or network location. There are two components of an entire backup of Secret Server: The Web application files and the database. Find these settings by selecting **Backup** from the **Admin** menu. See [Backup and Disaster Recovery](#) for more information.

To configure the backup paths, see [Backup Configuration File Path Settings](#) (KB).

**Note** The file paths configured on this page by default must be either changed or created on each server that the Secret Server application and database reside on.

## TOPIC 6: INTEGRATING WITH ACTIVE DIRECTORY

To allow users to log in with their Active Directory (AD) credentials, you can configure your AD domain settings in Secret Server and then add users either individually or by group.

### Setting up Active Directory

See [Configuring Active Directory](#).

### Enabling Active Directory Users

See [Enabling and Disabling Active Directory Users](#).

### Managing Active Directory Users via a Distributed Engine

See [Syncing and Authenticating AD Users via a Distributed Engine](#).

## TOPIC 7: CREATING SECRET SERVER INFRASTRUCTURE AND SECRETS

To try out Secret Server, you must have folders, roles, users, and secrets to operate on:

1. Setup some folders and roles: We encourage is for you to setup a folder structure and a few roles. The folder structure is how you will keep your secrets organized and provide access to shared secrets. Additionally, roles ensure you can control access to different parts of Secret Server and assign permissions to view certain folders and secrets. See [Secret Folders](#) and [Roles](#).
2. Add users if you have not already from AD. See [Creating Users](#) and [Creating User Groups](#).
3. Add an Active Directory or other secrets. If you plan on using discovery, the account will also need permissions to scan computers on the network for accounts. See [Managing Secrets](#).

## TOPIC 8: RUNNING DISCOVERY

Secret Server has a discovery feature that can automatically find local Windows accounts, Active Directory service, Unix, VMware ESX/ESXi, and Active Directory domain accounts. Account and dependency types not supported out-of-the-box in Secret Server can still be discovered by writing PowerShell scripts that can be run as custom scanners. This allows administrators to quickly import accounts found by Secret Server on specified domains or IP addresses.

**Note:** Please see the [Discovery Guide](#) for a comprehensive guide to configuring and using discovery.

To run discovery on a domain, IP address range, or a custom source, you must first enable the discovery feature for Secret Server. Second, you must enable discovery for each discovery source you would like to be scanned.

See one of the following to set up discovery:

- [Enabling Discovery for Secret Server](#)
- [Enabling Discovery for an Active Directory Domain](#)
- [Enabling Discovery for Specific OUs of a Domain](#)

## **TOPIC 9: CONFIGURING REMOTE PASSWORD CHANGING**

Secret Server remote password changing (RPC) provides the ability to either start a password change manually or schedule automatic password changes to occur at a regular interval.

### **Enabling Remote Password Changing**

See [Enabling RPC](#).

### **Performing a Manual RPC**

See [Run a Manual RPC](#).

### **Common RPC Error Codes**

See [RPC Error Codes](#)

## **TOPIC 10: CONFIGURING HEARTBEAT**

Heartbeat allows you to determine from Secret Server whether the credentials in a secret authenticate successfully with their target system. By default, heartbeat is turned off in Secret Server. See [Heartbeats: Automatically Testing Secret Credentials](#) for general information.

### **Enabling Heartbeat**

See [Enabling Heartbeat in RPC](#).

### **Running Heartbeat**

See [Running Heartbeat for a Secret](#).

## **TOPIC 11: RUNNING AUDITS AND REPORTS**

Before running reports and audits, you must create something to report on—to that end:

- Import a few accounts or create secrets manually
- Rotate passwords a few times



- View a couple of your secrets

This generates enough audit logs to provide meaningful outputs in your reports:

- Security Hardening Report
- What secrets have been accessed
- What secrets failed heartbeat
- Failed login attempts
- Secret activity

See [Built-In Reports](#) (KB) for the most up-to-date list of reports included.

For details on using reports, see:

- [Creating and Editing Reports](#)
- [Viewing Reports](#)

## TOPIC 12: CONTROLLING SECRET ACCESS AND WORKFLOW

Sometimes, depending on your scenario, you want to add extra protections to highly sensitive secrets. Secret Server has access request and workflow features:

- [Secret Check-Outs](#): Grant access to a single user
- [Basic Secret-Access Requests](#): Require approval prior to accessing a secret for a defined time period
- [Advanced Secret-Access Requests with Workflow Templates](#): Require multi-level and multi-user approval prior to accessing a secret for a defined time period
- [Secret DoubleLocks](#): Add another security layer by encrypting secret data with a supplemental custom encryption key that is only accessible with an additional password, regardless of regular permissions.

## TOPIC 13: ACCESSING REMOTE MACHINES WITH SECRET LAUNCHERS.

A secret *launcher* opens a connection to the remote computer or device or logs into a website using the secret's credentials directly from the Web page. While this provides a convenient method of opening RDP and PuTTY connections, it also circumvents users being required to know their passwords. A user can still gain access to a needed machine, but it is not required to view or copy the password out of Secret Server. A Web launcher automatically logs into websites using the client's browser.

Secret Server launchers, also called protocol handlers, come in three primary types:

- **Remote Desktop:** Launches a Windows Remote Desktop session and automatically authenticates the user to the machine.
- **PuTTY:** Opens a PuTTY session and authenticates the user to a Unix system.
- **Web Password Filler:** Uses a bookmarklet or a Chrome extension to automatically log the user into a website with secret credentials. See [Web Password Filler](#).
- **Web Launcher:** An alternative method to automatically log on websites. See [Web Launcher](#).

See [Secret Launchers](#) for more information.

## TOPIC 14: RECORDING SESSIONS

Session recording provides an additional level of security by recording a user's actions after a launcher is used. Session recording works for any launcher, including PuTTY and SSH, Windows Remote Desktop, Microsoft SQL Management Studio, and custom executables. The resulting movie is viewable from the secret audit. Detailed information on supported codecs can be found in [Session Recording](#). There are two types of session recording:

- [Basic Session Recording](#)
- [Advanced Session Recording](#)

## TOPIC 15: ACCESSING SECRET SERVER WITH APIS AND THE CLI

You can access Secret Server without using the user interface for automation and integration purposes. Currently, there are two APIs:

- An asynchronous REST (representational state transfer) API for Web services, which is based on JSON (JavaScript Object Notation). This is the preferred method. It is faster and easier to read than the SOAP API and is still actively updated.
- A synchronous SOAP (Simple Object Access Protocol) for Web services, which is based on XML. This method is deprecated, but we still support it. It is based on an older technology, which has largely been replaced in recent years. There will be no enhancements to this API. There are, however, a few, rarely used capabilities that only our SOAP API has.

We offer a software development kit (SDK) that contains a .NET framework and a command line interface (CLI) for accessing the REST API with Windows applications or scripting languages.

Both APIs, the .NET framework, and the CLI support:

- GET Requests: Retrieve information from Secret Server, including entire secrets, individual secret fields, and security tokens
- POST Requests: Create Secret Server data

- PUT Requests: Update Secret Server data
- DELETE Requests: Remove Secret Server data
- Once-per-session permissions (tested once and then based on the IP address), administered with a Secret Server rule

#### SDK Documentation:

- [Secret Server SDK Guide](#): Includes these topics:
  - Secret Server configuration
  - Roles and permissions
  - SDK client installation
  - Connecting to Secret Server
  - SDK client caching
  - Examples
- [Secret Server SDK Downloads](#): Includes these topics:
  - SDK downloads
  - Download
  - SDK release notes
  - NuGet packages
- [SDK Integration Document](#): Includes these topics:
  - Integrating using C#
  - Integrating using the `web.config` file
  - Methods of the `SecretServerClient()` class

#### REST API Documentation:

- [REST Web Services API - Secret Server](#): Links to online reference guides (by Secret Server release)
- [REST API PowerShell Scripts - Getting Started](#)
- [REST API Perl Examples](#)
- [REST API Java Examples](#): Downloadable Zip file

SOAP API Documentation:

- [SOAP Web Services API - Secret Server](#): Reference guide in a downloadable PDF
- [Using Web Services with SOAP and JavaScript](#)
- [SOAP-based Web services API - Getting Started](#)

## **TOPIC 16: FINDING ADDITIONAL RESOURCES FOR SECRET SERVER**

You have finished this "Getting Started" introduction to Secret Server. There is much more to explore within Secret Server, such as scripting, third-party integrations (SIEM, CRM, HSM, and more), and connecting to Privilege Manager to monitor and protect endpoints.

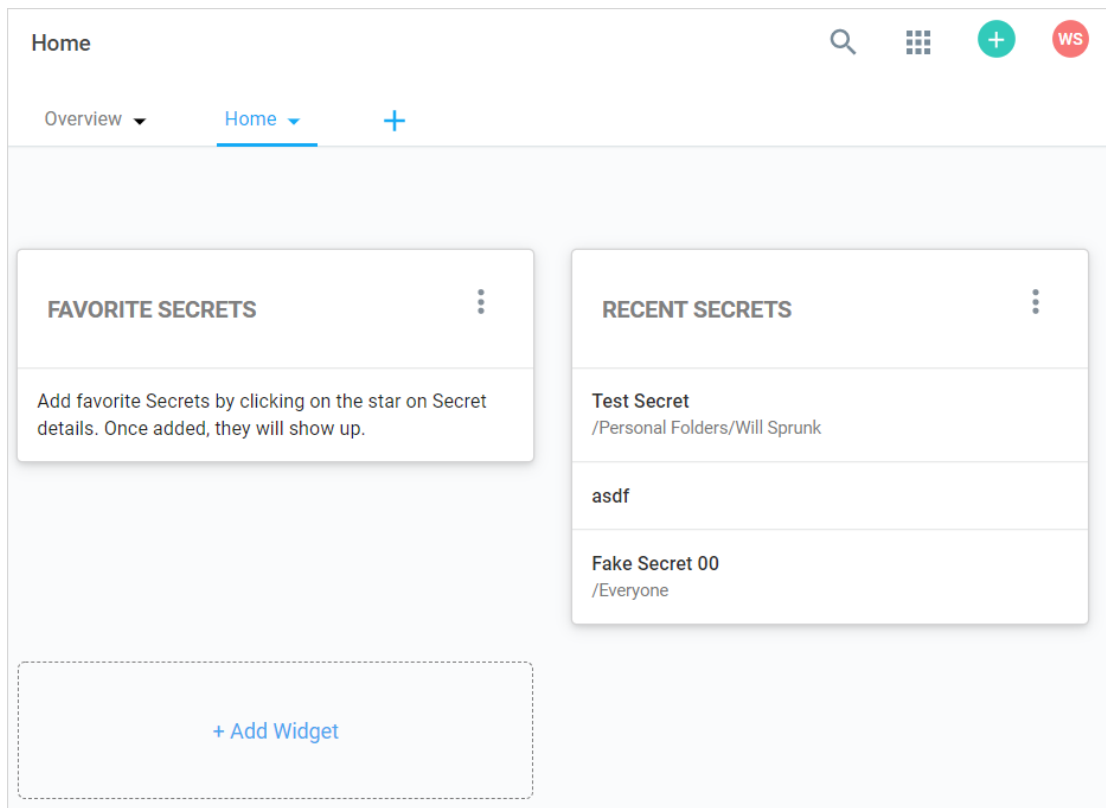
See [Additional Resources](#) to learn more about Secret Server and other Thycotic products.

# Secret Server Dashboard

## OVERVIEW

The Secret Server Dashboard is the main page for searching and viewing secrets:

**Note:** For a visual demonstration of the Dashboard, see the video at <http://my.thycotic.com/movies/secretserver/welcome/>.



By default, it contains the Favorite Secrets, Recent Secrets, and + Add Widget widgets (function boxes). You can add these widgets:

- Expired Secrets
- Out-of-Sync Secrets
- Reports
- Request Management

## DASHBOARD WIDGETS

### Table: Dashboard Widgets

Widget	Description
Expired Secrets	Displays expired secrets.
Favorite Secrets	Displays secrets marked as favorites.
Out-of-Sync Secrets	Displays secrets that are out-of-sync—the heartbeat or RPC have failed.
Recent Secrets	Displays the secrets viewed most recently.
Reports	Displays a report. Click the <b>Report Category</b> list to select a report from the drop-down menu. One report can be displayed per widget. Click the title of the report to navigate to the Report View page.
Request Management	Displays any requests pending for the logged in user.
+ Add Widget	When clicked, adds a widget that is not currently displayed to the Dashboard. This widget's function is duplicated automatically when you add a new Dashboard tab. You cannot remove this widget.

**Note:** The Search and Browse widgets cannot be rearranged. They always remain in the top left region of the tab.



## Managing Widgets

The following operations are available (by clicking the  icon) for managing widgets:

- **Delete:** Hide the widget.
- **Refresh:** Update the information in the widget. This is not available for all widgets.

## CUSTOMIZING DASHBOARD TABS

The following operations are available for customizing tabs:

- **Create:** Click the + to the right of the tabs to create a new empty tab.
- **Delete:** Click the  icon on a tab and select **Delete** to delete a tab. You can cancel changes by clicking the Cancel button. A confirmation pop up page appears.
- **Rename:** Click the  icon on a tab and select **Rename** to change the tab name. You can cancel changes by clicking the Cancel button.
- **Reorder:** Click and drag a tab to the left or right of an existing tab.

## OVERVIEW TAB

The Overview tab provides several widgets for getting a quick understanding of your Secret Server installation:

- **Active Monitoring Sessions:** Your current monitored sessions. See [Session Recording](#).
- **Approvals:** Your current in-process approvals. See [Secret Access Requests](#).
- **Heartbeat Status:** A graphic of the current status of your heartbeats: success, pending, or failed. When you click on one of the statuses, you are brought to a report page for that status. For example, **Reports > Secrets Failing Heartbeat**. When you click the **Current** link, you are brought to the **Reports > Heartbeat Status by Day** page. See [Heartbeats: Automatically Testing Secret Credentials](#)
- **Most Used Secrets:** A table of the most recently accessed secrets, listed by date and folder.
- **Password Rotation:** The state of your current password rotations. When you click the **Today** link you are brought to the **Reports > RPC by Day** report page. See [Remote Password Changing](#).

**Note:** To see an overview of incoming system and subscription alerts, see the [Inbox](#).

## RUNNING DASHBOARD BULK OPERATIONS

You can perform bulk operations from the Dashboard on multiple secrets:

1. Select the secrets that you want to include. To select all, select the box in the column header row.
2. From the list below the list of secrets, select the bulk operation. Available bulk operations include:
  - Add share
  - Assign secret policy
  - Assign to site
  - Change password remotely
  - Change to inherit permissions
  - Convert secret template
  - Delete
  - Disable autochange
  - Disable check out
  - Disable comment on view
  - Disable heartbeat

- Edit share
- Enable autochange
- Enable check out
- Enable comment on view
- Enable heartbeat
- Hide launcher password
- Move to folder
- Run heartbeat
- Set privileged account
- Undelete
- Unhide launcher password

**Note:** Bulk operations differ by Secret Server version.

## SECRETS

### Introduction

*Secrets* are individually named sets of sensitive information. Secrets address a broad spectrum of secure data, each type represented and created by a *secret template*. You can centrally manage secret security through sharing settings for each secret. Additionally, using folder structure, you can allow one or more secrets to inherit permissions from their parent folder. All secret text-entry field information is securely encrypted before being stored in the database, including a detailed audit trail for access and history.

**Note:** You can "favorite" a secret in the main menu by right clicking it.

### Secret Tabs

#### Secret Personalize Tab

These settings only apply to the user who is editing the settings. They do not apply to the other users who have View, Edit, or Owner permission to the secret.

To use the settings in the Email Notifications section, you must have email configured correctly in your configuration settings. You also need a valid email address entered for each user account to use these settings. This can be set in the **Administration > Users** section.

The following email notification settings are available:

- **Send Email When Changed:** Email the user when the secret is edited by any user.



- **Send Email When Heartbeat Fails:** Email the user when a heartbeat function fails for the secret. The email contains the secret name, error code and details.
- **Send Email When Viewed:** Email the user when the secret is viewed by any user.

The Personalize tab also contains settings that pertain to the type of launcher configured for a secret. If the launcher type is Remote Desktop Protocol (RDP), the following settings are available:

- **Connect to Console:** Remote Desktop (RD) may connect to the console session.
- **Allow Access to Printers:** RD may access local printers.
- **Allow Access to Drives:** RD may access drives connected to the local machine.
- **Allow Access to Clipboard:** RD may access to the clipboard of the local machine.
- **Use Custom Window Size:** Users may specify custom window height and width. Use Preferences refer to the user's settings under **Profile > Preferences** in the **Launcher** tab.

Users may enable or disable these settings or to defer to what is configured in their user settings by selecting **Use Preferences**.

### Secret Expiration Tab

Inside the Expiration tab, the expiration period can be modified. The following options are available:

- **Template Interval:** Default expiration period configured for new secrets based on the current template.
- **Custom Interval:** A custom expiration period in days.
- **Custom Date:** A custom expiration date in month/day/year format.

**Note:** See [Secret Expiration](#) for details.

### Secret Security Tab

The Security tab contains settings that can be enabled to increase security for a secret. The settings listed below may or may not be visible, depending on your configuration settings:

- **Require Check Out:** Only one user at a time has access to a secret. See [Secret Check-Outs](#) for details.
- **Enable DoubleLock:** User must enter a doubleLock password to decrypt and view a secret.
- **Enable Requires Approval for Access:** Users must request access to view a secret.

- **Require Comment:** Users must enter a comment before being granted access to view the secret. The comment is stored in the audit log for that secret.
- **Enable Session Recording:** Record the Launcher session. This applies to secrets with a launcher associated with the secret template. See [Session Recording](#).
- **Hide Launcher Password:** Restrict users with View permission from copying passwords to the clipboard or unmasking the password text-entry field of the secret. This applies to secrets with a launcher associated with the secret template.
- **Customize Password Requirement:** Specify a password requirement for each password text-entry field.

## Secret Launcher Tab

The Launcher tab appears for secrets that use either a custom launcher or Web launcher.

If a custom launcher is associated with a secret template, a secret owner can configure associated secrets or a privileged secret to run the launcher process. The associated secret can be tied in to the command line parameters on the custom launcher, and the privileged secret is the identity that kicks off the launcher process.

If a Web launcher is associated with a secret template, the launcher tab displays how the Web launcher is configured for that secret. The following options are available:

- **Edit Fields:** Modify which secret text-entry fields are mapped to the HTML input controls on the target website.
- **Reconfigure Web Launcher:** Reset the Web launcher configuration.
- **Test Launcher:** Test the current Web Launcher configuration.
- **Use Web Password Filler:** Use the Web password filler rather than the Web launcher.

**Note:** See [Web Launcher](#) for details.

## Secret RPC Tab

The settings inside the Remote Password Changing tab are used for secrets that are Remote Password Changing (RPC) enabled:

- **Auto Change:** Enable or disable auto change for the secret.
- **Next Password:** Specify the next password

**Note:** See [Remote Password Changing](#) for details.

## Secret Dependencies Tab

The settings inside the Dependencies tab are used for secrets that have RPC enabled.

See [Manually Adding Dependencies](#) for details.

## Secret Configuration Options

### Common Configuration Options

These are the configuration options that are common to every secret:

- **Convert Template:** Change which template is being used to store and display information in this Secret.
- **Copy Secret:** Create a duplicate copy of the secret, which may also be renamed and modified.
- **Delete:** Delete the secret.
- **Edit:** Edit the secret parameters.
- **Favorite:** Click the star from the Dashboard or check this box on the Secret View page to mark the Secret as a favorite. It then be displays in the Favorite Secrets widget.
- **Folder:** Folder location of the secret. The secret inherits permissions of this folder, depending on the Default Secret Permissions setting in the Secret Server Configuration options.
- **Share:** Configure the sharing settings, or permissions, for the secret.
- **View Audit:** View the Secret audit log to see which users have accessed the Secret and the actions that have been performed.

### Advanced Configuration Options

These are the buttons, fields, and icons that are available for more advanced secrets:

- **Expire Now:** Expire the secret manually.
- **RDP Launcher Icon:** Click to open the Remote Desktop Protocol (RDP) Launcher. See further details in the Launcher section.
- **Run Heartbeat:** Initiate heartbeat, which attempts to verify that the Secret credentials can authenticate.
- **Site:** Edit the secret to set the distributed engine site. This determines where password changing, heartbeat, and proxied sessions run from.

## Managing Secrets

### Viewing Secrets

To view the information contained in a secret:

1. Locate the desired secret in one of these ways:
  - On the main menu, drill down the folders tree to select the secret.
  - Click the **Secret** menu item on the main menu and find the secret in the **All Secrets** table. You can filter the list or click the magnifying glass icon to search for the secret.
2. Click on the secret's name link. The secret's view page opens to the General tab.


## Customizing the All Secrets Table

On the main menu, there is a **Secrets** folder tree. When you click on the root or any subfolder, you see a list of all the secrets in that folder with multiple columns. You can customize what you see in one of three ways:

### *Filtering Search Results*

You can filter secret search results by selecting a folder on the left, either by clicking it or using the search text-entry field above the folder tree. On the right side of the widget, secrets can be filtered further by specifying search criteria in the top text box. The Advanced section allows filtering by secret template and status, as well as the option to include secrets contained in subfolders. Advanced criteria only remain in effect while those options are expanded (visible).

### *Customizing Visible Columns*

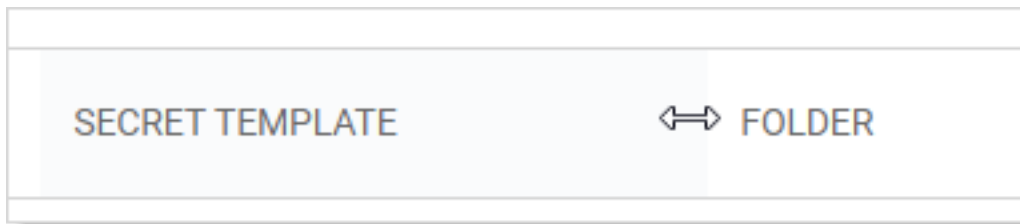
You can display additional columns on the grid by clicking the  icon. This data can be either secret metadata or template text-entry fields that have been set to be available for viewing. To select additional columns to display, click the **Advanced** link and then the **Column Selection** link. You can display the following metadata fields:

- Auto Change Enabled
- Checked out
- Checkout Enabled
- Created
- Days until Expiration
- Deleted
- Double Lock Enabled
- Expiration Field Changed
- Folder
- Inherits Permissions

- Heartbeat
- Hide Password
- Last Accessed
- Machine
- Notes
- Requires Approval
- Requires Comment
- Secret Template
- Username

### *Sizing Columns*

You can resize any of the columns by hovering the cursor over the border between them till it turns into a double arrow:

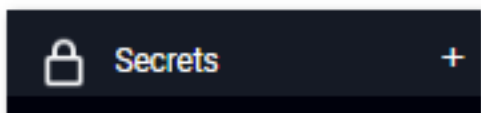


Click and drag to resize the column.

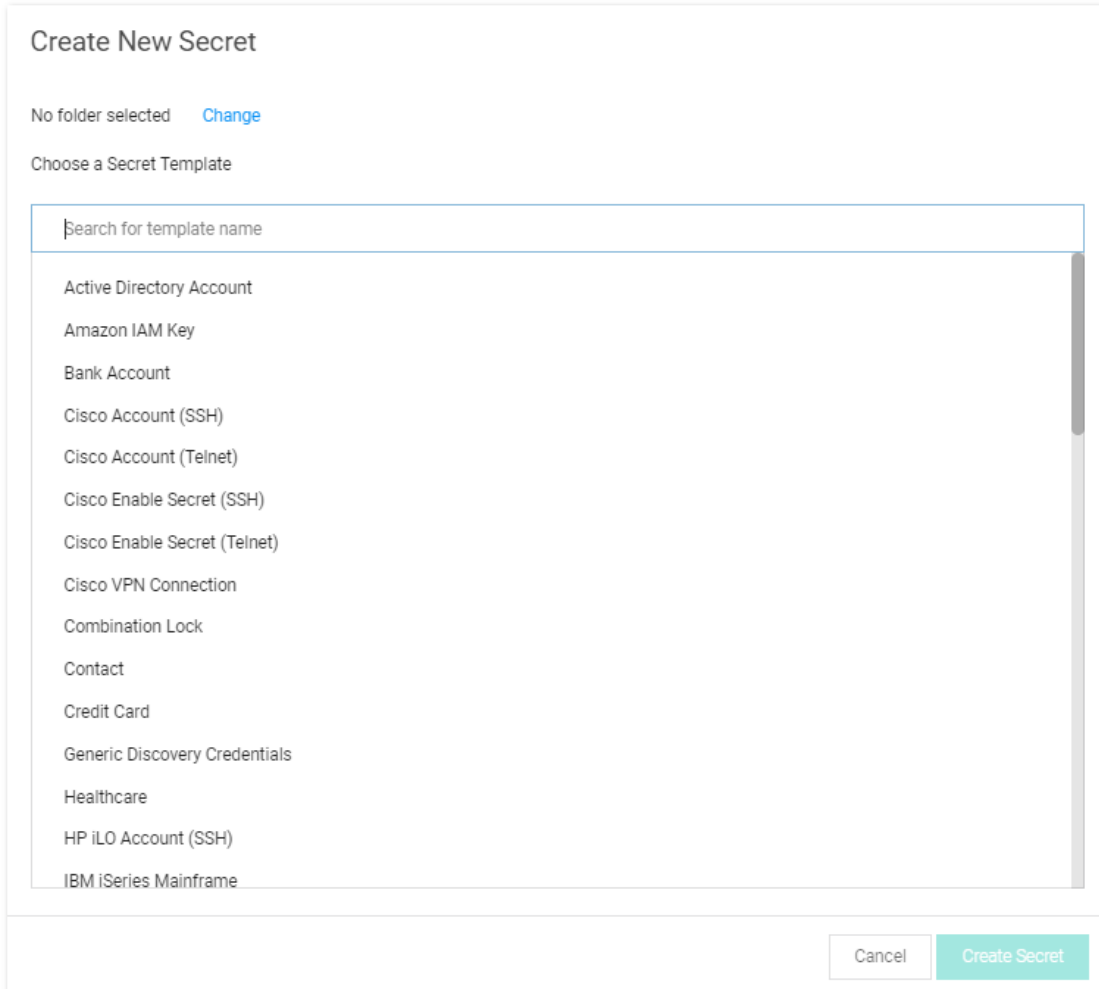
### **Creating Secrets**

To create a secret:

1. Click the **+** on the Secrets item on the main menu:



or click the  icon and select **New Secret**. The Create New Secret page appears:



2. Click the **Chose a Secret Template** list to choose a template from which to create the secret .

**Note:** If you do not find a suitable template available, you can create a custom template.

3. Click the **Create Secret** button. A Create New Secret page appears.

**Note:** These pages differ significantly, based on the secret template you chose. For this instruction, we chose the frequently used Web Password template.

Create New Secret

Template Web Password [Change](#)

Folder Everyone [Clear](#)

Name \*

URL \*

UserName \*

Password \*  Show Generate

Notes

Auto Change Enabled


Cancel Create Secret

- Complete the text boxes and selection controls on the page.

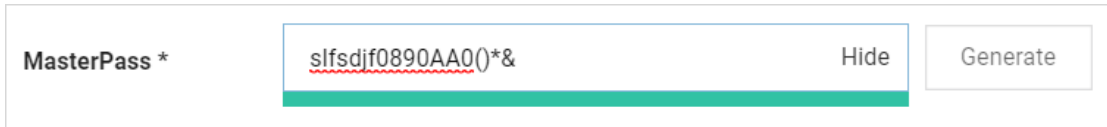
**Note:** The password generator is governed by a [password requirement](#), which is usually set via the secret template. However, you can override the template for this secret and set the requirement to something different in the Password Requirements section of the Security tab, after you create the secret.

- Click the **Generate** button to create a strong password that meets the requirements for that type of secret. You can also add your own. If you do, the password box will remain red until you enter a password that meets the requirements. The bar below the text box indicates the strength of the password you enter:

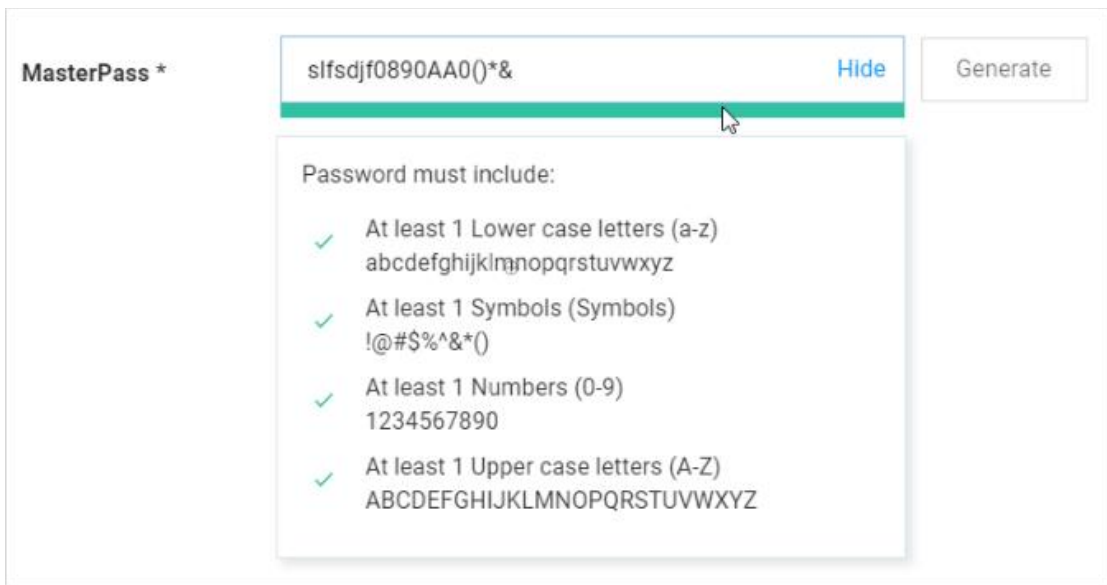
MasterPass \*  Hide Generate



When you type one that qualifies, the box and bar turn green:



If you want to see what requirements are governing the password, hover the mouse over the password strength bar:



6. Click the **Sites** list to select a site the secret belongs to.
7. (Optional) Click to select the **Auto Change Enabled** check box to enable automatic remote password change (RPC) for the secret.
8. Click the **Create Secret** button.

**Note:** It is possible to import data as secrets. See [Importing Secrets](#).

## Editing Secrets

**Note:** If using the Dashboard, see [Secret Server Dashboard](#).

To edit a secret:

1. Navigate to its secret **View** page by searching or drilling down the folder tree.
2. Click the **Edit All Fields** link. All text-entry fields become editable.

**Note:** The password generator is governed by a [password requirement](#), which is usually set via the secret template. However, you can override the template for this secret and set



the requirement to something different in the Password Requirements section of the Security tab after you create the secret.

3. For passwords, you can create a random password with the **Generate** button. This generates a password according to the rules set at the template level (see secret templates for more information about password requirements).
4. Click **Save**.

## Deleting and Undeleting Secrets

To delete a secret:

1. Navigate to the secret **View** page by searching or drilling down the folder tree.
2. Click the **Options** dropdown list and select **Delete**. A confirmation appears.
3. Click the **Confirm Delete Secret** button.
4. The secret is logically deleted and hidden from users who do not have a role containing the View Deleted Secrets permission.

Secret Server uses these "soft deletes" to maintain the audit history for all data. However, deleted secrets are still accessible by administrators (like a permanent Recycle Bin) to ensure that audit history is maintained and to support recovery. A user must have the View Deleted Secrets permission in addition to Owner permission on a secret to access the secret View page for a deleted secret. For more information about these permissions, see [Roles](#) and [Sharing a Secret](#).

To undelete a secret, navigate to the secret View page and click **Undelete**.

**Note:** Secrets can also be deleted in bulk. See [Running Dashboard Bulk Operations](#).

## Duplicating Secrets

The secret duplication function allows for easier, automatic secret duplication. Any user with the Owner Secret permission on a secret can click to select **Duplicate** in the **Options** dropdown list to create a new secret with information based on the original secret. Secret text-entry field information, launcher settings, secret settings, double locks, email settings, and permissions are copied over. Audit records are written to the source secret and target secret to indicate that a copy operation took place. Currently, file attachments are not copied.

## Overriding the Secret Template's Password Requirements

All secrets inherit a set of password requirements (see [Template Password Requirements](#)) from their parent secret template. After you create a secret, you can choose to use a different password requirement for this one secret, which leaves other secrets based on the template as they were. To choose a different password requirement for the secret:

1. Navigate to the secret **View** page by searching or drilling down the folder tree.

2. Click the secret to open the secret's page.
3. Click the **Security** tab.
4. Click the **Edit** Link in the **Password Requirements** subsection in the **Other Security** section. The Edit Password popup appears.
5. Click the Password Requirement dropdown list to select the password requirement you desire.
6. Click **Save**.

## Sharing Secrets

Sharing passwords is crucial for information technology teams. Due to the sensitive nature of sharing secure information, Secret Server ensures shared passwords are tracked and guarded.

### Permissions

There are three permission levels to choose from when sharing secrets with another user or group:

- **View:** User may see all secret data, such as username and password, and metadata, such as permissions, auditing, history, and security settings.
- **Edit:** User may edit the secret data. Also allows users to move the secret to another folder unless the Inherit Permissions from Folder setting is turned on, in which case the user needs Owner permissions to move the secret.
- **List:** User may see the secret in a list, such as a list returned by running a search, but not to view any more details about a secret or edit it.
- **Owner:** User may change all the secret's metadata.

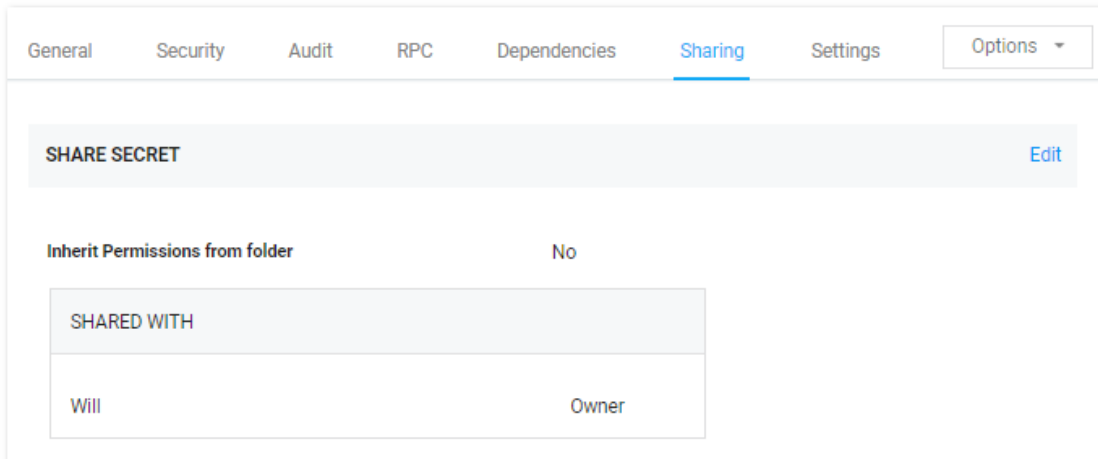
**Note:** Password text-entry fields are not visible if a secret has a launcher and the Hide Launcher Password setting is on or the user does not have the View Launcher Password role permission.

Secrets can be shared with either groups or individual users. The Secret Sharing section allows secrets to be configured for access.

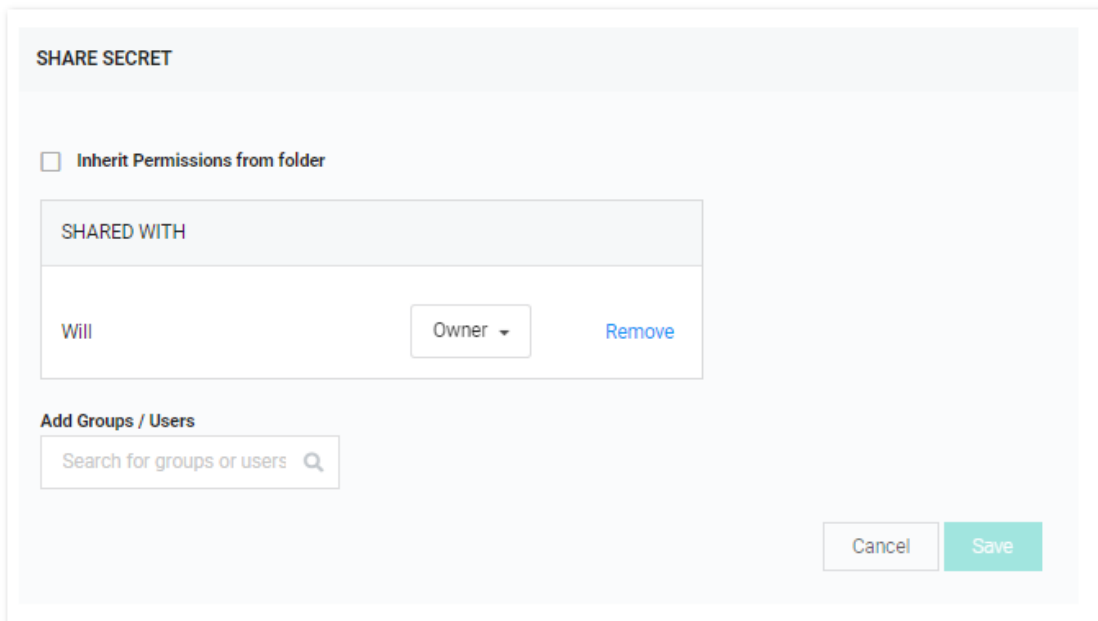
### Procedure

To add or remove secret sharing:

1. [View the secret](#) you want to share.
2. Click the **Sharing** tab.



3. Click the **Edit** link. The page becomes editable:



4. Click the **Remove** link next to any share you want to delete.
5. Type any user or group you want to share with in the **Add Groups / Users** search text box.
6. When the user or group appears in the dropdown list, click to select it. The user or group appears in the **Shared with** table.
7. Click the unlabeled permission dropdown list box to select the desired permission.
8. Repeat the process for additional users or groups.

9. Click **Save** to commit the changes.

You can also modify sharing settings for users or groups that already have sharing enabled for the secret. If a user or group is not displayed, they do not have access to the secret.

To further simplify the sharing process, secrets can automatically inherit the settings from the folder they are stored in. By enabling the **Inherit Permissions from Folder** option on the **Sharing Edit** page, a secret inherits all the parent folder's sharing settings. For more on folder security, see the [Folders](#) section.

## Setting Up Password Masking

Password masking prevents over-the-shoulder viewing of your passwords by a casual observer (passwords show as \*\*\*\*\*). For security, the number of asterisks does not relate to the length of the password.

As an administrator, you can force all the secret password text-entry fields in the system when viewed to be masked. To do this, enable the **Force Password Masking** setting in the **Configuration** settings. Only secret text-entry fields marked as a password text-entry field on the secret template is masked.

There is also a user preference setting that forces password masking on all secret password text-entry fields viewed by the user. This Mask passwords when viewing secrets setting is found in the **Profile > Preference** section for each user. If the configuration setting discussed above is enabled, this user preference setting is overridden and cannot be disabled.

## SECRET FOLDERS

### Introduction

Folders allow you to create containers based on your needs. They help organize your customers, computers, regions, and branch offices, to name a few. Folders can be nested within other folders to create sub-categories for each set of classifications. Secrets can be assigned to these folders and sub-folders. Folders allow you to customize permissions at the folder level, and all secrets within can inherit the folder's permissions. Setting permissions at the folder level ensures future secrets placed in that folder have the same permissions, simplifying management across users and groups.

**Note:** You can "favorite" a folder in the main menu by right clicking it.

### Folder Permissions

If the new folder is a subfolder, you can have it use the sharing settings of its parent folder by enabling the Inherit Permissions from Parent setting for the folder.

Folders can apply one the following permissions to users or groups in the folder's Permissions table:

- **View:** Allows the user to see the folder and secrets in that folder that are inheriting permissions from their folder.
- **Edit:** Allows the user to create new folders in that folder, which forces the "Inherit Permissions from Parent" permission on the new folder, move secrets into that folder, and add new secrets into that folder.
- **Add Secret:** Allows the user to add a secret in that folder. Does not grant access to the added secret.
- **Owner:** Allows the user to create new folders in that folder without forcing inheritance, move the folder, delete the folder, rename the folder, and change the permissions and inheritance settings on the folder.

Depending on your configuration, these settings could affect the permissions of subfolders and secrets contained in this folder. Folders are not visible to users that do not have at least View permission. This allows users to create and manage their own folders without making them visible to all users.

## Personal Folders

In Secret Server, a *personal folder* is a folder that one (and only one) individual has owner access to. No user can modify sharing permissions on these folders. A user cannot add subfolders to their personal folder. The purpose of this folder is to allow a user to securely store work-related secrets that other users do not require access to. Note that when in break-the-glass mode, an unlimited admin can access a user's personal folder in order to recover secrets if needed.

## Required Role Permissions for Managing Folders

Folder management is subject to these role permissions:

- The Administer Folders role permission allows a user to create new folders and manage folders, but specific folder permissions still apply.
- Any user with the Administer Folders role permission can create new folders; however, to create folders at the root level, the user also needs the Create Root Folders permission. They also can add new folders to any folders where they have Edit or Owner permission on that folder.
- They must have Owner permission to delete a folder.
- Users can also move folders where they have Owner permission on the source folder and Edit or Owner permission on the target folder (where they are moving it). The folder automatically inherits Permissions from its parent when it is moved, which is the same as when secrets are moved.


## Managing Folders

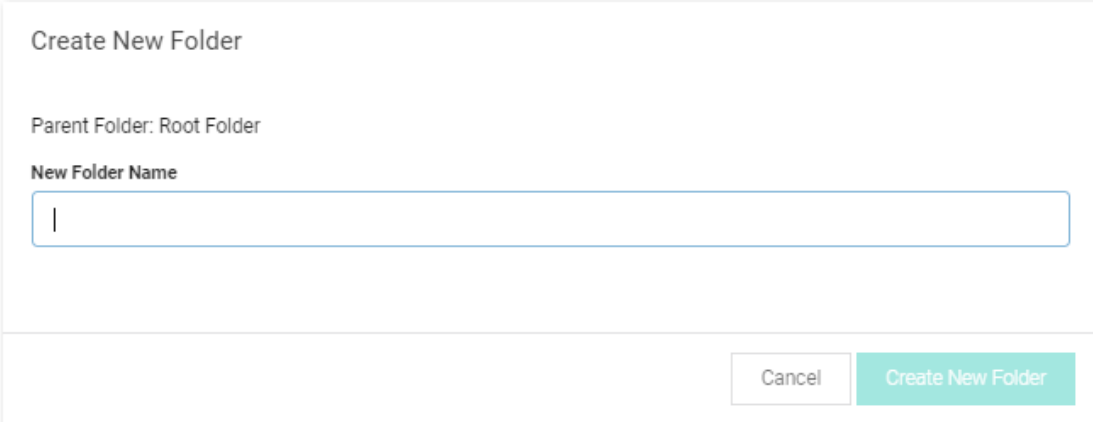
### Creating Folders

To create a folder:

**Note:** To create folders, you must have a role with the Administer Folder permission. You also must have Edit or Owner permission for the parent folder.

1. Click the parent folder for the new folder in the folder tree in the main menu. If you do not select one, the root is assumed.

2. Click the  icon and select **New Folder**. The Create New Folder pop-up page appears:



Create New Folder

Parent Folder: Root Folder

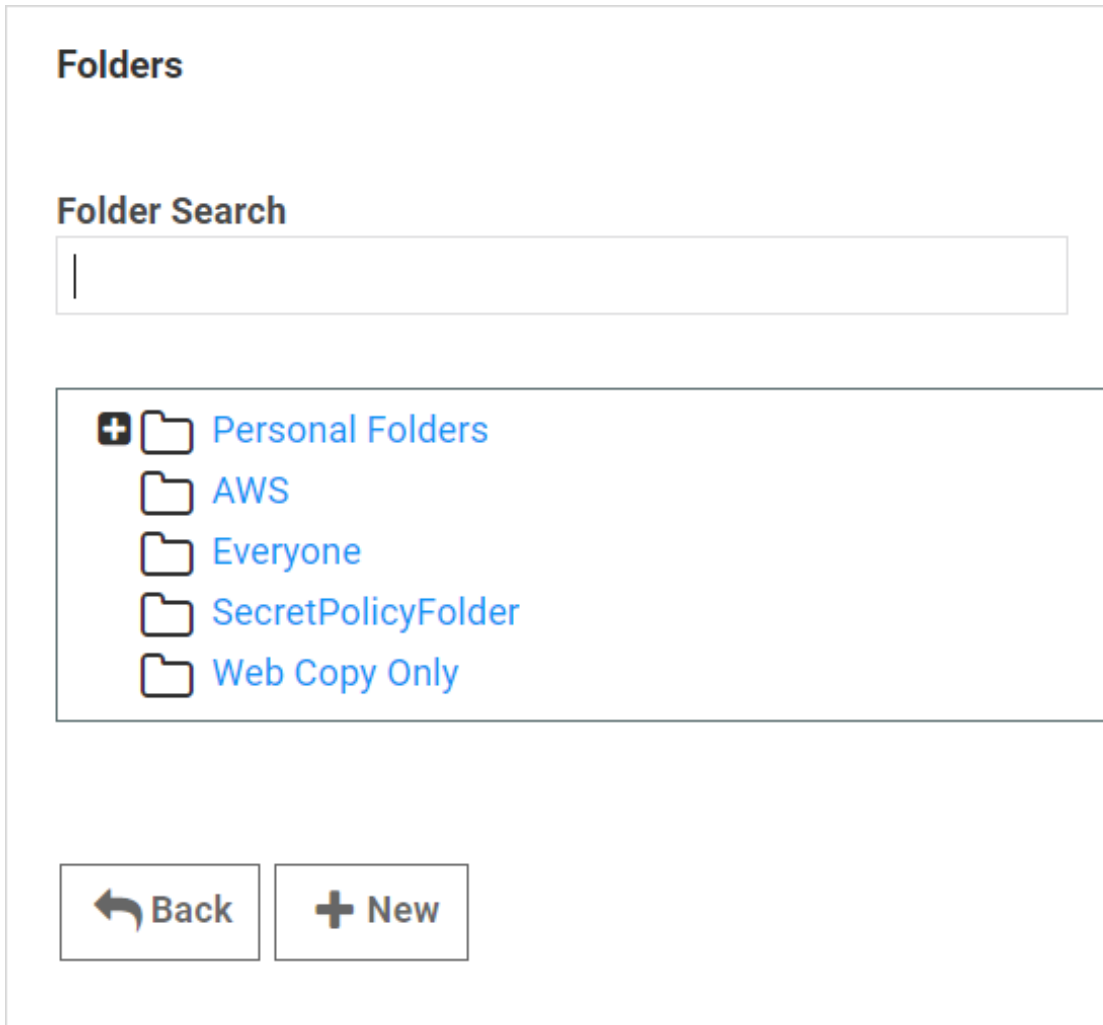
New Folder Name

Cancel Create New Folder

3. Type the folder name in the **New Folder Name** text box.
4. Click **Create New Folder**. The new folder appears in the folder tree under its parent folder.
5. Proceed to [Editing Folder Permissions](#) to customize permissions for the new folder.

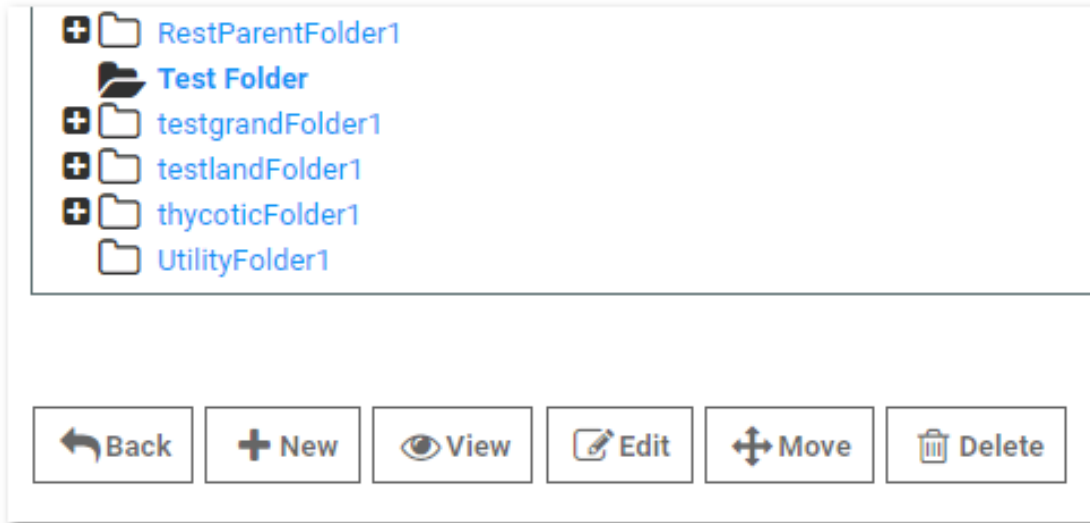
### Editing Folder Permissions

1. Click **Admin > Folders**. The Folders page appears:



1567715914715

2. Navigate to or search for the desired folder.
3. Click the folder's name. The folder is bolded, which indicates it is selected, as does the appearance of several new buttons:



4. Click **Edit**. The Edit Existing Folder page appears:



### Edit Existing Folder

Folder Path: \

Folder Name:  \*

Folder Icon:  ▾

Inherit Secret Policy:

Secret Policy:  ▾

Inherit Permissions from Parent:

---

**PERMISSIONS FOR**

NAME	FOLDER PERMISSIONS ⓘ	SECRET PERMISSIONS ⓘ
Will	<input type="text" value="Owner"/> ▾	Owner <input type="checkbox"/> Override

**Add Group/User**



---

**RESTRICT SECRET TEMPLATES**

Secrets from all Secret Templates may be used within this folder. Enable this setting to allow only Secrets from specific Secret Templates within this folder.

5. Edit the following folder-specific settings as desired:

**Important:** A secret only inherits permissions from a folder if the secret has the "Inherit Permissions from Folder" check box enabled on the secret's Sharing tab. Otherwise, folder permissions are ignored.

- **Folder Path label:** The location in the folder tree, which only changes by moving the folder.
- **Folder Name text box:** The folder's name
- **Folder Icon list:** The icon for the folder. "Customer" creates a user icon, and "Computer" creates a monitor icon, representing a computer.

- **Inherit Secret Policy check box:** Any added or created secrets inherit their policy from the folder's parent (or higher) folder, thus having the same policy as the folder. Secret policies are sets of configurations for secrets. When this control is selected, the Secret Policy list is disabled.
  - **Secret Policy list:** Specifies the secret policy for the folder, if any, which is applied if the Inherit Secret Policy check box is disabled.
  - **Inherit Permissions from Parent check box:** Added or created secrets get their permissions from the folder's parent folders. Permissions are rules on what users and roles can and cannot do. When this check box is enabled, the Permissions table becomes disabled because the folder no longer enforces its own permissions.
6. Add users or groups to the folder by typing their name in the **Add Group/User** search text box and clicking the result in the dropdown. A new user or group appears in the Permissions table:

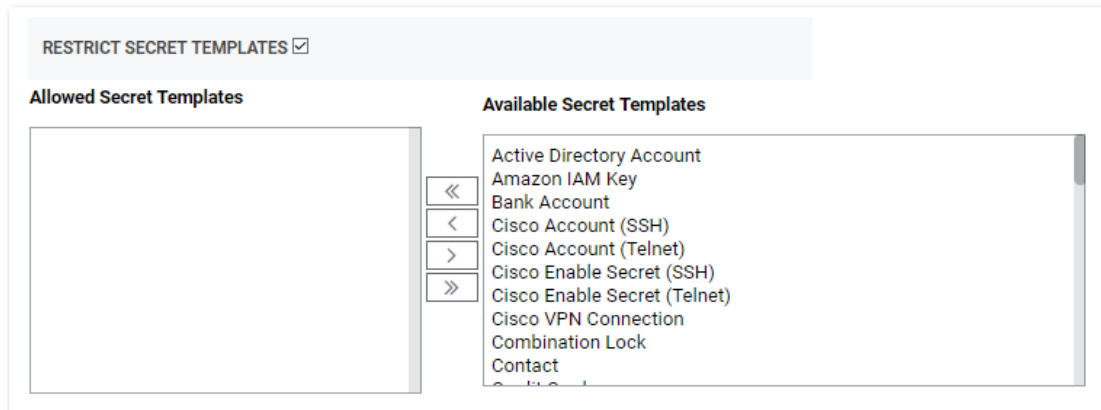


7. Click the **Folder Permissions** dropdown list for the user to select folder permission level for the user or groups: View (folder), Add Secret (to folder), Edit (folder), or Owner (of folder).
8. Click to select the **Override** check box to override that user or group's assigned permission in the secret itself (on the Sharing tab). The Secret Permissions list box for that user or group becomes enabled so you can choose what new permission to override the secret permission with.
9. Click the **Secret Permissions** list for the user to select secret-related permissions for the user or groups: List (secrets in folder), View (secrets in folder), Edit (secrets in folder), or Owner (of secrets in folder).
10. Proceed to [Restricting Secret Templates for Folders](#) to customize allowed secret templates for the new folder.

**Note:** It is possible to setup an automatically replicated folder structure from an external database, such as ConnectWise or other CRM systems. This topic is discussed later in [Folder Synchronization](#).

### Restricting Secret Templates for Folders

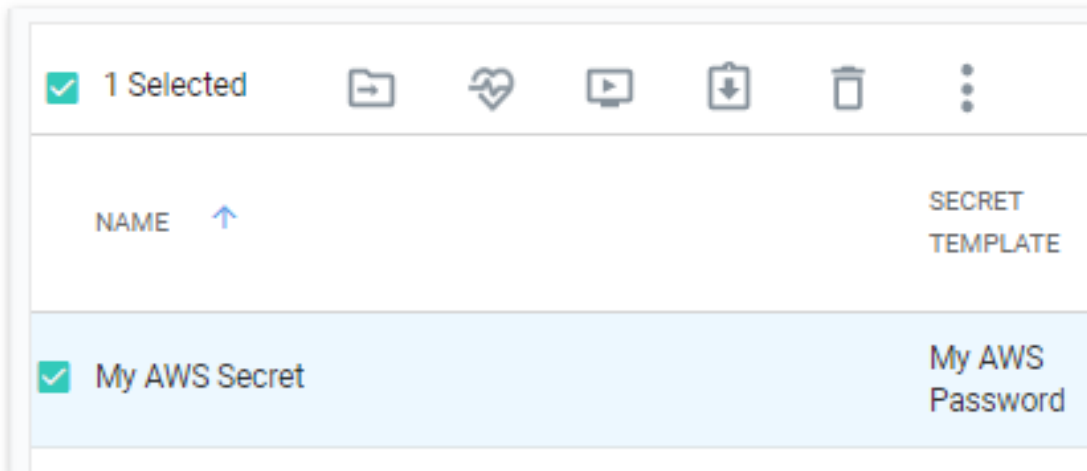
1. On the **Edit Existing Folder** page, click to select the **Restrict Secret Templates** check box. The Allowed and Available Secret Template lists appear:




2. Select one or more of the secret templates in the **Available Secret Templates** list and use the arrow buttons to move the template to the **Allowed Secret Templates** list.
3. Click **Save**.

### Adding and Moving Secrets Between Folders

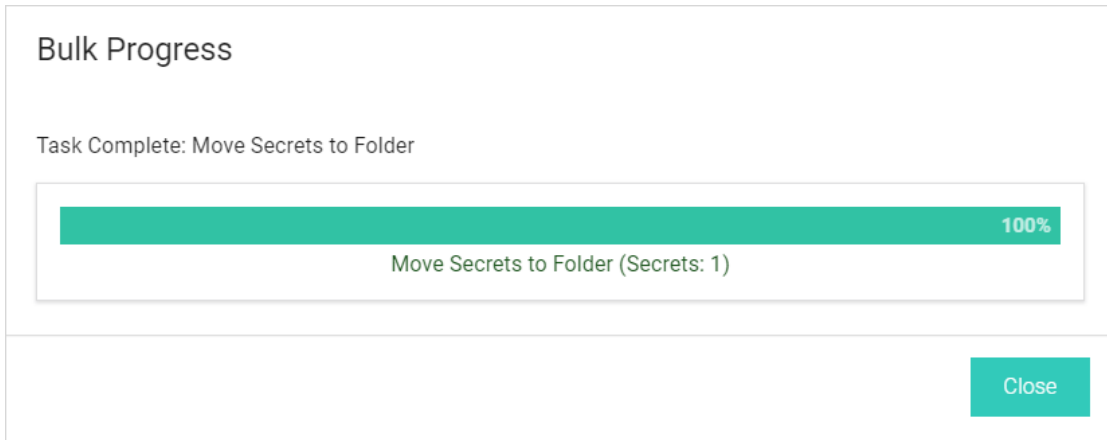
1. Consider the following before moving a secret between folders:
  - To add or move a secret to a folder, you must have Edit permission on that folder (either direct or through inheritance).
  - To move a secret from a folder, you must have Edit permission on that secret. If the secret has the "Inherit Permissions from folder" setting enabled, then you must have Owner permission to move that secret to a new folder.
  - When a secret is moved to a folder, it automatically gets the "Inherit Permissions from folder" setting even if it had specific permissions before the move.
2. Navigate to the folder containing the secret or secrets you want to move.
3. For each secret:
  1. Hover the mouse pointer over the secret. A check box appears on the left end.
  2. Click to select the check box. A command row of icons appears:



4. Click the Move to Folder  icon. The Move Secrets pop-up page appears:



5. Navigate to and select the target folder for the secret or secrets.
6. Click the **Move Secrets** button. The Bulk Progress popup appears:

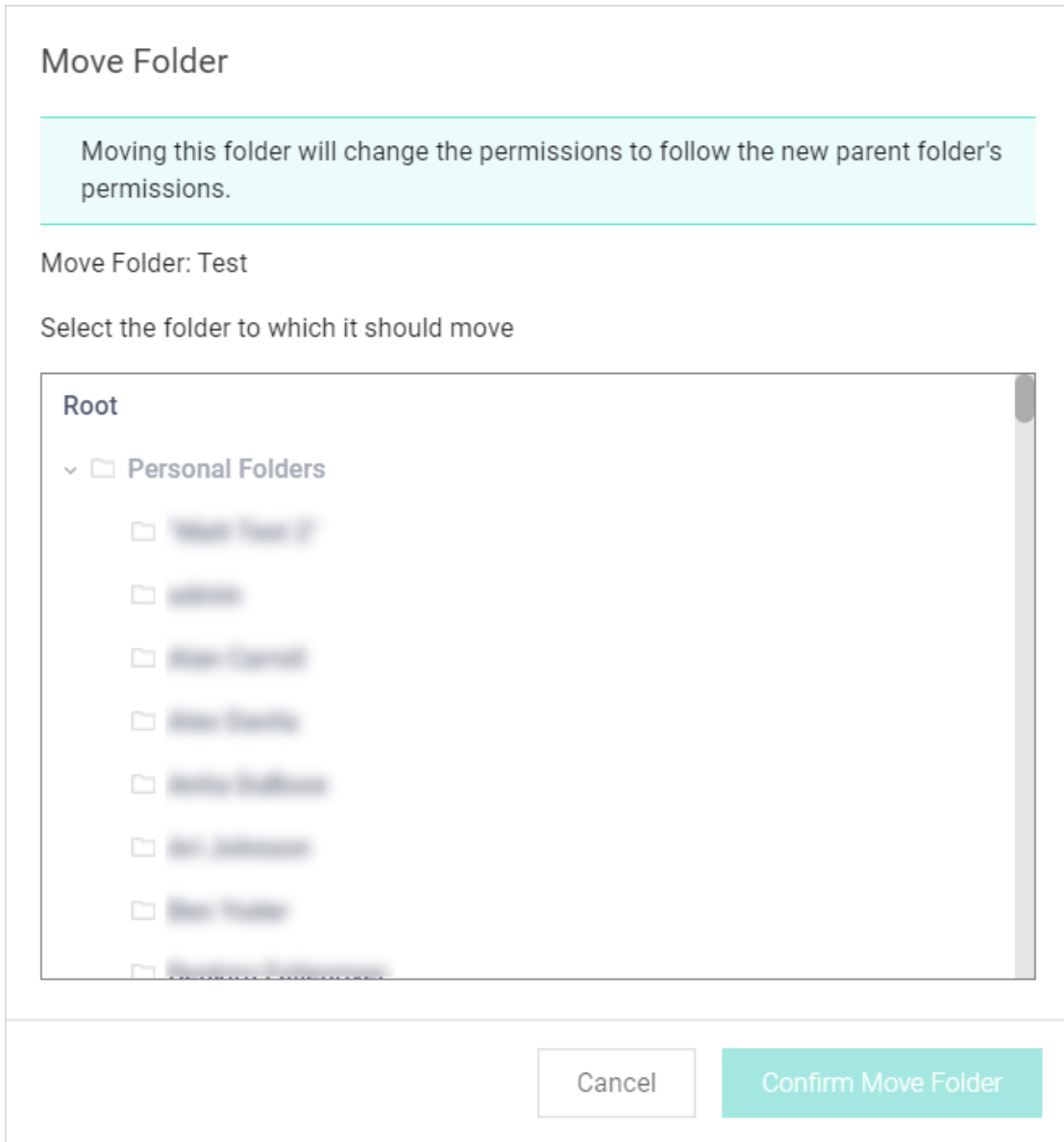


7. The secret moves to the selected folder.

### Moving Folders

There are two ways to move folders. The **easiest way is to drag a folder** over another and drop it. However, this method does not work on the root folder. The other way is as follows:

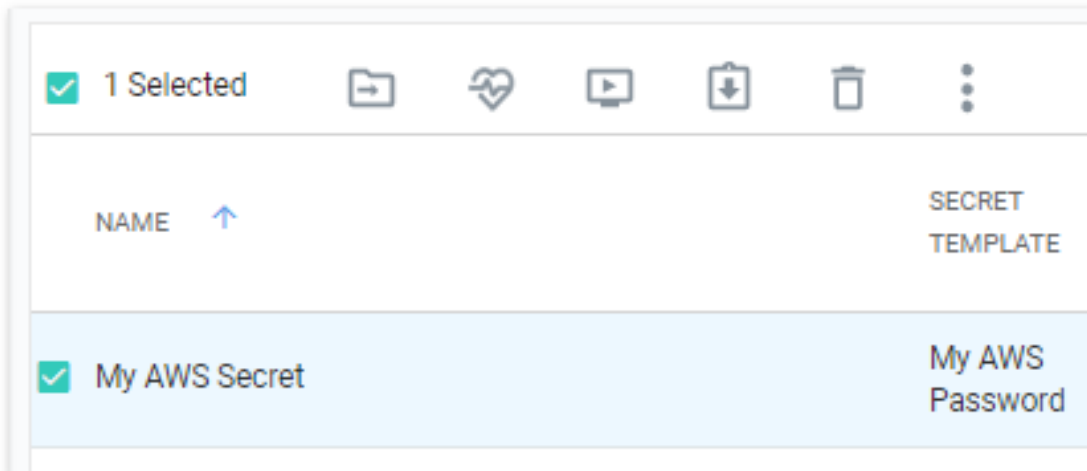
1. Ensure that you have edit permission for both the source and destination folders.
2. Right click the folder in the navigation pane and select **Move Folder**. The Move Folder page appears:




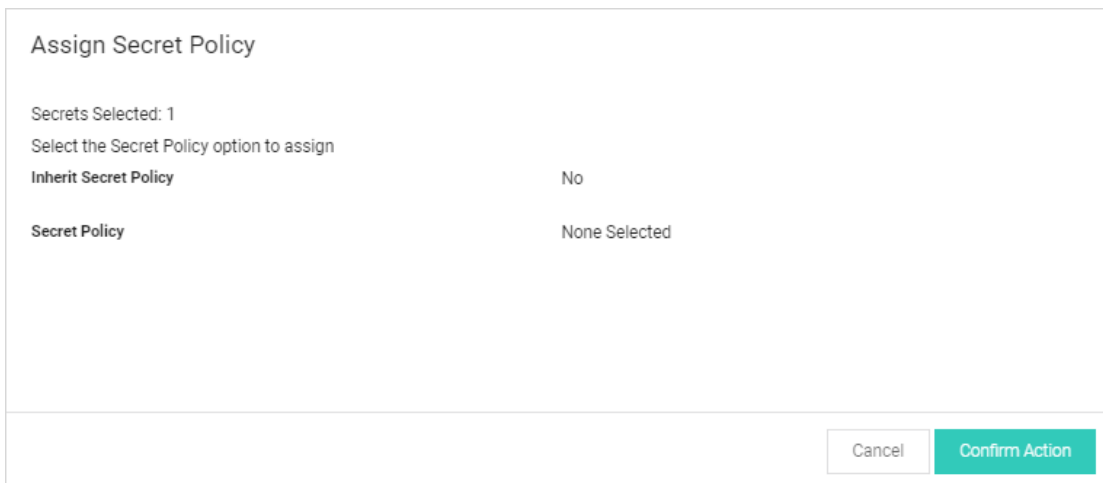
3. Navigate to and select the destination folder in the folder tree.
4. Click the **Confirm Move** button.

### Assigning Secret Policies to Folders

1. Navigate to the folder containing the secret you want to assign a policy to.
2. Hover the mouse pointer over the secret. A check box appears on the left end.
3. Click to select the check box. A command row of icons appears:



- Click the Assign Secret Policy  icon. The Assign Secret Policy pop-up page appears:



- Click **Confirm Action**.

### Modifying Folders with Secret Policies

You can configure secret policies to apply RPC and security settings to an entire folder of secrets.

## Secret Policy

[Explain](#)

< 1 to 1 of 1 >

Secret Policy Name	Description	Active
<a href="#">Enable Auto Change</a>	Force Auto Change to be enabled for all Secrets in the folder.	Yes

Show Inactive

[← Back](#) [+ Create New](#)

To create a new secret policy:

1. Click **Admin > Secret Policy**. A Secret Policy page appears:



## Secret Policy


[Explain](#)

< 1 to 9 of 9 >

SECRET POLICY NAME	DESCRIPTION	ACTIVE
Checkout_Enforced		Yes
Enforced_Autochange		Yes
Privilage account		Yes
Secret_Policy_test_folder		Yes
site_Enforced		Yes
Skipped policy		Yes
Test_Policy		Yes
TestWK		Yes
Wkflow		Yes

Show Inactive

 Back

 Create New

2. Click the **Create New** button. The (new) Secret Policy page appears:

**Secret Policy**

[Explain](#)

**Secret Policy Name**  \*

**Description**

**Active**

SECTION	SECRET POLICY ITEM NAME	SETTING	VALUE
General	Site		< Not Set > ▾
Remote Password Changing	Auto Change		< Not Set > ▾

3. Type a name for the new secret policy in the **Secret Policy Name** text box.
4. Click the Setting dropdown list, and choose the policy's settings for each relevant section. Aside from < Not Set >, which means that the setting is not applied, there are two options:
  - **Default:** The policy is applied to all secrets in the folder initially, but it **is** possible to manually change the applied secret settings as well.
  - **Enforced:** The policy is applied to all secrets in the folder initially, and it **is not** possible to change those applied settings on secrets in that folder.
5. Click to select the **Value** check box in that row to apply the setting. Applying the setting may enable configuration of related settings in the grid. For example, enabling Auto Change causes the Auto Change Schedule to be available for configuration:

**Secret Policy**

[Explain](#)

**Secret Policy Name**  \*

**Description**

**Active**

SECTION	SECRET POLICY ITEM NAME	SETTING	VALUE
General	Site	< Not Set > ▾	
Remote Password Changing	Auto Change	Enforced ▾	<input checked="" type="checkbox"/>

6. Click **Save** to make the policy available for assignment to folders.

**Note:** To deactivate a policy that you no longer want, edit the policy and deselect the **Active** check box. For information about applying a secret policy to a folder, see [Editing Folder Permissions](#).

### Enabling Personal Folders

To use personal folders, you must first enable them:

1. Click **Admin > Configuration**.
2. Click the **Folders** tab:

**Configuration**

General Login SAML **Folders** Local User Passwords Security Ticket System Email Session Recording

Require View Permission on Specific Folder for Visibility	Yes
Enable Personal Folders	Yes
Personal Folder name	Personal Folders
Show user warning message	Yes
Warning message text	This folder is for work related Secrets only. Do not store personal non-work Secrets, such as your Online Banking password, in this folder.

3. Click **Edit**:

**Configuration**

General Login SAML **Folders** Local User Passwords Security Ticket System Email Session Recording

Require View Permission on Specific Folder for Visibility	<input checked="" type="checkbox"/>
Enable Personal Folders	<input checked="" type="checkbox"/>
Personal Folder name	<input type="text" value="Personal Folders"/>
Show user warning message	<input checked="" type="checkbox"/>
Warning message text	<input type="text" value="This folder is for work related Secrets only. Do not store personal non-work Secrets, such as your Online Banking password, in this folder."/>

4. Select the **Enable Personal Folders** check box.
5. (Optional) Type a new folder name in the **Personal Folder name** text box to customize the root-level folder that contains all personal folders.




6. (Optional) If you want to display a warning message to users when placing secrets in their personal folders:
  1. Click to select the **Show user warning message** check box.
  2. (Optional) Edit the **Warning message text** box.
7. Click **Save**. A personal folder for each user is now created in a root-level folder with the personal folder name specified.

**Note:** When personal folders are enabled, a user requires the Personal Folders role permission in their role to be able to view and use their own personal folder.

## SECRET TEMPLATES

### Secret Template Settings

The secret Template Designer provides several settings to customize secret template text-entry fields:

- To add a secret text-entry field, fill out the values and click the **+** button.
- To delete a text-entry field, click the  icon. There is a confirmation dialog box before deletion takes place.
- To edit a text-entry field, click the  icon. Click either the  icon to save or the **X** icon to discard the changes.

#### *Secret Template Text-Entry Field and Control Settings*


The settings available for text-entry fields are:

- **Field Name:** Name of the text-entry field. This name is used for the Create New drop-down list on either the Dashboard's Create Secret Widget or Home page.
- **Field Description:** Description of the text-entry field.
- **Field Type:** Type of the text-entry field. See below for a description of the different text-entry fields.
- **Is Required:** Whether the text-entry field should require a value. These check boxes are checked for correct content when the user attempts to create this secret. A validation error is displayed if not entered correctly.
- **History:** Number of values to keep in the text-entry field's history of values.
- **Searchable:** Whether that text-entry field should be indexed for searching. By default, passwords are not indexed. File attachments and history cannot be indexed for searching.

- **Edit Requires:** Minimum permissions on the secret needed in order to edit the value on the secret. The options are Edit, Owner and Not Editable. This enables the secret text-entry field to be locked down at a more granular level than other text-entry fields on the template.
- **Hide on View:** If checked, this text-entry field is not displayed to users when viewing the secret. The text-entry field is only be displayed when the secret is in Edit mode.
- **Expose for Display:** If checked, this text-entry field is available to be displayed as a Custom Column on the Secret Server Dashboard.

**Note:** All text-entry fields that are set to "Expose for Display" are **not** encrypted in the database. Only check this value if the secret text-entry field data is not considered privileged information.

The order of the text-entry fields in the Template Designer grid is the same as those that appear when the user views or edits a secret created from the template. The order can be modified through the up and down arrows on the grid.

Default values can be specified on each text-entry field by clicking the edit defaults  button . These added values appear as a list on any secret created from this template.

### *Secret Template Field Types*

Template text-entry fields can be specified as one of several different types to enhance customization:

- **Text:** Single-line text-entry field.
- **Notes:** Multi-line text-entry field.
- **URL:** Clickable hyperlink.
- **Password:** Password type text-entry field.
- **File:** File attachment link. File attachments are stored in the Microsoft SQL Server database.

## **Template Character Sets**

Character sets are a collection of distinct characters that are used in password requirements and password rules. Custom sets can be created, and both ASCII and Unicode are supported. For more information on setting up compliance checks and password generation standards, see [Password Requirements](#). The five standard character sets are:

- Lower Case (a-z)
- Upper Case (A-Z)

- Numeric (0-9)
- Non-Alphanumeric (!@#\$%^&\*())
- Default – Includes all the above

To manage character sets, click the **Character Sets** button on the **Administration > Secret Templates** page. Only character sets which are not currently used by a password requirement can be deleted.

## Template Password Requirements

### Overview

Set requirements on a password text-entry field to validate user-entered passwords or make auto-generated passwords conform to set specifications.

A password requirement is made up of a minimum and maximum length, a set of characters, and optional rules such as "At least three upper-case characters" or "The first character must be lower-case". The default password requirement is 12 characters from the default character set, with at least one upper-case, lower-case, numeric, and symbol character.

Create or edit password requirements by clicking the **Password Requirements** button on the **Administration > Secret Templates** page.

Click the **Character Sets** button next to the Password Requirements button to create or delete character sets.

### Setting the Password Requirement for a Secret Template

To set the password requirement for a text-entry field for a secret template:

1. Go to **Admin > Secret Templates**. The Manage Secret Templates page appears:

**Manage Secret Templates**

Active Directory Account  Show Inactive

[Back](#) [Edit](#) [+ Create New](#) [Export](#) [View Audit](#) [Active Templates](#)

[\\* Password Requirements](#) [A Character Sets](#) [Configure Launchers](#)

[Configure Secret Template Permissions](#)

**Other Templates**

[Configure Dependency Templates](#) [Configure Scan Templates](#)

**Import Secret Templates**

Please paste your XML from the online [Secret Templates Gallery](#) into the box below to add your new Secret Template.


[Import](#)

2. Select the desired template in the unlabeled dropdown list.
3. Click **Edit**. The Secret Template Designer page appears:







Secret Template Designer

**SETTINGS**

Secret Template Name: Test Template  
 Secret Template Icon:   
 Active?:   
 Expiration Enabled?:   
 Validate Password Requirements On Create?:   
 Validate Password Requirements On Edit?:   
 Field Displayed on Basic Home: Folder Name

**FIELDS**

FIELD NAME	FIELD DESCRIPTION	FIELD TYPE	IS REQUIRED?	HISTORY	SEARCHABLE	EDIT REQUIRES	HIDE ON VIEW	EXPOSE FOR DISPLAY	
MasterPass	Master Password	Password	<input checked="" type="checkbox"/>	All	<input type="checkbox"/>	Edit	<input type="checkbox"/>	<input type="checkbox"/>	   
	<input type="text"/>	<input type="text"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> All	<input type="checkbox"/>	<input type="text" value="Edit"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="button" value="Add"/>


Show Inactive Fields

There is/are 1 Test Template Secret(s).

- Click the **Assign Password Requirement** button. The Secret Template Passwords page for that template appears:

**Secret Template Passwords**

**Passwords for Test Template.**

FIELD NAME	PASSWORD REQUIREMENT	
MasterPass	Default	

- Click the pencil edit icon for the field you desire. The password requirement turns into a dropdown list.
- Click to select the desired password requirement.
- Click the **Save** icon to save the changes.

## Creating a Custom Password Requirement

To create a new password requirement:

1. Go to **Admin > Secret Templates**. The Manage Secret Templates page appears:


The screenshot shows the 'Manage Secret Templates' page. At the top, there is a dropdown menu set to 'Active Directory Account' and a checkbox for 'Show Inactive'. Below this is a row of buttons: 'Back', 'Edit', 'Create New', 'Export', 'View Audit', and 'Active Templates'. A second row contains 'Password Requirements', 'Character Sets', and 'Configure Launchers'. A third row has 'Configure Secret Template Permissions'. The 'Other Templates' section includes 'Configure Dependency Templates' and 'Configure Scan Templates'. The 'Import Secret Templates' section contains a text box with the instruction: 'Please paste your XML from the online [Secret Templates Gallery](#) into the box below to add your new Secret Template.' Below the text box is an 'Import' button.

2. Click the **Password Requirements** button. The Password Requirements page appears:

Password Requirements				
NAME	DESCRIPTION	MINIMUM LENGTH	MAXIMUM LENGTH	DEFAULT
Default	The default password requirement, which uses the alpha-numeric character set and requires one lowercase, one uppercase, one number, and one symbol.	12	12	Yes
SAP	SAP Password Requirement	12	12	No
Mainframe	Mainframe Password Requirement	8	8	No

3. Click **Create New**.

### Password Requirement Edit

 **Example:**

**Name**

**Description**

**Is Default**

---

**GENERATE PASSWORD**


Prevent Username In Password

Length between \*  and \* .

Using  [Character Set.](#)

---

**Password Rules**

Minimum of  from  

[Show Usages](#)

4. Type the name and description.
5. If you want the requirement to become the new default, click to select the **Is Default** check box.
6. Set the general options for the requirement in the **Generate Password** section.

**Note:** You can also create a custom character set by clicking the Character Set link.

7. Add one or more password rules:
  1. Click to select the type of rule in the first dropdown list in the **Password Rules** section.
  2. Set that type's parameter in the following text box.
  3. Click to select the character set from the "from" dropdown list.
  4. Click the + icon to save the rule.
8. Click **Save**.

**Note:** To set a custom password requirement for a specific secret, use the "Customize Password Requirement" in the Security tab of a secret. For details, see the [Secret Security Tab](#) section.

**Note:** You can enable or disable the validation of manually entered passwords at the secret template level via the "Validate Password Requirements on Create" and "Validate Password Requirements on Edit" settings.

**Note:** The "What Secrets Do Not Meet Password Requirements" report shows secrets containing a password that does not meet the password requirements set for its secret template.

**Note:** Password requirements cannot include rules with overlapping character sets. For example, if an attempt is made to add both a "Minimum of 1 upper-case" rule and a "Minimum of 3 Default" rule to a new password requirement, an error displays.

## TEMPLATE NAMING PATTERNS

Secret Server supports naming patterns for secret templates. Naming patterns are a way for administrators to maintain consistency for secret names and can help ease both browsing and grouping secrets by name. Patterns are created using regular expressions. Regular expressions are a formal set of symbols commonly used to match text to patterns. For example, the regular expression `^\w+\\w+$`, allows `NTDOMAIN01\USER3454` but not `USER3454` on `NTDOMAIN01`.

**Note:** Regular expressions are beyond the scope of this document. They are very powerful and can get quite complex—books have been written on the topic. Microsoft offers a good overview at their [Regular Expression Language Quick Reference](#) Web page.

## SSH Authentication Templates

With this Secret Server feature, admins can use private SSH keys for PuTTY launcher sessions as well as for RPC tasks (configurable through password changer settings) and Unix and Linux discovery. Passphrases can additionally be stored, if necessary, to decrypt the private keys for additional security. The Unix Account (SSH) secret template includes text-entry fields for the private key and passphrase by default:

The SSH Key template is included by default and can be used to store SSH keys that can later be selected for use in RPC, discovery or launcher authentication for other secrets:

**Note:** Starting with version 10.1.000000, Secret Server also supports SSH key rotation on secrets.

The **Unix Account (SSH Key Rotation)** and **Unix Privileged Account (SSH Key Rotation)** secret templates use password changers that change the public key in the account's `authorized_keys` file as well as change the password on the account. Secret Server ships with a password changer and custom command sets that allow an account to change its own public key and password, and a password changer and custom command sets that changes a user's public key and password using a privileged account. These scripts can be customized for different Unix environments.

For more information about SSH Key Rotation, see the [SSH Key Rotation](#) and [SSH Key Rotation Quick Start](#).

## Managing Secret Templates

### Creating or Editing Secret Templates

1. Select **Admin > Secret Templates**. The Manage Secret Templates page appears:

**Manage Secret Templates**

Active Directory Account  Show Inactive

[Back](#) [Edit](#) [+ Create New](#) [Export](#) [View Audit](#) [Active Templates](#) [Password Requirements](#)

[A Character Sets](#) [Configure Launchers](#) [Configure Secret Template Permissions](#)

**Other Templates**

[Configure Dependency Templates](#) [Configure Scan Templates](#)

**Import Secret Templates**

Please paste your XML from the online [Secret Templates Gallery](#) into the box below to add your new Secret Template.

[Import](#)

2. If editing an existing template:
  1. Click to select that template in the unlabeled secret template dropdown list.
  2. Click **Edit**. The Secret Template Designer page appears (see below).
3. If creating a new template:
  1. Click **Create New**. The Create New Secret Template pop-up page appears:

1. Type the name of the new template in the text box.
2. Click **Create**.

The Secret Template Designer page appears:


The Secret Template Designer page provides all the options for configuring a secret template, as well as which text-entry fields appear on any secret created from that template.


4. Add template fields as desired. See [Secret Template Settings](#).
5. Click **Edit** to customize the template general settings. The Secret Template Designer appears:



### Secret Template Designer

Secret Template Name

Secret Template Icon  [Change](#)

 You can use a naming pattern to enforce a standardized name for this Secret Template. The naming pattern uses **Regular Expressions**. For example, the expression `"\w+\\w+$"` would allow "NTDOMAIN01\USER3454" but not "USER3454 on NTDOMAIN01".

Name Pattern

Name Pattern Error Message

Description


Active?

Keep Secret Name History?

Expiration Enabled?

Validate Password Requirements On Create?

Validate Password Requirements On Edit?

Field Displayed on Basic Home  

These settings are available:

- **Secret Template Name** check box.
- **Secret Template Icon** link: Click to change the icon displayed for the template.

- **Name Pattern** text box. See [Template Naming Patterns](#).
  - **Name Pattern Error Message** text box. See [Template Naming Patterns](#).
  - **Keep Secret Name History?** check box: If Keep Secret Name History is enabled, Secret Server keeps the specified number of entries for viewing. This feature creates a record of every name used when a new secret is created.
  - **Expiration Enabled?** check box: Secret templates allow expiration on certain text-entry fields. When the check box is selected, an expiration time interval can be specified for a selected text-entry field using the dropdown menu. With this option enabled and a time duration specified, Secret Server begins providing alerts if the secret text-entry field is not changed within the specified expiration requirements. See [Secret Expiration](#).
  - **Validate Password Requirements on Create?** check box: Ensure requirements are met on secret creation.
  - **Validate Password Requirements on Edit?** check box: Ensure requirements are met when editing secret.
  - **Field Displayed on Basic Home** dropdown list box: Choose the field that appears on the Basic Home view.
6. Click **Save**. The Secret Template Designer page reappears.
7. Select the following buttons to further configure the secret template:
- **Edit Passwords Button:** Only visible for templates that contain a text-entry field that is of the password type. It is used to alter the minimum password length, as well as the character set used, for the auto-generation of the secret's password. See [Editing or Deleting Secrets](#) for further details on password auto-generation.
  - **Configure Password Changing Button:** Used to enable RPC on these secrets. For details, see [Remote Password Changing](#).
  - **Configure Launcher Button:** Used to enable Remote Desktop or PuTTY Launcher or custom launchers on these secrets. For details, see [Secret Launchers](#).
  - **Configure Extended Mappings Button:** Extended Mappings allows you to tie a text-entry field value to a Secret Server defined system type for additional functionality. For example, you may have a generic password secret template that has a username and password text-entry field. For purposes of looking up credentials, such as a ticket system authentication secret, Secret Server needs to know that actual type of the text-entry fields since the text-entry field name can be custom. Extended mappings available are:
    - **SSH Private Key:** Defines which text-entry fields make up the SSH Key components of Private Key, Private Key Passphrase, and Public Key.

- **Username and Password:** Defines which text-entry fields contain the username and password.
- **Remote Server SSH Key for Validation:** Ensures the machine SHA1 digest for validating the machine connected to is correct.
- **OATH Secret Key:** For password changing on the Amazon Root Account using the Web Password Changer. If you enter the OATH secret for two factor, Secret Server generates the one-time password (OTP) automatically for password changing and heartbeat, allowing you to automate that while enforcing two-factor authentication on the AWS root credential.

## Activating and Deactivating Templates

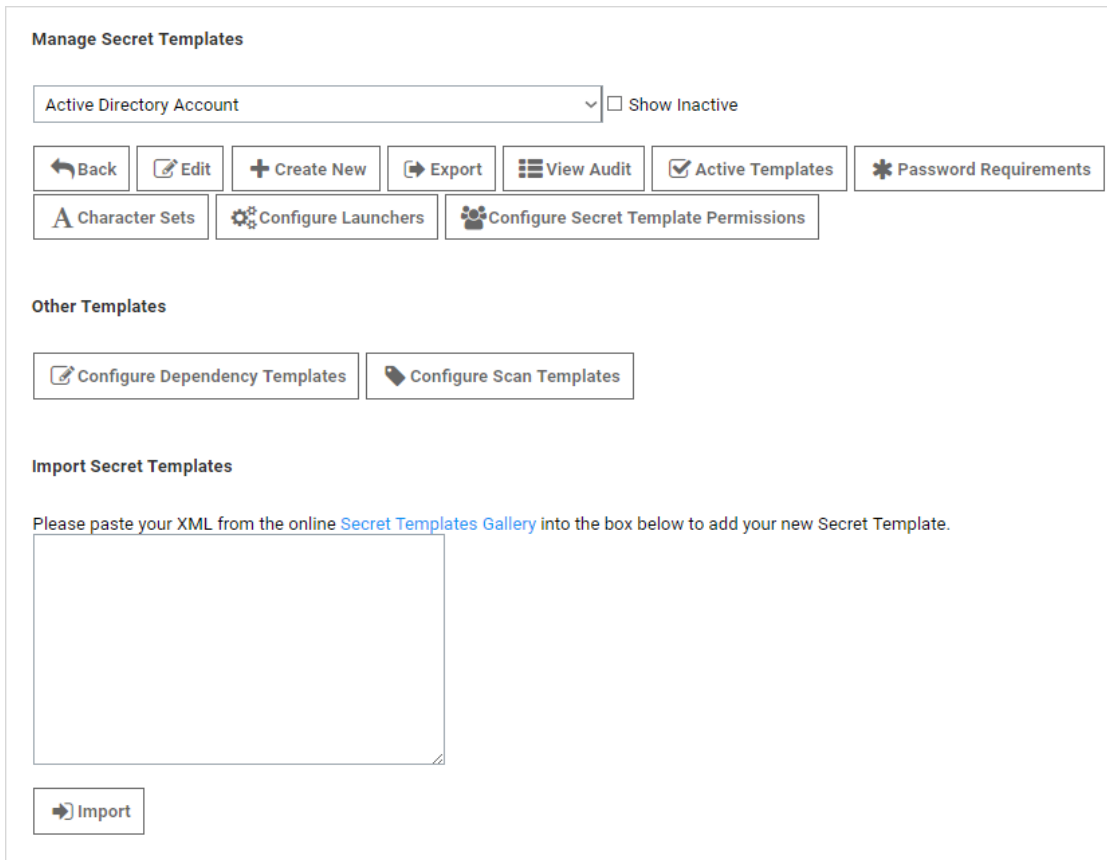
If a template is no longer relevant or outdated, it can be inactivated. This can be done from the specific template's Secret Template Edit page.

Templates can also be inactivated in bulk from the Manage Secret Templates page. Click the **Active Templates** button to navigate to the Set Active Secret Templates page. This screen displays all the secret templates in Secret Server. Each secret template can be set as active or inactive. Once the secret templates are chosen as active or inactive, then saving changes brings the secret templates into effect immediately. Inactivating a secret template does not inactivate any secrets using that secret template—those secrets still exist, but users are not able to create new secrets using an inactivated secret template.

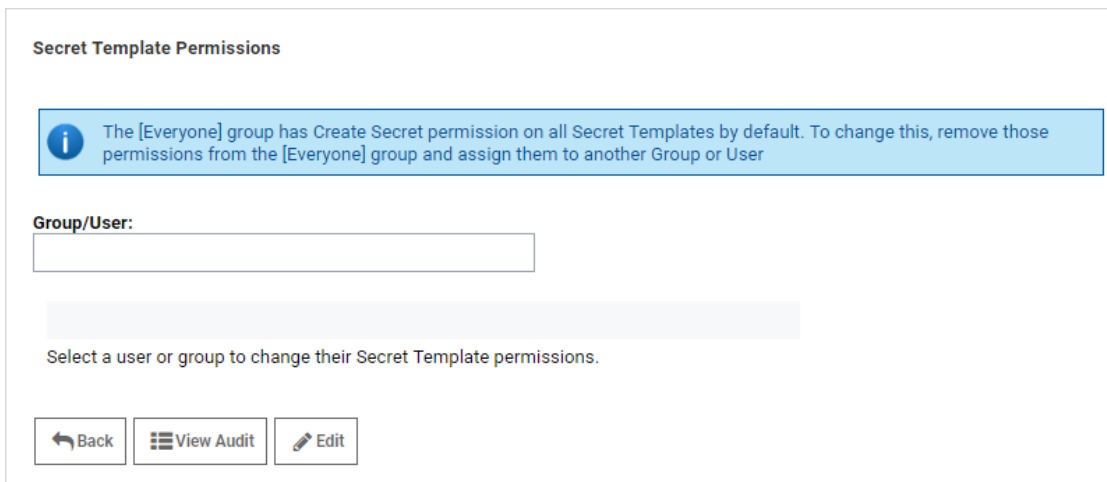
## Configuring Secret-Template Permissions

As of Secret Server 10.3 it is possible to assign users and groups to specific secret templates so they can either manage or create secrets based on those templates. This allows you to have more granular control over what secret templates are seen by users and groups when they are managing the templates or creating secrets. To configure permissions:

1. Select **Admin > Secret Templates**. The Manage Secret Templates page appears:



2. Click **Configure Secret Template Permissions**. The Secret Template Permissions page appears:



3. Select a group or user by typing in the **Group/User** text box. The page changes:

**Group/User:**

Will

Will (Will)

Select a user or group to change their Secret Template permissions.

4. Click the desired user or group in the **Group/User** dropdown list that is displayed.
5. Click **Edit**.

**Group/User:**

Will

[View Effective Permission report for Users](#)

PERMISSIONS FOR

**i** No Secret Template permissions are directly assigned. To see all the Secret Template permissions that this User/Group has, click the report link listed above.

< Select Secret Template >

6. Select a secret template you wish to assign them to. You may either assign "Template Create secret" or "Template Owner" to a user or group.
  - Template Create secret allows a user or group to create secrets based on the selected secret template.
  - Template Owner allows a user or group to edit a secret template and create secrets based on the selected secret template. By default, the Everyone group that targets all users of Secret Server can create secrets based on any secret template.

**Note:** Users' secret Template permissions are based on the permissions directly assigned to them, as well as the permissions assigned to all of the groups they are a member of. If a user or group does not have Template Create secret or Template Owner permissions, they are unable to create a secret based on that secret template or see that it exists in Secret Server.

1. Click **Save**.

## Changing a Secret's Template

To convert secrets from one secret template to another:

1. View a secret and click **Convert Template**.
2. Click to select the target template from the **Secret Template** list.
3. Map each text-entry field to a new field:
  1. Go through each list and select the target text-entry field for each source text-entry field on your secret.
  2. If you want to remove the value for a text-entry field instead of converting it, then select the <Remove> option on the list for that text-entry field.
  3. When you are done selecting, you can choose a folder.
4. Click **Save**.

The Convert Template button is only available to users and groups with the "Owner" permission to the secret.

**Note:** To preserve audit data, when a secret is converted from one type to another, the old Secret is deleted, and a new Secret is created. An admin can view old Secret by searching for deleted secrets on the Dashboard. A user needs "Add Secret," "Edit Secret," "Delete Secret," and "Own Secret" role permissions in order to convert a secret to a new template.

## SEARCHING SECRETS

To search for secrets:


1. Click the **Secrets** menu item in the main menu. The All Secrets page appears:

All Secrets

9 Items Active ▾ All Templates ▾ 🔍

NAME ↑	SECRET TEMPLATE	FOLDER	LAST ACCESSED	
AAas	SonicWall NSA Web Admin Account	DecimalFolder1		
ADWindowaccount	Windows Account	ActiveFolder1		
Contact Secret Shared With Everyone	Contact			
My AWS Secret	My AWS Password	Personal Folders/Will	4 days, 18 minutes	
Pincheckout ★	Pin	ActiveFolder1/Acti.../2019 15:42:38		
pincheckout1 ★	Pin	ActiveFolder1/Acti.../2019 15:42:38		
pinnnn	Pin		28 days, 2 hours	
Secret_Custom_Launch	Test_Custom	CustomerFolder1/Cu.../2019 15:42:38	28 days, 2 hours	
testacc	Bank Account	CustomerFolder1/Cu.../2019 15:42:38		

2. Type the secret name or other text in the unlabeled search text box at the top of the page.

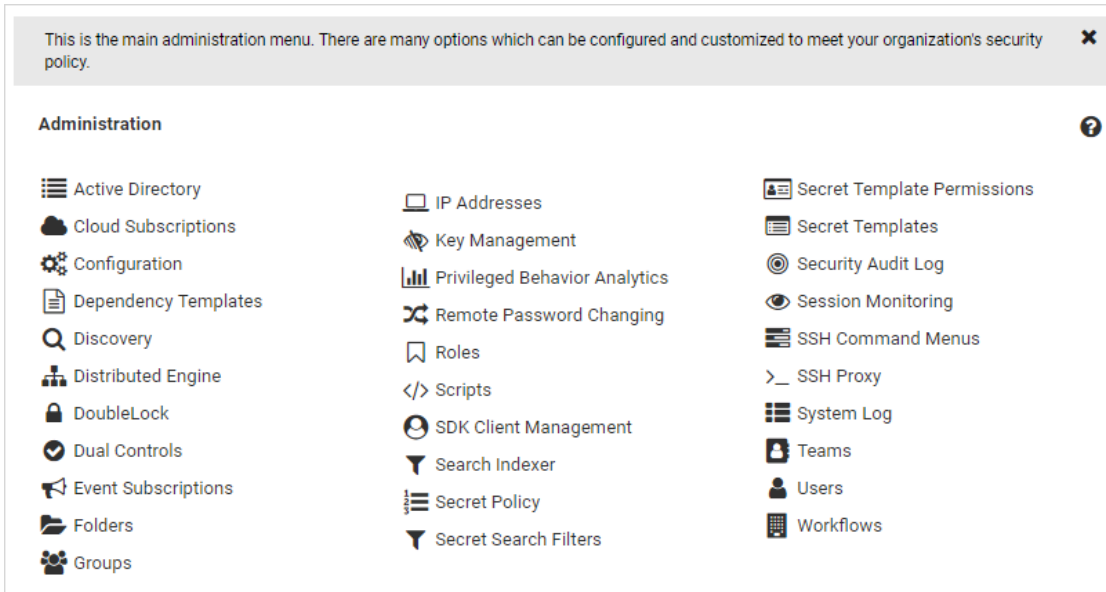
3. Click the  button. The All Secrets table only displays matching secrets. Searches search for all text-entry fields that are configured as searchable on the secret's template if the extended search indexer is enabled.

**Important:** If the search indexer is not enabled, searches are only performed on the **Secret Name** text field.

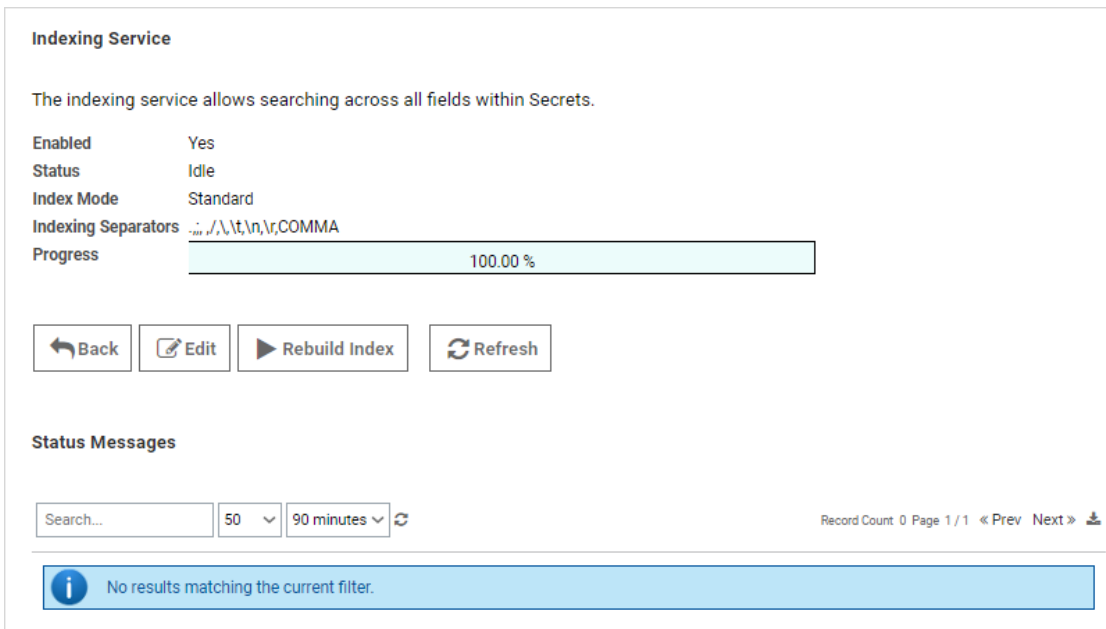
## Search Indexer

The *search indexer* allows searching on all text-entry fields set to searchable on the template. To enable and configure the search indexer:

1. Click **Admin** on the main menu and select **See All**. The Administration page appears:



2. Click **Search Indexer**. The Indexing Service page appears:



3. Click **Edit**. The page becomes editable:



**Indexing Service**

The indexing service allows searching across all fields within Secrets.

**Enabled**

**Indexing Separators**

**Index Mode**

Standard

Extended

[Explain](#)

4. Ensure the **Enabled** check box is selected.
5. Click either the **Standard** or **Extended** selection button.
  - *Standard search mode* is the default and searches on whole words in a field value. For example, a field value of "My AWS Secret" would match when you search for *My AWS Secret*, *My*, or *Secret*.
  - *Extended search mode* searches for whole words or a partial words by up to twelve characters. For example, a field value of "My AWS Secret" would match when you search for *My AWS Secret*, *My*, *Secret*, *WS*, or *ecret*. This is more useful, but may impact search performance and creates a larger index table.

**Note:** Indexing separators are used to split the text text-entry fields into search terms. By default, the separators are semi-colon, space, forward slash, back slash, tab (\t), new-line (\n), return (\r), and comma. Changes to the indexing separators require a full rebuild of the search index.

6. Click **Save**. The Indexing Service page reappears, and the indexing begins in the background. Depending on the size of the Secret Server installation, it may take awhile. Progress is shown on the Progress bar.
7. If you changed the indexing separators, click **Rebuild Index**.


## IMPORTING SECRETS

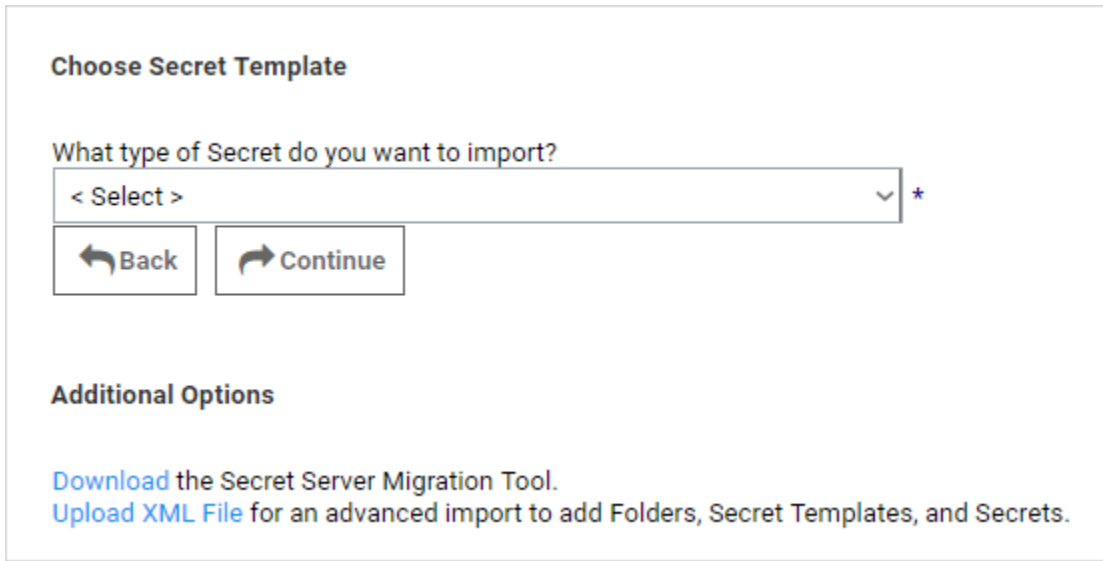
### Introduction

Secret Server's importation feature simplifies integration with legacy systems and allows users to easily add large numbers of secrets from an Excel or comma-separated values (CSV) file.

Secrets are batch imported by template, so multiple types of input data must be imported in several batches. The Password Migration Tool supports easy addition of existing secrets from other third-party password-storing applications.

## Configuring Data for Importation

1. Click the  button on the Dashboard and select **Import Secrets**. The Choose Secret Template page appears:



**Choose Secret Template**

What type of Secret do you want to import?

< Select > \*

[← Back](#) [→ Continue](#)

**Additional Options**

[Download](#) the Secret Server Migration Tool.  
[Upload XML File](#) for an advanced import to add Folders, Secret Templates, and Secrets.

2. Click the **What type of Secret...** list box to select the type of secrets you intend to import.
3. Click **Continue**. The Import Secrets page appears:

**Import Secrets**

Paste your Secrets directly from Microsoft Excel® or in comma/tab separated format and click 'Next'.  
Do not include a header line.  
Secret Name must be included but others fields can be blank.  
Fields containing commas or tabs must be surrounded with double quotes.  
It is permissible to include quotes if they are escaped with a \ (for example, pa\"word comes out as pa"word)  
Fields must be in the following order:

**Secret Name,AccessKey,SecretKey,Username,SecretId,Trigger**

⏪ Back Next ⏩

Allow Duplicate Secrets  Import With Folder

4. Paste the secrets for importation from MS Excel or a CSV file directly into the text box in the **Import Secrets** page. The order of the imported fields is based on the template selected. Consider the following:
  - Do not include a header line. The field names are determined by the order, not a header line.
  - The fields **must** be in this order: Secret Name, AccessKey, SecretKey, Username, SecretId, and Trigger.
  - Secret names must be included, but other text-entry fields can be blank unless the secret template indicates that the text-entry field is required
  - Fields containing commas or tabs must be surrounded with double quotation marks
  - If you have to include double quotation marks inside your data, escape all of them with a \ character so the importer does not get confused.
5. Click to select the **Allow Duplicate Secrets** check box if you wish to import a secret with the same name as an existing one.
6. Click to select the **Import with Folder** check box if you included an additional field in the importation text with a fully qualified folder name for the secret to be created in.

7. Click the Next button. Secret Server displays a preview:

### Import Secrets

Paste your Secrets directly from Microsoft Excel® or in comma/tab separated format and click 'Next'. Do not include a header line. Secret Name must be included but others fields can be blank. Fields containing commas or tabs must be surrounded with double quotes. It is permissible to include quotes if they are escaped with a \ (for example, pa\"word comes out as pa"word) Fields must be in the following order:

**Secret Name,AccessKey,SecretKey,Username,SecretId,Trigger**

Mister Secret, sdklfjsd, sdlkfjsdlk, Will, MyID1

Allow Duplicate Secrets  Import With Folder

SECRETNAME	ACCESSKEY	SECRETKEY	USERNAME	SECRETID	TRIGGER	ERROR
Mister Secret	sdklfjsd	sdlkfjsdlk	Will	MyID1		

8. If you are happy with what you see, click the **Yes, Import these Secrets** button.

## Importing Secrets with the Secret-Server Migration Tool

Secret Server offers a migration utility for users wishing to import secrets from other applications. Currently, the migration tool supports to following applications:

- KeePass
- Password Corral
- Password Safe

**Note:** This is done with another exportation tool that creates a single XML file. Please contact Thycotic Support for details.

## Importing Secrets with Advanced XML Importation

Advanced importation adds folders, secret templates, and secrets based on an XML file. Permissions can be specified on the folders and secrets or the default is to inherit permissions. This import can only be done by administrators with proper role permissions.

**Note:** For details on the XML file, see [Advanced Import with XML](#).

## SECRET LAUNCHERS

### Introduction

A secret *launcher* opens a connection to the remote computer or device or logs into a website using the secret's credentials directly from the Web page. While this provides a convenient method of opening RDP and PuTTY connections, it also circumvents users being required to know their passwords. A user can still gain access to a needed machine, but it is not required to view or copy the password out of Secret Server. A Web launcher automatically logs into websites using the client's browser.

### Built-In Launcher Types

Secret Server launchers, also called protocol handlers, come in three primary types:


- **Remote Desktop:** Launches a Windows Remote Desktop session and automatically authenticates the user to the machine.
- **PuTTY:** Opens a PuTTY session and authenticates the user to a Unix system.
- **Web Password Filler:** Uses a bookmarklet or a Chrome extension to automatically log the user into a website with secret credentials. See [Web Password Filler](#).
- **Web Launcher:** An alternative method to automatically log on websites. See [Web Launcher](#).

### Enabling Launchers

By default, the launcher is enabled by the **Enable Launcher** setting under **Admin > Configuration**.

The launcher can be deployed in two ways—with the ClickOnce or Protocol Handler applications. This can also be set in the configuration settings.

The Protocol Handler application allows the launcher to be used in virtualized environments or any environment in which the user does not have access to a Windows Temp directory. The

Protocol Handler can be downloaded by clicking the  button on the Dashboard and selecting **Launcher Tools**:

## Launcher Tools

### LOGIN ASSIST CHROME EXTENSION

#### Preferred solution for logging into websites from Chrome.

Offers similar functionality to the Web Password Filler, but for a wider range of websites.

Install the Login Assist extension by adding it to the browser from the Chrome web store:  
[Chrome Web Store - Secret Server Login Assist](#)

### WEB PASSWORD FILLER

#### Quick, Convenient and Secure logging into Websites.

Install the Web Password Filler by adding this link to your web browser's bookmark bar:  
[Secret Server Web Password Filler](#)

- Log into most websites with a single click.
- Click while on a website.
- Automatically fill in the Username and Password.

### PROTOCOL HANDLER INSTALLER

#### Allows launcher to function in virtualized environments. For more information [click here](#).

The MSI can be installed directly or through group policy. A reboot may be necessary on certain operating systems.

[Download Protocol Handler MSI \(64 bit\)](#)

[Download Protocol Handler MSI \(32 bit\)](#)

[Download Protocol Handler PKG \(Apple OSX\)](#)

 Back

For details, see the [Protocol Handler Launcher](#).

## Launching Sessions

On the Secret View page, clicking the Launcher icon launches the Remote Desktop, PuTTY, or custom session directly from the browser or log into the website. The mapped text fields are passed to the launcher for automatic authentication.

If the machine is set for Remote Desktop, the console launches and allows the machine to be specified from the RDP dialog.

If the Host is set to <user>, a prompt asks for the specific machine before launching the PuTTY session.

For some browser security levels, you might must click **Allow** for the launcher application to open.

**Note:** The View Launcher Password permission can be removed to prevent users from viewing the credentials but can still use the authentication session to access the computer.

The settings under the Launcher tab are used for secrets that are enabled for SSH and custom launchers.

## Remote Desktop Launchers

### Browser Configuration

Remote Desktop (RD) launchers require the following:

- **Firefox Configuration:** Firefox requires a helper add-on application to run the RD and PuTTY launchers. The Microsoft .Net Framework Assistant add-on and .NET framework version 4.5.1 SP1 needs to be installed.
- **Chrome Configuration:** If using ClickOnce, Chrome requires a Helper Add-on application to run the RDP and PuTTY Launcher. The ClickOnce add-on for Google Chrome Add-on needs to be installed. The launcher requires .NET framework version 4.5.1 SP1 as well.
- **SSL Certificates:** SSL must be set up properly for the RD launcher to work correctly. If Secret Server is using SSL certificates, they must be trusted at the user's computer. This is only an issue with self-created certificates.

### Setting Up Secret Templates for RD Launchers

Launchers can be accessed from any secret created from a properly configured template.

By default, the templates Windows Account, Active Directory Account, Cisco Account (SSH), HP iLO Account (SSH), Unix Account (SSH), Web Password, and SQL Server Account have the launcher configured.

Secrets can be configured for the launcher from within the Secret Template Designer page.

Clicking **Configure Launcher** displays the options available.

## Adding RD Launchers

1. Click **Add New Launcher** to add a launcher to the template.
2. On the following page, select a launcher type from the drop-down menu. The text-entry fields below reflect the text-entry fields necessary to map to the launcher. In the case of a custom launcher, these text-entry fields are used to run the launcher process if the launcher is configured to run as secret credentials.
3. Choose a secret text-entry field in the drop-down menu on the right to map to each launcher value on the left. See the following section for further details on editing launcher configuration.
4. Click **Save** to add the launcher to the template.

## Editing RD Launchers

Click **Edit** to modify the settings for a launcher that has already been added to the template. For a launcher to work properly, Secret Server requires credentials to be taken from secret text-entry fields. Fields must be assigned their corresponding credentials from the list. In addition to the secret fields, the domain can be mapped to <blank>, which passes an empty string to be used with local accounts, and the machine or host can be mapped to <user input>, which prompts the user for a specific machine to be used with domain accounts.

In cases where there are multiple endpoints to connect to, such as with a domain account, the machines can be restricted to a set list. Under the **Advanced** section of the secret template launcher configuration, enable **Restrict User Input**. When that option is on, the launcher shows a drop down of machines to connect to, based on a comma-separated list in the specified secret field.

## Web Launchers

Web launchers are a separate login method from the Web password filler and provide a convenient click to automatically log on simpler websites. Web launchers do not work on complex login pages that rely on JavaScript. For those login pages, use the bookmarklet or browser extension for the Web password filler. By default, Web launchers are enabled on the Web Password Secret template, but they can be enabled on custom templates as well, as described in [Enabling Launchers](#).

### *Configuring Web Launchers for Secrets*

Once enabled on the template, a Web launcher needs to be configured for the secret. Each website login is unique and requires the secret text-entry fields to be mapped to the form controls. For a new secret the Launcher icon appears and clicking on it takes the user to a configuration screen. The user can also view and access the configuration screen from the Launcher tab. Depending on whether other secrets with the same website have been configured, the user has different options.



**Note:** Configuring the Secret for use with the Web Launcher requires the user to have Owner permission on the Secret.

First, there is the option of downloading the setting from Thycotic.com. When the Configure Web Launcher page is loaded, Secret Server checks online at Thycotic.com for pre-approved matching websites. If any are found, they are downloaded and made available to pick from in the dropdown list.

**Note:** This functionality can be disabled in Secret Server in the Configuration Settings.

The list displays all downloaded configurations and other secrets' configuration for the same domain that the user has permission to view. Select one from the list and click **Next** to create a copy of the settings for the secret.

There is also an option to create a configuration that allows the Web launcher to be used on most websites and not rely on published configuration settings. To use this, select the last item in the dropdown list and click **Next**. The next section discusses the create process.

### *Creating a Configuration*

When configuring the Web Launcher:

- **Entering the Login URL:** Secret Server needs to know the exact URL used to login to be able to figure out the controls and perform the automatic login. Some example login URLs:
  - `https://login.yahoo.com/config/login`
  - `https://MyServer/Billing/login.aspx`
  - `https://firewall07/login/`

**Note:** The Login URL is typically a secure site with a prefix of `https://`. If allowed to access the site, Secret Server automatically detects if `https` should be used to ensure the credentials are passed securely.

- **Providing the Page Source:** If Secret Server is not allowed access to sites, or the login URL is not accessible by an external site, the page source needs to be provided for the Web launcher controls to be obtained. Ensure the login URL is correct when the page source is taken. If the site can be accessed by Secret Server the page source is automatically obtained and this step is not present.
- **Choosing the Form:** The page is read, and the exact login form needs to be identified. The page forms are listed in the list with the most likely selected. If no forms or no likely forms are found, the user needs to update the URL or page source, as configuration must have at least one textbox and one password box.
- **Wiring Up the Fields to Controls:** In most cases, Secret Server automatically wires up the Username and Password text fields to the correct page controls. If not, the user completes the control mapping on the Launcher tab.

## Launching to a Website

The Web launcher can be used by clicking the Launcher icon on the Secret View page. The Web launcher opens a new window in the browser, which attempts to login to the site using the credentials on the secret. The launcher can also be used with the Test Launcher button on the Launcher tab. Testing the Launcher creates a dialog to offer troubleshooting help and means to upload the configuration to Thycotic.com. The uploaded configuration is reviewed and published by Thycotic for all Secret Server customers to use with the check online feature. No secret or identifiable information is uploaded to Thycotic.com. Only the website URL and control names are sent.

## Custom Launchers

Secret Server can configure a program to run when clicking the launcher on a secret. You can customize process launchers to work with any application that can be started by command-line and passes values to the command-line from the secret text fields. For process launchers to work, the client machine needs to have the program installed and typically needs the program folder in the PATH environment variable.

There are three types of custom launchers to choose from:

- **Process:** Launch a process on the client machine that connects directly to the target system from the client.
- **Proxied SSH Process:** Launch a process on the client machine that proxies its connection to the target system through Secret Server.

**Note:** See [Configuring SSH Proxies for Launchers](#).

- **Batch File:** Launch a batch file from the client machine.

To create a new custom launcher:

1. Select **Secret Templates** from the **Admin** main menu item. The Manage Secret Templates page appears:

**Manage Secret Templates**

Active Directory Account  Show Inactive

**Other Templates**

**Import Secret Templates**

Please paste your XML from the online [Secret Templates Gallery](#) into the box below to add your new Secret Template.

2. Click the **Configure Launchers** button.
3. Click the **New** button. The Launcher page appears:

### Launcher

#### GENERAL SETTINGS

**Launcher Type** Process
  
Launches the process on the user's machine and replaces \$ parameters with values from the Secret and its associated Secret. For more information see [this KB Article](#)


**Launcher Name** \*  

**Active**

**Use Secret Server RDP Client**

**Use Additional Prompt**

**Launcher Image**  Use Custom Image?



#### WINDOWS SETTINGS

**Process Name**   ex. powershell
  
[How do I configure process arguments?](#)

**Process Arguments**   ex. -user \$USERNAME -pwd \$PASSWORD -f

**Run Process As Secret Credentials**

**Use Operating System Shell**

[Advanced](#)

#### MAC SETTINGS

**Process Name**   ex. /Applications/TextEdit.app/Contents/MacOS/TextEdit
  
[How do I configure Mac process name and arguments?](#)

**Process Arguments**   ex. -user \$USERNAME -pwd \$PASSWORD -f

Save
Cancel

The following settings are available in the General Settings section:

**Note:** Not all of the following are available for all types of launchers.

- **Launcher Type:** Select Process, Proxied SSH Process, or Batch File.
- **Launcher Name:** Name of the launcher that is displayed to the user.
- **Active:** Whether the launcher is active for use.
- **User Secret Server RDP Client:** Use the RDP client.
- **Use Additional Prompt:** User is prompted for additional information when using the launcher. When selected, the Additional Prompt Field Name text box appears.

- **Additional Prompt Field Name:** Name of the text field that is prompted for when the user uses the launcher. This value can be referenced in the process arguments with a \$ prefix.
- **Launcher Image:** Upload a custom image for the launcher.

The following settings are available in the Windows Settings section:

- **Process Name:** Name of the process that is launched. Example: powershell
- **Batch File:** As an alternative to opening a process, upload a .bat file that is downloaded and executed on the client when the user runs a launcher. The file is deleted from the client after execution.
- **Process Arguments:** Process arguments depend on the process that is being launched. View the built-in SQL Server launcher for examples on how the text-entry fields are substituted. For greater flexibility, other secrets can be linked on the Launcher tab on the secret. The text-entry field values from those secrets can also be used in the process arguments using the same prefix `$(1)[FieldName]` syntax as the SSH custom commands. There is a launcher specific token `$SESSIONKEY` that can be passed to the command line. This passes an identifier to the customer launcher that can be used to anonymously check in the secret using the `CheckInSecretByKey` Web service method. Example: `-user $USERNAME -pwd $PASSWORD -f`. See [Configuring Custom Launcher Process Arguments](#) for details.
- **Run Process as Secret Credentials:** The process authenticates with the secret credentials (username, domain, and password) instead of the client user that is using the launcher. This can be overridden at the secret level to use a privileged account to run the process.
- **Use Operating System Shell:** Use the OS shell for the launcher. Useful for processes requiring UAC confirmation.

The following settings are available in the Advanced Windows Settings section, which is accessible by clicking the **Advanced** link:

- **Escape Character:** The character to use as an escape character in passwords. Escape characters are required to allow the use of characters that are otherwise not allowed in passwords because they have special meaning to the launcher's target application.
- **Characters to Escape:** The characters that require escaping for the target application.

The following settings are available in the Mac Settings section:

- **Process Name:** Name of the process that is launched. Example: `/Applications/TextEdit.app/Contents/MacOS/TextEdit`
- **Process Arguments:** Process arguments depend on the process that is being launched. View the built-in SQL Server launcher for examples on how the text-entry fields are substituted. For greater flexibility, other secrets can be linked on the Launcher tab on the


secret. The text-entry field values from those secrets can also be used in the process arguments using the same prefix `$(1)[FieldName]` syntax as the SSH custom commands. There is a launcher specific token `$SESSIONKEY` that can be passed to the command line. This passes an identifier to the customer launcher that can be used to anonymously check in the secret using the `CheckInSecretByKey` Web service method. Example: `-user $USERNAME -pwd $PASSWORD -f`. See [Configuring Custom Launcher Process Arguments](#) for details.

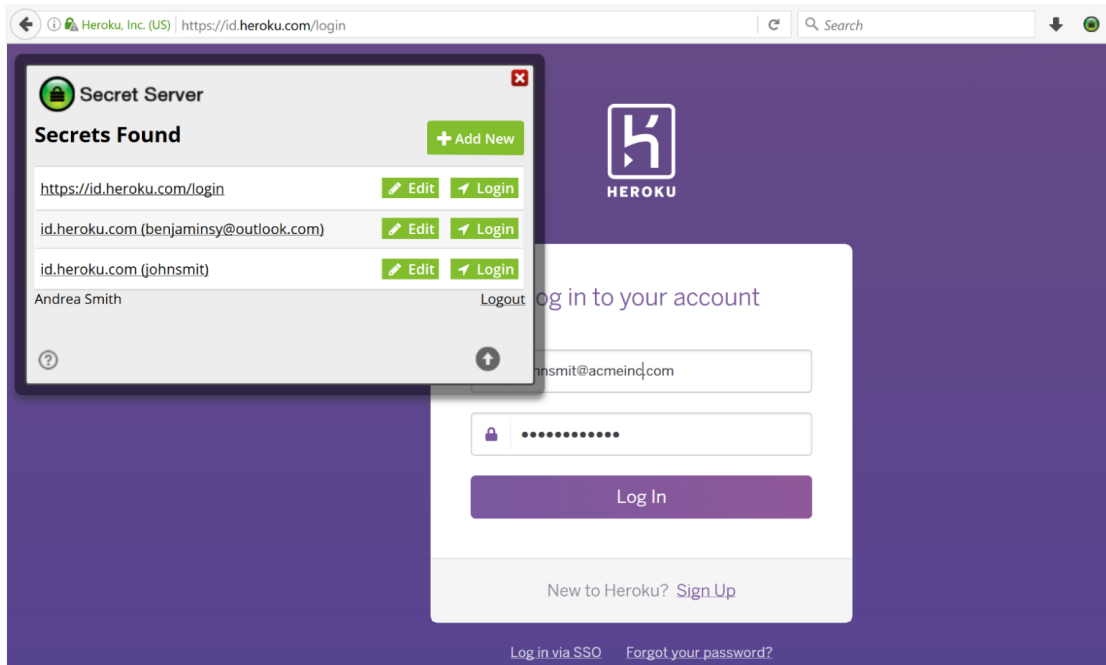
## Web Password Filler

The *Web password filler* is a log-on helper that you can use on any Web site with a log on. To use the Web password filler, install the browser extension for Chrome or Firefox. For Internet Explorer you must drag a link to the bookmark bar of your browser. The link is available by going to any secret which uses the Web Password Secret template or any other secret template that has a searchable URL text field.

- **Chrome:** Install the extension by clicking on the Web launcher icon on a Web password secret or install the extension in Chrome from the [Chrome store](#).
- **Firefox:** Install the Firefox add on by clicking on the Web launcher icon on a Web password secret or install the add on from the [Firefox listing](#).
- **Internet Explorer:** Drag the link from **Tools > Launcher Tools** for the Web password filler to the bookmark bar to create a bookmarklet.

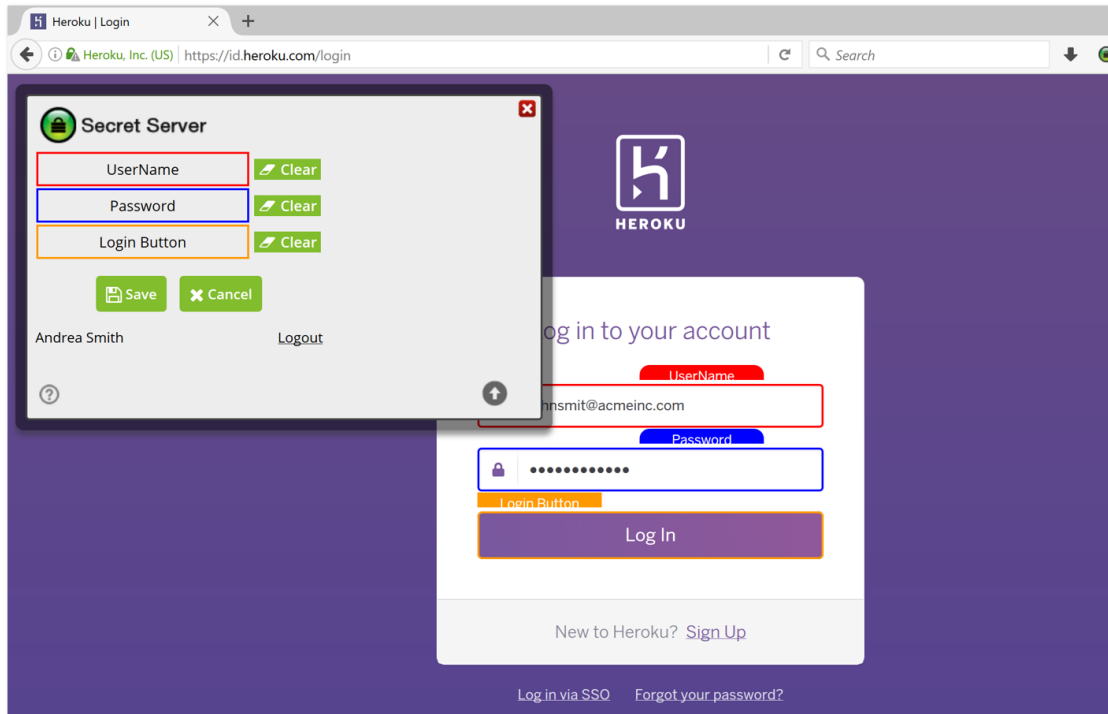
### *Using with Firefox or Internet Explorer*

Once you have the bookmarklet or extension installed, it is ready to use. Navigate to the login page of the website you wish to log in to, and then click the  extension icon or bookmarklet link. A dialog opens on the login page with the Web password filler:



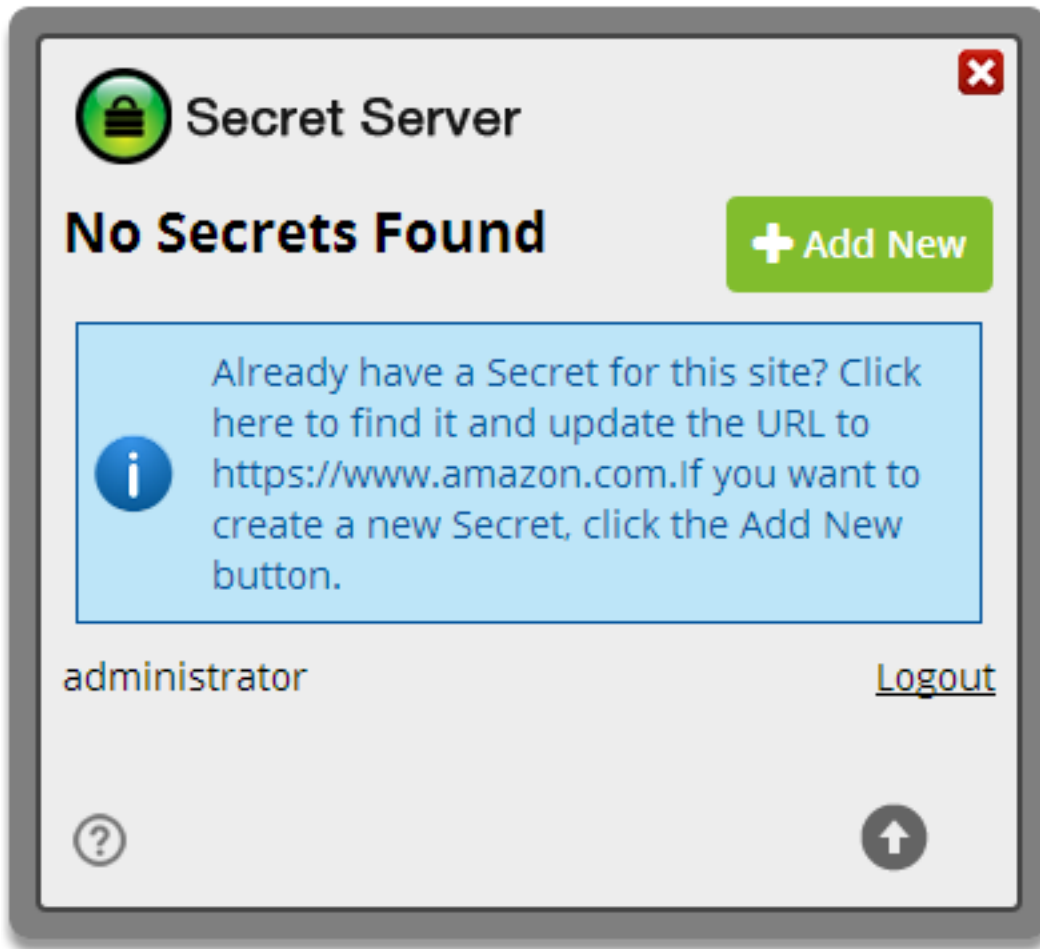
The Web password filler shows you available secrets that match the current URL for you to login with. Click the **Login** button or the secret name to fill out the username and password.

If the Web password filler is unable to correctly fill in the username and password text fields, you can manually set the mappings from the secret fields to the website fields by clicking **Edit** on a secret and selecting a secret text-entry field and then clicking on the correct text field in the login form:



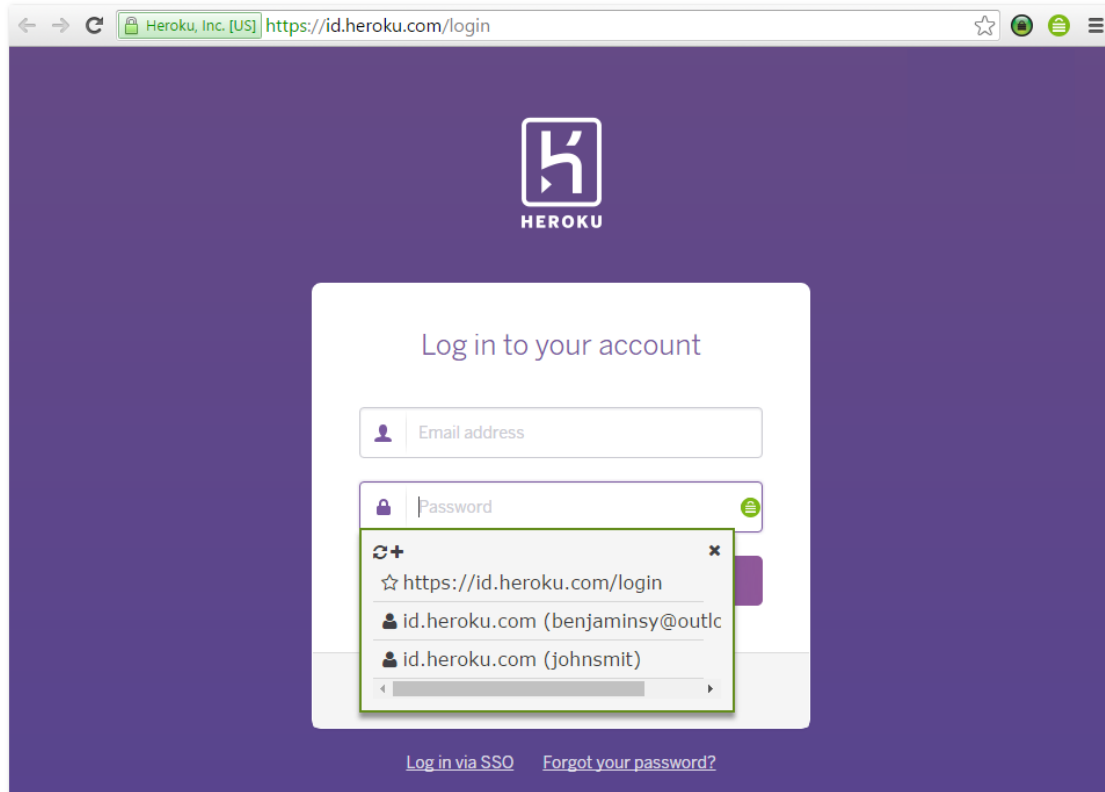
If no secrets exist, you can click the extension and then click the **Add New** button to create a secret for that URL:





### *Using with Chrome*

Login forms are populated with a secret lock icon that you can click on to bring up a list of secrets:



Secrets are prioritized based on whether they are marked as favorites, are in your personal folder, and then by URL.

To add a secret if none exist, click the **+** symbol in the **Secret List**.

## Launcher Configuration and Support

### Default Launcher Requirements

- **SQL Server Launcher:** Requires SQL Server Management Studio to be installed. When installed, the program is automatically added to the PATH.
- **PowerShell Launcher:** Requires PowerShell to be installed. When installed, the program is automatically added to the PATH.
- **Sybase iSQL Launcher:** Requires that `isql.exe` is installed.

### Configuring Launchers on the Secret

Custom and SSH launchers provide additional settings on the Launcher tab of the secret for customizing authentication to the target.

- **Run Launcher using SSH Key:** If there is an SSH key set on the secret, it is used by default for authenticating to the target. Alternatively, you can specify a key from a different secret. For details about SSH keys, see [SSH Key Authentication](#).

- **Connect As:** When an SSH secret is proxied, you can choose to connect as another user and then do an **su** to the current secret's user. This is a common practice for connecting with a lower privileged account and then switching to the root user.

## Configuring SSH Proxies for Launchers

Launchers using an SSH connection can alternatively use Secret Server as a proxy rather than the launcher connecting directly to the target system from the machine it is being launched from. When proxying is enabled, all RD sessions are routed through Secret Server. In Secret Server Cloud, the Distributed Engine service also supports acting as a proxy for session launchers for greater network flexibility and offloading connections from the Secret Server instance.

To configure this:

1. Select **Admin > SSH Proxy**:

The screenshot displays the 'SSH Proxy Configuration' page. It includes an 'Explain' link, a 'SETTINGS' section with various configuration options, an 'Edit' button, and a 'SITES' table.

SSH Proxy Configuration	
<a href="#">Explain</a>	
<b>SETTINGS</b>	
Enable Proxy	Yes
Enable SSH Tunneling	Yes
Proxy New Secrets By Default	Yes
SSH Banner	Welcome to Secret Server
SSH Proxy Host Fingerprint	SHA1 - 50:2d:99:d9:f3:2a:b8:9d:68:b4:9e:a5:2b:a2:9a:18:2f:b8:bf:61 MD5 - 04:9e:8b:44:f1:ed:5b:fd:e1:18:79:9c:9c:fb:66:41
Enable Inactivity Timeout	No
<a href="#">Edit</a>	
<b>SITES</b>	
SITE NAME (ID)	PROXY ENABLED
Default (1)	No

2. Scroll down and click **Edit** to enter your SSH proxy configuration settings. The SSH Proxy Configuration page appears:

### SSH Proxy Configuration

[Explain](#)

SSH PROXY SETTINGS

Enable Proxy

Enable SSH Tunneling

Proxy New Secrets By Default

SSH Proxy Port

SSH Banner

SSH Proxy Host Private Key

Enable Inactivity Timeout

The **SSH Proxy Settings** are:

- **Enable Proxy:** Enable or disable SSH proxying.
- **Enable SSH Tunneling:** SSH Tunneling allows Remote Desktop Sessions to be proxied using the same proxy configuration settings.
- **Proxy New secrets By Default:** This setting determines whether newly created secrets have their SSH proxy setting enabled; secret policy takes precedence over this default.
- **SSH Proxy Port:** The default port to apply to all connections, unless another port is assigned to a specific connection.

- **SSH Banner:** Users connecting through Secret Server see this text banner on the SSH client.
- **SSH Proxy Private Key:** The Secret Server SSH private key, this can be generated using the **Generate New SSH Key** button.
- **Enable Inactivity Timeout:** Enable or disable closing the session if there is inactivity for a defined number of seconds. When enabled, a **Timeout (seconds)** text box appears.

The **SSH Terminal Settings** are:

- **Enable Inactivity Timeout:** Enable or disable closing the SSH terminal session if there is inactivity for a defined number of seconds. When enabled, a **Timeout (seconds)** text box appears.
- **Enable Terminal:** Enable or disable the SSH terminal.
- **SSH Terminal Banner:** The text banner you want displayed when somebody opens an SSH terminal session.

**Note:** For details about connecting to Secret Server with an SSH terminal, see the [SSH Terminal Administration Guide](#).

**Note:** To manipulate a secret via an SSH terminal, the secret's proxy setting must be enabled, and the secret must be shared with the authenticated terminal user.

3. Click the edit icon next to one of the machines in the **Nodes** section.

The **Nodes** settings are:

- **Machine Name:** The public host name of the node server.
- **SSH Public IP Address of Nodes:** The public IP that the client launcher connects to. In most cases, this can be the same as the SSH bind address; however, there may be cases where the public IP or host differs from the private IP that Secret Server should bind to, such as NAT or an Amazon EC2 instance.

The **Sites** settings are:

- **Proxy Enabled:** Enable or disable SSH proxying for a specific site.
- **Site Name:** Site name or ID.
- **SSH Port:** The port Secret Server listens on. The default is 22.

The **Engines** settings are:

- **Friendly Name:** Human readable site name or ID.

- **Hostname/IP Address:** The public hostname or IP that the client launcher connects to. In most cases this can be the same as the SSH Bind Address, however there may be cases where the public IP or host differs than the private IP that Secret Server should bind to, such as NAT or an Amazon EC2 instance.
  - **SSH Bind Address:** The IP Address of the network adapter that the Secret Server SSH listener should bind to. This should not be localhost or 127.0.0.1. If you are not sure which bind IP Address to use, you may use 0.0.0.0, which binds to all IPv4 interfaces on the machine.
4. To enable secrets assigned to a site, edit the corresponding site and check the **Proxy Enabled** check box and optionally specify a custom SSH port.
  5. The Distributed Engines on that site now appear in the **Engines** section, and you can configure the **Hostname/IP Address** and **SSH Bind Address** text boxes on each one. The default values are the FQDN of the machine and 0.0.0.0 which should work for many internal connections but may must be edited depending on how users are connecting to them.

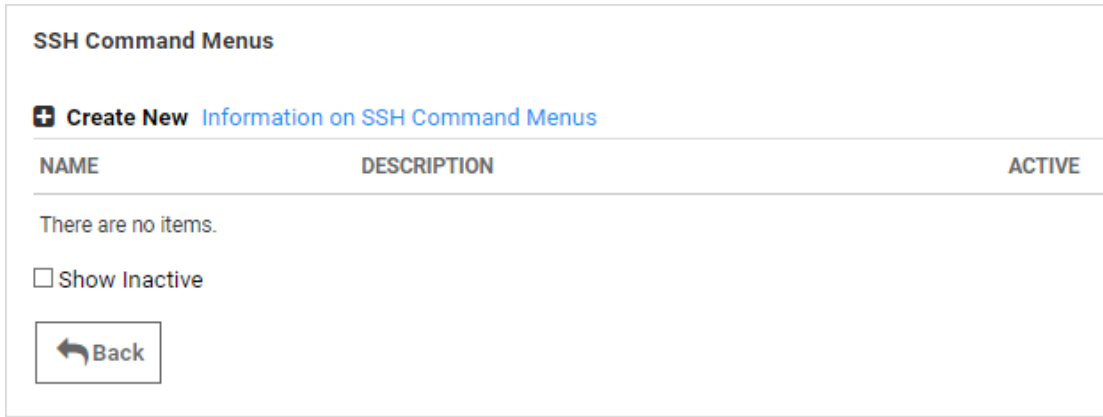
**Note:** The flow for when a user proxies through a Distributed Engine, rather than Secret Server, is the same, except that rather than the user's session launcher connecting to the public host on the node, it connects to the public host of an engine that is part of a site the secret is assigned to.
  6. Once SSH Proxy has been configured, secrets using an SSH launcher have a **Show Proxy Credentials** button available. Click it to display credentials that can be used to connect through Secret Server to the target system, that is, where a user would like to start an SSH session manually.

## Managing SuperUser Privilege

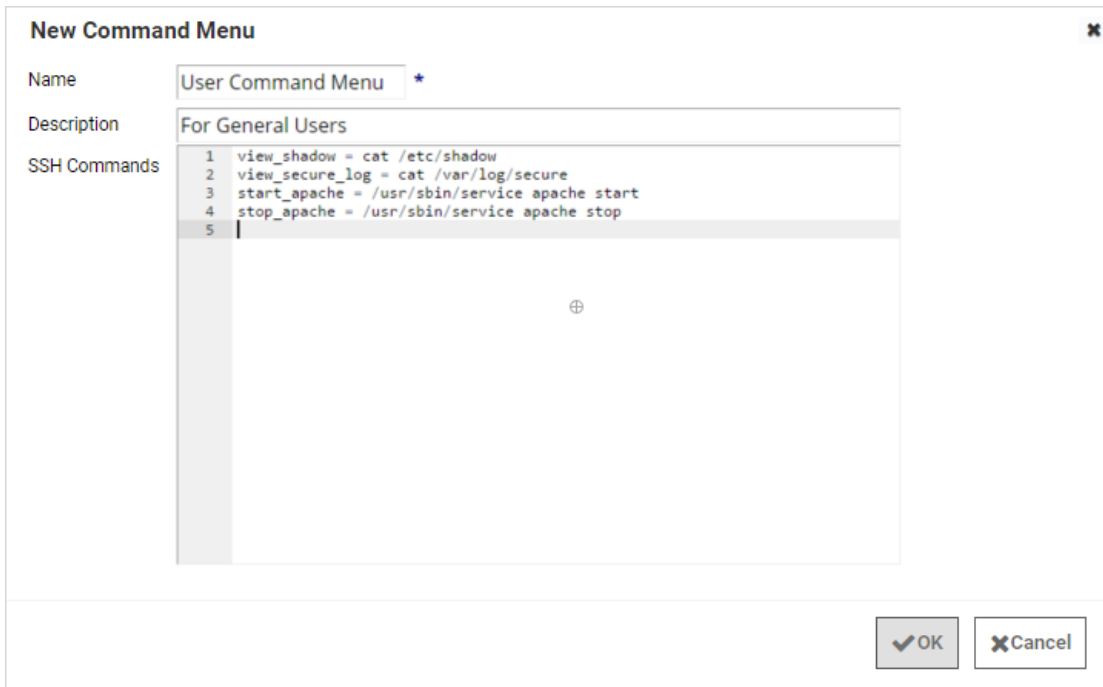
Administrators can create command menus for use with a proxied SSH connection to restrict what commands can be run by users or groups on the connected server. This feature requires an additional license. To add a command menu:

**Note:** For details, see [SSH Command Menus](#).

1. Navigate to **Admin > All**.
2. Click the **SSH Command Menus** button.



3. Click the **Create New** button.
4. Type a name, description and the SSH commands:



Once one or more command menus have been created, access can be controlled to individual Unix SSH secrets.

On the **Security** tab of a secret that can use a proxied PuTTY session, proxy must be enabled as well as command menu restrictions. If **Allow Owners Unrestricted SSH Commands** is enabled, any user who is an owner of the secret has unrestricted use of the PuTTY session, that is, that user is able to type in commands as in a normal session. Additionally, other groups can be assigned the Unrestricted role as well.

In the following example, the "admin" group is unrestricted, while everyone who is not in the admin group is restricted to only being able to run the commands that are enumerated in the user command menu, created above.

**SSH Unix Secret (Unix Account (SSH))**

General Personalize Expiration Launcher **Security** Dependencies

**Require Check Out**   
**Enable DoubleLock**   
*(You have not created a DoubleLock password.)*  
**Enable Requires Approval for Access**   
**Require Comment**   
**Enable Proxy**   
**Hide Launcher Password**   
**Enable SSH Command Restrictions**   
**Allow Owners Unrestricted SSH Commands**

Name	SSH Command Menu		
admin	Unrestricted		
Everyone			

**Add New**  
--Groups-- ▾

**Customize Password Requirement**

A user who is subject to SSH Command Restrictions are presented with a screen similar to the following when connecting to an SSH session:



```

Using username "729ddaef-38d0-48e0-b9dc-d4911e76d0c1".

1. User Command Menu

    ?. Show Command Menus
    exit. Exit session
Last login: Thu Mar 17 12:38:46 2016 from 192.168.60.153
[runscripts@centostestserver ~]$ █

```

The user simply enters the number of the command menu to see available commands, or types "?" to display the options again.

```

Using username "729ddaef-38d0-48e0-b9dc-d4911e76d0c1".

1. User Command Menu

    ?. Show Command Menus
    exit. Exit session
Last login: Thu Mar 17 12:38:46 2016 from 192.168.60.153
[runscripts@centostestserver ~]$ 1

1. view_shadow = cat /etc/shadow
2. view_secure_log = cat /var/log/secure
3. start_apache = /usr/sbin/service apache start
4. stop_apache = /usr/sbin/service apache stop

    up. Return to Command Menu selection. You may also type ..
    ?. Show Commands
    exit. Exit session

[runscripts@centostestserver ~]$ █

```

Only the commands listed can be run by this user. The user can either enter the number of the command to be run, or the name of the command, which is the word to the left of the equal (=) sign. Other options are available (as shown) to navigate through the available command menus, display help, or exit the session.

### Adding a Program Folder to the Windows PATH

If a launcher does not automatically add the program's folder to the Windows PATH:

1. Right click on **Computer** and go to **Properties**.
2. In the Properties window, click Advanced System Settings.
3. On the **Advanced** tab, click the **Environment Variables** button.
4. In the **System Variables** section scroll to **Path**.
5. Click **Edit** then at the very end of the text box, paste the full path to the folder where the program file is located, but make sure not to replace any existing entries. The list is semi-colon separated.
6. Click **OK** to close the dialogs.

## Understanding Session Recording and Launchers

Session recording provides an additional level of security by recording a user's actions after a launcher is used. Session recording works for any launcher, including PuTTY and SSH, Windows Remote Desktop, Microsoft SQL Management Studio, and custom executables. The resulting movie is viewable from the secret audit. Session recording can be toggled on or off globally on the Configuration page and set for individual secrets on the Security tab. Detailed information on supported codecs can be found in [Session Recording](#). When a user launches a session with session recording enabled, a brief message is displayed to inform the user that their actions are recorded.

**Note:** When multiple Launchers are enabled for a secret template, enabling session recording for a secret applies the setting to all launchers for that secret.

## Common Launcher Errors

Two of the most common launcher errors:

- **The process (process name) was not found:** The application has not been installed on the machine. If the application was installed, the program folder needs to be added to the path.
- **The stub received bad data (1783):** The process is set to launch as the credentials of the secret but the username or domain is not correct on the secret or the client machine cannot find the user or domain credentials specified.

## SECRET EXPIRATION

### Introduction

Secret expiration is a core Secret Server feature. Any template can be set to expire within a fixed time interval. For a secret to expire, a text field must be selected as the target of the expiration. For example, a secret template for Active Directory accounts might require a change on the password text field every 90 days. If the password remains unchanged past the

length of time specified, that secret has expired and appears in the Expired Secrets panel on either the Dashboard's Expired secrets widget or the Home page.

Secret expiration provides additional security by reminding users when sensitive data requires review. This assists in meeting compliance requirements that mandate certain passwords be regularly changed. When expiration is combined with RPC, Secret Server can completely automate the process of regularly changing entire sets of passwords to meet security needs.

## Setting up Secret Templates for Secret Expiration

To set up expiration on a secret, you must first enable expiration on the template from which the secret is created.

To enable secret expiration for a secret template:

1. Navigate to **Admin > Secret Templates**.
2. On the **Manage Secret Templates** page, select the template from the dropdown list.
3. Click **Edit**.
4. On the **Secret Template Designer** page, click on the **Change** link.
5. On this subsequent page, click to select the **Expiration Enabled?** check box.
6. Enter the expiration interval (every x number of days), as well as the text field on the secret you wish to expire and require to be changed.

**Note:** You can override the interval setting for individual secrets.

**Note:** Enabling expiration for a template enables expiration for all the secrets that were created using that template.

## Setting up Secrets

Once you enable expiration for the template, expiration is also enabled for secrets that were created using that template as well as secrets created in the future. The Expiration tab appears on the Secret View page and requires the user to have Owner permission on the secret.

To set a custom expiration at the secret level, you adjust the expiration interval for the secret by clicking the **Expiration** tab in the **Secret View** page. There, you can set the secret to expire using the template settings (default), a custom interval, or a specific date in the future.

## Forcing Expirations

To force expiration:

1. Navigate to the **Secret View** page.
2. Click the **Expire Now** button. This forces the secret to expire immediately regardless of the interval setting. The expiration date displays "Expiration Forced."

## Resetting Expired Secrets

To reset an expired secret, you must change the text field that has expired and is required to change. For example, if the text field set to expire is the password text field and the current password is "asdf," then a change to "jklh" resets the expiration interval and thus removes the expiration text on the Secret View page.

If you do not know which text field is set to expire:

1. Go to the secret template that the secret was created from.
2. Navigate to **Admin > Secret Template**.
3. Select the template.
4. Click **Edit**.
5. On the next page, click the **Change** link. In the **Change Required On** text box you can see the text field that is set to expire.

## SECRET DOUBLELOCKS

### Introduction

Secret Server's *doublelock* is a feature that provides an additional security layer by encrypting secret data with a supplemental custom encryption key that is only accessible with an additional password, regardless of regular permissions, Secret Server login access, or physical access to the machine running Secret Server. Doublelock uses private and public key encryption technology to securely share access to doublelock.

A shortcut way of thinking about doublelocks is as a special extra password for secrets that is held by a set group of users. In addition, both the password and the group of users are reusable for other secrets.

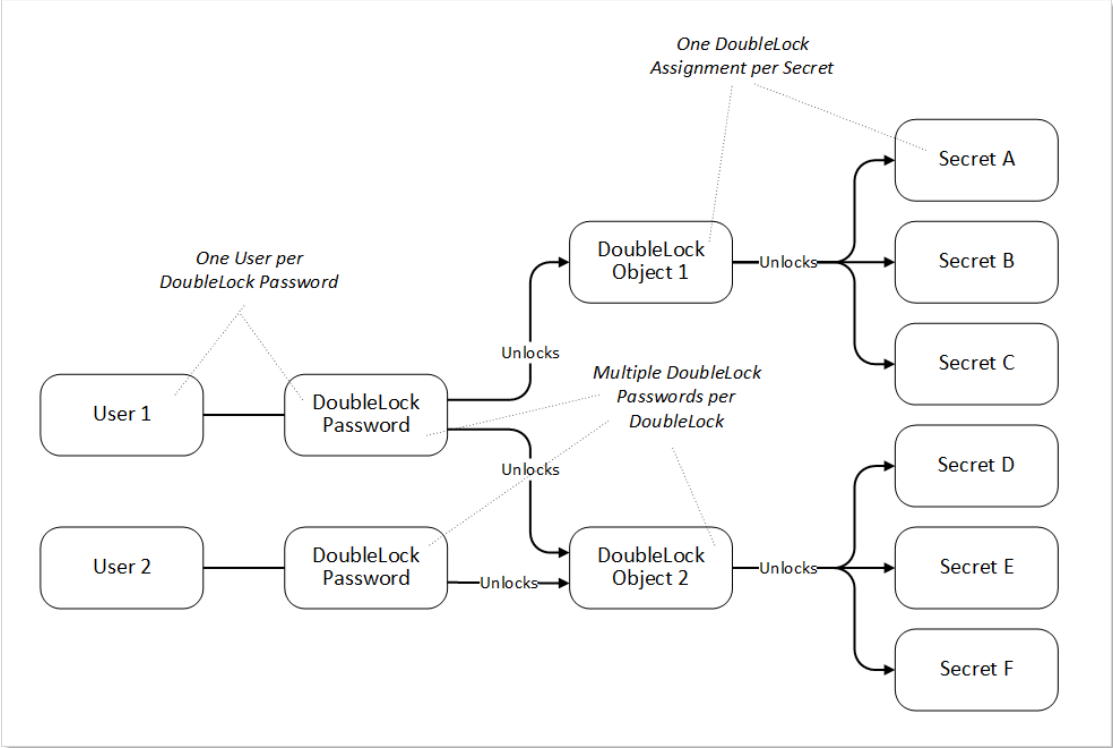
### DoubleLock Objects and Relationships

The doublelock system is a group of interrelated objects (see the following diagram):

- **Doublelock object:** A named object that is associated with one or more secrets and one or more users (via password objects). Doublelock objects, or simply *doublelocks*, point to secrets (what can be accessed) and doublelock password objects (who can access it).
- **Doublelock password object:** An encrypted password that is associated with one user. The same doublelock password object, or simply *doublelock password*, is used for all doublelocks to which a user has access. Once a user is assigned to a doublelock, that user has access to any secret using that doublelock, using a single password. A doublelock password has nothing to do with the user's Secret Server access password.

- **Secret:** A secret that has a single doublelock assigned to it. Multiple secrets can have the same doublelock assigned to them.
- **User:** A Secret Server user, which can have a single doublelock password assigned to it.

**Figure: DoubleLock Object Relationships**



**Password Loss and Assignment**

Because users with access to a given doublelock each have their own separate password. Users that forget their doublelock password cannot simply ask another person using that doublelock for the password. Instead, one of the other users must reassign that forgetful user to the doublelock, and the user must choose a new password. This must occur for every doublelock the user was associated with. If no other doublelock users are available for the assignment to a given secret (there is only one associated doublelock password), the forgetful user is out of luck, and the secret will be destroyed when the user receives a new doublelock password.

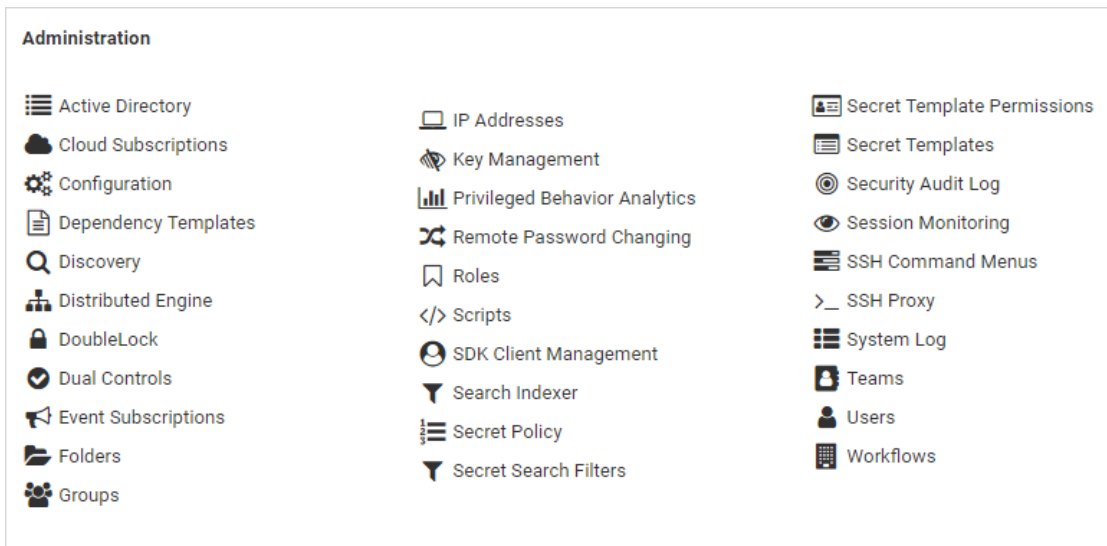
**Using a DoubleLock**

As an admin, to use doublelocks on a secret, you must first create complete these steps for a new doublelock:

1. Create a doublelock password (one time per user). This is automatically required of you when you create a doublelock or access a secret with an existing one (that somebody else assigned to you). You can also create one manually ahead of time.
2. Create a doublelock, which can be used on multiple secrets by multiple users (one time).
3. Assign the doublelock to a secret or secret template (one or more times).
4. Assign users to that doublelock (one time per user). Users without an existing doublelock password are required to create one.
5. A user unlocks the doublelock with his doublelock password, which in turn gives the user access to the secret associated with the doublelock (every time the user wants access to the secret).

## Creating a DoubleLock and a DoubleLock Password

1. Navigate to **Admin > See All**. The Administration page appears:



2. Click the **DoubleLock** button. The DoubleLocks page appears:

**Note:** If there are no existing doublelocks, you will instead go directly to the Create DoubleLock page.

**DoubleLocks**

Save To File < 1 to 3 of 3 >

DOUBLELOCK NAME	ENABLED	CREATED
Indium	Yes	2019. 03. 05.
Test_doublee	Yes	2019. 02. 22.
Will	Yes	2019. 05. 08.

Show Inactive DoubleLocks?

- Click the **Create New** button. The Create DoubleLock Password page appears:

**Note:** This is the same procedure as seen in [Assigning a User a DoubleLock Password](#). Secret Server automatically provides it here as a convenience.

**Create DoubleLock Password**

*Please enter a new DoubleLock password and press the Create Password button. This will allow you to access Secrets with DoubleLock.*

Password \*

Confirm Password \*

- Type your desired doublelock password in the **Password** and **Confirm Password** text boxes.


**Important:** It is critical that you remember or securely store this password. It cannot be recovered.

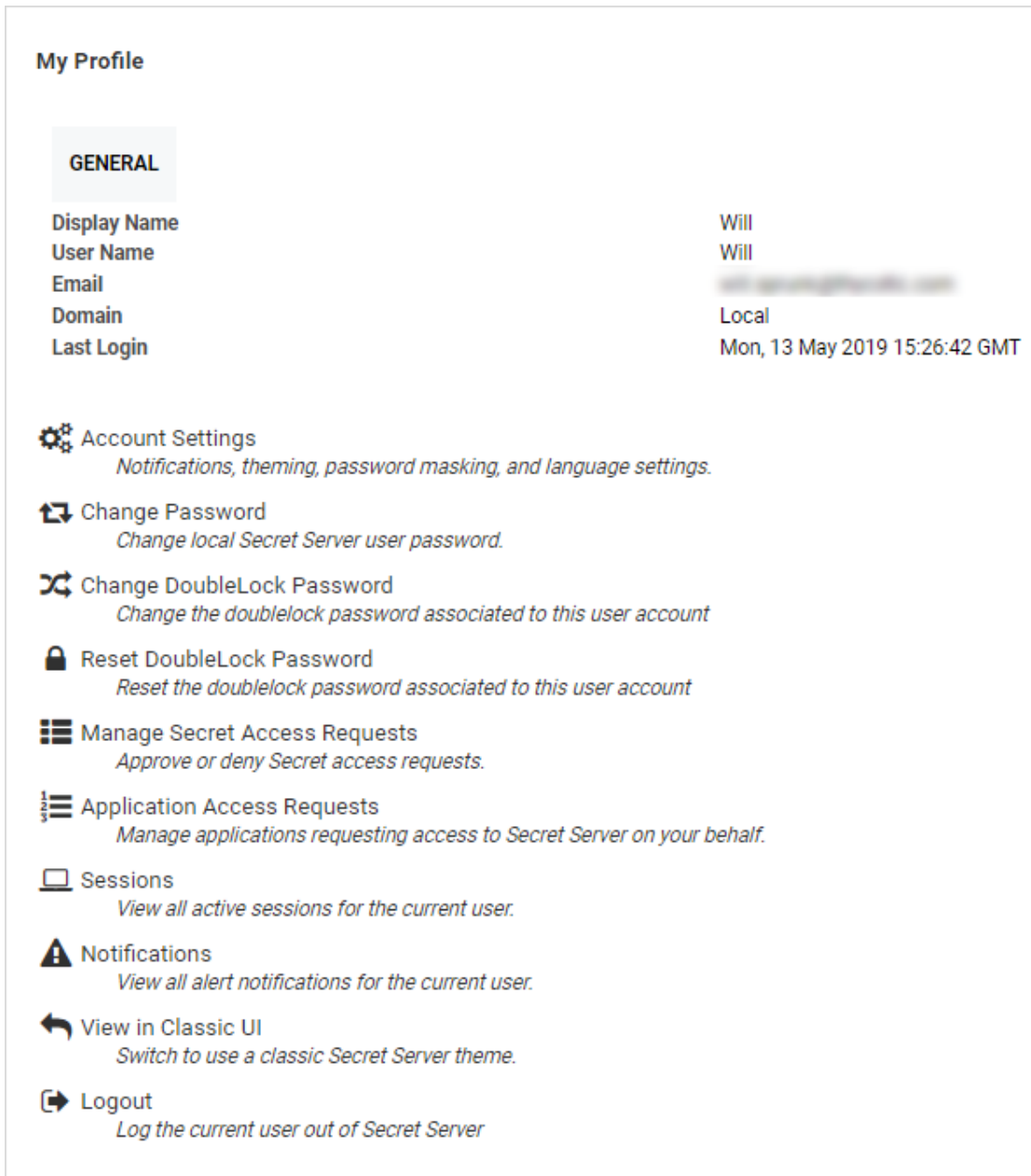
- Click the **Create Password** button. The password is created, and the DoubleLocks page reappears.

**Note:** The newly created doublelock does **not** appear on the page.

**Note:** A new doublelock and doublelock password are created at the same time. In fact, it is impossible to create a doublelock password without immediately assigning it to a doublelock. For an existing doublelock, you are assigned access to it. Upon first access, you must create a doublelock password if you do not already have one.

## Assigning a User a DoubleLock Password











1. Click the  icon at the top right of Secret Server. Your My Profile page appears:



**My Profile**

**GENERAL**


Display Name	Will
User Name	Will
Email	<a href="#">will.williams@secretserver.com</a>
Domain	Local
Last Login	Mon, 13 May 2019 15:26:42 GMT

-  **Account Settings**  
*Notifications, theming, password masking, and language settings.*
-  **Change Password**  
*Change local Secret Server user password.*
-  **Change DoubleLock Password**  
*Change the doublelock password associated to this user account*
-  **Reset DoubleLock Password**  
*Reset the doublelock password associated to this user account*
-  **Manage Secret Access Requests**  
*Approve or deny Secret access requests.*
-  **Application Access Requests**  
*Manage applications requesting access to Secret Server on your behalf.*
-  **Sessions**  
*View all active sessions for the current user.*
-  **Notifications**  
*View all alert notifications for the current user.*
-  **View in Classic UI**  
*Switch to use a classic Secret Server theme.*
-  **Logout**  
*Log the current user out of Secret Server*

2. Click the **Change DoubleLock Password** button. The Create DoubleLock Password page appears:



**Create DoubleLock Password**

 Please enter a new DoubleLock password and press the Create Password button. This will allow you to access Secrets with DoubleLock.

Password \*

Confirm Password \*

3. Type your desired doublelock password in the **Password** and **Confirm Password** text boxes.

**Important:** It is critical that you remember or securely store this password. It cannot be recovered.


4. Click the **Create Password** button. The password is created.

### Assigning a DoubleLock to a Secret

1. Navigate to the secret you wish to doublelock by clicking **Secrets** on the main menu.
2. Either drill down to the desired secret in the folders on the main menu, or click the secret in the **All Secrets** table to arrive at the secret's page:

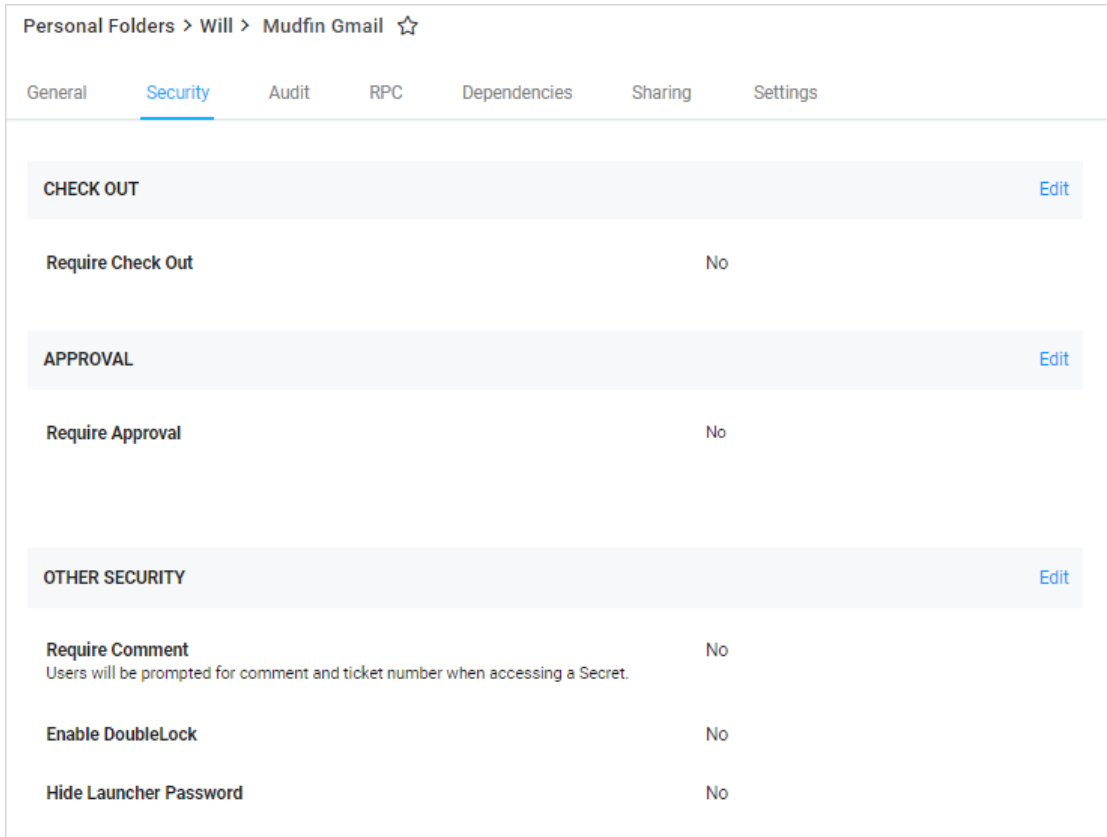
Personal Folders > Will > Mudfin Gmail ☆

[General](#) [Security](#) [Audit](#) [RPC](#) [Dependencies](#) [Sharing](#) [Settings](#)

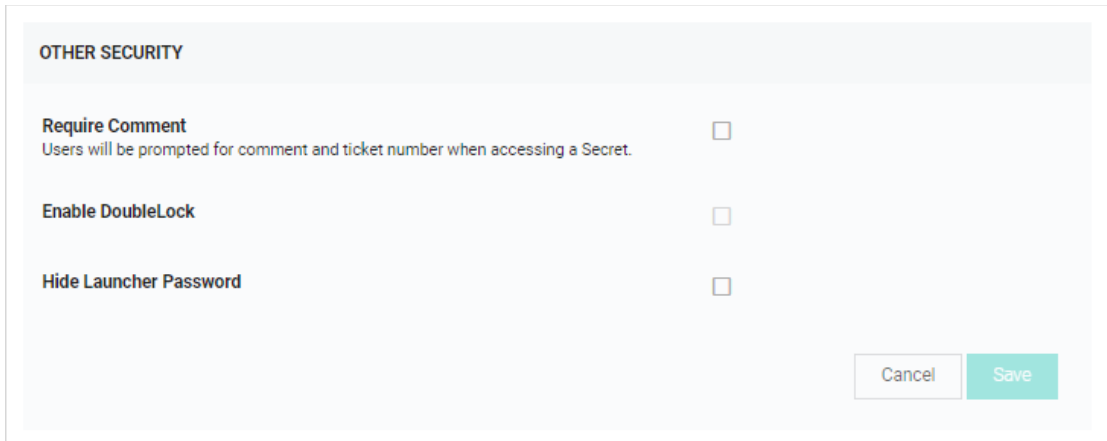
Secret Name *	Mudfin Gmail	<a href="#">Edit</a>
Template	Web Password	<a href="#">Edit</a>
URL *	<a href="https://mail.google.com">https://mail.google.com</a>	<a href="#">Edit</a>
UserName *	smedlymufin	<a href="#">Edit</a>
Password *	***** <a href="#">Show</a>	<a href="#">Edit</a>
Notes		<a href="#">Edit</a>
Launchers	 Web Password Filler	

[Show Advanced](#) [Edit all fields](#)

3. Click the **Security** tab.



4. Click the **Edit** link for the **Other Security** section. The section becomes editable:



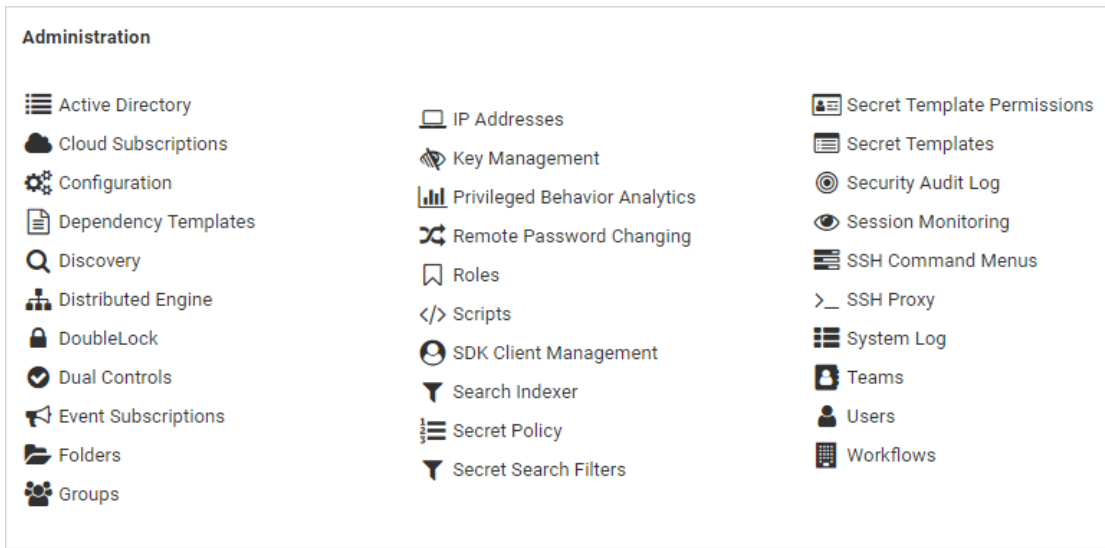
5. Click to select the **Enable DoubleLock** check box. The DoubleLock dropdown list appears.
6. Click to select the doublelock you created earlier.

**Important:** Enabling doublelock on this secret only grant users access if they have access to the doublelock and enter their doublelock password. Enabling doublelock disables the RPC features for the secret.

7. Click **Save**. The doublelock is now enforced for the secret.

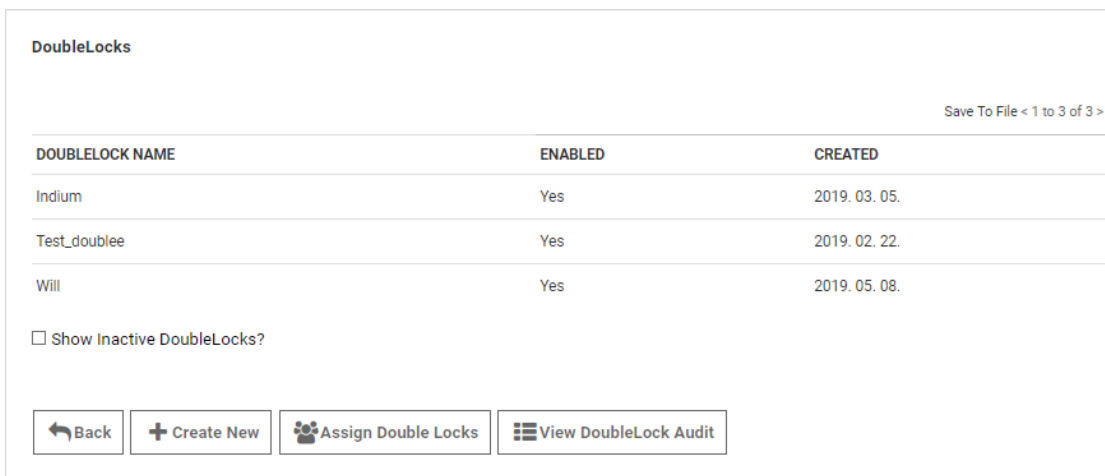
## Assigning Users to Existing DoubleLocks

1. Navigate to **Admin > See All**. The Administration page appears:



2. Click the **DoubleLock** button. The DoubleLocks page appears:

**Note:** If there are no existing doublelocks, you will instead go directly to the Create DoubleLock page.



3. Click the **Assign Double Locks** button. The Create DoubleLock Password page appears:

### View User Assignment

By DoubleLock    By User


DoubleLock

---

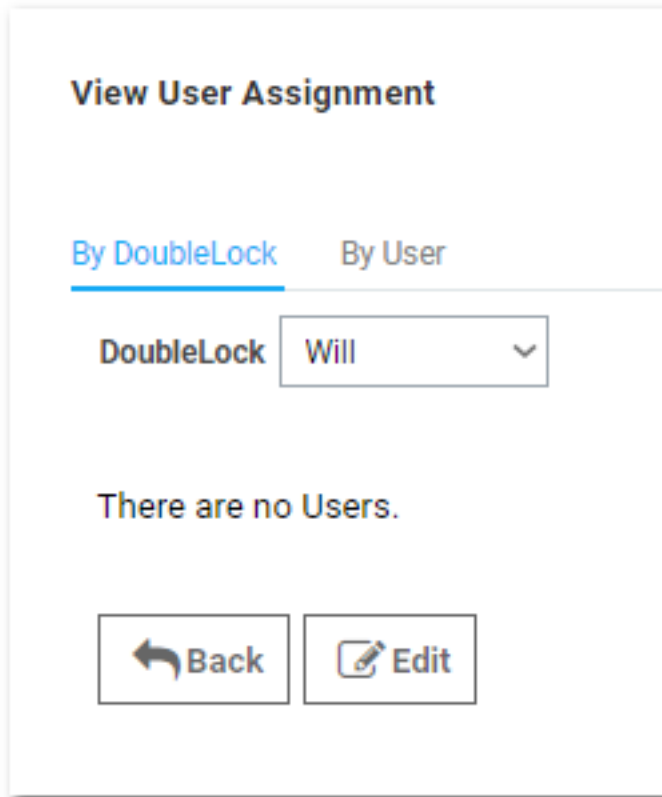
**NAME**

Joshi

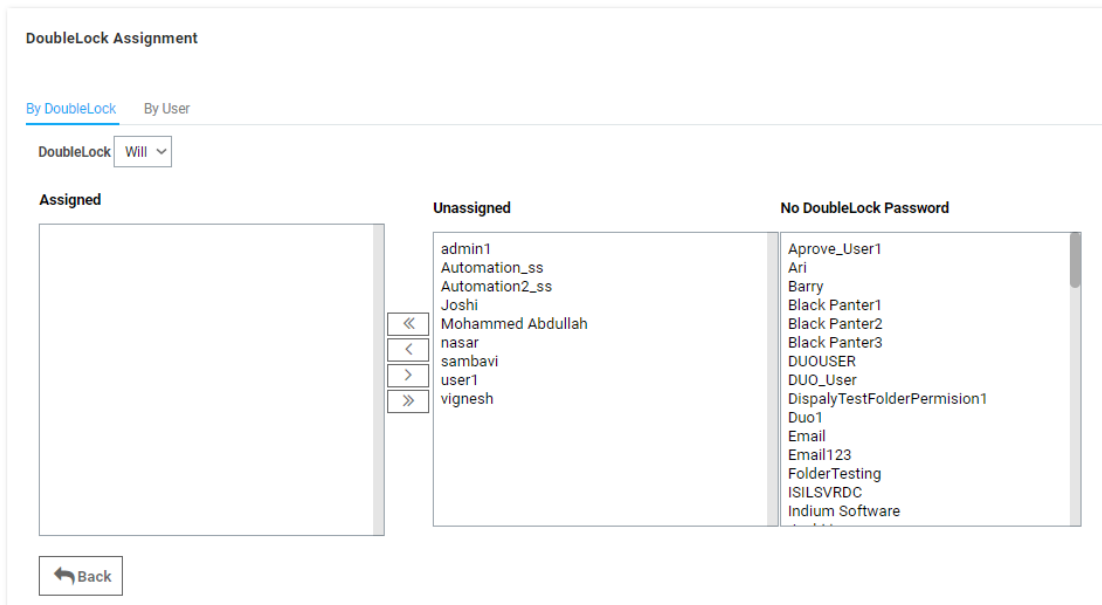
sambavi



4. Ensure the **By DoubleLock** tab is selected.
5. Click the **DoubleLock** dropdown list to select the doublelock to assign.



6. Click **Edit**. The DoubleLock Assignment page appears:

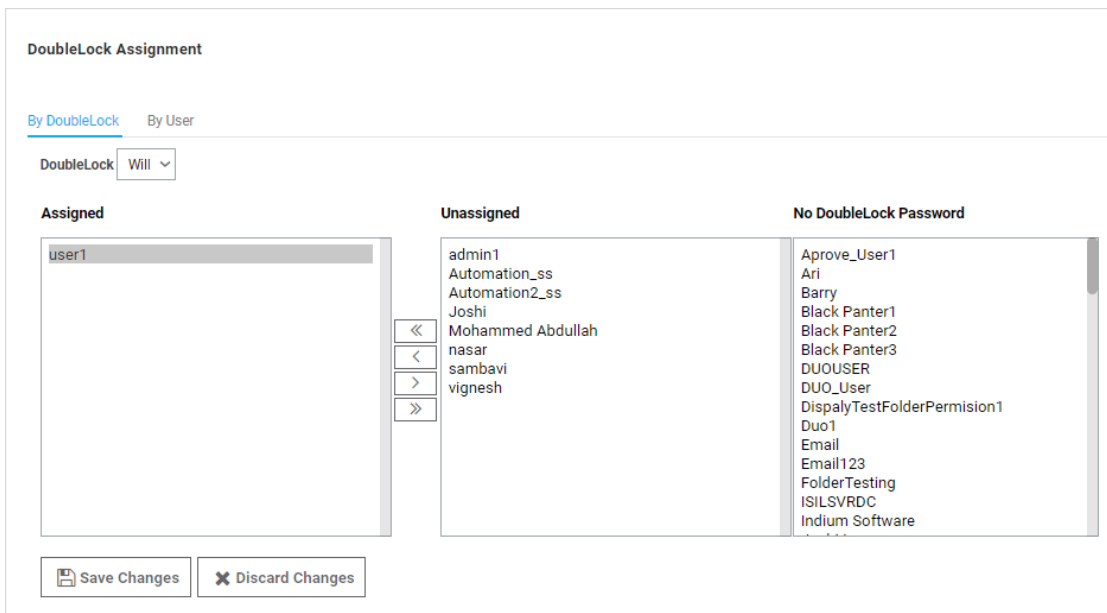


– The "Unassigned list" has users that are not assigned to any doublelock.

- The "No DoubleLock Password" list contains users that have never been assigned a doublelock password. The users will be prompted to create a doublelock password when they attempt to access a doublelocked secret.

**Note:** The "No DoubleLock Password" list is for information only. It does not have any direct function on this page. Instead, it tells you users who are available but first must create a doublelock password for themselves.

7. Click the desired user in one of the two lists.
8. Click the < button to move that user to the **Assigned** list:



9. Click the **Save Changes** button.

## Resetting a DoubleLock Password

When users forget their doublelock passwords, there are multiple steps and considerations. Data loss may or may not result from resetting:

1. When you forget your doublelock password, you typically come to that realization when attempting to access a secret protected by that doublelock:

DoubleLock - Mudfin Gmail


Please enter your DoubleLock password to gain access to the requested resource.

Password \*

[Forgot DoubleLock Password?](#)


- Click the **Forgot DoubleLock Password?** link. The Reset DoubleLock Password page appears:

Reset DoubleLock Password

 Resetting your forgotten DoubleLock password is irreversible and could result in permanent loss of the data. In the case you are the only user with access to the DoubleLocked Secrets, the data will be lost and the Secrets deleted. If another user has access to the Secret, they will need to re-assign you to the DoubleLock. Please review the DoubleLocks and Secrets that will be impacted on reset.

**DOUBLELOCKS**

**Will**

 No one will have access to these Secret(s). The data will be permanently lost and Secrets deleted.

NAME	TEMPLATE	FOLDER	CREATED
Mudfin Gmail	Web Password	Will	2019. 05. 07.

Please enter your login password to confirm the DoubleLock reset, and acknowledge the Secrets will be lost.

Login Password

- At this stage, there are two possibilities:
  - You are the only one with access to the doublelocked secret: When you reset the doublelock password, the secret and its data is deleted. **This is permanent.**
  - Others have access to the secret via that doublelock: You can reset the doublelock, and you lose access to the secret, but it is not deleted. You must ask one of those others to re-assign you to the doublelock after you reset it.
- Type your main Secret Server password in the **Login Password** text box.
- Click the **Reset DoubleLock Password** button. The password is reset, and if you are the only one with access to it, the secret is deleted.



- (Optional) Ask one of the others with the doublelock password to re-assign you to the doublelock.

## SECRET CHECK-OUTS

### Introduction

The Secret Server *check-out* feature forces accountability on secrets by granting exclusive access to a single user. If a secret is configured for check out, a user can then access it. If **Change Password on Check In** is turned on, after check in, Secret Server automatically forces a password change on the remote machine. No other user can access a secret while it is checked out, except unlimited administrators. This guarantees that if the remote machine is accessed using the secret, the user who had it checked out was the only one with proper credentials at that time.

**Note:** The exception to the exclusive access rule is unlimited administrators. If Unlimited Administration is enabled, users with Unlimited Administrator role permission can access checked out secrets.

**Note:** Secrets with a doublelock cannot be configured for check out.

### Configuring Password Changing on Check in

To configure password checking on check in, navigate to the **Remote Password Changing Administration** page and set **Enable Password Changing on Check In**. If RPC is turned off, enable it before configuring checkout. Once RPC and checkout are enabled, secrets can be configured for interval that specifies how long a user has exclusive secret access.

Remote Password Changing Configuration	
Enable Remote Password Changing	Yes
Enable Password Changing on Check In	Yes
Check Out Interval	30 minutes
Enable Heartbeat	Yes

Navigation buttons: Back, Edit, Configure Password Changers, Configure Dependency Changers, Distributed Engine Configuration, View Audit

### Checking Out Secrets

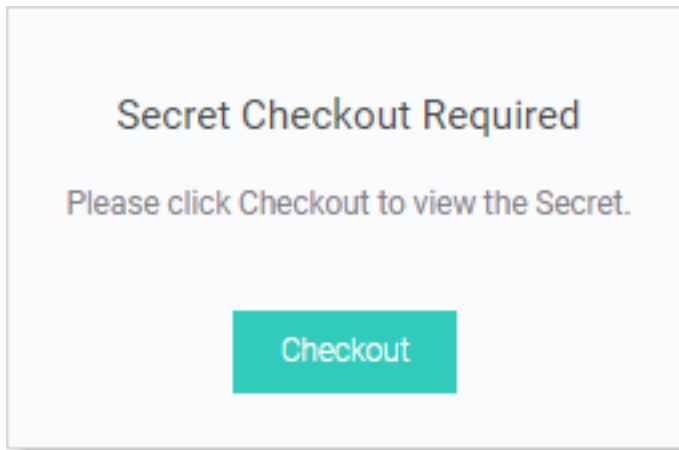
Each secret must be individually set to require check out:

- From the **Secret View** page, open the **Security** tab to modify a secret's **Check Out** setting.

2. You must configure RPC before **Change Password on Check in** can be set.
3. Enable **Require Check Out** to force users to check out the secret before gaining access.
4. Enable **Change Password on Check In** to have the password change after the secret is checked in.

## Configuring a Secret for Check Out

After Require Check Out is enabled, users are prompted for check out when attempting to view that secret.



## Exclusive Access

Any user attempting to view a checked-out secret is directed to a notification dialog informing them when the secret is available. Secret Server automatically checks in secrets after either 30 minutes or the interval specified on the secret. Users can check in the secret earlier from the secret's page.

## Check-Out Hooks

In addition to changing the password on check in, secret owners can also specify administrator-created PowerShell scripts, called *hooks*, to run before or after checkout and check in. These are accessed from the **Hooks** tab of the secret, which only shows if checkout is enabled and PowerShell scripts have been created by an admin. To specify a before- or after-checkout hook, click **Create New Hook** and specify the following settings:

- **Before/After:** Whether the PowerShell script should run before or after the Event Action.
- **Event Action:** The hook runs at either check in or checkout.
- **Name:** A descriptive name for the hook.

- **Description:** An extended description for the purpose of the hook.
- **PowerShell Script:** Administrator-created PowerShell script to run.
- **Arguments:** Any command line arguments to pass to the PowerShell script.
- **Stop on Failure:** If enabled, Secret Server prevents the event action if the script returns an error. For example, if "Stop on Failure" is selected for a checkout action, then Secret Server prevents the user from checking out the secret if the script fails.
- **Privileged Account:** If needed, the script can run as another secret's identity.

## SECRET ACCESS REQUESTS

### Basic Secret-Access Requests

The access request feature allows a secret to require approval prior to accessing the secret. Note the following:

- Establishing a workflow model, the user must request access from the approval group or groups.
- An email is sent to everyone in the approval groups, notifying them of the request.
- The request can be approved or denied by any members of the approval groups.
- Access is granted for a set time period.
- If **Owners and Approvers also Require Approval** is enabled, then even owners or those in an approval group needs to request access.

### Setting up Access Requests for Secrets

To enable Access Request for a secret, navigate to the **Secret View** page for the secret:

1. Go into the **Security** tab and click **Edit**.
2. Check the **Enable Requires Approval for Access** checkbox to enable the setting.
3. Once enabled, select users or groups as approvers for the secret. Unless the **Owners and Approvers also Require Approval** option is turned on, owners or users that are members of the Approvers group do not must request access to view the secret.

**Note:** Users need at least view access to the secret to be able to access the secret even with **Access Request** enabled. If the users do not have view permission they are unable to find the secret with Search or Browse.

**Note:** The email configuration settings need setting up, including valid email addresses, for the users in the approval group for emailing to work.

## Requesting Access After Approval Is Granted

To start the request process for access to a secret, the user must simply attempt to view the secret. The user is then sent to the Request page. In there, the user can explain the reason for the request and then click **Request Access** to submit the request.

If a member of the Approval Group either approves or denies the request (see below for details), the requestor is sent an email with the details. If approved, the requestor can access the secret via the link contained in the email.

## Approving a Request

- Once a request for access to a secret has been made, approvers receive an email.
- The email contains one link to the secret **Access Request Approval** page for that request in Secret Server, and five additional links to approve or deny the request if the **Allow Approval for Access from Email** configuration setting is enabled.
- The approver can either click one of the links contained in the email or navigate to the **Notification Center** in the user menu within Secret Server.

The screenshot shows the 'Alert Notification Center' interface. It features a 'FILTER' section with two columns: 'Notification Type' and 'Priority'. Under 'Notification Type', there are checkboxes for 'Event Subscription', 'Secret Access Requests', 'Application Access Requests', 'System Alerts', and 'Include Archived'. Under 'Priority', there are checkboxes for 'Requires Interaction', 'Critical', and 'Informational'. Below the filters is a table with three columns: 'PRIORITY', 'NAME', and 'DESCRIPTION'. The table contains one row with a gear icon in the 'PRIORITY' column, an 'i' icon in the 'NAME' column, and the text 'Pending Engine' in the 'DESCRIPTION' column.

PRIORITY	NAME	DESCRIPTION
	<b>i</b>	Pending Engine

If choosing the latter, in the displayed grid click the access request name. This takes you to the secret's Access Request Approval page.

- From here, you can accept or deny the request as well as set an expiration date.
- The requestor has access to the secret until the specified date.
- Selecting the current date is the smallest window of time allowed and grants access to the end of the day.

- With **Allow Approval for Access from Email** enabled, clicking one of the five additional links in the email allows access for 1, 2, 4, or 8 hours or deny the request, per the link description in the email.

**Note:** The expiration date referred to in approval requests is **not** the same as secret expiration.

## Duo Push Notifications

Users can now approve secret access requests and workflows using Duo push notifications. The push notification includes information, displayed on the user's screen, that helps the approver make the access decision.

### *Prerequisites*

To use Duo push notifications:

- Duo must set up for Secret Server. See [Duo Security Authentication](#).
- Duo user must be set up for Duo two-factor authentication. See [Setting up Duo \(User\)](#).
- The permission "Approve via DUO" must be granted to a role that is assigned to a group that includes all who will be approving requests via Duo. This allows enough flexibility so that those not wanting Duo push approvals can be configured to not receive them.

### *Assigning the Duo Approval Permission*

To associate the permission with users:

1. Go to **Admin > Roles**.
2. Click the **Create New** button to create a new role. Name it "Duo Push Approver" or another name of your choosing.
3. Assign the **Approve Via DUO Push** permission to the new role.
4. Click **Save**.
5. If you choose to create a separate group for approvers, do this by navigating to **Admin > Groups**.
6. Click the **Create New** button to create a new group.
7. Add the desired users (chosen approvers) to that group.

**Note:** You can also assign users to the group later. This method is a shortcut when creating a group.

8. Click **Save**.
9. Go to **Admin > Roles**.
10. Click the **Assign Roles** button. The View Role Assignment page appears.

11. Click the **Role** dropdown list to select the role you created. Note that there are no groups or users.
12. Click **Edit**. The Role Assignment page appears.
13. Assign the **Approve via DUO Push** role to the **Assigned** list box.
14. Click the **Save Changes** button. Setup is now complete.

**Note:** In addition to having the role you created, the user must be properly set up to receive Duo push notifications. See [Setting up Duo \(User\)](#).

**Note:** Any notifications will all be sent out at the same time, and the first response (approve or deny) will be the determinant response. A non-response will not result in either an approve or deny response.

## Advanced Secret-Access Requests with Workflow Templates

### Workflow Templates

Starting in 10.6, Secret Server introduced *access-request workflow templates*. These allow users to build more complex interactions based on events within Secret Server than currently possible. The first release of workflows offers access requests. Workflow templates define the series of steps and reviewers required for an access request. You can assign workflow templates to secrets or secret policies.

With Access-Request Workflow Templates, you can:

- Require that multiple people approve a request before access is granted
- Require multiple workflow steps, each with different reviewers and number of required approvers, if desired.
- Select "Owners" as a review group

### Access Requests

Access Requests already existed in Secret Server, but with 10.6 they become much more powerful. Previously, if access requests enabled on a secret, requests were granted after a single reviewer approved the request. Now, approval workflows can require multiple approvers, and multiple approval levels.

### New Features

#### *Multi-Level Workflow*

The current implementation is one level or step--anyone approving approves the request--no other input is required. Workflows now allow up to 15 approval steps where approval by reviews in step 1 moves the request to step 2, approval at step 2 moves it to step 3 and so forth. Denial at any step denies the request.

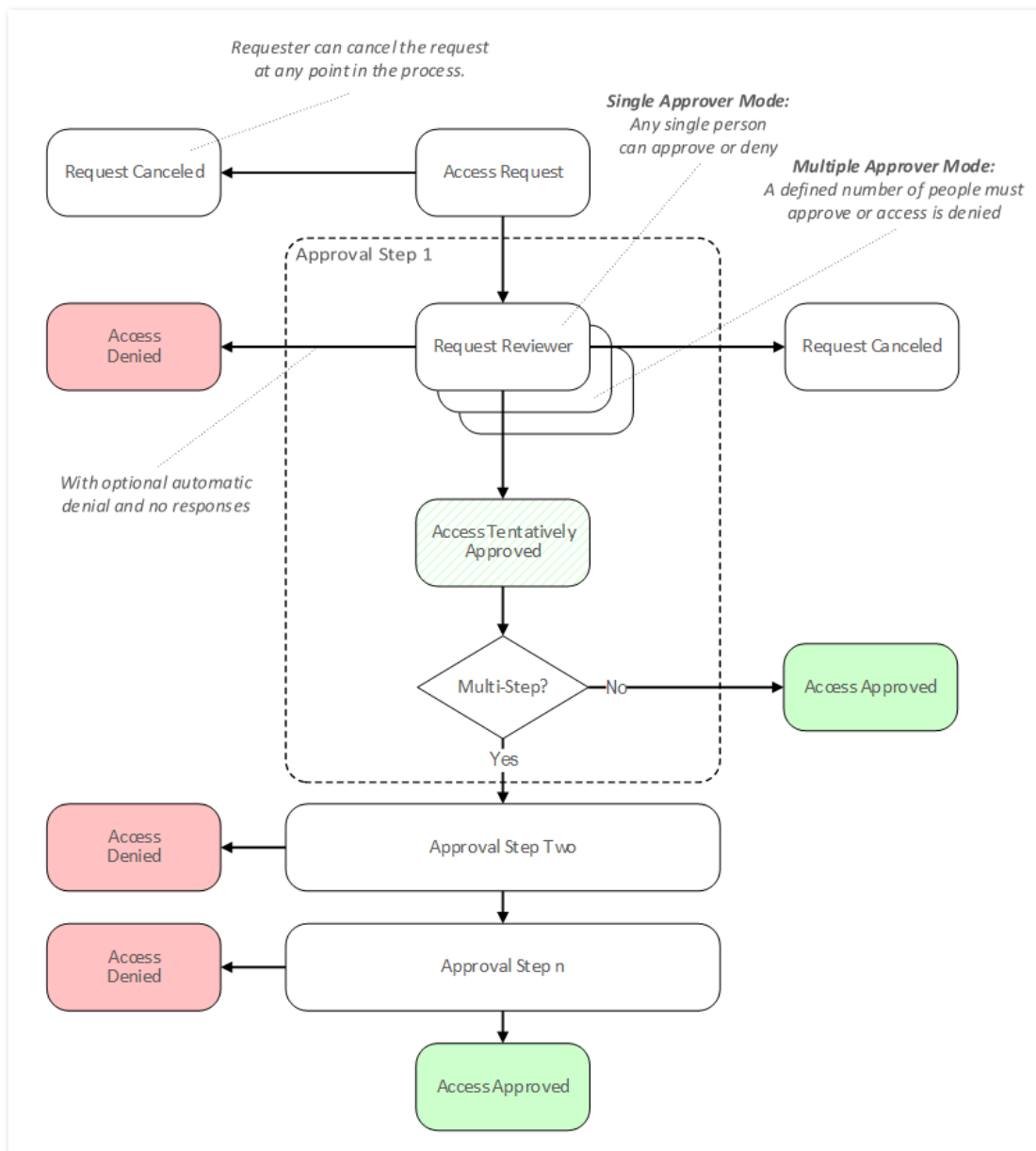
### Multiple Approvers to Advance

The new workflow feature can be configured where one approver at a given step is not enough. In effect, approvers in each step can "vote" for approval—you stipulate how many approvers at a step must approve for the approval to move on to the next step.

### Approval Process Workflow

The following diagram is the entire process summarized:

**Figure: The Approval Process Workflow**



## Workflow Versus Basic Access Requests

In general, "simple access requests," the only type available to older versions of Secret Server, are the same as a one-step stepped approval. The major exception is that with stepped requests, once a workflow access request has been approved, denied, or canceled, its status cannot be changed. In contrast, simple, non-workflow, access requests retain the original behavior of allowing a request to be approved after it has been denied or denied after it has been approved.

## Access-Request Workflow Procedures

### *Understanding Workflow Template Design Best Practices*

Consider the following when setting up an access-request workflow template:

- Use multiple-step approval workflows when you must have different people (such as different departments) sign off on an approval request.
- We do not recommend assigning equally important approvers or groups to multiple steps. Having a single step with multiple approvers works better. Remember, steps are best used for hierarchal approval--an approval chain.
- A reviewer can only respond to a request once. If you have the same user as a reviewer in multiple steps, that approver cannot respond if he or she already responded on an earlier step. In addition, the reviewer's earlier approval does **not** count towards the number of approvals required in later steps. Thus, if you want to assign the same user as a reviewer in multiple steps, make sure that you have enough reviewers in each step to approve without that user.
- A well-crafted workflow template design ensures there are enough approvers in a group to satisfy the multiple approver (x of n reviewers must approve) requirement, but group membership can change after the workflow is created. Thus, if you remove members from groups used by workflows, ensure there are still enough members in those groups to approve requests.

### *Accessing the Workflow Designer*

To access workflow templates:

1. Go to **Admin > Workflows**. The Workflow Template page appears:



**Workflow Templates** Create Workflow Template

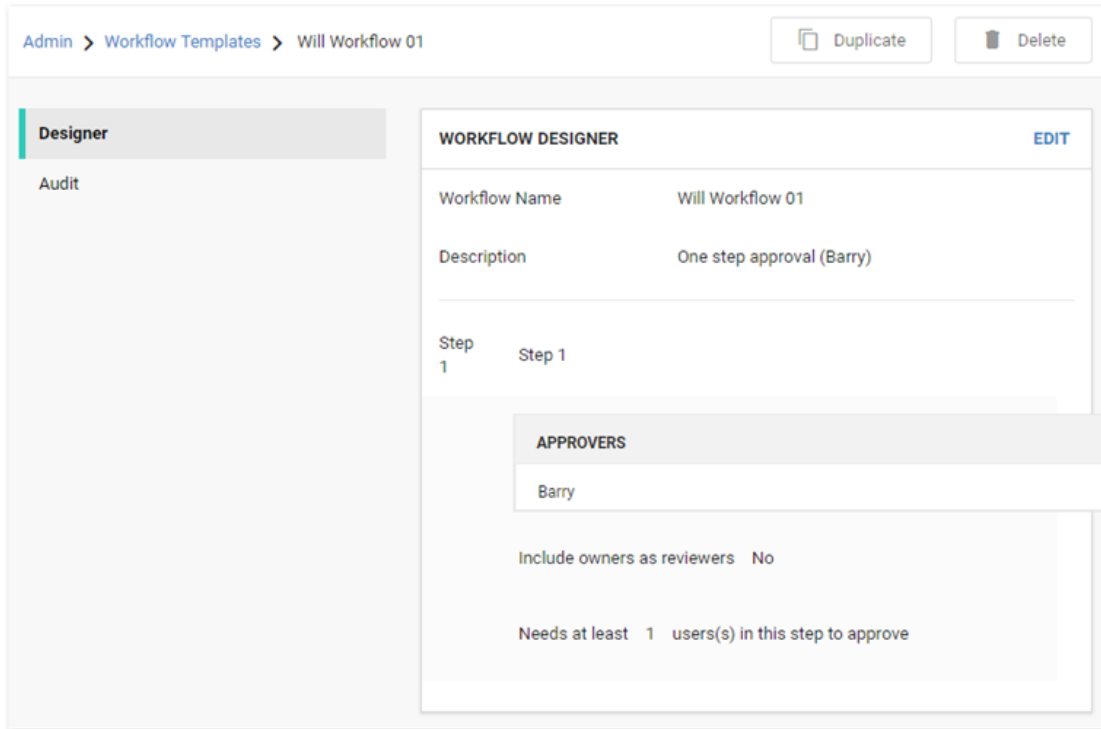
52 Items Show Inactive

1 of 4 ◀ ▶

WORKFLOW TEMPLATE NAME <span style="font-size: small;">↓</span>	TYPE	ACTIVE	⋮
workflow_test_01	Access Request	Yes	
workflow_Step	Access Request	Yes	
workflow_Policy	Access Request	Yes	
workflow_group	Access Request	Yes	
Workflow_Del	Access Request	Yes	
Workflow_01	Access Request	Yes	
Workflow Template 2 Step - Marrio - Barry	Access Request	Yes	
Workflow Template 1-Step Barry	Access Request	Yes	
WK01	Access Request	Yes	
Will Workflow 01	Access Request	Yes	
WFT_001	Access Request	Yes	
WF_template01	Access Request	Yes	
testWF	Access Request	Yes	

The page lists all active workflow templates.

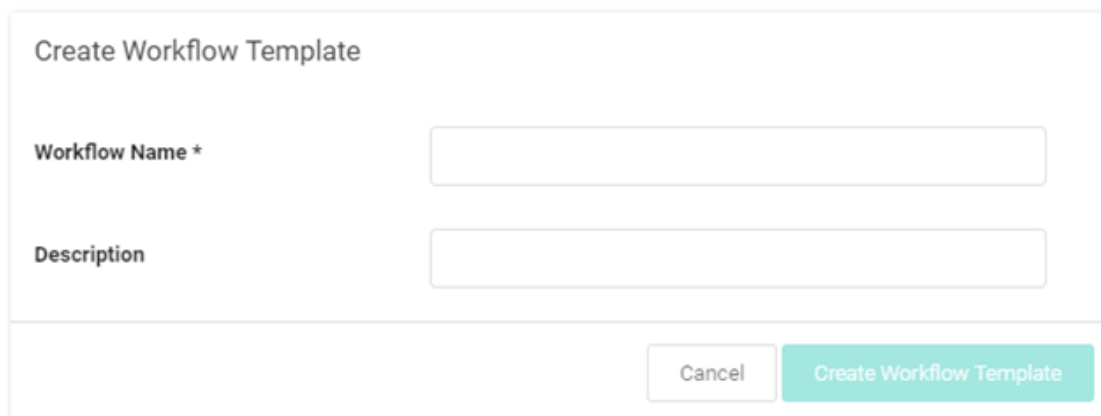
2. (Optional) Click to enable the **Show Inactive** toggle button, under the **Create Workflow Template button**, to show both active and inactive templates. When the toggle button is disabled, it only shows active workflow templates.
3. Click any workflow template in the list to go to the designer page for that workflow:



### Creating New Workflow Templates

**Task 1:** Access the Workflow Designer:

1. Click **Create Workflow Template**.



2. Type the workflow template's name and descriptions in their text boxes. Once you type the name, the Create Workflow Template button becomes enabled.
3. Click **Create Workflow Template**. The Edit page for the new workflow template appears.

**WORKFLOW DESIGNER**

Workflow Name

Description

---

Step 1

**APPROVERS**

No approvers have been added

Add Groups / User

Include owners as reviewers

Needs at least  users(s) in this step to approve

A new workflow template has only one empty step by default.

**Task 2:** Set up the first step:

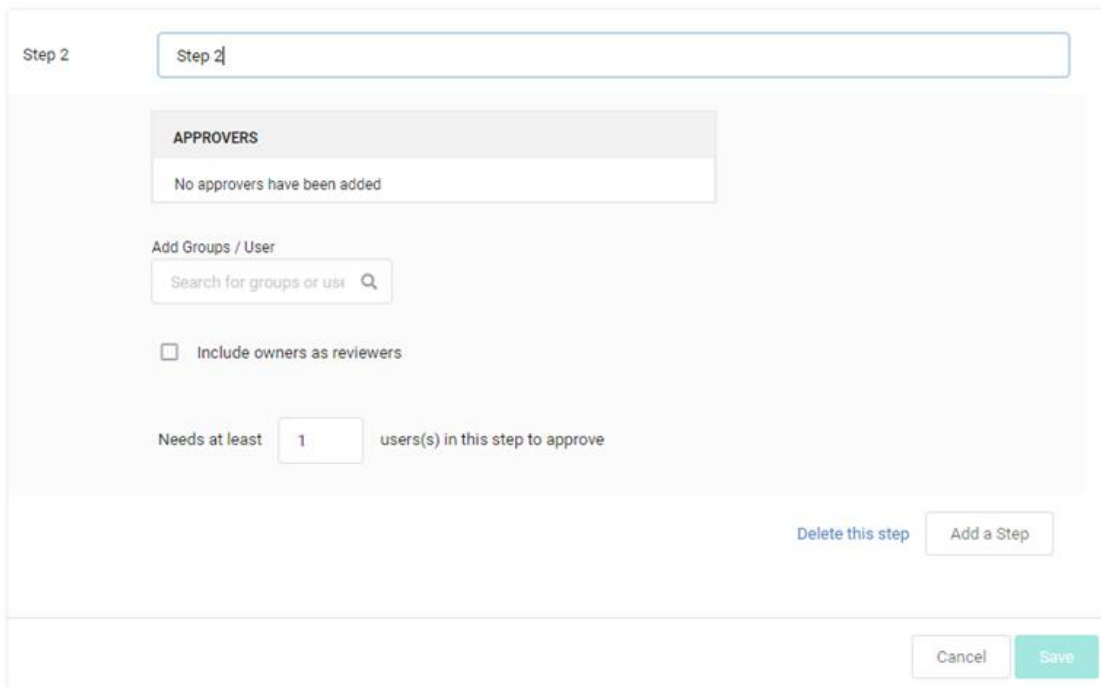
1. (Optional) Type a name for the first step in the **Step 1** text box, such as "Line Managers."
2. Click the **Add Groups / Users** (search) text box.
3. Type the name of the user or group you desire as approvers, options appear in the dropdown.
4. Click the desired user or group. It appears in the Approvers table:



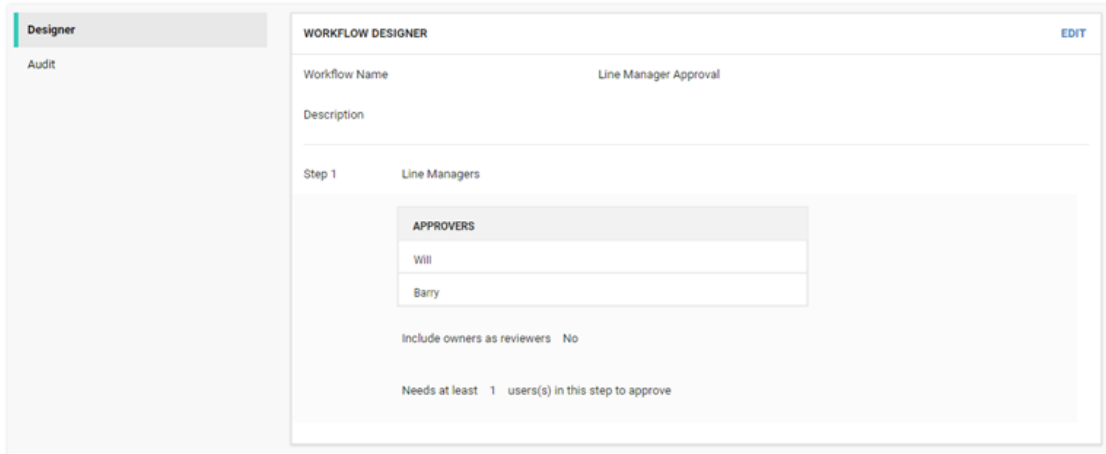
5. Repeat as desired.
6. (Optional) To automatically include the owner of the secret the template is assigned to, click to select the **Include owners as reviewers** check box.
7. (Optional) If you wish to have multiple approvers required on the step, type the minimum required in the **Needs at least...** text box.

**Task 3:** (Optional) Add more steps:

1. Click **Add a Step**.



2. Repeat the process for step one.
3. (Optional) Keep adding steps.
4. Click **Save** to create the access-request workflow template. The template exits editable mode:



5. Click the **Workflow Templates** link to return to the table.

### *Editing Workflow Templates*

To edit the template:

1. Click **Edit**. The Workflow Designer page becomes editable:
2. At this stage the process is nearly identical to creating a new workflow template. The only difference is many of the parameters and additional steps are already completed. Change them as desired. If you want to eliminate an entire step, click the **Delete This Step** link for that step.

**Note:** You cannot make any changes to the behavior of a workflow template if there are active requests using that template without cancelling those requests. An active request is any unexpired request that has not been approved, denied, or canceled by the user. If you do make an alteration, any requests are canceled and those affected are notified by email so they can resubmit their requests. Any user editing the template is notified when he or she tries to save changes on the canceled request.

### *Deleting Workflow Templates*

To delete a workflow template:

1. Access the Workflow Designer:

**WORKFLOW DESIGNER**

Workflow Name

Description

---

Step 1

**APPROVERS**

Barry	<a href="#">Remove</a>
-------	------------------------

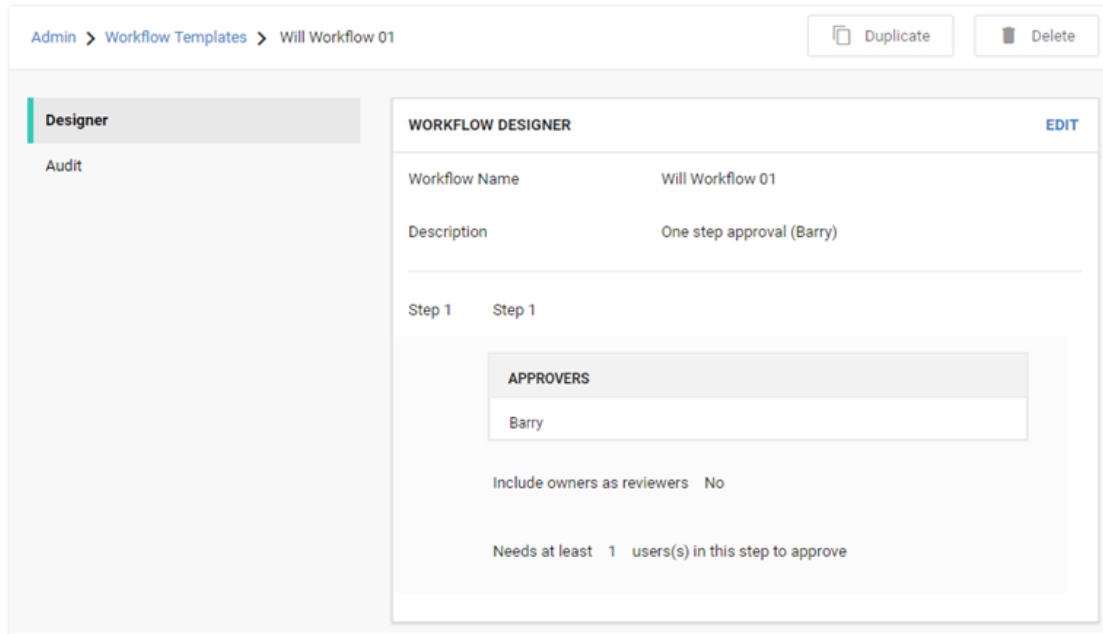
Add Groups / User

Include owners as reviewers

Needs at least  users(s) in this step to approve

[Delete this step](#)

2. Click the workflow template you want to copy in the **Workflow Templates** table. That template appears:



3. Click **Delete**. A confirmation popup page appears.
4. Click **Yes, Delete**.

**Note:** Because workflows based on the template may still be in play, the template is not completely deleted. Instead, it is inactivated. You can reactivate the template later. See [Accessing the Workflow Designer](#)."

### *Duplicating Workflow Templates*

If you must create a new workflow template that is like one you already have, you can save time by copying the similar template and then making the any changes:

1. Access the Workflow Templates page:

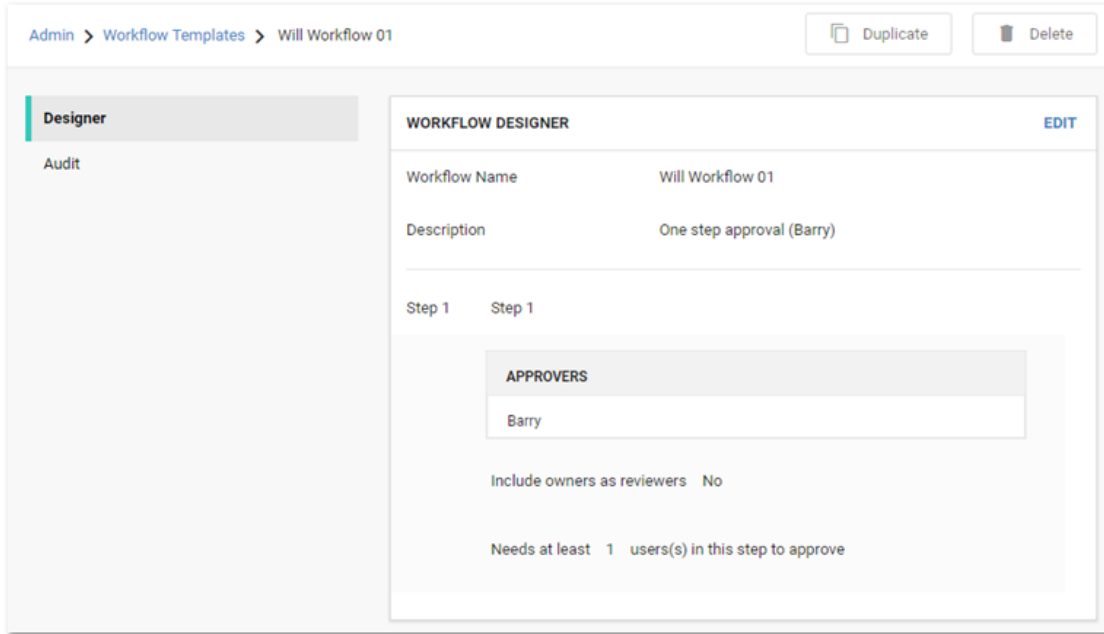
**Workflow Templates** Create Workflow Template

52 Items Show Inactive   
1 of 4 ◀ ▶

WORKFLOW TEMPLATE NAME ↓	TYPE	ACTIVE	⋮
workflow_test_01	Access Request	Yes	
workflow_Step	Access Request	Yes	
workflow_Policy	Access Request	Yes	
workflow_group	Access Request	Yes	
Workflow_Del	Access Request	Yes	
Workflow_01	Access Request	Yes	
Workflow Template 2 Step - Marrio - Barry	Access Request	Yes	
Workflow Template 1-Step Barry	Access Request	Yes	
WK01	Access Request	Yes	
Will Workflow 01	Access Request	Yes	
WFT_001	Access Request	Yes	
WF_template01	Access Request	Yes	
testWF	Access Request	Yes	

- Click the workflow template you want to copy in the **Workflow Templates** table. That template appears:





3. Click **Duplicate**. The new template appears, filled in the same as the original, including the name:

**WORKFLOW DESIGNER**

Workflow Name

Description

---

Step 1

**APPROVERS**

Barry	<a href="#">Remove</a>
-------	------------------------

Add Groups / User

Include owners as reviewers

Needs at least  users(s) in this step to approve

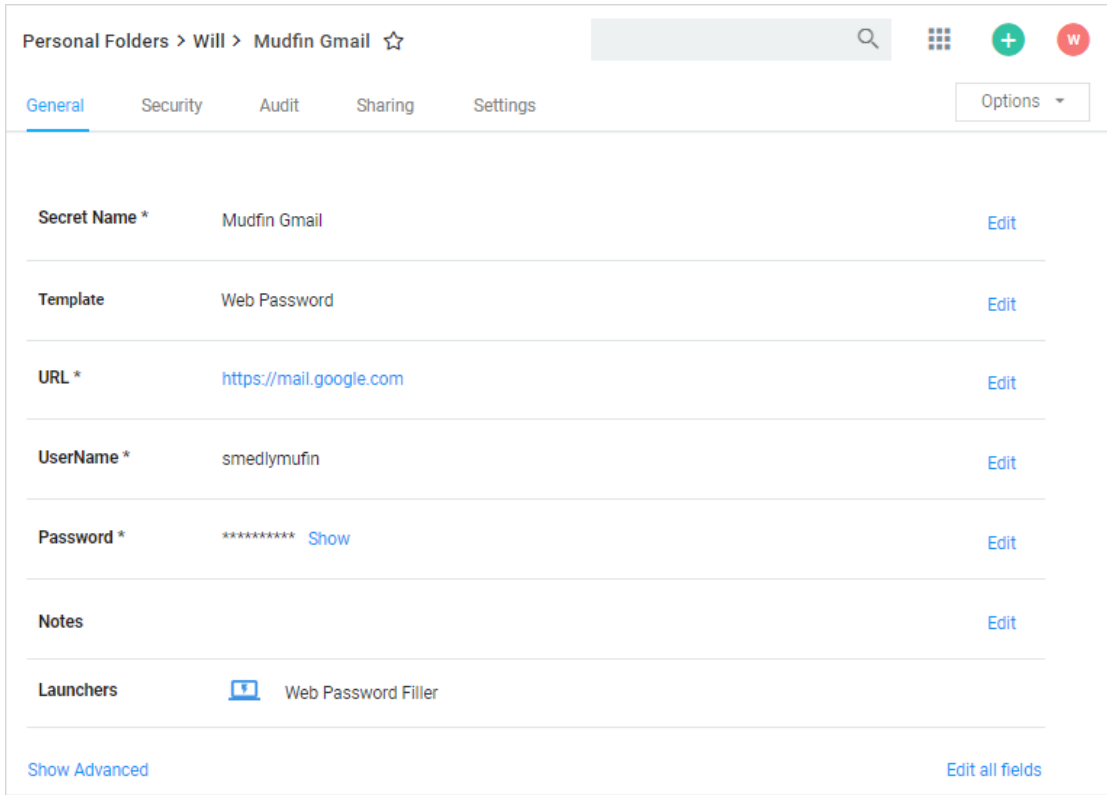
[Delete this step](#)

4. Change the name and edit as desired.

5. Click **Save** when finished.

#### *Assigning Workflows to Secrets*

1. Click the secret on the Dashboard. The secret's page appears:



2. Click the **Security** tab:

<b>CHECK OUT</b>		<a href="#">Edit</a>
Require Check Out	Require Check Out	No
<b>APPROVAL</b>		<a href="#">Edit</a>
Require Approval		No
<b>OTHER SECURITY</b>		<a href="#">Edit</a>
<b>Require Comment</b>	Users will be prompted for comment and ticket number when accessing a Secret.	No
Enable DoubleLock		Yes
Hide Launcher Password		No

3. Click the **Edit** link for the Approval section:

<b>CHECK OUT</b>		<a href="#">Edit</a>
Require Check Out	Require Check Out	No
<b>APPROVAL</b>		
Require Approval		No
		<input type="button" value="Cancel"/> <input type="button" value="Save"/>

4. Click the **Require Approval** list box and select **Standard including Editors...** The Approval section expands:

**APPROVAL**

**Require Approval** Standard including Editors (Owners and approvers do not need approval) ▼

**Approval Workflow** Create a basic (single level) workflow ▼

**APPROVERS**

No approvers have been added

Add Groups / Users

Search for groups or users 🔍

**Note:** By default, the secret is set to use regular non-stepped access approval.

- Click the **Click to Edit Approval Workflow** link. The Security tab of the secret appears:

Personal Folders > Will > Duckware Software ☆ Launch More ▼

General

**Security**

Audit

Remote Password Changing

Dependencies

Sharing

Settings

CHECK OUT	<a href="#">EDIT</a>
Require Check Out	No

APPROVAL	<a href="#">EDIT</a>
Require Approval	No

OTHER SECURITY	<a href="#">EDIT</a>
<b>Require Comment</b> <small>Users will be prompted for comment and ticket number when accessing a Secret.</small>	No
<b>Enable DoubleLock</b>	No
<b>Hide Launcher Password</b>	No

Note that Require Approval is set to No.

- Click **Edit**. The Approval section expands:

APPROVAL

Require Approval

7. Click the **Require Approval** list. The Approval section expands:

APPROVAL

Require Approval

Approval Workflow

**APPROVERS**

No approvers have been added

Add Groups / User

8. Click the **Approval Workflow** list and select the access-request workflow template you want to use.
9. Click **Save**.

#### *Assigning Workflows to Secret Policies*

1. Click **Admin > Secret Policy**. The Secret Policy page appears:

## Secret Policy

[Explain](#)

< 1 to 6 of 6 >

Secret Policy Name	Description	Active
<a href="#">Default</a>		Yes
<a href="#">policy</a>		Yes
<a href="#">policy_flow_1</a>		Yes
<a href="#">Policy_Workflow</a>		Yes
<a href="#">test</a>		Yes
<a href="#">Test Access Policy</a>		Yes

Show Inactive

← Back
+ Create New

2. For this instruction, we are going to create a new policy.
3. Click **+ Create New**. Another Secret Policy page appears:

**Secret Policy**

[Explain](#)

**Secret Policy Name**  \*

**Description**

**Active**

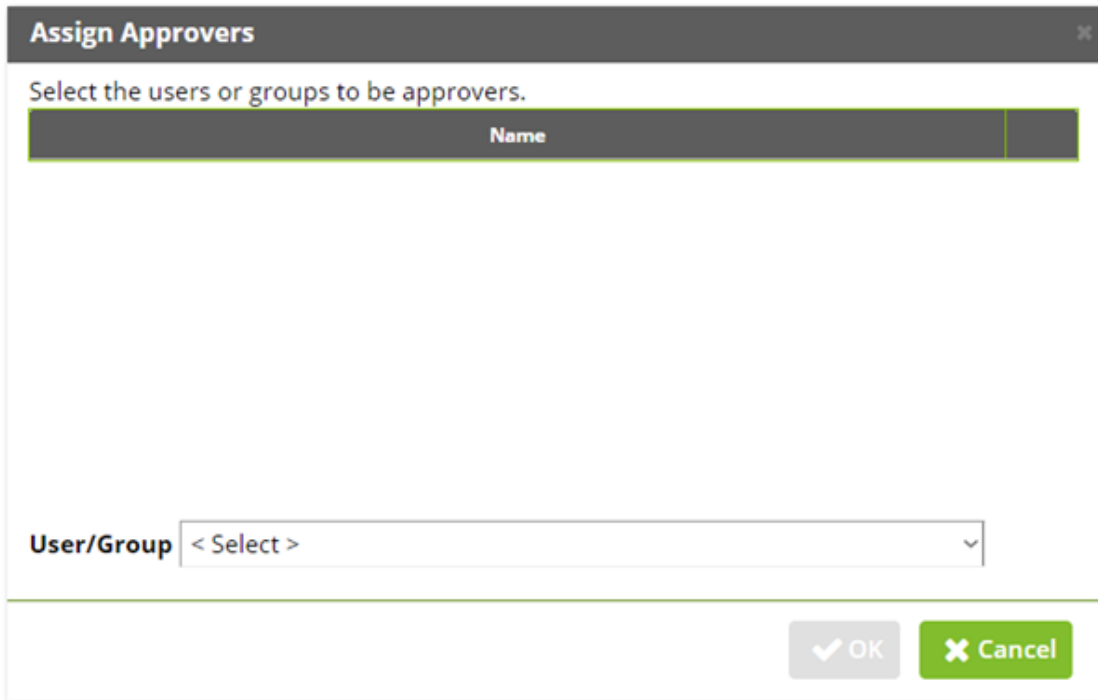
Section	Secret Policy Item Name	Setting	Value
General	Site		< Not Set > v

4. Type the new policy name in the **Secret Policy Name** text box.
5. Scroll down the page to the **Security Settings**:

Security Settings	Enable Requires Approval for Access	< Not Set > v
Security Settings	Request Access Approvers <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > v
Security Settings	Request Access Workflow <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > v
Security Settings	Editors also Require Approval <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > v
Security Settings	Owners and Approvers also Require Approval <i>(Dependent on: Enable Requires Approval for Access)</i>	< Not Set > v

6. Click the **Enable Requires Approval for Access** list and select **Enforced**.
7. Click to select the check box next to the list. The Assign Approvers popup page appears:





8. Click the **Cancel** button. The other access approval setting become enabled:

**Note:** You cannot set approvers and use a workflow at the same time. The intent of the next few instructions is avoid attempting to do so, which causes an error.



1. Click the **Request Access Approvers** list and select **Not Set**.
2. Click the **Request Access Workflow** list and select **Enforced**. A new list appears alongside.
3. Click the new unlabeled list and select the access template workflow to associate with the policy.

4. Click **Save** at the bottom of the page. The policy is now available for assignment to secrets and folders, just like any other policy.

## REMOTE PASSWORD CHANGING (RPC)

### Introduction

*Remote Password Changing* (RPC) allows properly configured secrets to automatically update a corresponding remote account. Secrets can be set for automatic expiry so Secret Server automatically generates a new strong password and change the remote password to keep all the account synchronized with Secret Server.

If Secret Server fails to change a remote password, an alert states there are secrets out of sync.

### Remote Accounts Supported

For the most up-to-date list of account types supported by RPC, see [List of Built-In Password Changers](#) (KB).

### Enabling RPC

RPC is enabled under the Administration, Remote Password Changing page. Click **Edit** to enable Remote Password Changing, Secret Heartbeat, and Secret Checkout. Once enabled, all secret templates with RPC configured are available to use RPC.

## Automatic RPC (AutoChange)

### Introduction

The Remote Password Changing tab contains the settings for configuring RPC on an individual secret. Enabling RPC *autochange* on a secret allows Secret Server to remotely change the password when it expires. The user must have Owner permission on the secret to enable autochange. When editing on the RPC tab, the Next Password text-entry field can be set or if left blank an auto-generated password is used.

**Note:** If the password change fails, Secret Server flags the secret as out of sync and continue to retry until it is successful. If the secret cannot be corrected or brought In sync, manually disabling autochange stops the secret from being retried.

### AutoChange Schedule

The AutoChange Schedule button is visible on the secret View RPC tab when RPC and autochange is enabled on a secret. The AutoChange Schedule page allows you to specify an interval, start date, start time, and time frame for when the password can be changed. This setting is useful for having the RPC occur during off-hours in order to prevent disruptions. By default, this setting is None, which allows the secret to be changed immediately. Note that

regardless of the autochange schedule, the password still has to expire before being automatically changed.

**Note:** While the password change is waiting for this next scheduled time, the RPC Log (visible by navigating to **Configuration > Remote Password Changing**) reports the secret could not be changed because of time schedule. The secret also remains expired until this autochange schedule is reached, even if the Secret was forced to expire.

## Privileged Accounts and Reset Secrets

By default, RPC uses the credentials on secret option, using the credentials stored in the secret to invoke a password change. For Windows and Active Directory accounts, a privileged account can be used instead by selecting the Privileged Account Credentials option and selecting an Active Directory secret with permission to change the account's password.

For secret templates with a custom commands password type, any number of associated reset secrets can assign for use in the custom commands. See [Custom Command Sets](#) (Professional or Premium Edition) for details on resetting secrets in custom commands.

When a secret is wired up with a privileged account or reset secrets, the ability to edit the username, host, domain, or machine is restricted if the user does not have access to those associated secrets. On the RPC tab, the user sees "You do not have access to View this secret" for the secret name and on the Edit page all text-entry fields mapped for RPC except the password is disabled. This added security prevents the user from changing the username and resetting another account's password.

**Note:** If the user does not have access to the privileged account or reset secrets, the ability to edit all secret text-entry fields mapped for RPC except the password text-entry field is restricted to prevent changing the password on another account.


## Run a Manual RPC

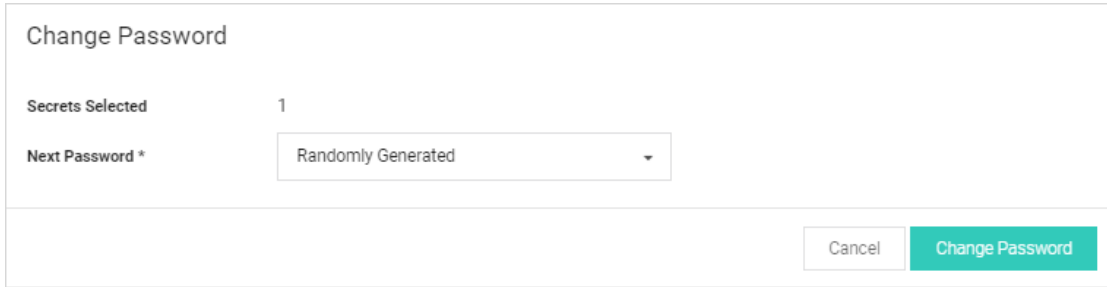
On the RPC tab there is a button called Change Password Remotely button that allows the use to change the password immediately instead of waiting for it to expire. When this button is clicked the user is taken to the Change Password Remotely page where they can enter in or generate the new password for the account. When the user clicks the Change button the secret enters the queue for having its password changed. The RPC Log found on the Remote Password Changing page details the results of the password change attempts and can be used for debugging.

If the secret is a Unix or Linux account and uses a password changer that supports SSH key rotation, the user can change the account's password, public and private keypair, and the private key passphrase. The user can enter or generate any of these items.

**Note:** If the password change fails, Secret Server continues to retry until it is successful, or the change is canceled by the user. To manually cancel the change, click Cancel Password Change on the RPC tab.

To run a manual RPC:

1. From **Dashboard**, click its check box to select secret you want to test.
2. Click the  Change Password Remotely button. The Change Password popup page appears:



The image shows a 'Change Password' popup form. At the top, it says 'Change Password'. Below that, there is a label 'Secrets Selected' followed by the number '1'. Underneath, there is a label 'Next Password \*' followed by a dropdown menu currently showing 'Randomly Generated'. At the bottom right of the form, there are two buttons: a 'Cancel' button and a teal 'Change Password' button.

3. Click to select the **Next Password** dropdown list and select **Manual** or **Randomly Generated**. If you chose manual:
  1. The Password text box appears.
  2. Type the new password in the **Password** text box.
  3. Click **Change Password**.

Otherwise, click the **Change Password**. The password change is now queued.

4. You can verify that the password change completed either by unmasking the password on this screen (click the lock icon beside the password field) or by looking at the **Remote Password Changing** log. You can find the Remote Password Changing log by going to **Admin > Remote Password Changing**.

## Mapping Account Fields for RPC

All the secret templates with the prefix RPC have RPC configured by default. For creating a custom template that uses RPC it can be configured from the Secret Template Designer. **Enable Remote Password Changing** must be turned on for secrets created from the template to make use of this feature. Select the password type for the account and map the text-entry fields to be used for authenticating to the remote server. The secret fields must be mapped to the corresponding required text-entry fields based on the password change type. Do that in the **Secret Template Edit Password Changing** page for the secret template:

**Secret Template Edit Password Changing**

**Enable Remote Password Changing**  
**Retry Interval**  
 Days   
 Hours   
 Minutes   
**Maximum Attempts**   
 **Enable Heartbeat**  
**Heartbeat Check Interval**  
 Days   
 Hours   
 Minutes

**Password Type to use**   
**Domain**  \*  
**Password**  \*  
**User Name**  \*  
**Default Privileged Account** [No Selected Secret](#)

The **Retry Interval** text box is the amount of time that a secret waits before once again attempting to change a password after a password change is unable to succeed.

The **Default Privileged Account** text box is the secret that is set as the privileged account for all new secrets that are created with this secret template. Changing this does not affect any existing secrets.

## RPC Ports

Table: Remote Password Changing Ports

Password Changer Type	Ports
Active Directory	389 or 636
Microsoft SQL Server	1433
Oracle	1521 or 1526
Sybase	5000
Unix SSH	22
Unix Telnet	23

Windows Kerberos	88 or 441
Windows NTLM	445

## RPC Logs

The RPC logs for a specific secret can be accessed by clicking the **View Audit** button on Secret View page and ticking the checkbox at the bottom of the page for display password changing Log. The RPC logs for all secrets can be accessed by navigating to **Administration > Remote Password Changing**.

## RPC Error Codes

The most common RPC errors are:

- **NERR\_PasswordPolicySettings:** The password Secret Server attempted to set is a repeating password or one that does not meet domain password policy standards. A common reason is minimum password age, which is often defaulted to 24 hours.
- **ERRORACCESSDENIED:** The user account's "Not Able to Change Password" setting could not be set or logon was denied.
- **ERRORINVALIDPASSWORD:** Either the user does not exist (ensure the usernames match) or the password is not correct.

For more information about common error messages for Remote Password Changing, see [Remote Password Changing Errors](#) (KB).

## RPC for Service Accounts and SSH Keys

### Service Accounts

RPC can be performed on service accounts where the dependent services is automatically updated and restarted as the service account password is changed. Administrators are notified if a dependency fails to restart. The supported dependency types are IIS application pools, IIS application pool recycle, scheduled tasks, windows services, passwords embedded in .ini, .config, and other text files. Custom dependencies can be created using SSH, PowerShell, or SQL scripts. The application pool recycle only recycles the specified application pool, it does not update the password of the service account running the application pool. Secret Server attempts to unlock the service account should the account become locked during the dependency password change if there is a privileged account assigned to the secret.

### SSH Keys

RPC can be performed on multiple public keys referencing the same private key in Secret Server. The dependency types for this situation are SSH key rotation and SSH key rotation privileged.

## Configuring Secret Dependencies for RPC

*Secret dependencies* are items that rely on the username, password, or SSH private key stored in the secret. By adding them to the Dependencies tab, they are automatically updated when the secret's password is changed, ensuring they are up to date with the account on which they depend.

Secret Dependency Templates Designer

[Explain](#)

**Create New Dependency Template** Filter by Dependency Type: All

DEPENDENCY TEMPLATE NAME	DEPENDENCY TYPE	ACTIVE	OPTIONS
Application Pool	Application Pool	Yes	
Application Pool Recycle	Application Pool Recycle	Yes	
COM+ Application	COM+ Application	Yes	
Remote File	Remote File (Regex Replace)	Yes	
Scheduled Task	Scheduled Task	Yes	
Windows Service	Windows Service	Yes	
SSH Key Rotation	SSH Script	Yes	
SSH Key Rotation Privileged	SSH Script	Yes	
ind	PowerShell Script	Yes	

Show Inactive

[Back](#) [Configure Dependency Changers](#)

Adding a custom dependency template may require additional settings (these settings are described in the following section):

### Dependency Settings and Information

Dependencies have the following settings:

**Note:** Not all dependency types have all these settings.

- **Change Fail Script:** For SSH key rotation and SSH key rotation privileged dependency types, this is the built-in script that determines if Secret Server was unable to update the public key on the dependency.
- **Change Script:** For SSH key rotation and SSH key rotation privileged dependency types, this is the built-in script that updates the public key on the dependency.




- **Change Success Script:** For SSH key rotation and SSH key rotation privileged dependency types, this is the built-in script that determines if Secret Server was able to update the public key on the dependency.
- **Database:** For SQL script dependency types, the database name for the script.
- **Dependency Group:** Name of the group to run the dependency update in.
- **Description:** Description of the dependency for documentation purposes.
- **Enabled:** Whether Secret Server attempts to update the dependency. A disabled dependency is ignored by Secret Server.
- **File Path:** For Remote File Dependency types, this is the UNC file path on the remote server where the embedded password exists.
- **Machine Name:** Computer name or IP address on which the dependency is located.
- **Name:** Name of the dependency on the remote machine.
- **Port:** For SQL and SSH script dependency types, the port name for the script.
- **Privileged Account:** The account Secret Server authenticates as when changing the dependency's credentials, so it must have privileges on the remote machine to edit the dependency.
- **Public Key:** For SSH key rotation and SSH key rotation privileged dependency types, this text-entry field holds the value of the public key stored on the dependency.
- **Regex:** For Remote File Dependency types, the regular expression used to locate the password embedded in the configuration file.
- **Restart:** Determines if the dependency is restarted once the account has been updated.
- **Run Condition:** Allows the dependency to run conditionally depending on the outcome of the dependencies above it.
- **Script:** Name of the PowerShell script, SSH script, or SQL script in the scripts repository configured on the Dependency Template. The actual script selected can be previewed by clicking the eye icon.
- **Server Key Digest:** For SSH key rotation and SSH key rotation privileged dependency types, a text-entry field that serves as a security control for specifying the SHA1 hash of the SSH host key on the remote server.
- **Server Name:** For SQL script dependency types, the server name for the script.
- **SSH Key Secret:** An account with SSH Key that Secret Server uses to authenticate when executing the SSH Script or SSH Key rotation dependency types.



- **Template:** Whether the dependency is an IIS application pool, Scheduled Task, windows service, remote file, COM+ application. Custom dependencies can also be created using a SQL, SSH, or PowerShell script.
- **Verification Script:** For SSH key rotation and SSH key rotation privileged dependency types, this is the built-in script that verifies that the new public key on the dependency matches the private key on the secret.
- **Wait(s):** Time in seconds that Secret Server pauses before changing the dependency.

Example values for a Windows service dependency on a remote computer might be: 192.11.158.99, Windows Service, aspnet\_state, or DOMAIN\admin.

The following operations can be performed in the Dependency grid:

- **Delete:** Click the  icon to delete the dependency.
- **Edit:** Click the  icon to edit dependency text boxes. Cancel changes by pressing the Cancel button.
- **Run Dependency:** Click the second arrow icon to run the script on the selected dependency and set the password on the selected dependency to the current password for the secret
- **Test Connection:** Click the return arrow icon to test the dependency connection, the tests results are displayed afterward.
- **View Dependency History:** Click the  icon to view the activity logs for the dependency.

**Note:** Due to security constraints, scheduled tasks require an Active Directory domain user as the privileged account.

## Manually Adding Dependencies

To manually add a dependency:

1. Click on the plus icon next to **Create New Dependency** on the **Dependencies** tab.
2. Choose your dependency type from the **Template** list.
3. Fill in the dependency name, machine name, and other information depending on the dependency type.
4. To choose the account used to change the dependency password, click on the link next to the **Privileged Account** label. If the privileged account is blank, the current secret's credentials are used.
5. Click the **OK** button to finish adding the dependency.

## Creating Custom Dependencies

If there are different dependency types that you want to manage that are not supported out of the box, new ones can be created based on a script. A custom dependency consists of two components:

- **Dependency Template:** The dependency template defines how a dependency is matched to discovered accounts and how it updates the target after a password change occurs on the account. To create a new dependency template, go to **Admin > Secret Templates** and click the **Dependency Templates** button.
- **Dependency Changer:** A dependency changer is a script and the associated parameters to be passed into the script. Dependency changers can be created and modified by going to **Admin > Remote Password Changing > Configure Dependency Changers**.

**Note:** Please see the [Secret Server Account Discovery Guide](#) for a comprehensive guide to configuring and using dependency changers and dependency templates.

## Dependency Groups

By default, all dependencies are updated in the order listed. There are cases where you may want to split out different sets of dependencies into separate groups. Typically, this is because a single service account may run services across different segregated networks that can communicate with the domain but not each other and have different distributed engine sites assigned. In this case you can create two dependency groups and assign them to different distributed engine sites to solve connectivity issues.

## Custom Password Changers

The Password Changers Configuration page can be accessed by navigating to **Admin > Remote Password Changing > Configure Password Changers**.

There are a few password changing types that allow the user to enter in specific commands that are sent to the computer where the password is changing. This enables the system to accommodate for differences in the standard password change procedure. For example: The Unix system that is being changed prompts for the current password twice instead of only once before asking for the new password.

## Modifying Password Changers

To modify a password changer, click the password changer name under **Admin > Remote Password Changing > Configure Password Changers** and then use the **Edit** or **Edit Commands** buttons to make changes. For more information about editing the custom PowerShell password changer, see [PowerShell Remote Password Changing \(KB\)](#).

**Note:** You can find the full, up-to-date list of password changers included with Secret Server by default in [List of Built-In Password Changers \(KB\)](#).

## Deactivating Password Changers

To make a password changer unavailable for use and to hide it from view in your list of password changers, you must mark it inactive:

1. From the **Password Changers Configuration** page, click the password type name of the password changer you would like to make inactive.
2. Click **Edit**.
3. Uncheck the **Active** box.
4. Click **Save**.

To view inactive password changers, check the **Show Inactive** box at the bottom of the list of password changers. The Active column in the table indicates the status of the password changer.

## Changing Ports and Line Endings

To change the port or line ending used on a password changer, click the password changer on the **Configure Password Changers** page and then click **Edit**. There, you can choose the line ending and port used by the device. By default, line endings are set to New Line (\n), however some devices and applications (such as HP iLO) use a different line ending system. The port defaults to 22 for SSH connections and 23 for Telnet connections.

For the built in Windows password changer there is a ports text-entry field available that can be filled in to help ensure a computer is listening. This can be used if DNS returns multiple IP addresses for a single box and only one is valid. For example, a laptop might get two IP addresses for an Ethernet and wireless connection, but if it is unplugged the Ethernet IP is invalid. In this case, Secret Server can do a reverse lookup and test each IP until it is able to connect on one of the specified ports. When it gets a response, it uses that IP for the password change.

## Editing Custom Commands

The SSH type changers use the SSH protocol to access the machine. This type contains custom commands for the password reset functionality and can contain commands for the verify password functionality but most SSH type changers simply verify that a connection can be established with the username and password. The Telnet type changers use the Telnet protocol in order to access the machine and contain custom commands for both the password reset and the verify password functionality. The verify functionality is used in the heartbeat, as well as verifying that the password was changed successfully.

SSH key rotation type changers also include post-reset success and failure custom commands. These extra command sets are run after both the reset and verify functions are run and are used to either finalize the key rotation and password change (success) or clean up after a failure. If both the reset and verify functions are successful, the post-reset success command set is run. If either the reset or the verify fail, the post-reset failure command set is run.

To edit the custom commands, click on the **Edit** Commands button. This sets the command grids into Edit mode where you can add, update, or delete the commands in order to suit their purpose.

Any secret text-entry field value can be substituted by prefacing the text-entry field name with a \$. For example, in order to echo the notes value for a secret, the user would enter: echo \$Notes as a command. Along with these secret field values, the following variables are available in custom commands:

#### *RPC-Mapped Text-Entry Fields*

- \$USERNAME The username text-entry field mapped in RPC on the secret template.
- \$CURRENTPASSWORD The password text-entry field mapped in RPC on the secret template.
- \$NEWPASSWORD The next password (filled in Next Password textbox or auto-generated).
- PRIVATEKEY The private key text-entry field mapped in RPC on the secret template.
- \$NEWPRIVATEKEY The next private key (filled in Next Private Key text box or auto-generated).
- \$CURRENTPUBLICKEY The public key text-entry field mapped in RPC on the secret template.
- \$NEWPUBLICKEY The next public key (generated from the next private key).
- \$PASSPHRASE The passphrase text-entry field mapped in RPC on the secret template.
- \$NEWPASSPHRASE The next passphrase (filled in Next Private Key Passphrase text box or auto-generated).

#### *Associated Reset Secrets*

- \$[1] Adding this prefix to any text-entry field targets the associated reset secret with order 1.
- \$[1]\$USERNAME The mapped username of the associated secret, identified by order. Can also reference any other property on the associated secret. Common examples include:
- \$[1]\$PASSWORD
- \$[1]\$CURRENTPASSWORD
- \$[1]\$PRIVATE KEY
- \$[1]\$PRIVATE KEY PASSPHRASE
- \$[SID:105] Adding this prefix to any text-entry field targets the associated reset secret with a secret Id of 105.

- `#[SID:105]$USERNAME` The mapped username of the associated secret, identified by secret id. Like referencing an associated secret by order, referencing by secret id can also access any text-entry field on the secret by name.

**Note:** Both the mapped text-entry fields and secret text-entry field names can be used.

#### *Check-Result Commands*

- `$$CHECKCONTAINS <text>` Checks that the response from last command contains `<text>`.
- `$$CHECKFOR <text>` Checks that the response from the last command equals `<text>`.
- `$$CHECKNOTCONTAINS <text>` Checks that the response from last command does not contain `<text>`.

**Note:** If these conditions are not met the process fails and immediately returns a result.

If you want to exit out of the command set early without triggering a failure, echo an "OK" on the line immediately preceding the `exit 0;` statement. "OK" must be the only text in the response from the server for this to work.

You can test out your password reset and verify password command sets by clicking on the **Test Action** buttons next to the relevant sections. All communication between Secret Server and the target machine is displayed when using these test buttons.

### **Mapping an SSH Key or Private Key Passphrase for Authentication**

Some password changers may be customized to use SSH key authentication. Secret Server needs to know which text-entry fields contain the key and the passphrase. These text-entry fields can be specified after clicking **Edit** from the password changer page.

## Unix Account Custom (SSH)

### Verify Password Changed Commands

 Test Action

#### AUTHENTICATE AS

Username \$USERNAME  
Password \$CURRENTPASSWORD  
Key < None >  
Passphrase < None >

ORDER	COMMAND	COMMENT	PAUSE(MS)
-------	---------	---------	-----------

### Password Change Commands

 Test Action

#### AUTHENTICATE AS


Username \$USERNAME  
Password \$CURRENTPASSWORD  
Key < None >  
Passphrase < None >

ORDER	COMMAND	COMMENT	PAUSE(MS)
1	passwd	Password Command	2000
2	\$CURRENTPASSWORD	Current Password	2000
3	\$NEWPASSWORD	New Password	2000
4	\$NEWPASSWORD	Confirmed Password	2000


[Advanced Post Change Commands](#)  
[Advanced Settings](#)

 Back

 Edit

 Edit Commands

 Configure Scan Template

 View Audit

The key and passphrase must be identified by a \$ sign and the secret text-entry field name, which can be obtained from the secret template.

To set which text-entry fields are your key and passphrase, go to the extended mappings for a secret template by clicking **Extended Mappings** from the **Secret Template Edit** page. Select the text-entry fields that correspond to the SSH private key and passphrase if applicable. No matter what you name your key text-entry field, Secret Server knows what it is. This is set up by default, so you should not must do this unless you've created custom Unix templates you want to use keys with.

Once Secret Server knows which text-entry fields contain the private key and private key passphrases, it can automatically use them as a part of launchers.

### Creating a Custom Password Changer

1. From the **Password Changers Configuration** page, click **New**.
2. Select a base password changer. We recommend you select the option that most closely matches the type of password changer you are creating, as this determines which customizable parameters and test actions are be available to you.
3. On the next page, make any customizations you would like. To save a new command, click the **+** icon at the end of the row. The command can be edited once more by clicking **Edit**, which is labeled with a small pencil icon at the end of the row.
4. To access the test actions for your new password changer, click **Back** to return to the overview screen.
5. To edit additional parameters (if applicable), click **Edit** from the password changer overview to change settings such as the name, line ending, and custom port.

**Note:** For more information about creating a custom PowerShell password changer, see [PowerShell Remote Password Changing \(KB\)](#).

## Distributed Engines and RPC

Distributed Engines allow RPC, heartbeat and discovery to occur on networks that are not directly connected to the network that Secret Server is installed on. See the linked KB and its associated white paper for details on configuration and functionality.

**Note:** Distributed Engines were released in version 8.9.000000 and replaced remote agents.

## Password Changing Scripts

PowerShell scripts, SSH scripts, and SQL scripts for password changing, dependencies, and discovery custom actions can be created by administrators with the role permission called Administer Scripts. The scripts can be accessed by going to **Administration > Remote Password Changing > Scripts**.

**Note:** Secret Server requires that WinRM is configured on the Web server. For instructions please see [Configuring WinRM for PowerShell](#).

## Creating Scripts

On the **Scripts** screen, select desired script tab and click **Create New** to enter the name of the script, a description, and the commands to run, then click **OK**. The script now shows up in the grid. Scripts can be deactivated and reactivated from the grid.

## Testing Scripts

All scripts run from the machine that Secret Server is installed on, or the site assigned to the secret. To test a script, click the **Test** button on the grid next to the corresponding script.

PowerShell scripts run as the identity of the secret, so enter in an Active Directory credential to run the script as or select a secret to pre-fill the run-as credentials. Then enter in any command line arguments that the script requires. The output of the script is displayed above the grid for debugging purposes. To test the script over an engine, select a site from the **Site** list. This helps in diagnosing server specific issues where engines are installed.

## Using Scripts

To use a script as a password changer or Dependency, it must be wired up to the appropriate action under **Admin > Remote Password Changing** on the password changer or dependency changer.

Discovery scripting is done under **Admin > Discovery > Extensible Discovery**. For more information on configuring extensible discovery see the [Extensible Discovery Overview](#).

## Viewing Audits

A full history of each PowerShell script is kept and can be downloaded from the audit trail. Click **View Audit** to view the audit trail for PowerShell. Each time a script is updated, the previous one can be downloaded from the corresponding audit record.

**Note:** For additional information on setting up PowerShell scripts, please read the following KB article: [Creating and Using PowerShell Scripts](#).

# HEARTBEATS: AUTOMATICALLY TESTING SECRET CREDENTIALS

## Introduction

The Secret Server *heartbeat* feature allows secrets to have their entered credentials automatically tested for accuracy at a given interval. Using heartbeat on secrets ensures those credentials are up-to-date and can alert administrators if the credentials are changed outside of Secret Server. Heartbeat helps manage secrets and prevent them from being out of sync.

## Remote Accounts Supported

For the most up-to-date list of account types supported by RPC, see [this KB article](#).



## Enabling Heartbeat in RPC

To enable heartbeat, ensure it is enabled on the **Remote Password Changing Configuration** page:

1. Navigate to **Admin > Remote Password Changing**.
2. Click **Edit**.
3. Click to select the **Enable Heartbeat** check box.
4. Click **Save**.

**Note:** Heartbeat must also be enabled on the secret template by setting the **Enable Remote Password Changing Heartbeat** setting.

## Configuring Heartbeat

Heartbeat is configured from the secret template designer. The heartbeat interval determines how often the secret credentials are tested.

## Running Heartbeat for a Secret

Heartbeat runs in a background thread to check each secret where it is enabled. If the credential test fails, the secret is flagged as heartbeat failed and out of sync. To avoid locking out the account, heartbeat no longer runs on that secret until the secret items are edited by the user. If the machine is determined to be unavailable, the secret is flagged as heartbeat unable to connect and the secret continues to be checked on the heartbeat interval.

To manually use heartbeat to check the credentials, the **Secret View** page has a **Heartbeat Now** button. The button marks the password as heartbeat pending. The background thread processes the secret in the next 10 seconds, and when the page is refreshed the heartbeat status is updated.

**Note:** Heartbeat does not work on Windows accounts on the server that is running Secret Server. These accounts are flagged with an "Incompatible Host" status.

To run heartbeat for a secret:

1. From **Dashboard**, click the secret you would like to test.
2. Click the **View** button. The **Last Heartbeat** field of the secret shows the last date and time that Heartbeat ran for this secret.
3. To run Heartbeat once more, click **Run Heartbeat** at the bottom of the Secret.
4. Monitor the **Last Heartbeat** field to see the updated status. This may take a few seconds to complete.

If you receive any Heartbeat status code aside from Success, you can check the Heartbeat log for details. To view the entry, Go to **Admin > Remote Password Changing** and then search for the secret name in the **Search** field of the **Heartbeat Log**.

## Heartbeat Logs

The heartbeat logs for a specific secret can be accessed by clicking the **View Audit** button on the **Secret View** page and clicking to enable the **Display Password Changing Log** check box. The heartbeat logs for all secrets can be accessed by navigating to **Administration > Remote Password Changing** and scrolling down to the second set of logs.

## Heartbeat Status Codes

- **Success:** The credentials in the secret authenticated successfully with the target system.
- **Failed:** The credentials in the secret failed authentication with the target system.
- **UnableToConnect:** Secret Server was unable to contact the target system. Ensure that the domain, IP address, or hostname is correct and resolvable from the server that Secret Server is installed on.
- **IncompatibleHost:** The most common reason for this code is an attempt to verify an account on the same server that Secret Server is installed on. If this is not the case, ensure that the domain, IP address, or hostname is correct and resolvable from the server that Secret Server is installed on.
- **UnknownError:** Check the Heartbeat log on the Remote Password Changing page for details, and contact [Support](#) for assistance.

## Alerts on Heartbeat Failure

On the **Preferences** page, the **Send Email Alerts when Heartbeat Fails for Secrets** setting can be enabled to email the user when heartbeat fails for any secret the user has view access to.

## AUTOMATIC SECRET DISCOVERY

### Introduction

Secret Server has a discovery feature that can automatically find local Windows accounts, Active Directory service, Unix, VMware ESX/ESXi, and Active Directory domain accounts. Account and dependency types not supported out-of-the-box in Secret Server can still be discovered by writing PowerShell scripts that can be run as custom scanners. This allows administrators to quickly import accounts found by Secret Server on specified domains or IP addresses.

**Note:** Please see the [Discovery Guide](#) for a comprehensive guide to configuring and using discovery.

To run discovery on a domain, IP address range, or a custom source, you must first enable the discovery feature for Secret Server. Second, you must enable discovery for each discovery source you would like to be scanned. For Active Directory sources, this also involves selecting either the entire domain or specific OU's to be scanned.



## Enabling Discovery for Secret Server

1. On the **Administration** menu click **Discovery**, and then click **Edit**.
2. Select the **Enable Discovery** check box.
3. Fill in the **Synchronization Interval for Discovery** text-entry fields for days, hours, or minutes. This determines how often Discovery runs.
4. Click **Save**.

## Enabling Discovery for an Active Directory Domain

1. On the **Administration** menu click **Active Directory**, and then click **Edit Domains**.
2. Click the domain value for the domain you would like to configure.
3. From the **Enable Discovery** dropdown menu, select **Entire Domain**.
4. Click **Save and Validate**.

## Enabling Discovery for Specific Organization Units of a Domain

1. On the **Administration** menu click **Discovery**, and then click **Edit Domains**.
2. Click the **Domain** you would like to configure.
3. From the **Enable Discovery** dropdown menu, select **Specific OUs**.
4. Click Save And Validate.
5. If you are not already redirected there, click the **Specific OUs** tab.
6. Type an OU name in the **Include** box to add an OU to the list. If the OU is found, it auto-populates below the box. Click the name to add it to the list. An included OU appears with an  icon.
7. Type an OU name in the **Exclude** box to exclude it from Discovery. An OU is only available for exclusion if it is contained within an OU that has already been included. An excluded OU appears with an  icon.
8. To remove an OU from the list, click the to the right of the OU.
9. To set a specific site or secret to scan the computers in that OU with use the icon to the right of the OU.

10. Click **Save**.

**Note:** The ports required for Discovery are documented in [Secret Server Ports](#).

## AWS Account Discovery

**Note:** Discovery must be enabled in Secret Server to discover AWS accounts.

Secret Server can scan Amazon Web Services (AWS) for accounts that can access the cloud resource. Two types of secrets can be discovered and managed through Secret Server:

- AWS Access Key: Keys used for programmatic integration with AWS.
- AWS Console Account: User login accounts for AWS.

### Enabling AWS Discovery

1. For Secret Server to communicate with AWS, users with sufficient privileges must create an access key for their account in AWS Identity and Access Management (IAM). The account used to do this requires the following permissions to discover users and access keys:

- `iam:ListUsers`
- `iam:GetLoginProfile`
- `iam:ListAccessKeys`

**Note:** These permissions are limited to the resources the user is allowed to access.

2. Once this access key is created, use the access key and secret key to create a secret in Secret Server using the Amazon IAM key template.
3. Create a new AWS discovery source and use the Amazon IAM key as the credentials secret for the discovery source.

**Note:** AWS only allows programmatic integration through access keys. This type of secret is required for discovery to work. Discovery must be enabled in Secret Server for this feature to work.

## Password Management in AWS

Secret Server can manage password and access keys for AWS IAM accounts.

### Amazon IAM Keys

Password changing, privileged password changing, and running heartbeats are available for Amazon IAM key secrets. When an Amazon IAM key has its password changed through Secret Server, the new secret key is generated automatically and is not set by user input.

During password changing, you can disable or remove old keys through settings available in the advanced configuration:

- `<add key="ShouldDeletePreviousKey" value="true" />`
- `<add key="ShouldInactivatePreviousKey" value="true" />`

### *Amazon IAM Console Password*

Password changing, and privileged password changing are available for Amazon IAM console password secrets. Due to AWS IAM's restrictions on programmatic integration, this secret type cannot use Secret Server heart beat.

In addition, an Amazon IAM key secret must be associated with an Amazon IAM console password secret for password changing to occur. To associate the two:

1. Create the Amazon IAM console password secret, and an Amazon IAM Key secret for an account that has the permissions to change the console user's password. This can be the console account's own access keys, if the user has permission.
2. Navigate to the RPC tab of the Amazon IAM Console Password.
3. Under **Change Password Using Privileged Account** select **Edit**, and choose the IAM key secret created in the previous step. RPC should now be possible on the console password secret.

### *Permissions Required for Secret Key Changes*

**Note:** These permissions are at the most granular level. You can implement broader methods through wildcard resource restrictions, permission policies, or groups.

Privileged Permissions: (those the AWS account needs to change another users' access keys):

- `iam:DeleteAccessKey` on resource `arn:aws:iam::<account>:user/<otherUserName>`
- `iam:UpdateAccessKey` on resource `arn:aws:iam::<account>:user/<otherUserName>`
- `iam:CreateAccessKey` on resource `arn:aws:iam::<account>:user/<otherUserName>`
- `iam:ListAccessKeys` on resource `arn:aws:iam::<account>:user/<otherUserName>`

Basic Permissions (those the AWS account needs to change its own access keys):

- `iam:DeleteAccessKey` on resource `arn:aws:iam::<account>:user/${aws:username}`
- `iam:UpdateAccessKey` on resource `arn:aws:iam::<account>:user/${aws:username}`
- `iam:CreateAccessKey` on resource `arn:aws:iam::<account>:user/${aws:username}`
- `iam:ListAccessKeys` on resource `arn:aws:iam::<account>:user/${aws:username}`

### *Permissions Required for Changing the Amazon IAM Console Password*

**Note:** These permissions are at the most granular level. You can implement broader methods through wildcard resource restrictions, permission policies, or groups.

The permissions are:

- Privileged Permission: `iam:UpdateLoginProfile` on resource `arn:aws:iam::<account>:user/<otherUserName>`
- Basic Permission: `iam:ChangePassword` on resource `arn:aws:iam::<account>:user/${aws:username}`

## SESSION RECORDING

### Overview

#### Basic Session Recording

Basic Session Recording is a licensed feature in Secret Server. It relies on the protocol handler configured on client machines through Secret Server's launcher. Using the launcher, Secret Server captures second-by-second screenshots on the client machine during a user's recorded session. These images of the user's screen are compiled into a video that can be downloaded and played back for auditing and security purposes. Activity recorded in the session is based on screen changes only.

Session monitoring allows administrators with the Session Monitoring permission to view all active launched sessions within Secret Server. If session recording is enabled on the secret, an administrator can watch the user's session in real time.

Admins can search through active and ended sessions. To review and search through sessions go to **Admin > Session Monitoring**.

Searching across sessions can search the following data. To select what data is searched across check the options on the search filters on the left-hand side.

Session Playback Search

**Search Filters**

Search for Sessions

**Search Across**

Secret Name

Secret Items

Username

Proxy Session Client Data

RDP Keystroke Data

**Date**

Last 30 Days

**Status**

All

**Launcher Type**

All

**Users**

**Groups**

**Secrets**

**Folder**

< All Folders >

10.0.0.243\winuser2 - Accessed By ssadmin Remote Desktop    · 4/11/2017 05:46 PM · 0:10:03 win-h0ko2iq58no · ssadmin <a href="#">View Secret</a>	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop    · 4/11/2017 05:41 PM · 0:00:59 win-h0ko2iq58no · user282 <a href="#">View Secret</a>	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop    · 4/11/2017 05:35 PM · 0:01:44 win-h0ko2iq58no · user282 <a href="#">View Secret</a>	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop  · 4/11/2017 05:35 PM · 0:00:11 win-h0ko2iq58no <a href="#">View Secret</a>	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop  · 4/11/2017 05:33 PM · 0:00:00 win-h0ko2iq58no <a href="#">View Secret</a>	
10.0.0.243\winuser1 - Accessed By user282 Remote Desktop    · 4/11/2017 05:19 PM · 0:00:32 win-h0ko2iq58no · user282	

Some search filters require additional components to be installed or configured:

- **Proxy Session Client Data:** Search within keystroke data of proxied SSH sessions. Requires that the SSH proxy is enabled and SSH sessions are using it.
- **RDP Keystroke Data:** Requires the RDP Session Monitoring Agent be installed on the target.
- **RDP Application Name:** Requires the additional RDP Session Monitoring Agent be installed on the target.

To view a recording, click the camera icon on the session. The Watch Session Recording page appears:

**Watch Session Recording**

Session Summary

Session Secret: 10.0.0.243\winuser2      Session User: Andrew Smithson      Session Start: 3/30/2017 11:10 PM  
Machine: win-h0ko2iq58no      Launcher Used: Remote Desktop      Session End: 3/30/2017 11:10 PM

Search Session Activity

Activity Type: All      Keyword:

Elapsed	Type	Activity	Jump To
00:00:00	explorer		○
00:00:00	rdpinput		○
00:00:00	TSTheme		○
00:00:00	rdpclip		○
00:00:00	Thycotic.SessionRecorder		○
00:00:00	taskhostx		○
00:00:00	explorer		○
00:00:04	TSTheme		○
00:00:04	powershell		○
00:00:04	conhost		○
00:00:04	powershell		○
00:00:06	hello		○
00:00:08	echo		○

If there is logged session activity, such as keystroke or application data from the RDP agent or SSH proxy then you can search through session activity and jump to points within the video playback. The playback also displays an activity map to show points of high activity, such as screen changes, keystrokes, and processes started and stopped.

Selecting an activity in the grid also shows additional details below such as the full folder path where the application started and the user that performed the operation.

**Note:** SSH Keystroke data is shown in one-minute segments. In a short session of less than minute, the "jump to" only goes to the beginning of the video.

For active sessions, there are two actions that can be taken:

- **Watch Live:** When session recording is turned on for the secret and admin can view and replay the user's activity.
- **Terminate:** Sends a message to the end user or terminates their session. The end user sees an alert dialog pop up on their machine with the message. Session recording does not must be enabled for this to work. For ended sessions admins can watch the recorded video and view the SSH log if session recording was turned on for the secret.

## Advanced Session Recording

Advanced Session Recording (ASR) is a licensed feature of Secret Server that adds capabilities to those offered by basic session recording. You install the Advanced Session Recording Agent (ASRA), which uses the Remote Desktop Protocol, on any client machine where you want more information from the sessions recorded.

**Note:** ASR is not available to those using our Mac launcher.



ASR enhances the launcher sessions, which typically only include screenshots, keystrokes, and process activity. ASR features include:

- **Screen Capture:** The Secret Server launcher records second-by-second screen images compiled into a playback video of the user's session. This is essentially the same as basic session recording.
- **Logged Processes:** The ASRA logs all processes started and stopped during a user's session.
- **Recorded Key Strokes:** The ASRA records all user keystrokes during the session.
- In addition to those, ASR includes these enhanced video playback features:
- **Searchable Video:** You can search video activity to find locations where specific activities, such as specific keystrokes or ran processes.
- **Enhanced Playback:** Sessions recorded using ASR display additional data on playback, such as the current active window, the used processes, and keystrokes in the session.

## Improvements for Secret Server 10.6 SP2

**Note:** See [Secret Server Advanced Session-Recording Agent Installation](#) for details.

As of Secret Server 10.6.24, several performance enhancements were added to session recording that fundamentally change how it functions:

- On-demand video processing
- Recording all sessions
- Inactivity timeout
- Maximum session length protection

The Windows protocol handler now encodes your session in WEBM format in real time and sends the recording to Secret Server. There is now an “Enable On-Demand Video Processing” option in Secret Server 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.

**Note:** The Mac protocol handler does not yet support this feature, so any recordings created with it are converted to the chosen legacy video codec format. We recommend H.264/MP4. You can set the advanced session recording agent to “Record All Sessions.” If someone logs into a server directly without launching from Secret Server, or even logs in at the console, the full session is recorded, including metadata.

## Metadata Recording

By default, session recording creates videos of the launched session. Secret Server supports logging additional metadata, such as keystrokes for RDP and SSH sessions. When these options are enabled, users can search for keystrokes or applications across sessions, and the session playback interface shows additional activity information. Remote Desktop session metadata requires Secret Server 10.6 and the advanced session recording feature, which in turn requires an installation of an advanced session recording agent (ASRA) on the target servers. See <https://thycotic.force.com/support/s/article/Secret-Server-INST-EXT-Adv-Session-Rec-Agent>. SSH keystroke data relies on the Secret Server SSH Proxy. This can be enabled under Admin > SSH Proxy. See the SSH Proxy configuration KB article for more information. Once proxying is enabled recorded SSH sessions will log SSH traffic which can be searched and is displayed in the session playback interface.

## Record All Sessions

As of Secret Server SP2, you can configure the ASRA to record all sessions. This causes it to record video and metadata for anyone logging into the server, even when not using Secret Server, including logging into the console. Since these recordings are not tied to any specific secret, you must go to the **Admin > Session Monitoring** page to view them.

## Enable On-Demand Video Processing

As described above, this feature was added in Secret Server 10.6.24 to greatly improve session recording performance.

The Windows protocol handler now encodes the recording on the fly in WEBM format and streams the video to Secret Server. Once the session has ended, Secret Server reconstructs the video and leaves it in WEBM format, which Chrome and Firefox can natively play back.

Internet Explorer and Edge currently have issues playing back WEBM videos, so if you are using those browsers and try to view an on-demand recording, you are presented with a “Request Video Processing” button, which converts the video to H.264/MP4, as soon as possible, which IE or Edge can then play back.

If this option is not checked, all sessions recorded by the Windows protocol handler are converted to H.264/MP4 automatically. If you have many IE or Edge users, Thycotic recommends leaving this option unchecked, but this will increase the processing time of videos and increase the load on your Secret Server servers that have the Session Recording role enabled.

This setting has no effect on sessions recorded with the Mac protocol handler, which is always encoded using your legacy video codec choice.

## Enable Inactivity Timeout

If enabled, if a session appears idle, users are given a five-minute warning that they will be disconnected. A prompt appears that lets them choose to disconnect immediately or to continue the session. If no response is received, the session is disconnected five minutes later.

**Note:** This feature was added in Secret Server SP2 and is currently only supported in the Windows protocol handler (not Mac).

## Session Recording Requirements

### Basic Session Recording

**Note:** See below for additional details.

**Table: Basic Session Recording Requirements**

Web Server (Secret Server)	Database Server (SQL Server)
8 CPU Cores	8 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

### Advanced Session Recording

**Note:** This applies to ASRA and Secret Server. See below for additional details.

**Table: Advanced Session Recording Requirements**

Web Server (Secret Server)	Database Server (SQL Server)	ASRA (Client Machines)
8 CPU Cores	8 CPU Cores	2 CPU Cores
32 GB RAM	32 GB RAM	16 GB RAM
50 GB Disk Space	100+ GB Disk Space	25 GB Disk Space
Windows Server 2012 or newer	Windows Server 2012 or newer	Windows XP (>5.1) or newer MacOS 10.11 (El Capitan) or newer
IIS 7 or newer	SQL Server 2012 or newer	
.NET 4.6.1 or newer		

## System Capacity Specifications

**Note:** This applies to both ASR and basic session recording. See below for details.

**Table: Session Recording Capacities**

Web Node	Maximum Concurrent Session Conversions per Node	Maximum Processing Time per Session	Recording Processing Time per Maximum Length Session
Dedicated for session recording	4	2 hours	10 minutes
Shared for front-end processing and session recording	2	2 hours	20 minutes

**Note:** The "Maximum Concurrent Session Conversions per Node" setting can be increased. See <https://thycotic.force.com/support/s/article/Configuring-Number-of-Max-Concurrent-Sessions-Per-Web-Node-Session-Recording>.

## Caveats and Recommendations

### General

System requirements apply to both physical and virtual machines.

- Thycotic does not support these Web servers:
- Any Client OS
- Domain Controllers
- SharePoint Servers
- Small Business Server (SBS)
- Windows Server Essentials
- For best performance, we recommend using dedicated (clean) servers for hosting Thycotic products.
- If .NET and IIS features are not already installed on the Web server, the Thycotic Installer adds and configure them automatically.

### Database

- Database disk storage depends directly on how many recorded videos are stored to disk. For active users, we recommend you **use a 1 TB shared or local drive for archival or storage space**. For light users, we recommend beginning with 300 GB. Monitor your disk space usage closely, and tailor it for best results.
- **Carefully consider how quickly your allotted storage might be exhausted.** Once again, it is highly variable, but you might expect around 15 hours of recording per GB of storage. Using the example of encoding capacity used in the Session Recording section, if you wanted to record one year of usage by your 60 8-hour users, you would need around 11

TBs of storage (given vacations and holidays). Our recommended 1 TB would last nearly a month in that scenario. A session retention policy using the automatic deletion feature is likely your best option.

- If MS SQL Server is not already installed on your database server, the Thycotic Installer can setup SQL Express on the Web server; however, **SQL Express is only for trials and sandbox environments**. Though Thycotic supports SQL Express, your users will likely experience performance issues due to memory and product limitations. If experiencing performance issues while using SQL Express, we highly recommended upgrading to MS SQL Server prior to contacting Thycotic Support.

**Note:** Please see Microsoft documentation on SQL Express at: <https://docs.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2017>

### *Network Bandwidth and Video*

- For Secret Server 10.6 ASR requires around 300 Kbps. Older versions of Session Recording require 1-3 Mbps.

**Note:** Our Mac launcher uses the older bit rate.

- Session recording bandwidth requirements vary widely based on monitor resolution and image complexity--higher resolutions and more complex images (simpler screen images compress better) use more bandwidth. For example, with a 1024×768 screen resolution, the required network bandwidth is typically between 0.1 Mbps and 1 Mbps.
- If your connection cannot support the needed bandwidth, the session data is still transmitted, but it takes longer to process each session.
- If a user tries to cancel the transmission, this activity appears in the audit record for the Session Recording Secret.
- All sessions are recorded at 1080p.

**Note:** Before Secret Server 10.6, session recordings 1080p or higher were not supported due to a limitation in Microsoft IIS. The session video would be recorded but may have been corrupted.

- Sessions are recorded using the H.264 MPEG-4 codec.

### *Session Recording*

- Server hosting session recording requires fixed RAM and disk space. We strongly recommend that you **do not apply dynamic settings**.
- **Do not record more sessions than you can encode.** If more concurrent sessions are recorded than the system can process, the sessions wait in a queue and are processed when enough server resources become available, which could be in a very long time or perhaps never if your storage is overwhelmed.

- The frame rate we can encode varies dramatically based on many factors, so **testing what encoding rate your session recording configuration can sustain is a must**. From there, you can get an idea of what is possible. For example, let us say you found that we can process 20 FPS on average on your Xeon processors. Given that rate, we could encode around 1 minute of a session recording in 3 seconds, or 1 hour in 3 minutes, or 1 day in 72 minutes--giving you perhaps 480 session hours per day. You could then parse that figure based on your typical usage to arrive at a maximum potential usage, for example, 60 people doing 8-hours of session recording.
- Typically, you can record **up to one hundred sessions at a time per web node**, load balanced, which should handle large use cases.
- CPU usage during video processing varies depending on concurrent users and recording length. We recommend that you **closely monitor CPU percentages on your web server** during video processing, as well on your client machines during recording, to increase CPU count for machines, if needed.
- We recommend that you **set up RabbitMQ as the backbone service bus** in session recording environments. To setup RabbitMQ. See: <https://thycotic.force.com/support/s/article/How-to-install-RabbitMq>

## WEB SERVICES

Secret Server provides a suite of web services which can be used to retrieve and update secrets, and folders. The web services allow Secret Server to be accessed using the mobile apps as well as custom built integrations. The web services are secure and require authentication in the same manner as regular access to Secret Server. All actions that involve data are also logged, such as secret views, updates, and adds.

### Enabling Web services

You can enable web services from the **Administration > Configuration** general tab. Enabling web services simply makes the ASP.NET web services built into Secret Server available. They are found under /webservices/sswebservice.asmx in your Secret Server directory. They run on the same port as the Web application. You can view them with a browser to see the functionality that is offered. Specific web service functionality is documented in the Secret Server Web Service API guide.

### Windows Integrated Authentication Webservice

Secret Server also provides a webservice that uses integrated Windows authentication instead of a username and password. This webservice can be used in an application or script to access Secret Server and retrieve secrets with storing the login credentials in the application or configuration file.

**Note:** See the [Windows Integrated Authentication Webservice](#) KB article for more advanced technical information on using this webservice.

## Using the Java Console API Access Secret Values

Secret Server can set up a Java Console API to retrieve values from Secret Server without embedding a password. This allows scripts to retrieve passwords from Secret Server while keeping both the password and credentials to Secret Server secure. The Secret Server Java Console is setup using a user in Secret Server, but the password is changed and hardware-specific, so copying the jar file to other machines does not allow it to access Secret Server. As a user in Secret Server, an admin can share only specific secrets with the account running the Java Console. As a Java implementation, this can be used on any OS including Windows, Mac, Linux and Unix. For installation instructions and examples see the [Application API Guide](#).

## FOLDER SYNCHRONIZATION

To setup this feature, navigate to **Administration > Folder Synchronization**. To edit the settings, you must have a role assignment with Administer ConnectWise Integration permissions.

Enabling folder synchronization requires specifying the synchronization interval in days, hours, and minutes. The "Folder to Synchronize" is the parent folder where you create the folder structure. There are two methods of Folder Synchronization, through the ConnectWise API or through a database view.

### Synchronizing with the ConnectWise API

The ConnectWise API is the recommended way to sync folders from ConnectWise. To sync:

1. Select ConnectWise API from the Folder Synchronization Method list.
2. Enter your ConnectWise site name.
3. Select a ConnectWise Integrator Secret for API Access.

### Folder Synchronization Configuration Edit

[Explain](#)

**Folder Synchronization Method** ConnectWise API ▾

**Synchronization Interval for Folder**

Days

Hours

Minutes

**Folder to Synchronize** 📁 \Clients [Clear](#)

**Site URL** \*

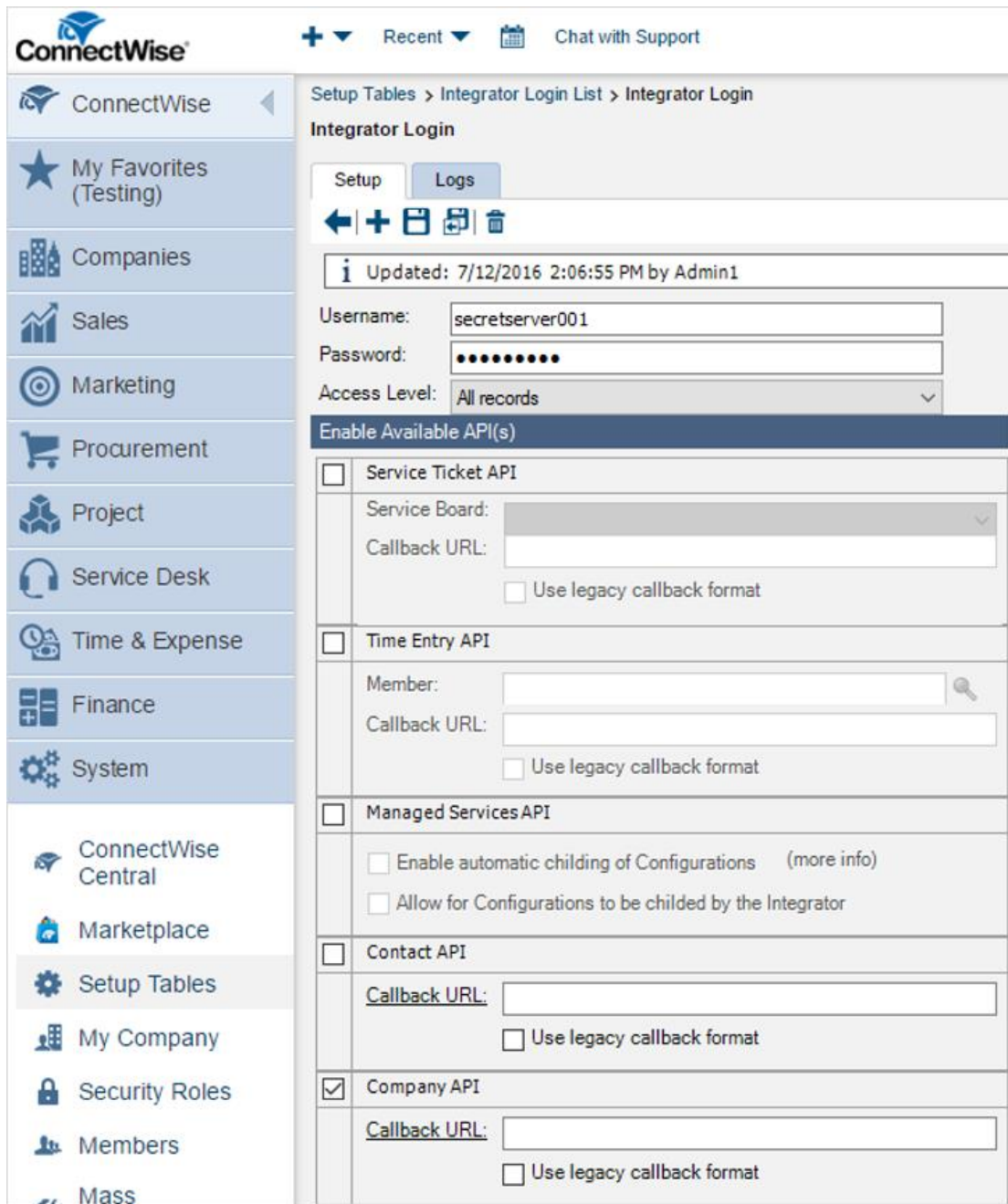
**Company ID** \*

**Integrator Credentials** ConnectWise (secretserver001) [Create New Secret](#) ↗

**Folder Structure**

**Note:** The Integrator account must have access to the Company API in ConnectWise and access to all records





Folder structure defines how folders are named under the client's folder. By default, \$TYPE\ \$STATUS creates sub-folders based on the customer type in ConnectWise, then further sorted by the active status in ConnectWise. For example, the active prospect "Acme Inc" in ConnectWise would get the following folder created: Clients\Prospects\Active\Acme Inc

The supported folder structure tokens are:

- **\$COMPANYINITIAL:** First letter of company name. Use to organize companies into subfolders of A, B, C, and the like.
- **\$STATUS:** Company status, such as active, inactive, or not-approved.
- **\$TYPE:** Company type, such as competition, customer, partner, prospect, suspect, or vendor.

When configured, save and scroll down to the bottom and click **Synchronize Now** to run the synchronization

## **Synchronizing with a Database (Advanced)**

The database synchronization method queries an on-premises database for a custom view and parse company information out of it.

Enter the SQL Server location, SQL database name, and the credential information for accessing the reference database, for example, to your ConnectWise instance. The SQL view defaults to a standard ConnectWise customer layout but can be customized to meet the desired folder Layout.

## Folder Synchronization Configuration Edit

[Explain](#)


**Folder Synchronization Method** Database (Advanced) ▾

**Synchronization Interval for Folder**

Days

Hours

Minutes

**Folder to Synchronize**  \Clients2 [Clear](#)

**SQL Server Location** \*

**SQL Database Name** \*

**SQL Username** \*

**SQL Password** \*

**SQL View** !

ConnectWise

Custom View

See the [How to create a custom view for ConnectWise synchronization](#) KB article for more advanced technical information on setting up the SQL View.

## USERS

### Creating Users

To manually create a single user, navigate to **Administration > Users** and click the **Create New** button. On the subsequent page, you can enter the relevant information for a user.

**Note:** To add many users from your Active Directory setup, you can use Active Directory synchronization (see [Active Directory Synchronization](#)).

### User Owners

User Administrators can also set another group or user as the user owners for a Secret Server local user. User owners can manage and edit just that user. For example, a developer might must unlock or reset the password for an application account but should not have access to all

users. Set **Managed by to User Owners** on a user and then select **Groups** or **Users**. Note that Unlimited Administrator mode can still be used to manage groups with user owners assigned.

## User Settings

Below is a brief explanation of each text-entry field or control:

- **Application Account:** If checked, this user can only be used to access Secret Server through the Java Client/Console API and does not take up a license. See the [Application Account KB](#) for more information.
- **Display Name:** Text that is used throughout the user interface, such as in audits.
- **Domain:** If a drop-down list is visible, selecting a domain from the list is one way to set the expected domain of the user. However, a more dynamic way to have this text-entry field (and all the other text-entry fields) set is through Active Directory synchronization.
- **Email Address:** Email address used for Request Access, email two-factor authentication, and the like.
- **Email Two-Factor Authentication:** On a login attempt, the user has an email sent to the email address entered above. This email contains a pin code that the user needs to log into the account. See [Email Two-Factor Authentication](#) for details.
- **Enabled:** Disabling this control removes the user from the system. Effectively, this is the way to delete a user. Secret Server does not allow complete deletion of users due to auditing requirements. To re-enable a user, navigate to the **Administration > Users page**, check the **Show Inactive Users** checkbox just under the **Users** grid, and edit the user to mark them enabled (see [Configuring Users](#)).
- **Locked Out:** If checked, then this user has been locked out of the system due to too many login failures. To remove the lock, uncheck the check box. For more details on locking out users, see Maximum Login Failures setting described in the Login Settings section.
- **Password:** Login password for the user. For the various login settings, see Login Settings section.
- **RADIUS Two-Factor Authentication:** This text-entry field only appears if RADIUS authentication is enabled in the configuration. On a login attempt, the user must enter the RADIUS token sent from the RADIUS server. See [RADIUS Authentication](#).
- **RADIUS User Name:** This text-entry field only appears if the above RADIUS Two Factor Authentication setting is enabled. This is the username the RADIUS server is expecting. See [RADIUS Authentication](#).
- **User Name:** Login name for the user.

**Note:** A new user is assigned the User role by default. For more information on roles, see "Roles."

## Configuring Users

User settings can be modified by clicking the username in the **User Name** column on the **Users** page. Search for users using the search bar at the top of the grid. To show users that are marked inactive, check the **Show Inactive Users** box below the grid.

## Bulk Operations on Users

Bulk operations on users can also be performed from the **Users** page. Select one or more users using the check boxes beside the **User Name** column, or select all or none by toggling the check box in the header row. Once the appropriate users have been selected, use the Bulk Operation list at the bottom of the grid to select an action. Bulk operations on users currently include enabling or disabling user access, as well as configuring users for email or RADIUS two-factor authentication.

## User Login Settings

Secret Server users can be set up with many different login requirements. For example, you can force strong Login passwords by requiring a minimum length and the use of various character sets.

The following settings are available under the **Administration > Configuration** page, inside the **Login** tab:

- **Allow AutoComplete:** AutoComplete is a feature provided by most Web browsers to automatically remember and pre-fill-in forms for you. This can be a great security concern since they typically do not save the data in a secure manner. You can enable or disable Web browser pre-fill on the login screen by using this option.
- **Allow Remember Me:** This option enables the Remember Me checkbox on the Login screen. When a user chooses to use remember me, an encrypted cookie is set in their browser. This enables the user to revisit Secret Server without the must log in. This cookie is no longer be valid when the remember me period has expired. They then have to enter their login information again. This option allows users to remain logged in for up to a specific period (specified in the "Remember Me Is Valid for" setting mentioned below). This option can be a security concern as it does not require re-entry of credentials to gain access to Secret Server.

**Note:** "Remember me" is only visible if the "Allow Remember Me" setting is enabled. This is the period that the remember me cookie mentioned above is valid. For example: if set to one day, then users taking advantage of "remember me" have to log in at least once a day. To set a time value (minutes, hours, or days), uncheck the Unlimited checkbox.

- **Enable RADIUS Integration:** Allow for RADIUS server integration with your user login authentication. Other RADIUS settings appear upon enabling this option. These settings are discussed in [RADIUS Authentication](#).

- **Maximum Concurrent Logins Per User:** This setting allows a user to log into Secret Server from multiple locations at once without logging out their sessions at other locations.
- **Maximum Login Failures:** Set the number of login attempts allowed before a user is locked out of their account. Once locked out, they need a Secret Server administrator to reset their password and enable their account. For details on how to reset a locked account, see [Creating a User](#).
- **Require Two Factor for these Login Types:** This setting specifies which types of login require two-factor authentication:
  - Website and Web service Log on
  - Website log on only
  - Web service log on only
- **Visual Encrypted Keyboard Enabled:** This setting enables a visual keyboard for logins.
- **Visual Encrypted Keyboard Required:** This setting requires a visual keyboard for logins.

## Password Settings

The following settings are found in the **Administration > Configuration** page, inside the **Local User Passwords** tab. These settings apply to users that were created manually, not users brought into Secret Server through Active Directory synchronization:

- **Allow Users to Reset Forgotten Passwords:** If enabled, the "Forgot your password?" link appears on all users' login screens. Clicking on this link prompts the user to enter the email address that is associated with the user's Secret Server account. If the email address is found, then an email containing a link for password reset is sent. Note that this only works for local user accounts and not for Active Directory accounts.
- **Enable Local User Password Expiration:** When enabled, Secret Server forces a password change for a user after a set interval. After the interval time has elapsed, the next time the user attempts to log in, they are prompted for the old password, a new password, and a confirmation of the new password. The new password is validated against all the password requirements. Newly created local users are also be prompted to change their password upon logging into Secret Server for the first time when this setting is enabled.
- **Enable Local User Password History:** If enabled, this prevents a user from reusing a password. For example, if set to "20 Passwords", this would prevent the user from using a password they have used the previous 20 times. This in conjunction with "Enable Minimum Local Password Age" helps ensure that users are using a new and unique password frequently rather than recycling old passwords.
- **Enable Minimum Local User Password Age:** If enabled, the value for this setting reflects the minimum amount of time that needs to elapse before a password can be changed.

This prevents a user from changing their password too frequently, which allows them to quickly re-use old passwords.

- **Local User Password is valid for:** If enabled, this is the interval that a local user password is valid before it must be changed (see "Enable Local User Password Expiration" setting for details). If this setting is disabled, the entered value displays as "Unlimited".
- **Lowercase Letters Required for Passwords:** Force all user Secret Server login passwords to contain at least one lowercase letter.
- **Minimum Password Length:** Force all user Secret Server login passwords to contain a set minimum number of characters.
- **Numbers Required for Passwords:** Force all user Secret Server login passwords to contain at least one number.
- **Symbols Required for Passwords:** Force all user Secret Server login passwords to contain at least one symbol, such as !@#\$%^&\*.
- **Uppercase Letters Required for Passwords:** Force all user Secret Server login passwords to contain at least one uppercase letter.

## User Restriction Settings

The following restriction settings are available:

- **Enable Login Policy:** If enabled, this simply displays the policy. To force the acceptance of the policy.
- **Force Inactivity Timeout:** This setting is the time limit on idle Secret Server sessions. Once a session expires, the user must login again with their username and password.
- **Force Login Policy:** This setting forces the checking of the "I accept these terms" checkbox before allowing the user to login to Secret Server.
- **IP Restrictions:** This setting can be entered by going to **Administration > IP Addresses**. In there, you can enter the IP ranges you wish your users to use. To configure a user to use the ranges, navigate to the **User View** page and click the **Change IP Restrictions** button. In the subsequent page, you can add all the ranges you want your user to use.
- **Login Policy Agreement:** The Login Policy Agreement is displayed on the login screen. You can change the contents of the Login Policy Statement by editing the file `policy.txt`. By default, this is not enabled. The settings to enable this are accessed by first navigating to **Administration > Configuration** and going into the **Login** tab. Then click the **Login Policy Agreement** button.

## User Preferences

**Note:** Users can set their preferences by hovering on their profile icon in the top right and selecting preferences.

## General Tab

The following configuration settings are available for users under the General tab:

- **Date Format and Time Format:** Date and time format displayed for a user in Secret Server.
- **Language and My Theme:** Customize the look of Secret Server on a per user basis. For details, see [Customizing Secret Server's Appearance](#).
- **Mask passwords when viewing Secrets:** When enabled, this masks the Password text box for a secret. There is a configuration setting that forces this to be enabled for all users. For details on password masking, see [Setting Up Password Masking](#).
- **Send email alerts when dependencies fail to update:** Enables emails to be sent when dependencies fail to update.
- **Send email alerts when Heartbeat fails for Secrets:** When enabled, the user is emailed when a heartbeat fails for any secret the user has view permission to.
- **Send email alerts when Secrets are changed:** Enables emails to be sent on all changes of any secret that the user has view permission. There is a limit of one mail per five minutes per edit of the same user. For example, if user "User1" edits the secret twice within this grace period, only one email is sent.
- **Send email alerts when Secrets are viewed:** Enables emails to be sent on all views of any secret that the user has view permission. There is a limit of one email per five minutes per view of the same user. For example, if user "User1" views the secret twice within this grace period, only one email is sent.
- **Show the full folder path on search results:** Enables the full path to be displayed in the Folder column on the Home page.
- **Use the TreeView control for search on the home screen:** Enables the TreeView control for the Search tab on the Legacy Home screen. This option does not apply to the Dashboard.

## Launcher Tab

The following configuration settings are available to users on the Launcher tab:

- **Allow Access to Printers, Allow Access to Drives, Allow Access to Clipboard:** Allow access to various items when using the launcher.
- **Connect to Console:** Allows you to connect to remote machines using the Remote Desktop launcher and connects as an administrator. This is the equivalent of using the `/admin` or `/console` switch when launching Remote Desktop.



- **Use Custom Window Size:** Checking this box displays Width and Height text boxes for the user to specify a custom window size for an RDP launcher.

## USER GROUPS

Secret Server allows administrators to manage users through *user groups*. Users can belong to different groups and receive the sharing permissions, as well as roles, attributed to those groups. This setup simplifies the management of the permissions and roles that can be assigned to a user. Additionally, groups can be synchronized with Active Directory to further simplify management.

Groups			
Search: <input type="text"/>	15	Save To File < 1 to 7 of 7 >	
Group Name	Enabled	Member Count	Created
<a href="#">Administrators</a>	Yes	4	08/28/2008
<a href="#">Developers</a>	Yes	4	08/28/2008
<a href="#">Everyone</a>	Yes	16	08/28/2008
<a href="#">Interns</a>	Yes	1	08/28/2008
<a href="#">IT Managers</a>	Yes	5	08/28/2008
<a href="#">Marketing</a>	Yes	3	08/28/2008
<a href="#">Sales</a>	Yes	3	08/28/2008

Show Inactive Groups?

## Creating User Groups

You can create and edit groups from the Groups page. You can get to the Groups page by navigating to **Administration > Groups**. By either selecting an already existing group from the list, or clicking **Create New**, you can modify or add the group.

**Note:** To add groups and the users inside them from your Active Directory setup, you can use Active Directory synchronization (see [Active Directory Synchronization](#)).

## Adding Users to Groups

On the Group View page, users can be added and removed from the group. Use the arrow buttons to move users into and out of the current group. If needed, a group can also be enabled or disabled from this page. When you have finished with your changes, click **Save** and your new group members are added.

**Group Edit**

**Group Name\***

**Enabled**

**Managed By**

**Members**

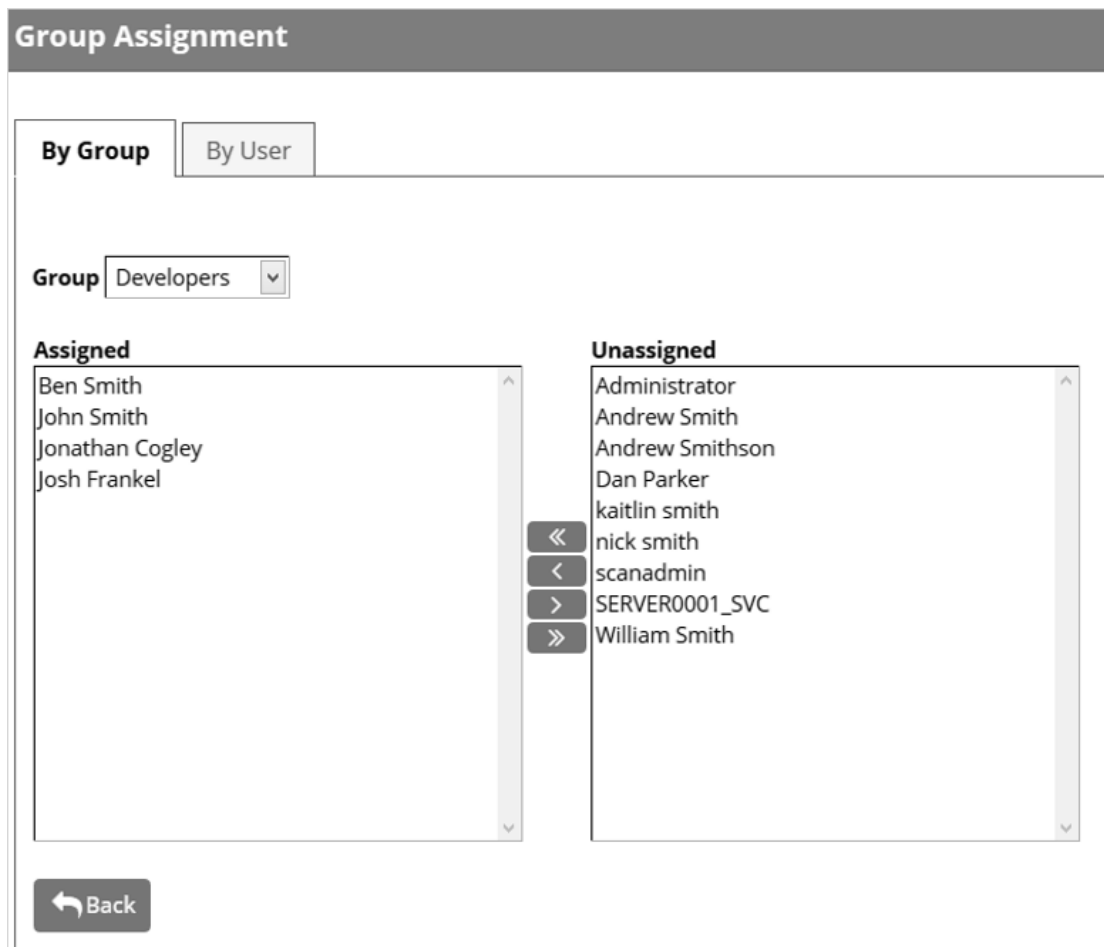
Ben Smith  
 John Smith  
 Jonathan Cogley  
 Josh Frankel

**All Users**

demo.thycotic.com\Administrator  
 qaparent.thycotic.com\Andrew Smith  
 Andrew Smithson  
 Dan Parker  
 kaitlin smith  
 nick smith  
 qaparent.thycotic.com\scanadmin  
 SERVER0001\_SVC  
 qaparent.thycotic.com\William Smith

## Assigning Group Assignment

Alternatively, you can click the **Assign Groups** button on the main **Groups** page. This allows you to select a group from a list and assign or unassign users to the group. In the **By User** tab, you can select a user from a list, and assign or unassign the user from the groups in the selectable lists.



**Note:** If the group was created using Active Directory synchronization, this group is not be editable. See [Active Directory Synchronization](#).

## Group Owners

Group Administrators can also set another group or user as the group owners for a Secret Server local group. Group owners can manage membership just for that group. Set the **Managed By** setting to **Group Owners** on a local group and then select groups or users. Note that unlimited administrator mode can still be used to manage groups with group owners assigned.

**Group Edit**

**Group Name** \*

**Enabled**

**Managed By**

**Group Owners**

Lockout Warning: Assigning owners will prevent Group Administrators from managing the group. Unlimited Administrator mode can be used to change ownership.

Assigned Users and Groups will be given the Group Owner role.

**Group Owners**

Name
IT Managers

**Add Group/User:**

## ACTIVE DIRECTORY SYNCHRONIZATION

Secret Server can integrate with Active Directory by allowing users to login to Secret Server using their Active Directory credentials. Microsoft Active Directory is a component of the Windows Server system that allows a centralized location of user management for a Windows network. Secret Server synchronizes Active Directory users from a security group in a domain at a scheduled interval. Secret Server does not store the domain user's passwords. Instead, it passes through the credentials to the domain for authentication. To synchronize with Active Directory, specify the domain to synchronize groups from, and then select the groups that Secret Server uses to replicate users and membership. When a new user is pulled in from Active Directory, Secret Server also replicates the email address if one exists. Secret Server can synchronize with multiple domains.

### Configuring Active Directory

To allow users to log in with their Active Directory (AD) credentials, you can configure your AD domain settings in Secret Server and then add users either individually or by group.

#### Task 1: Adding a Domain

1. Select **Admin > Active Directory**. The Active Directory Integration page appears.
2. Click the **Edit Domains** button. The Active Directory Domains page appears.
3. Click the **Create New** button. The Credentials tab appears.
4. Fill in the domain information and the username and password that will be used for connecting to the domain and synchronizing users and groups.
5. Click the **Save and Validate** button.

## Task 2: Enabling Active Directory Integration

1. Select **Admin > Active Directory**. The Active Directory Integration page appears.
2. Click **Edit**. The Edit Active Directory Configuration page appears.
3. Click to select the **Enable Active Directory Integration** check box.
4. Click **Save**.

Now you are ready to add individual users or groups of users for access to Secret Server with AD credentials. See the relevant section below for instructions.

## Task 3: Adding Users and Groups

### *Adding Users*

To add an individual AD user:

1. Click **Admin > Users**. The Users page appears.
2. Click the **Create New** button. The Edit User Page appears.
3. Select the desired domain from the **Domain** dropdown list.
4. Type the user's Active Directory username in the **User Name** text box.
5. Type the user's display name in the **Display Name** text box.

**Note:** The user's email address is synced from AD, if available, so it is not necessary to type that in.

6. Click **Save**.

### *Adding Groups*

Secret Server can sync with security groups from AD to automatically add, enable, and disable users. This can streamline the process of managing which users are enabled.

**Note:** Enabled users count towards your Secret Server user licensing.

## Task 4: Enabling Active Directory Synchronization

### *Procedure*

1. From the **Active Directory** page, click **Edit**. The Edit Active Directory Configuration page appears.
2. Click to select the **Enable Synchronization of Active Directory** check box. Additional settings appear.
3. Choose how often you want Secret Server to sync with AD by configuring the **Synchronization Interval**. The default value is one day.

4. Click the **User Account Options** Dropdown list to select a default status for users. See below for a description of each option. We recommend selecting **Users are disabled by default (Manual)** for initial testing.
5. Click **Save**.

#### *User Account Options*

- **Users are enabled by default (Manual):** Secret Server users are automatically enabled when they are synced as new users from AD. If they were disabled explicitly in Secret Server, they are not automatically re-enabled. If creating a new user will cause the user count to exceed your license limit, the user created disabled.
- **Users are disabled by default (Manual):** Secret Server users are automatically disabled when they are pulled in as new users from AD. If they were enabled explicitly in Secret Server, they are not automatically re-disabled.
- **User status mirrors Active Directory (Automatic):** When new users are pulled in from AD, they are automatically enabled if active on the domain. The exception is when this will cause you to exceed your license count. For existing users, they are automatically be disabled if they are removed from all synchronization groups, deleted in AD, or disabled in AD. They are automatically re-enabled when they are part of a synchronization group and are active in AD.

### **Task 5: Choosing Synchronization Groups**

Choose the security groups from AD you want to sync with Secret Server:

1. On the **Active Directory** page, click the **Edit Synchronization** button. The Synchronization Edit page appears.
2. Click the Select Domain dropdown list to choose your domain. More options appear.
3. Click **Search**. Select the group(s) you would like to sync from the **Available Groups** list, then click the single left arrow < to add them to **Synchronized Groups**.
4. Click **Save**.

### **Task 6: Running Active Directory Synchronization**

From the **Active Directory** page, click the **Synchronize Now** button to run a sync. As the sync progresses, you can click the **Refresh** button to monitor the logs until you see the message **Completed Domain synchronization for all domains**.

## **Enabling and Disabling Active Directory Users**

If you selected a manual setting for **User Account Options**, you can now enable or disable your AD users' access to Secret Server:

1. Go to **Admin > Users**. The Users page appears.

2. To enable users:
  1. Click to select the **Show Inactive Users** check box.
  2. Click to select the check box next to the users to enable.
  3. Click The **Bulk Operation** dropdown list and select **Enable Users**.
3. To disable users, use the same process, selecting **Disable Users** from the **Bulk Operation** dropdown list.

## Unlocking Local Accounts

If a user fails their login too many times (specified in the **Local User Passwords** section of the configuration page), their account is locked out and they are not be able to log in.

To unlock the account:

1. Log on as an administrator.
2. Click on **Admin > Users**.
3. Click on the user who is locked out.
4. Click **Edit**.
5. Click to deselect the **Locked out** check box.
6. Click **Save**.

## Syncing and Authenticating AD Users via a Distributed Engine

In addition to syncing AD with Secret Server via your local site, Secret Server can also synchronize and authenticate users from distributed engine (DE). You can install a DE in a remote site, allowing all users to use the same Secret Server with their AD credentials. This feature allows organizations with users in different locations to easily get access to Secret Server, and now organizations with Secret Server Cloud can use local AD credentials for authentication. To setup AD to sync from a DE:

1. Create a synced secret. Before synchronizing or creating users, create a secret for use as the sync secret. This secret should contain Domain Admin credentials (or an account with appropriate permissions for read access to all your organization's AD objects).
2. Specify the domain to authenticate against:
  1. Before synchronizing or creating users, you must first specify which domains Secret Server can authenticate against. Secret Server can synchronize with any number of domains.
  2. Go to **Admin > Active Directory**. The Active Directory Configuration page appears.

3. Click the **Edit Domains** button.
4. Click the **Create New** button. The Active Directory Domain page appears.
5. Type the domain information that you want to authenticate to.
6. Click the **Link a Secret** selection button.
7. Click the **Sync Secret** list to select the AD secret you created earlier.

**Note:** If you do not have a secret setup yet, click the **Create New Secret** link to create your AD secret. **Note:** The AD sync secret is used to synchronize users and groups. It requires permission to search and view the attributes of the users and groups. If you plan on using Secret Server discovery, the account will also need permissions to scan computers on the network for accounts.

8. Click the **Save and Validate** button.
3. Set up the synchronization groups:
    1. Once the domain has been added, go to **Admin > Active Directory**. The Active Directory Configuration page appears.
    2. Click the **Edit Synchronization** button. The Synchronization Edit page appears. The Available Groups represent all accessible groups on the specified AD domain. You can preview the user membership with the Group Preview control.
  4. Select the desired group from the Available Groups that contains the AD accounts for users you would like to create in Secret Server.
  5. Configure AD:

**Note:** See [Active Directory Configuration Parameters](#) for more information.

1. Go to **Admin > Active Directory**. The Active Directory Configuration page appears.
2. Click on **Edit**. The Edit Active Directory Configuration page appears.
3. Click to select the **Enable Active Directory Integration** check box.
4. Click to select the **Enable Synchronization of Active Directory** check box.
5. Click **Save**.
6. Turn on AD sync.

## Active Directory Configuration Parameters

Active Directory configuration can be enabled by a user with the Administer Active Directory role. To change these settings, select **Active Directory** from the **Administration** menu and then click **Edit**.



The configuration screen offers several options:

- **Enable Active Directory Integration:** Enable or disable the Active Directory Integration feature.
- **Enable Integrated Windows Authentication:** Enable or disable the Windows integrated authentication feature.
- **Enable Synchronization of Active Directory:** Enable or disable the automatic synchronization of the selected Synchronization Groups from Active Directory. If you have manually added users and will not use the Synchronization group, do not enable this setting or manual users can be locked out.
- **Synchronization Interval for Active Directory:** Set the interval that Secret Server synchronizes its users and groups with the Active Directory.
- User Account Options:
- **Users are enabled by default (Manual):** Secret Server users are automatically be enabled when they are synced as new users from Active Directory. If they were disabled explicitly in Secret Server, they are not be automatically re-enabled. If creating a new user causes the user count to exceed your license limit, the user is created as disabled.
- **Users are disabled by default (Manual):** Secret Server users are automatically disabled when they are pulled in as new users from Active Directory. If they were enabled explicitly in Secret Server, they are not automatically re-disabled.
- **User status mirrors Active Directory (Automatic):** When a new user is pulled in from Active Directory, they are automatically enabled if active on the domain. The exception is when this causes you to exceed your license count. For existing users, they are automatically be disabled if they are removed from all synchronization groups, deleted in AD, or disabled in AD. They are automatically re-enabled when they are part of a synchronization group and are active in AD.

## Creating Active Directory Users

Active Directory users can be created manually by a user that has the Administer Users role. You can do this by going to **Administration > Users**, then clicking the **Create New** button. See [Creating a User](#).

## Converting Local Users to Domain Users

Local users can be converted to a domain user in a one-way irreversible process. This feature helps existing customers with extensive groups and permissions setup for a local user that they want to convert to an Active Directory user. The page can be accessed on the **Administration > Users** page by clicking the **Migrate to AD** button. For the conversion to work, the domain user must not exist within Secret Server. The username is changed to match the domain user throughout the system.

# TEAMS

## Overview

### What Are Secret Server Teams for?

With Secret Server teams, administrators can create special groups called *teams* to restrict what users can see. A team bundles users and groups to assign them the same rules as to what other users and sites are visible to them. For example, a managed service provider could isolate their customers from seeing other customer's user accounts or a large company could "firewall" their users by department. Site visibility can also be restricted by teams.

### Team-Related Permissions

Team visibility and management are controlled by user roles. Those roles, and by extension users, are governed by the following team-related role permissions:

- **Administer Teams:** Users can create, edit, and view all teams.
- **No Teams-related Permissions:** Users can only view other users within their team.
- **Unrestricted by Teams:** Users can view all users, groups, and sites, regardless of Team affiliation. Essentially, teams do not exist for the users with this permission, and the Teams page is not available to them. The default user role has this permission.
- **View Teams:** Users can view all teams. This is essentially a read-only Administer Teams.

## Team Management

### Configuring Team Management

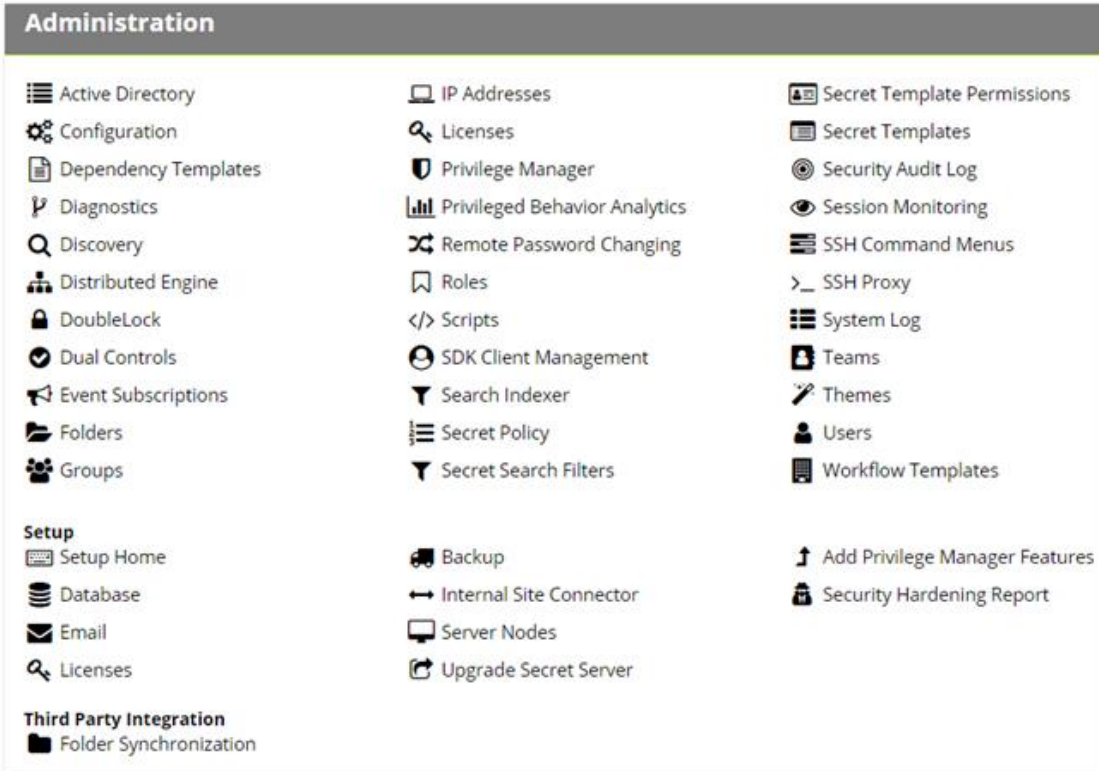
To set up Secret Server to use the team management feature:

1. Create a new role called *Team Limited User*.
2. Assign all permissions of the standard user role except *Unrestricted by Teams*.
3. Assign users you want restricted by teams this role.
4. Remove the User role from their account.

**Note:** If you want all new users restricted by team, you can configure Secret Server to assign the Team Limited User role as the default upon creation of a new user.

### Viewing a User's Teams

1. In Secret Server, click the **Admin** menu item. The Administration page appears:

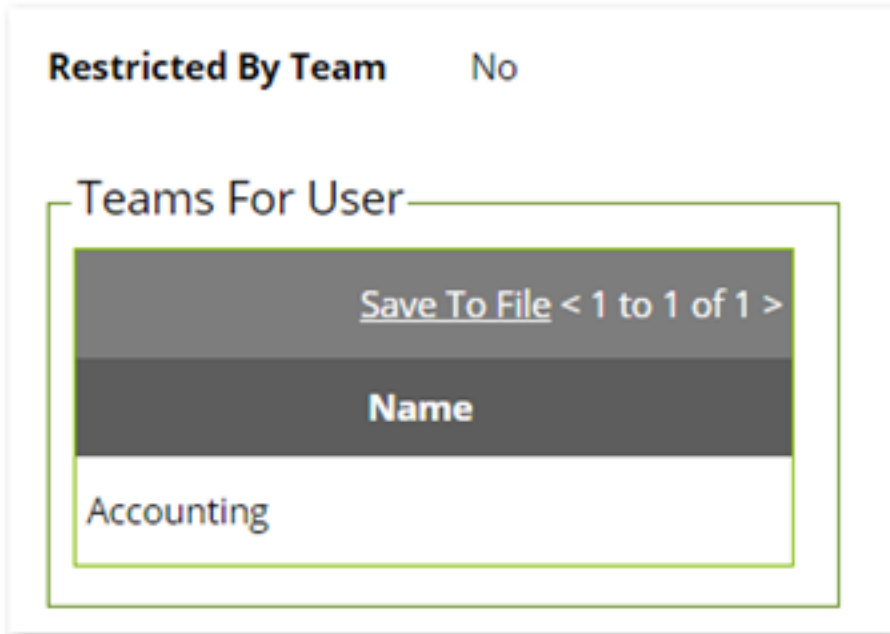


2. Click the **Users** button. The View User page appears:

### View User

<b>User Name</b>	Will
<b>Display Name</b>	Will
<b>Email Address</b>	[Redacted]
<b>Domain</b>	Local
<b>Two Factor</b>	< None >
<b>Enabled</b>	Yes
<b>Locked Out</b>	No
<b>Application Account</b>	No
<b>IP Address Restrictions</b>	
None	
<b>Restricted By Team</b>	No

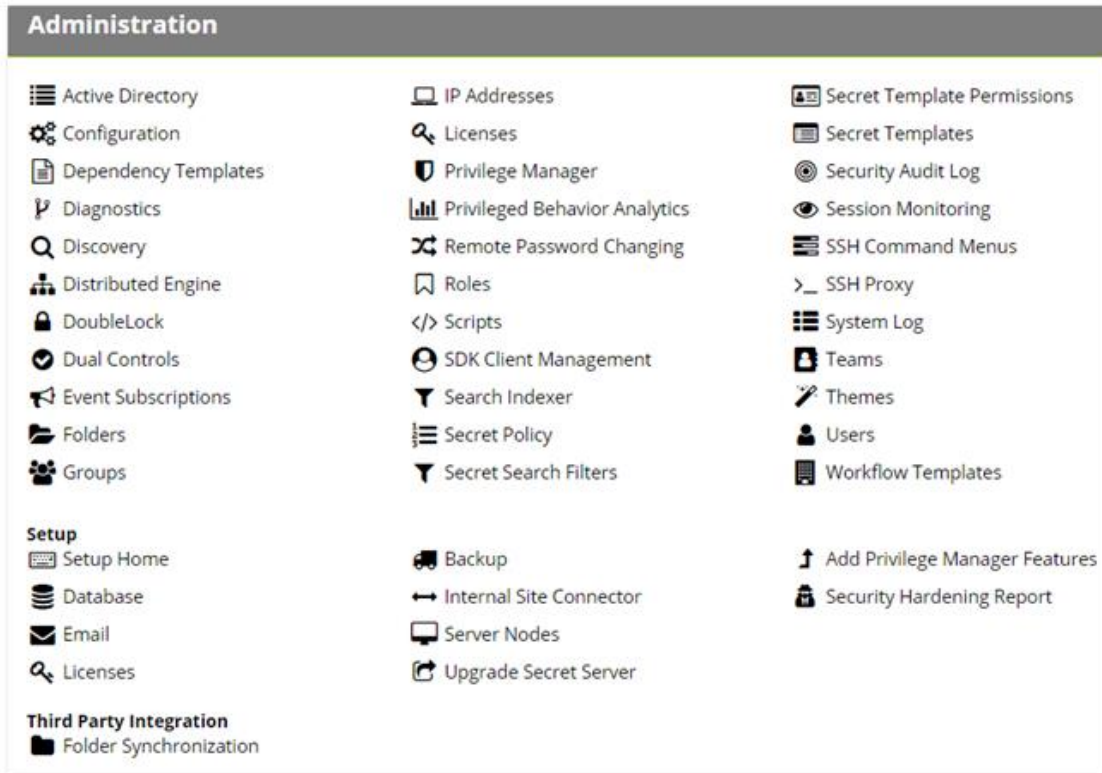
3. Scroll down to the **Teams for User** section:



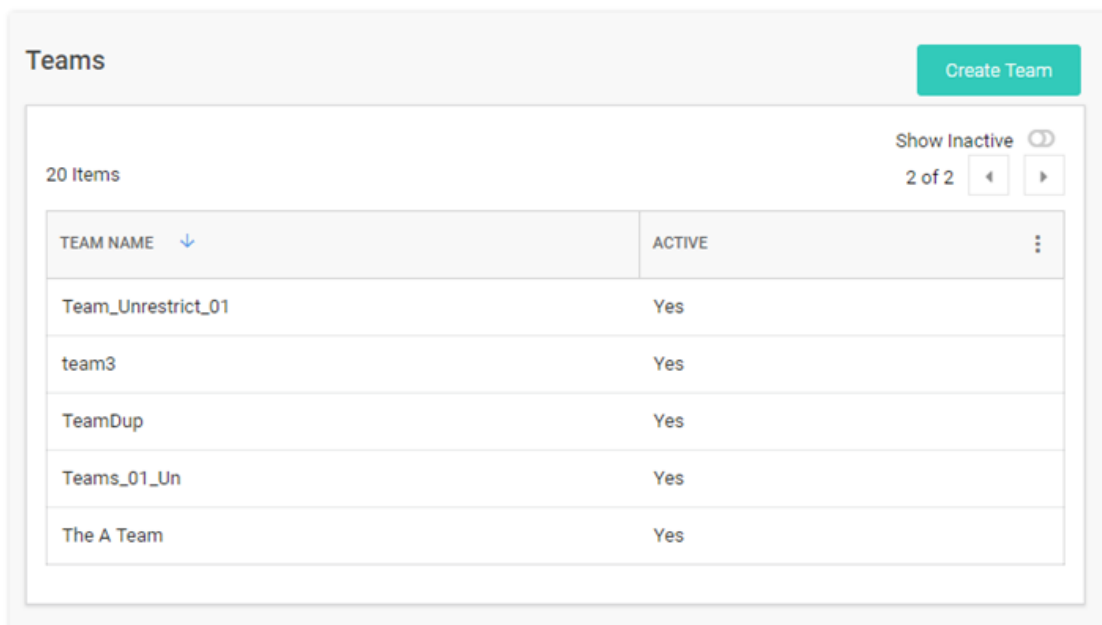
You can see if the user belongs to a team, and if so, what teams the user belongs to. If the Restricted by Team line says *No*, it means the user has been granted the Unrestricted by Teams permission, which means the user can view all users, groups, and sites.

### Creating Teams

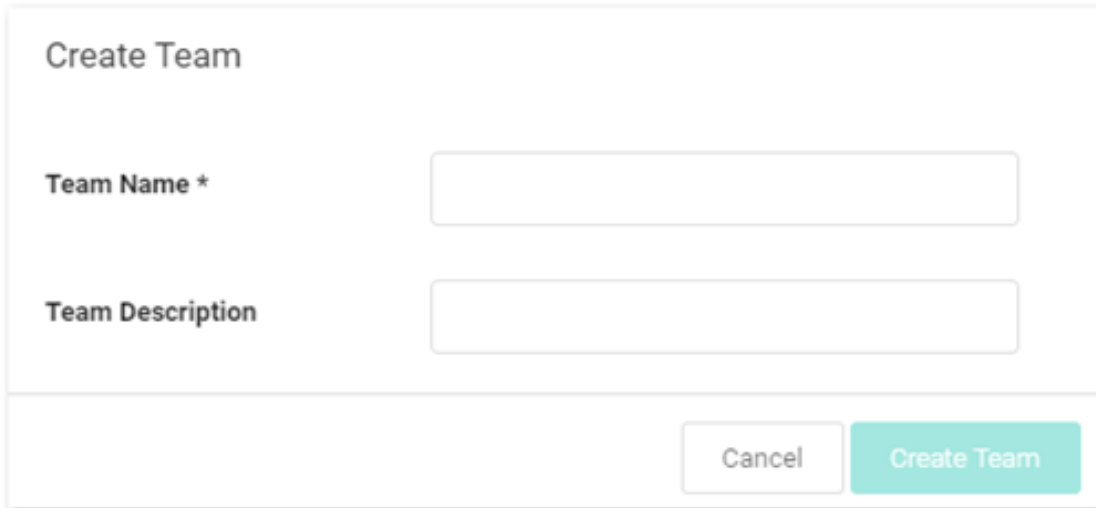
1. In Secret Server, click the **Admin** menu item. The Administration page appears:



2. Click the **Teams** button in the list. The Teams page appears:

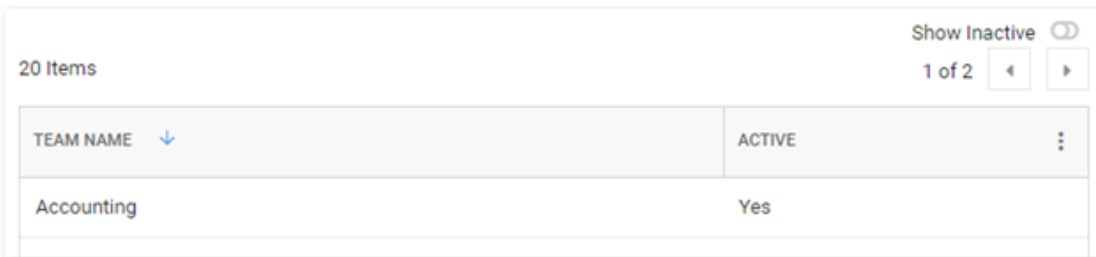


3. Click the **Create Team** button. The Create Team popup page appears:



The image shows a 'Create Team' form. It has a title 'Create Team' at the top left. Below the title are two text input fields: 'Team Name \*' and 'Team Description'. At the bottom right of the form are two buttons: 'Cancel' and 'Create Team'.

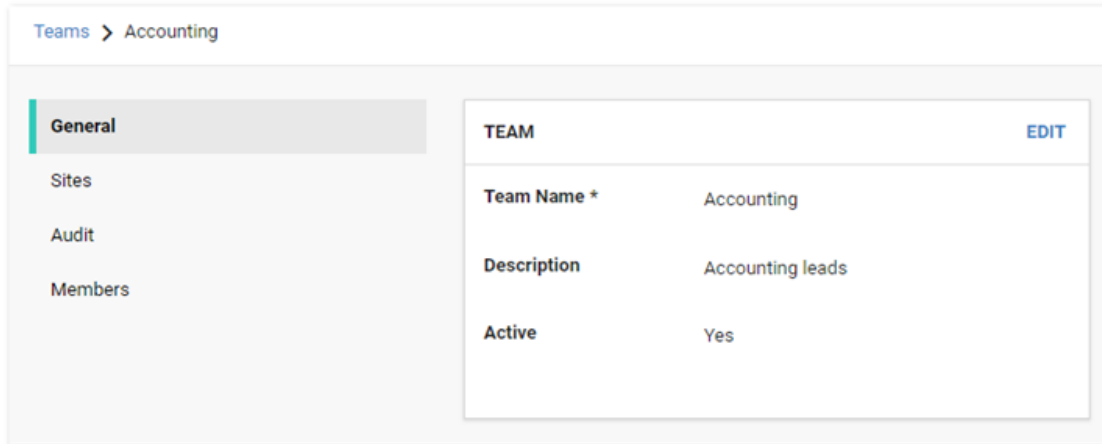
4. Type the name for the new team in the **Team Name** text box.
5. (Optional) Type a description in the **Team Description** text box.
6. Click the **Create Team** button. The new team appears on the Teams page:



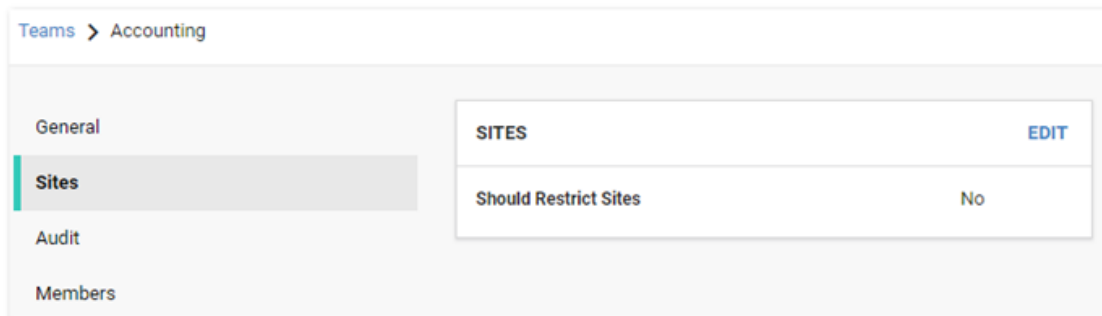
The image shows a table with 20 items. The table has two columns: 'TEAM NAME' and 'ACTIVE'. The first row shows 'Accounting' in the 'TEAM NAME' column and 'Yes' in the 'ACTIVE' column. The table also has a 'Show Inactive' toggle and a pagination indicator '1 of 2'.

TEAM NAME	ACTIVE
Accounting	Yes

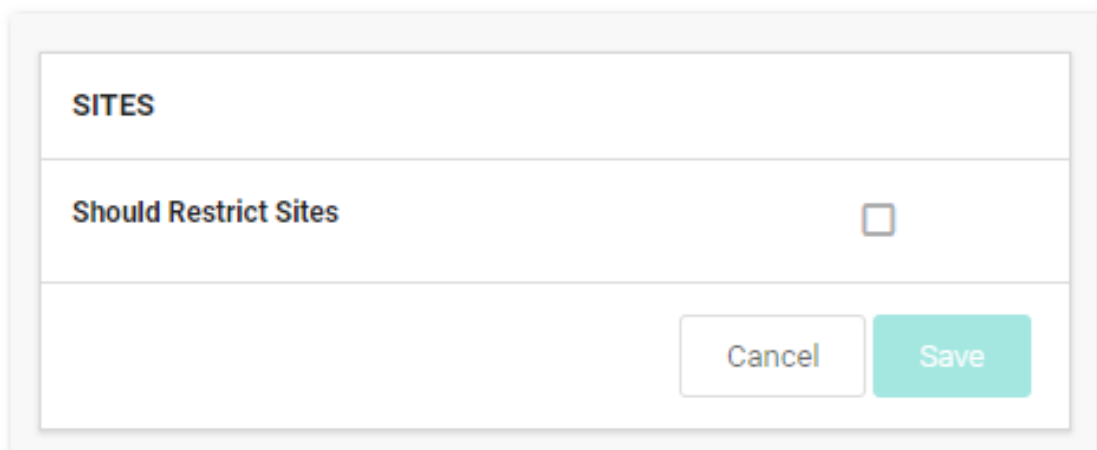
7. Click the table row for the newly created team. That team's page appears:



- Click the **Sites** button on the left. The Sites page appears:



- Click **Edit**. The page becomes editable:



- Click to select the **Should Restrict Sites** check box. A Site dropdown list appears:



### SITES

**Should Restrict Sites**

SITE
Site

Site

Select one ▼

11. Click the **Site** list to select a site to restrict the team to. The selected site appears in the Site table:

**SITES**

**Should Restrict Sites**

SITE
Local

**Site**

Select one ▾

Cancel Save

12. Click **Save**.

13. Click the **Members** button on the left. The Members page appears:

**MEMBERS** [EDIT](#)

<b>USERS AND GROUPS</b>
-------------------------

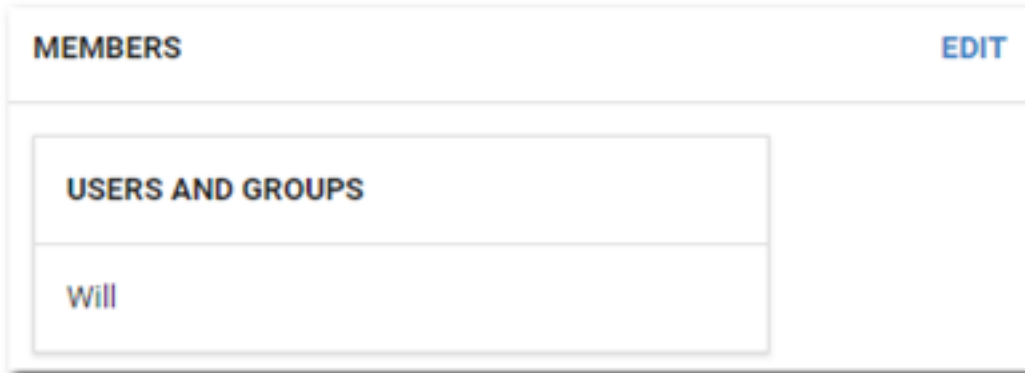
14. Click **Edit**. The page becomes editable:

The screenshot shows a web interface for managing members. At the top, there is a header labeled "MEMBERS". Below this is a table with the heading "USERS AND GROUPS", which is currently empty. Underneath the table is a section titled "Add Groups / User" containing a search input field with the placeholder text "Search for groups or use" and a magnifying glass icon. At the bottom right of the interface are two buttons: "Cancel" and "Save".

15. Type the name of the desired user or group to add in the **Add Groups / User** search box. When you begin typing, a list of available groups and users appear below. Select one. The user or group appears in the Users and Groups table:

This screenshot shows the same "MEMBERS" page as the previous one, but with a single entry in the "USERS AND GROUPS" table. The entry is "Will" and has a "Remove" button next to it. The "Add Groups / User" search box and the "Cancel" and "Save" buttons remain visible at the bottom.

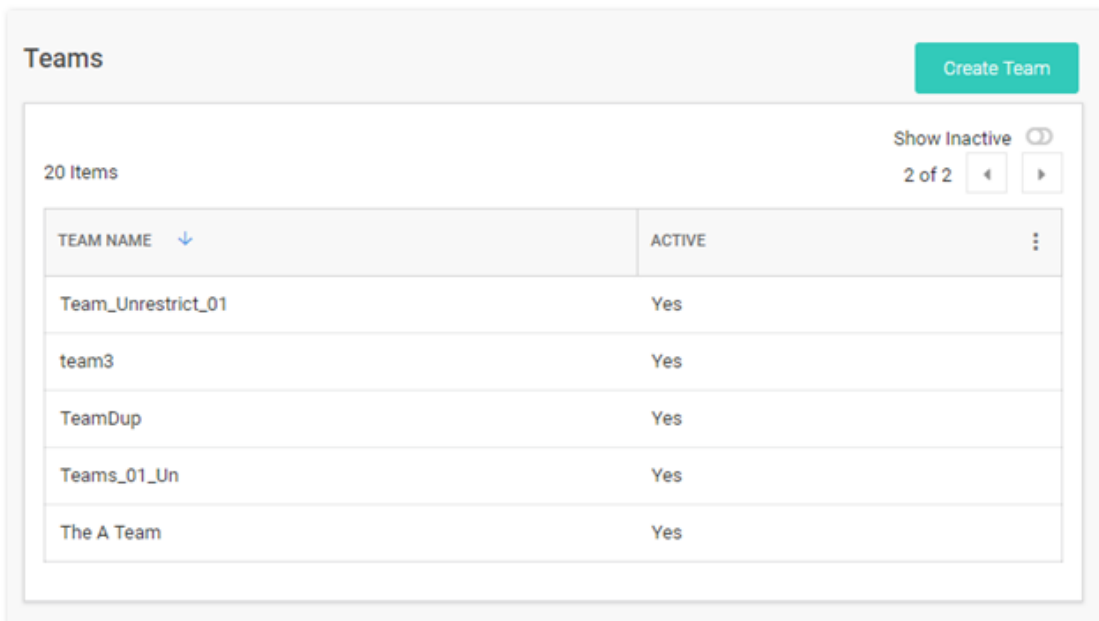
16. Click **Save**. The member appears on the Members page:



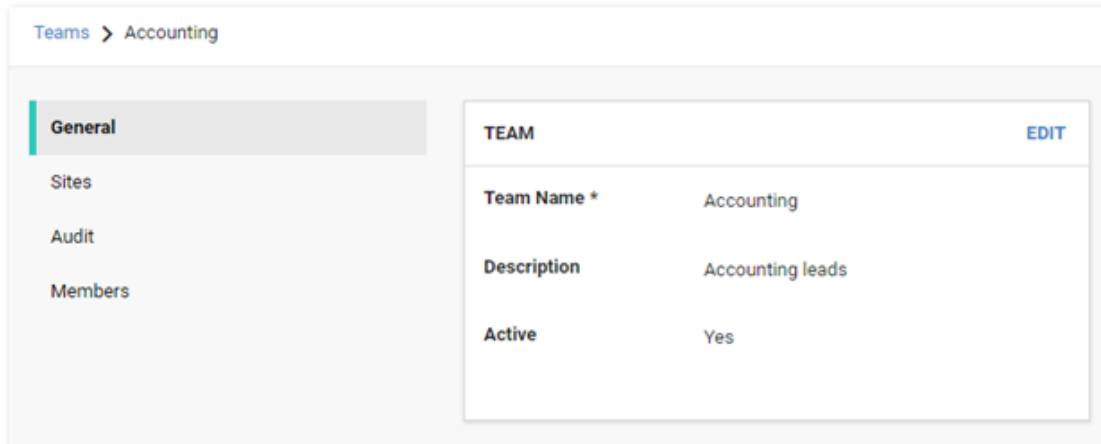
### Deactivating Teams

**Note:** You cannot delete teams because of auditing restrictions.

1. In Secret Server, click the **Admin** menu item. The Administration page appears.
2. Click the **Teams** button in the list. The Teams page appears:



3. Click the table row for the desired team. That team's page appears:



4. On the **General** page, click **Edit**. The tab becomes editable:

**TEAM**

Team Name \*

Description

Active

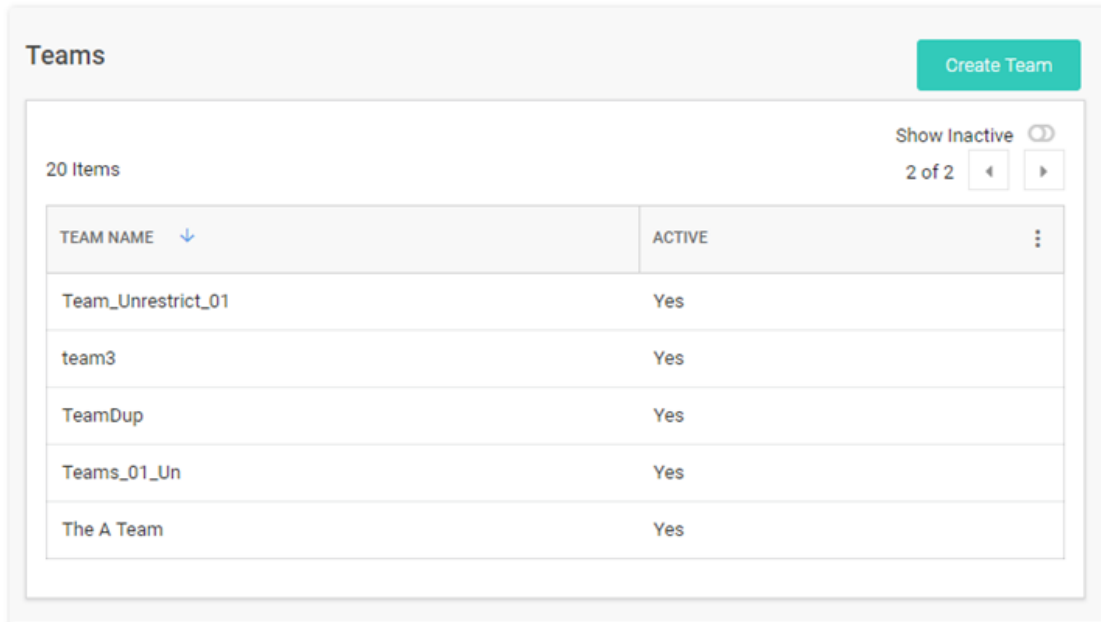
Cancel Save

5. Click the **Active** check box to deselect it.
6. Click **Save**. The team is deactivated.

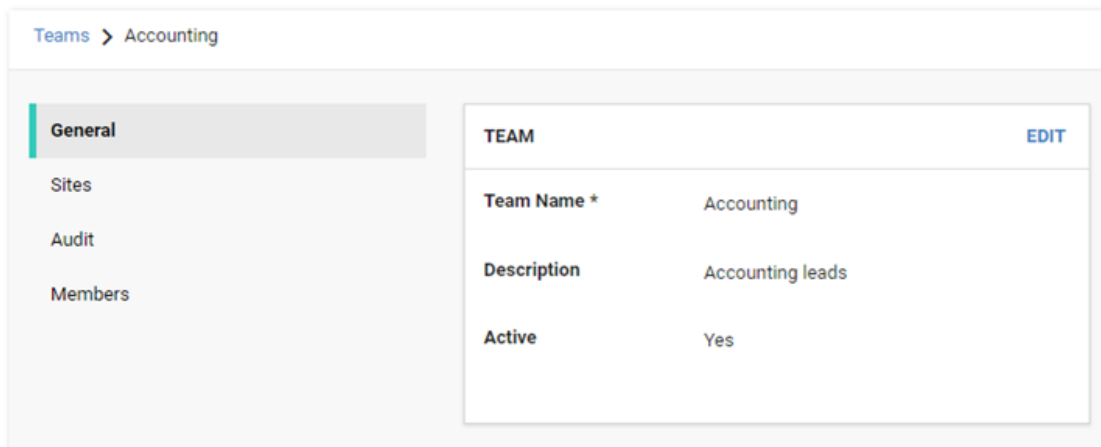
### Editing Teams

1. In Secret Server, click the **Admin** menu item. The Administration page appears:

- Click the **Teams** button in the list. The Teams page appears:

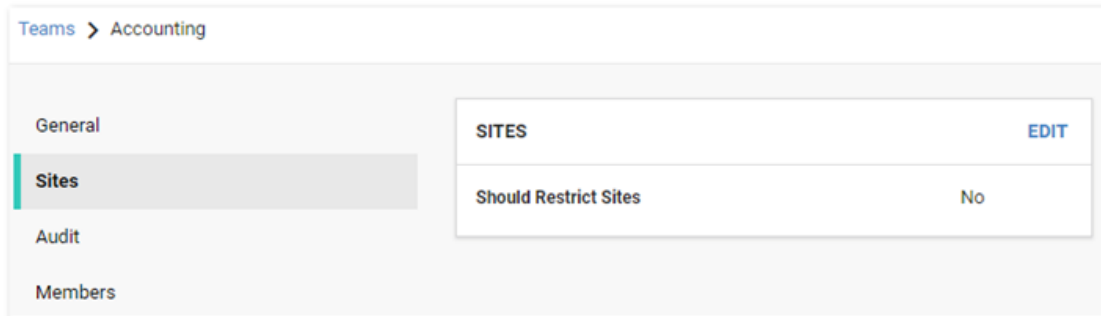


- Click the table row for the desired team. That team's page appears:

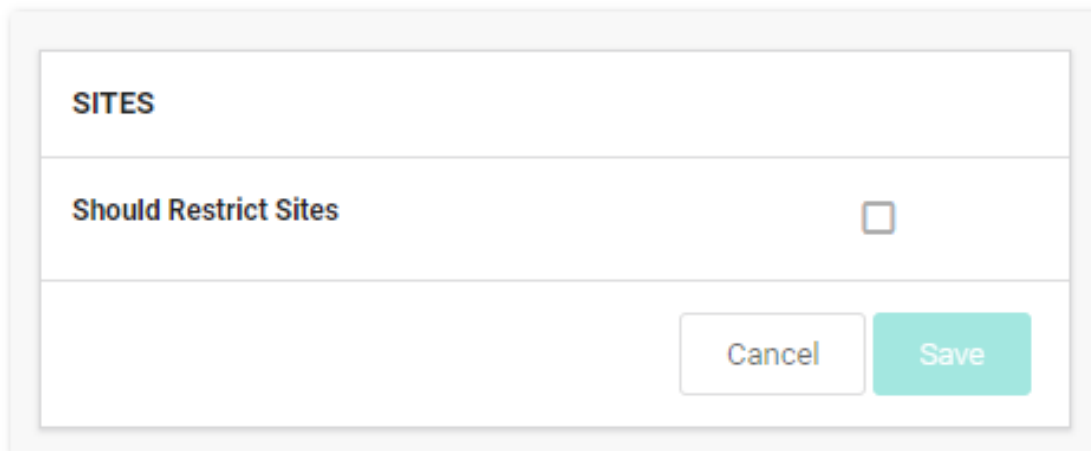


- On the **General** page, click **Edit** to change:
  - The team name
  - The team's description
  - The team's status
- To restrict the visible sites:

6. Click **Sites**. The Sites page appears



7. Click **Edit**. The page becomes editable:



8. Click to select or deselect the **Should Restrict Sites** check box. If you enabled it, a Site dropdown list appears:

### SITES

Should Restrict Sites

SITE
Site

Select one ▼

Cancel Save

9. Click the **Site** list to select a site to restrict the team to. The selected site appears in the Site table:



**SITES**

**Should Restrict Sites**

**SITE**

Local

**Site**

Select one ▾

Cancel Save

10. Click **Save**.
11. To edit the team's member users or groups:
12. Click **Members**. The Members page appears:

**MEMBERS** **EDIT**

**USERS AND GROUPS**

13. Click **Edit**. The page becomes editable:

**MEMBERS**

**USERS AND GROUPS**

**Add Groups / User**

Search for groups or use

Cancel Save

14. Type the name of the desired user or group to add in the **Add Groups / User** search box. When you begin typing, a list of available groups and users appear below. Select one. The user or group appears in the Users and Groups table:

**MEMBERS**

**USERS AND GROUPS**

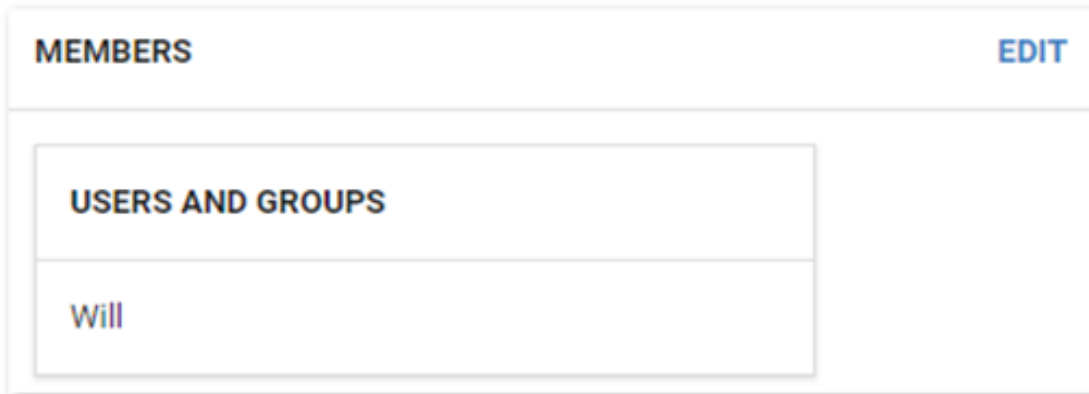
Will	Remove
------	--------

**Add Groups / User**

Search for groups or use

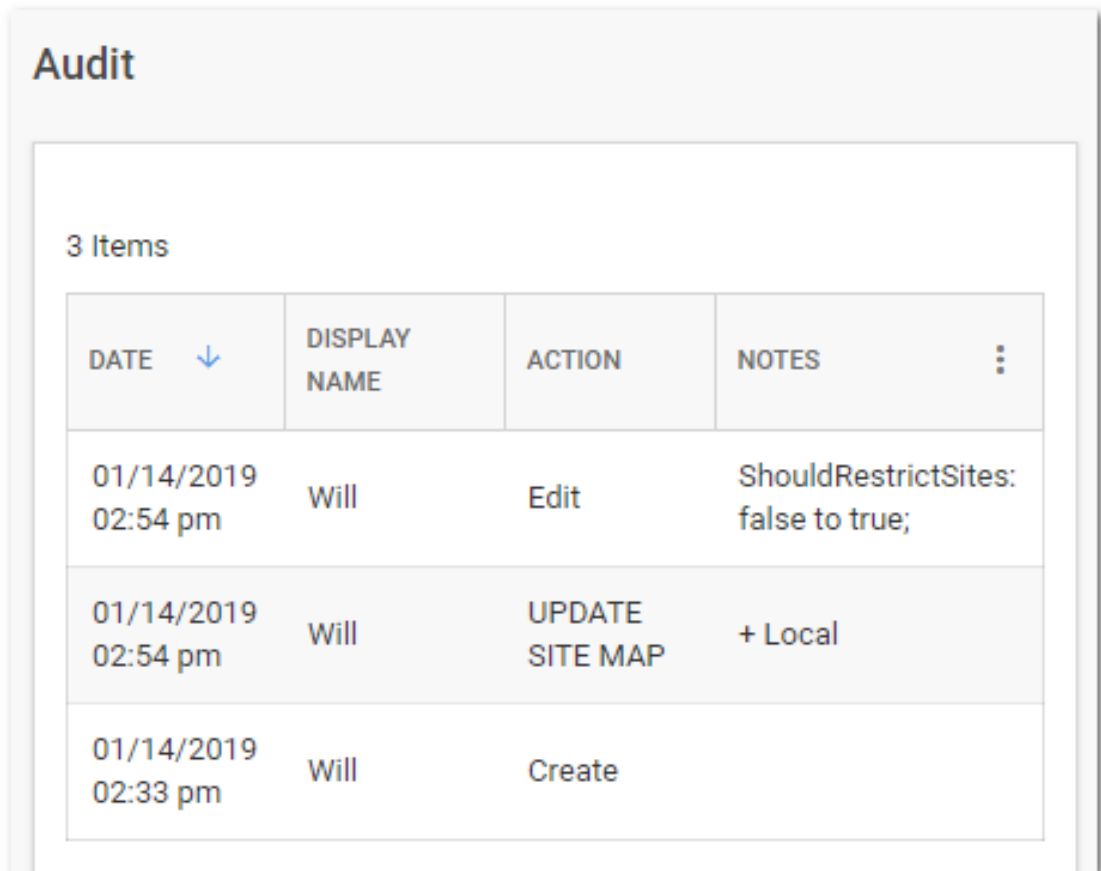
Cancel Save

15. Click **Save**. The member appears on the Members page:



16. View events for the team using its audit trail:

1. Click **Audit**. The Audit page appears:



2. Audit events occur when:

- The team is created
- General tab: name, description, or active status is changed
- Sites tab: restrictions are added, removed, or changed
- Members: users or groups are added or removed

## Troubleshooting

Users can view other users not in their teams if that user already had a connection, such as a shared secret, with the other user prior to setting up the team restrictions.

The API does not restrict who can be assigned if they use the known group ID of a user or group not in their team. This is designed so secret permissions can be saved across teams without removing the permissions of another team.

## ROLES

Modeled after the role-based access control (RBAC) mechanism, role-based security (RBS) is Secret Server's method of regulating permission to system access. Each user and group must be assigned to a role. Secret Server ships with three roles: Administrator, User, and Read-Only User. Each role contains various permissions to match the job function of the user. With RBS, strict granular access to Secret Server is ensured. A list of role permissions and their descriptions can be found in [this KB article](#).

You can assign multiple permissions to a role. For example, you could assign Administer Users, Edit Secret, Own Secret, and View Active Directory permissions to a role. That role can then be assigned to a user or group.

**Note:** The Unlimited Administrator permission allows the user to have unlimited administrator rights when Unlimited Administrator is enabled in the configuration. By default, it is disabled.

## Creating Roles

You can create roles from the Roles page. To get to the Roles page, navigate to **Administration > Roles**. Click **Create New** to add the role.

## Editing Role Permissions

To add or remove permissions to an existing role, click the role name of the role you wish to edit.

On this Role View page, permissions can be added and removed from the role by clicking **Edit**. Use the arrow buttons to move permissions into and out of the current role. If needed, a role can also be enabled or disabled from this page. If you have finished with your changes, you must click **Save** to have the changes take effect.

## Assigning Roles to a User

To assign roles to a user, click **Assign Roles** on the main **Roles** page. Depending on which tab is selected, this page allows you either view the roles that are assigned to users or view the users that are assigned to roles. To change these settings, click **Edit**. Now select a role from the list and assign or unassign users to the role. In the **By User or Group** tab, you can select a user or group from the list and assign or unassign roles to them in the selectable list boxes.

## Creating Synchronization Secrets

Before synchronizing or creating users, you must create a secret to be used as the **Sync secret**. This secret should contain Domain Admin credentials (or an account with appropriate permissions to search and view the attributes to all your organization's users and groups).

## Adding Domains

To add domains:

1. From the **Admin | Active Directory** page, click **Edit Domains** and then **Create New** to add a new Active Directory domain.
2. If you wish to use Secure LDAP, enable the **Use LDAPS** checkbox under the **Advanced** section. For more information on Secure LDAP, please see the Using Secure LDAP KB Article.
3. It is possible to set **Automatically enable Two Factor Authentication** for users synchronized from this domain. This option is also available under the **Advanced** section.

## Local Sites Versus Distributed Engine Sites

When synchronizing with Active Directory, you have two choices for how Secret Server connects to the domain: from the Web server *or* routed through a distributed engine. If your Web server can reach your domain without issue, then using the local site option is recommended. When a user authenticates or AD synchronization is run, the connection to the domain is from the Web server. If your Web server cannot connect to the target domain, if it is a VM in a cloud environment for example, you can setup an engine on-premises and assign it to the domain. When a user authenticates, Secret Server routes the domain calls through the on-premises engine, eliminating the need for site to site connections or persistent VPNs. Review the Distributed Engine guide for steps on setting up sites and engines.

**Note:** The Active Directory secret is used to synchronize users and groups, it requires permission to search and view the attributes of the users and groups. If you plan on using discovery, the account also needs permissions to scan computers on the network for accounts.

## Setting Up Synchronization Groups

Once a domain has been added, the **Synchronization Groups** needs to be set by clicking the **Edit Synchronization** button on the **Active Directory Configuration** page. The Available

groups represent all accessible groups on the specified Active Directory domain. The user membership can be previewed with the **Group Preview** control. Select the desired group from the available groups that contains the Active Directory accounts for users you would like to create in Secret Server. If the specific group does not exist, one can be created by your Active Directory administrator. If you create domain users manually or converting local users to domain users, then see the corresponding sections below before setting the synchronization group.

## ADVANCED AUTHENTICATION

Secret Server provides integration options for Windows authentication and SAML to automatically authenticate users to the application when they browse to Secret Server on their workstations.

## INTEGRATED WINDOWS AUTHENTICATION

Windows integrated authentication allows Active Directory users that are synced with Secret Server to log into workstations and be automatically authenticated to the application. A user's Active Directory credentials are automatically passed through to IIS, logging them into the site.

For further information, Microsoft has a [knowledge base article](#) troubleshooting some common client-side issues with integrated authentication.

### Enabling Integrated Windows Authentication

Active Directory integration and synchronization must be enabled before configuring integrated Windows authentication:

1. Navigate to **Administration > Active Directory**.
2. Click **Edit**.
3. Check the Enable Integrated Windows Authentication box.
4. Click **Save**.

### Configuring IIS

Open IIS and highlight your Secret Server website or application. In the right pane, double-click **Authentication**. Enable Windows Authentication and disable **Anonymous Authentication**.

**Note:** For additional information on requirements and troubleshooting, see our [KB article on Integrated Windows Authentication](#).

### Logging on As a Local Account

After you have set up integrated Windows authentication, you may sometimes want to log in as a local admin account to configure Secret Server, perform an upgrade, or if AD is down.

1. Log on your computer as an Active Directory account that has read access to the Secret Server application directory but is not enabled in Secret Server.
2. Browse to Secret Server using Firefox or Chrome.
3. Go to your Secret Server website. You may be prompted for your AD credentials. If you are, log on as a user with read access to the Secret Server application directory that is not enabled in Secret Server. You should then be redirected to the log on page of Secret Server.
4. Select the "local" domain and enter your local account username and password.

## SAML

Secret Server provides the option to integrate your SAML implementation to automatically authenticate users to the application:

- To configure SAML for versions 10.5+, see [the SAML 2.0 Configuration Guide](#).
- To configure SAML for versions 10.2-10.4, see [this document on SAML](#).

## IP ADDRESS RESTRICTIONS

IP address restrictions allow you to control which IP address ranges users can use to log in to Secret Server.

### Creating IP Address Ranges

To create an IP address range:

1. Go to the **IP Addresses** under Administration.
2. Click the **Create New** button.
3. In the **IP Address/Network Name** text box, enter a descriptive name for your range.
4. In the **IP Address Range** text box, enter an IP Address or IP Address range. Secret Server supports single IP Addresses (10.0.0.4), a range separated by a hyphen (10.0.0.1-10.0.0.255), and CIDR notation (10.0.0.0/24).
5. Click **Save**.

### Editing and Deleting IP Address Ranges

To edit an IP address range, go to the **IP Addresses** page, click on a range, and click **Edit**. To delete a range, click on the range and click **Delete**.

## Assigning an IP Address Range

To assign a range to a user, go to the Users page under administration, click on a username, and click Change IP Restrictions. Next, check or uncheck the boxes next to the ranges to choose which IP Addresses a user can use to access Secret Server. If no boxes are checked, the user can access Secret Server through any IP Address.

**Note:** Regardless of the restrictions, users can always log in when accessing Secret Server on the server using a local IP address (127.0.0.1). This prevents total lockout from Secret Server.



# Administration Tabs

Secret Server is highly customizable. Administrators can increase site security through various configuration settings such as force inactivity timeouts and specifying a SMTP server. This level of configuration allows Secret Server to be altered to meet the needed requirements for the instance. The settings are explained below.

## GENERAL TAB

The following configuration settings are available in the General tab:

- **Allow Approval for Access from Email:** Adds links in request for approval emails allowing approvers to approve or deny access to a secret without logging into Secret Server. See [Requires Approval for Access](#) for details.
- **Allow Automatic Checks for Software Updates:** Enable this option to be notified of a new Secret Server release. If a new update is available, displayed at the top of each Secret Server page is a link to the latest update. This feature is only available to those with support licenses.
- **Allow Secret Server to Retrieve Website Content:** Enables the Web launcher to retrieve the Web site content in order to parse the form and find the login controls.
- **Allow Users to Select Themes:** Allows users to customize the theme for Secret Server. This selected theme would only apply to their login.
- **Allow Web Launcher Mappings to be Downloaded:** Enables a Web launcher configuration to download pre-approved website launcher settings from Thycotic.com.
- **Allow Web Launcher Mappings to be Uploaded Off-site:** Enables the user to upload successful Web launcher configurations to Thycotic.com where they are approved and shared with other customers.
- **Default Theme:** Select the default Secret Server theme users see.
- **Enable CredSSP Authentication for WinRM:** Allow credential delegation for PowerShell scripts that may must access resources outside of the Secret Server machine.
- **Enable Launcher:** Enables Remote Desktop Launcher capabilities for Secret Server. See the [Launcher](#) section for further details.
- **Enable Syslog/CEF Logging:** Allow Secret Server to export logs to a SIEM tool server.
- **Enable Webservice:** Enable other applications to interact with Secret Server (still requires them to login as a Secret Server user).
- **Force Inactivity Timeout:** Used to time out a user's login after inactivity for the specified time interval. See [Configuring Users](#).

- **Force Password Masking:** For more information, see [Setting Up Password Masking](#).
- **Launcher Deployment Type:** Select either Protocol Handler (default) or ClickOnce.
- **Maximum Time for Offline Access on Mobile Devices:** Amount of time that a mobile device can be disconnected from the server before it removes cached Secret Server data from the device.
- **Prevent Application from Sleeping When Idle:** Prevents the application pool that Secret Server is running under from going to sleep.
- **Prevent Application from Sleeping When Idle:** Prevents the application pool that Secret Server is running under from going to sleep.
- **Require Folder for Secrets:** Enable this setting to force users to select a folder to place a secret in when creating or moving a secret. See [Folders](#) for more details.
- **Secret View Interval Minutes:** The number of minutes after which users must enter another comment when Require Comment is enabled.
- **Session Timeout for Webservices:** Set a session time limit on use of the Web services API. Once the Web services session token expires, the user must login again with their username and password.
- **WinRM Endpoint URL:** URL for WinRM, which is used for PowerShell hooks.

**Note:** No secret data is uploaded to Thycotic.com—only the website URL and control names are sent.

- **Default Secret Permissions:** See [Secret Folders](#) for more information.
- **Time Zone:** Time zone that all dates are displayed in.
- **Default Date, Time Format:** Default date and time format used for all users. This setting can be overridden by each user. See [User Preferences](#) for details.
- **Secret Password History:** Enforces whether a recent password can be set on a secret's password text-entry field based on the history. Defaults to 1, which means the same password cannot be immediately re-used on a secret.
- **Change Administration Mode:** This button takes you to a page where you can enable or disable Unlimited Administration mode.

## LOGIN TAB

The Login tab contains the following options:

- **Allow AutoComplete:** AutoComplete is a feature provided by most Web browsers to automatically remember and prefill forms for you. This can be a great security concern

since they typically do not save the data in a secure manner. You can enable or disable Web browser prefill on the Login page by using this option.

- **Allow Remember Me:** This option enables the Remember Me checkbox on the login page. When a user chooses to use "remember me," an encrypted cookie is set in their browser. This enables users to revisit Secret Server without the must login. This cookie is no longer be valid when the "remember me" period has expired, and users have to log in again.
- **Default Login Domain:** Allows for the selection of a default domain for user login.
- **Enable Duo Security Integration:** Enabling Duo integration allows users to use Duo two-factor authentication.
- **Enable Login Failure CAPTCHA:** Enforces a CAPTCHA image if the user fails one or more logins to prevent brute force attacks of user credentials or brute force lockouts.
- **Enable RADIUS Integration:** Enabling RADIUS integration enables another form of two factor authentication for users.
- **Enable SAML Integration:** Enabling SAML integration allows users to log-in to Secret Server using your SAML identity provider.
- **Maximum Login Failures:** Set the number of login attempts allowed before a user is locked out of their account. Once locked out, they need a Secret Server administrator to reset their password and enable their account.
- **Require Two Factor for these Login Types:** When enabled on a specific user logging into Secret Server, you can choose from a list to enable it for website, Web service, or both.
- **Visual Encrypted Keyboard Enabled:** Enables or disables the Visual Encrypted Keyboard for logins.
- **Visual Encrypted Keyboard Required:** Require the visual keyboard for logins.

## FOLDERS TAB

The Folders tab contains the following configuration options:

- **Enable Personal Folders:** Each user has a personal folder created and assigned to them.
- **Personal Folder Name:** The name of the root personal folder. Each user's personal folder is named based on the user.
- **Require View Permission on Specific Folder for Visibility:** Users only see folders they have view permissions on.
- **Show user warning message:** Enable warning message for users when creating secrets.
- **Warning Message Text:** Warning message to display to the users, instructing them to store only work-related data in Secret Server.

## LOCAL USER PASSWORDS TAB

This tab contains the following configuration options:

- **Allow Users to Reset Forgotten Passwords:** Allows users to reset their passwords in case they forget them.
- **Enable Local User Password Expiration:** Local user's passwords expire after a specified interval.
- **Enable Local User Password History:** Local users cannot change their password if it has been recently used.
- **Enable Minimum Local User Password Age:** Local users cannot change their passwords until the password meets a minimum age.
- **Local User Password is valid for:** Specifies the maximum time a local user can keep a password.
- **Lowercase Letters Required for Passwords:** Force all local users to include lowercase letters within their login passwords.
- **Minimum Password Length:** Require a minimum length on all local users' login passwords.
- **Numbers Required for Passwords:** Force all local users to include numbers within their login passwords.
- **Symbols Required for Passwords:** Force all local users to include special characters within their login passwords (%#@).
- **Uppercase Letters Required for Passwords:** Force all local users to include uppercase letters within their login passwords.

## SECURITY TAB

The Security tab contains the following configuration options:

- **Allow HTTP Get:** Allows the HTTP Get verb for Web services. This allows REST-style calls to many Web service methods but reduces security.
- **Enable FIPS Compliance:** See [FIPS Compliance](#).
- **Enable HSTS:** Enable HTTP Strict Transport Security. Not available if Force HTTPS/SSL is turned off.
- **Encrypt Key using DPAPI:** This encrypts the Secret Server AES 256 key using the machine key. It provides protection from admins copying Secret Server from the server to their own machine. Note that a backup of the encryption key should be made before using

this option. Otherwise, disaster recovery is impossible if the server dies. After encrypting the key, an administrator of Secret Server can decrypt it.

- **Force HTTPS/SSL:** Require HTTPS; users cannot access Secret Server using HTTP.
- **Frame Blocking:** Prevents users from accessing the Secret Server site if it is embedded in an iFrame.

## TICKET SYSTEM TAB

Secret Server can allow users to enter a ticket number when viewing a secret. This number can be validated through a regular expression, and can also be marked as required, if needed. Secret Server can integrate with third party ticket systems. For more information on the ticket system integration, see [Ticket System Integration with Secret Server \(KB\)](#).

You can add multiple ticket systems from the **Ticket System** tab. To add a new system, click **New Ticket System**.

You can make a select ticket system be Secret Server's default ticketing system by clicking on the link of the desired system, then clicking **Set as Default**.

## Ticket Number Validation

Secret Server can require users to enter a ticket number when viewing a secret. Admins can track access to secrets based on an external ticket system. On the **Ticket System** tab of the **Configuration** page, an administrator can enter the settings to match the ticket system.

After the ticket system is enabled in Secret Server, a user can enter a ticket number on the Comment screen or the Request Access screen.

The secret needs to have **Require Comment** or **Requires Approval for Access** enabled to allow the user to enter a ticket number. When a ticket number is required, this secret setting is displayed as "Require Comment/Ticket Number" on the Security tab.

Configurable settings:

- **Auditing:** The ticket number appears in the audit log and can be queried in reports. If the **View Ticket URL** has been set, the log shows the ticket number as a hyperlink linking to the external ticket system. Information on setting the URL can be found in [View Ticket URL Template Format \(KB\)](#).
- **View Ticket URL Template:** The format of the URL to be used for viewing the ticket. This is placed in the audit log so you can easily view the corresponding ticket from Secret Server. For details on this format, see [View Ticket URL Template Format \(KB\)](#).
- **Ticket Number and Reason Options:** This option allows fine-grained control of what the user must enter when **Require Comment** is enabled and ticket system integration is turned on.

- **Reason Only Required:** Ticket number is optional, reason is required.
- **Both Required:** Ticket number and reason are required.
- **Ticket Number or Reason Required:** Either ticket number or reason must be entered.
- **Ticket Number Only Required:** Ticket number is required, reason is optional.
- **Ticket Number Format Pattern (Regex):** A regular expression to use for validating the ticket number entered. This can help prevent typos in the number. For details on creating this expression, see the [Setting a Ticket Pattern Regex](#) (KB).
- **Ticket Number Label:** The text that displays next to the Ticket Number box on the Comment or Request Access page.
- **Ticket Number Validation Error Message:** The error message to display to the user when their entered ticket number fails the validation pattern regex.

## BMC Remedy Integration

Secret Server can integrate with BMC Remedy's Incident and Change Management. This integration includes validating ticket numbers, their status, and adding work detail items to the request.

The integration with BMC Remedy leverages the out-of-the-box, SOAP-based Web services that are installed with the ITSM product installation. These services must be installed on your mid-tier BMC Remedy server to allow for this integration if they are not already installed and configured.

### Requirements

- BMC Remedy SOAP Web Services enabled
- A username and password that has access to execute the Web services. This can be set up in the developer studio by accessing the application in the navigator and viewing Permissions for the CHG\_ChangeInterface\_WS or HPD\_IncidentInterface\_WS. This user should also have access to query requests and add work items to requests for the appropriate module.
- Secret Server environment needs to be able to connect to the BMC Remedy Web services via port 80 or 443. SSL is highly recommended because the SOAP messages contain a username and password.

### Testing Your Integration Setup

After configuring the ticket system (see configurable settings below), use the **Test Validation** button to verify that Secret Server can successfully access BMC Remedy. This button opens a dialog in which you can enter a ticket number from BMC Remedy. This validation process returns success or an error code. BMC Remedy may not return much detail in the error

message so you must look at the BMC Remedy API log to see a detailed error message, see [BMC Remedy Error Messages](#) (KB).

## Configurable Settings

### *Validating Ticket Status*

When a BMC Remedy request number is entered into Secret Server, the status of that request is retrieved to ensure that it is an open state. For example, if an incident number is entered that is in the "Closed" state, the user is informed that the ticket is closed.

Incident Management: Service Incident request cannot be closed or canceled. Change Management: Change management requests cannot be complete, closed, or canceled.

### *View Ticket URL Template*

The format of the URL to be used for viewing the ticket. This is placed in the audit log so you can easily view the corresponding ticket from Secret Server. For details on this format, see [View Ticket URL Template Format](#) (KB). Depending on your version of BMC Remedy, the URL to link directly to a request may be slightly different.

Incident management:

```
https://<midtier_server>//arsys/forms/<servername>/SHR%3ALandingConsole/Default+AdmSearchTicketWithQual&F304255610='Incident Number'%3D%22$TICKETID%22
```

Change management:

```
https://<midtier_server>//arsys/forms/<servername>/SHR%3ALandingConsole/Default+AdmSearchTicketWithQual&F304255610='Change Number'%3D%22$TICKETID%22
```

### *Ticket Number Format Pattern (Regex)*

Before even making a call to the BMC Remedy Web service, you can have Secret Server validate that the number matches a pattern. For example, your incident numbers might all be prefixed with "INC" and you want to ensure users enter the prefix. Some sample expressions to validate the ticket number are listed below:

Incident management: `^INC_CAL_[\d]{7}$`

Change management: `^CRQ_CAL_[\d]{7}$`

### *Ticket Number Validation Error Message*

The error message to display to the user when their entered ticket number fails the validation pattern regex.

### *Service Endpoint URL*

This is the URL for the SOAP-based Web services. Below are some samples for what is expected. You can find the actual endpoint using BMC Remedy Developer Studio and accessing

the correct application from the AR System Navigator and viewing the Web services section of the application.

Incident management: HPD\_IncidentInterface\_WS

Change management: CHG\_ChangeInterface\_WS

### *System Credentials*

Select or create a secret that contains the username and password for a user that has access to execute the SOAP Web services. The username and password are added to the authentication header for the SOAP request.

### *Authentication*

If your installation of BMC Remedy uses an authentication server, enter it in this text-entry field. Most installations allow this text-entry field to be blank.

### *Add Comments to Ticket*

Check this box if you want the comment that a user enters to be added to the request in BMC Remedy. This adds information such as the secret for which access is requested, who requested access, and the requester's comments.

### *Comment Work Type*

When a comment is added to a request as a work item, the Work Item type is required. "General Information" is selected by default, but all default Work Type options are supported.

## **ServiceNow Integration**

Secret Server can integrate with ServiceNow's Incident and Change Management service. This integration includes validating ticket numbers, their status, and adding Work Detail items to the request. The integration with ServiceNow leverages the out-of-the-box REST-based Web services.

### **Requirements**

- ServiceNow instance running the Eureka version or later with REST services enabled.
- A username and password that has access to execute the REST services, specifically GET and MODIFY on the following tables: Change Request and Incident.
- The Secret Server environment needs to be able to connect to the ServiceNow Web services via port 80 or 443. SSL is highly recommended because the REST messages authenticate with a username and password.

### **Testing your Integration Setup**

After configuring the ticket system (see configurable settings below), use the **Test Validation** button to verify Secret Server can successfully access ServiceNow. This button opens a dialog



in which you can enter a ticket number from ServiceNow. This validation process either succeeds or shows an error code.

## Configurable Settings

### *View Ticket URL Template*

The format of the URL to be used for viewing the ticket. This appears in the audit log so you can easily view the corresponding ticket from Secret Server. For details on this format, see [View Ticket URL Template Format \(KB\)](#).

Incident management: `https://<instance name>.service-now.com/nav_to.do?uri=incident.do?sysparm_query=number=$TICKETID`

Change management: `https://<instance name>.service-now.com/nav_to.do?uri=change_request.do?sysparm_query=number=$TICKETID`

### *Ticket Number Format Pattern (Regex)*

Before even making a call to the ServiceNow Web service you can have Secret Server validate the number matches a pattern. For example, your incident numbers might all be prefixed with "INC" and you want to ensure they enter this prefix. Some sample expressions to validate the ticket number are listed below:

Incident management: `^INC[\d]{7}$`

Change management: `^CHG[\d]{7}$`

### *Ticket Number Validation Error Message*

The error message to display to the user when their entered ticket number fails the validation pattern regex.

### *Instance Name*

This is the name of your instance in the format `https://<instance name>.service-now.com`.

### *System Credentials*

Select or create a secret that contains the username and password for a user that has access to execute the REST Web services. Secret Server uses these credentials to authenticate to ServiceNow.

### *Add Comments to Ticket*

Check this box if you want the comment that a user enters to be added to the request in ServiceNow. This adds information such as the Secret to which access is requested, who requested access, and their comments. The comment is added as a work note in the activity section of the request.

## PowerShell Integration

Secret Server can integrate with your ticketing system via PowerShell. This integration includes validating ticket numbers, their status, and adding comments. In our example we are connecting to a ServiceNow instance.

### Requirements

- PowerShell, see [Creating and Using PowerShell Scripts](#) (KB).
- Access to your ticket system via some API that can be accessed in PowerShell. This could be a REST API, SOAP API, or native calls.

### Configurable Settings

- **Run as Credentials:** In Secret Server a domain credential is required to execute the PowerShell script. This is a required text-entry field.
- **System Credentials:** The system credentials are specific to your ticketing system. Any secret using the username and password extended mapping can be used as your system credential. Additional arguments can be populated from this text-entry field on this secret and referenced in your script.
- **Ticket Number Format Pattern (Regex):** Before making a call to the PowerShell script you can have Secret Server validate the number matches a pattern. For example, your incident numbers might all be prefixed with "INC" and you want to ensure they enter this prefix. See [Setting a Ticket Pattern Regex](#) (KB).
- **Ticket Number Validation Error Message:** The error message to display to the user when their entered ticket number fails the validation pattern regex.
- **Validating Ticket Status:** To validate tickets you must create a PowerShell script to retrieve and validate the ticket. The integration uses arguments to pass custom values to your script. By default, we map some text-entry fields to the first set of arguments.
- **View Ticket URL Template:** You can configure the view ticket URL if you have a Web-based ticketing system to allow easy access to link to your ticketing system from Secret Server.

### Adding Comments to Tickets

To add a comment to tickets, create a script that does just that. The arguments are passed in the following order:

1. `$ticket = $args[0]`
2. `$comment = $args[1]`
3. `$user = $args[2]`
4. `$password = $args[3]`

5. `$url = $args[4]`

## Adding Comments to a General Audit Log

In addition to adding comments to specific ticket you may want general audit entries made in your ticket system. The arguments are passed in the following order:

1. `$comment = $args[1]`

2. `$user = $args[2]`

3. `$password = $args[3]`

## EMAIL TAB

The Email tab contains the following configuration options:

- **Domain:** The domain of the credentials to use (optional).
- **Email Server:** Specify the domain name or IP address of your SMTP server. For example: `smtp.yourcompany.com`.
- **From Email Address:** The return email address for Secret Server emails.
- **Use Credentials:** Whether to use credentials when sending emails. Requires username and password to be entered when enabled.
- **Use Custom Port:** Whether to use a custom port when sending emails. Requires a custom port to be specified when enabled.
- **Use SSL:** Whether to use SSL when sending emails.

## SESSION RECORDING TAB

The Session Recording tab contains the following configuration options:

- **Enable Deleting:** After the "Days Until Deleting" value, Secret Server deletes the videos from disk.
- **Enable Moving to Disk:** After the "Days Until Moved to Disk" value, Secret Server can move videos from the database to an archive path on disk.
- **Enable Session Recording:** Enable session recording for launched sessions.
- **Save Videos To:** By default, videos are stored in the database, Secret Server can also store them directly to a network share. This network share must be accessible from all Web servers that Secret Server is installed on.
- **Video Code:** Specify the codec to use to create the videos from the launcher screenshots. This codec must be installed on the Web server (or servers if clustering is enabled) that Secret Server is installed on.

**Note:** The Microsoft Video 1 codec is for testing only and does not support in browser playback. Sessions encoded with Microsoft Video 1 can still be downloaded for review.

For details on the settings in the Login and "Local User Passwords" tab, see [Configuring Users](#).

## **HSM TAB**

From the Hardware Security Module (HSM) tab, you can enable or disable HSM for encryption. For more details about HSM configuration, see our [HSM Integration Guide](#) (PDF).

# Administration Auditing

Secret Server keeps a detailed audit history for users and secrets. Secret Server implements a detailed tracking system for actions made on secrets. Auditing users is an indispensable component of any password management system. The audit trail allows administrators to know which secrets were accessed and ensures that secrets are being properly used. Additionally, the User Audit report helps SEC regulated companies comply with the Sarbanes Oxley Act of 2002 as well as other regulatory compliance mandates.

## VIEWING A USER AUDIT REPORT

1. From the **Reports** page, click the **User Audit** tab.
2. From the dialog on the tab, select a user and a date range to view.
3. Click **Search History** to view the user's audit trail.

The audit search displays results for all the secrets the selected user has viewed or edited during the selected time period. The administrator has the option of expiring all the viewed secrets, to notify users to change sensitive information, or to force password changing (if the RPC is configured).

To get a full view of the actions taken on a secret, select that secret from the results list. The secret audit displays the specific user actions for a secret.

## SECRET AUDIT LOG

The audit log for a secret can be accessed by clicking the **View Audit** button on the **Secret View** page or navigating from the User Audit report. The log shows the date, the username, the action, and any other details about the event. Secret auditing provides a detailed view of each change or view on a secret.

Secret Audits are taken for the following user actions:

- Adding, updating and removing secret dependencies
- Check out
- Editing permissions
- Forced expiration
- Hide launcher password changes
- Set for check-in
- Update
- View

For certain audit items, action notes are added providing additional details. For example, if permissions are edited, an audit record is generated detailing which users or groups gained or lost permissions. Detailed audit records add accountability to sensitive secrets where auditors or administrators must know exactly what was modified.

Below the audit records is a checkbox for Display Password Change Log. Clicking to select this check box displays logs for Heartbeat and Remote Password Changing amongst the audit items.

## **REPORT AUDITING**

In addition to the user audit and individual secret audit, the reporting feature provides a series of activity, user, and secret reports. See [Built-In Reports](#) (KB) for the most up-to-date list of reports included.

**Note:** Users can also create their own, custom reports. See [Creating and Editing Reports](#).

# Backup and Disaster Recovery

Secret Server supports manual and scheduled database and IIS directory backups. The database access settings support SQL Mirror and automatic failover. As an additional disaster recovery measure, administrators can export secrets to a CSV spreadsheet.

## BACKUP SETTINGS

The following configuration options are available on the **Tools | Backup** page of Secret Server:

- **Backup Database File Path:** This folder must be accessible by the SQL server and stores the database .bak file.
- **Backup File Path:** This directory must exist on the Web server and stores the zip file of the application directory.
- **Database Backup SQL Timeout (Minutes):** Number of minutes that Secret Server waits for the database backup to complete successfully before timing out.
- **Enable Scheduled Backup:** Enables automatic backups on a set schedule.
- **Keep Number of Backups:** Number of previous backups to keep.
- **Notify Administrators on Backup Failure:** Users with the Administer Backup role permission are notified if the backup fails.

## FOLDER PERMISSIONS

From the **Backup Administration** page, specify the correct directory paths for the IIS Secret Server file directory and the database backups to be stored. The backup path must be local to the server where the Secret Server database or file directory exists. The directories must also have the proper permissions to allow Secret Server to automatically store backups at those locations. The account that requires permission is displayed as an alert on the Backup page.

## MANUAL BACKUPS

On the **Backup Administration** page, click **Backup Now** to force an immediate backup. This is useful for testing the backup settings and is recommended to be done before upgrading.

## SCHEDULED BACKUPS

"There are numerous options to consider when backing up Secret Server. Backups can be scheduled to run on a specific time interval. To prevent the directory from growing too large, the number of backups to keep can be defined as well. Depending on size constraints or preferences of the DBA, the database backup can either truncate the transaction log or keep it intact. The additional schedule settings are available when "Enable Schedule Backup" is enabled, and the view page indicates the time and date of the next scheduled backup.

## FILE ATTACHMENT BACKUPS

Files uploaded to secrets can be backed up using the standard Secret Server backup function. Upon backup completion, they retain their encrypted status and are inside the application backup file (the .zip file).

## EXPORTING SECRETS

From within the **Administration > Export** page, select the folder that needs to be exported. By default, all secrets are exported if a folder is not selected. If no folder is selected, all secrets are exported by default. The administrative password must be entered, as it is a security measure to verify the permission of the user performing the export.

**Note:** Only the secrets the user has view access to are exported.

Exports can be configured further with options to "Export with Folder Path" and "Export Child Folders." Export with Folder Path adds the full folder path to the export. Folder paths in the export file provide organizational structure if secrets must be imported later.

By default, the option to "Export Child Folders" is active. While this option is enabled, any export of a specified folder also exports content located in folders beneath the initial selection.

## Exported File Format

Secrets are exported as a comma-separated-value (CSV) file or as XML. The CSV file can be easily handled in Excel or other spreadsheet applications. The file is grouped by secret template and each cluster of secrets has a header row that contains the template text-entry field names followed by all exported secrets based on that template.

The XML file follows the exact structure of the advanced xml import. As such, this can be useful with migrating data from one Secret Server installation to another.

Secrets are exported in the exact structure as a secret Import. If exports are maintained, an installation of Secret Server can be completely reproduced on a separate instance by applying the exported file.

## Recovery

Recovery requires using the application and database backups. To restore Web application directory, extract the root directory to the Web server. The encryption.config file is most important for being able to read the contents of the database. The SQL database can be restored using the standard process in SQL Server Management Studio from the .bak file.

**Note:** For detailed instructions, see the [Restoring Secret Server from a Backup](#) KB article.

## UNLIMITED ADMINISTRATION MODE

*Unlimited administration mode* is a feature designed to allow an administrator access to all secrets and folders in their Secret Server instance without explicit permission. This can be



used in the instance a company has an emergency where access to a secret is needed when no users who have permission are available. Alternately, it can be used when company policies require administrators to have access to all information in the system.

**Note:** An alert visible to all users displays at the top of the Secret View page when unlimited administration mode is enabled.

For a user to be an unlimited administrator they must be assigned a role with the Unlimited Administrator permission and Unlimited Administration Mode must be enabled in Configuration settings.

To navigate to the **Unlimited Administration** section, select **Configuration** from the **Administration** menu, and then click **Change Administration Mode**. We recommend administrators have specific permissions to folders and secrets and this mode is only used temporarily to assign the correct permissions.

**Note:** Changes to the administration mode are logged in an audit grid. The grid shows the user, time of the change, and any notes made by the user.

# Events and Alerts

## SYSTEM LOG

The System Log is used to communicate the different events that are occurring while Secret Server is executing. It can be helpful in troubleshooting unexpected behavior. The system log can be enabled by clicking **Edit** and checking the **Enable System Log** check box on the **Administration > System Log** page.

System log parameters include:

- **Maximum Log Length:** This is the maximum number of rows to keep in the system log table in the SQL database. When it reaches that amount, it is reduced by 25%.
- **Notify Administrators when System Log is Shrunk:** This setting is used to send an email to all system log administrators when the system log has been truncated. A system log administrator is any user in a role with the Administer System Log permission included.

To clear the system log of all its records, click **Clear**.

## EVENT SUBSCRIPTION PAGE

- **Additional Email Recipients:** List of additional email addresses to send the email to.

**Note:** These entries are meant to be outside of the users' email addresses as known to Secret Server. One of these might be, for example, the user's home email address.

- **Send Email Alerts:** Sends an email to both users and all the users contained in the groups for this subscription. It also sends an email to all email addresses in the Additional Email Recipients list (see below).
- **Send Email with High Priority:** Sends the email for this subscription with high priority set.
- **Subscribed Events:** List of the events that are contained in this subscription.
- **Subscribed Users:** List of the Secret Server users and groups subscribed to this event.
- **Subscription Name:** Name for the subscription.

## Creating Event Subscriptions

To add an event subscription:

1. Navigate to **Administration > Event** Subscriptions.
2. Click **New**.
3. In the **Subscription Name** text box, enter a name for this new event subscription.

4. Add users and groups to this subscription by selecting them from the **Add New** list. They are added to the **Subscribed Users** list above the **Add New** list.
5. Add events to this subscription by adding rows to the **Subscribed Events** data grid. To do this, select an entity type from the list in the **Entity** column of the first row.
6. After an entity is chosen, you can now select an action, such as Create, Delete, or Edit Permissions.
7. After an action is selected, a condition may be available. Select the condition you wish to implement.
8. To add this event to the subscription, click the button. This must be done before **Save** at the bottom of the page is clicked in order to add this event to the subscription.
9. Click **Save**.

## Editing a Subscription

To edit an event subscription:

1. Navigate to **Administration > Event Subscriptions**, click the subscription name, and then **Edit**.
2. To remove a subscribed user, group, or event, click the button next to the entry in the appropriate list.
3. To add entries to either list, see "Creating Event Subscriptions."
4. Click **Save** to save all changes.

## Deleting a Subscription

To delete an event subscription:

1. Navigate to **Administration > Event Subscriptions**.
2. Click the subscription name.
3. Click **Delete** on the following page.

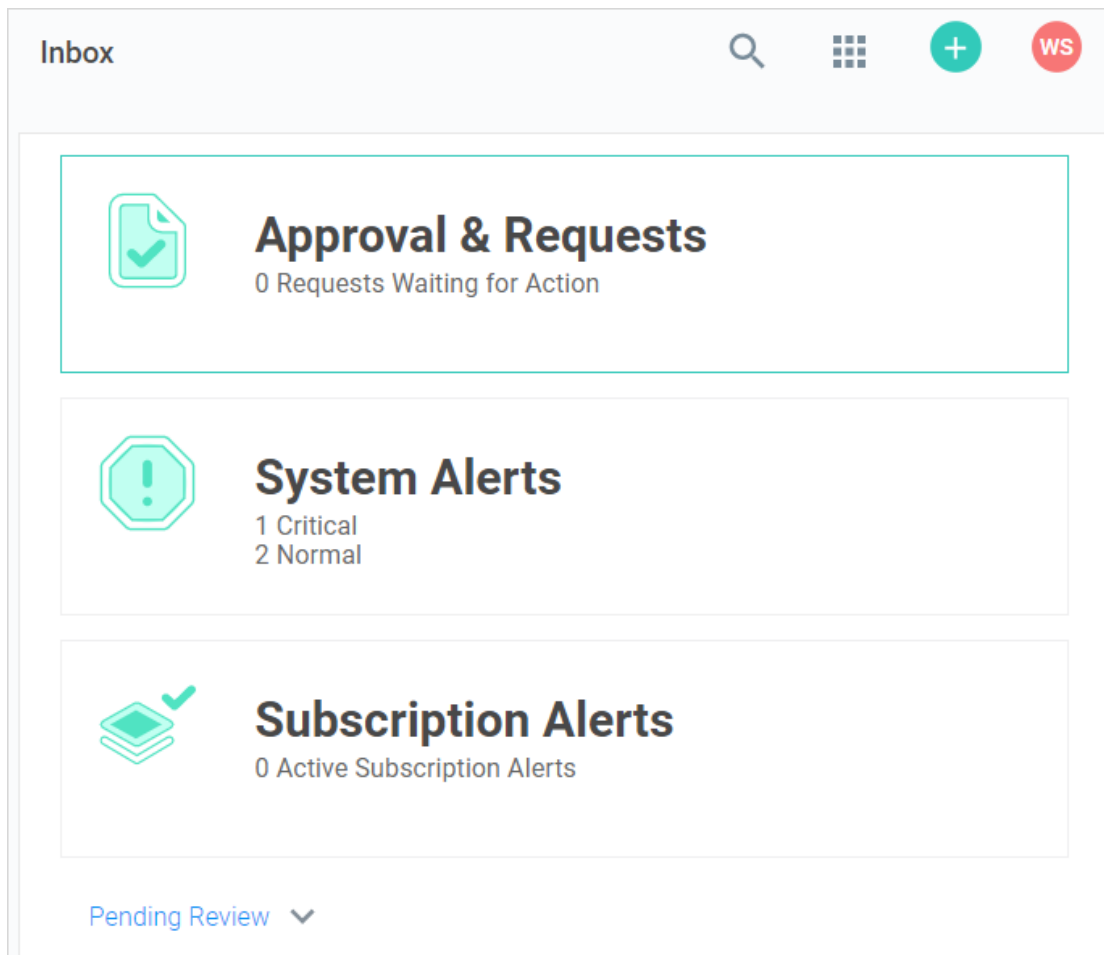
## VIEWING EVENT SUBSCRIPTION LOGS

To view the events that have been triggered in a subscription, navigate to **Administration > Event Subscriptions** and click **View Audit**. In the Event Subscription Activity list, the most recent events to have been triggered are on top of the list. To select a specific time frame, click the **...** buttons and select start and end dates at the top of the page. Click **Update Report** to return the corresponding log entries.

**Note:** It may take a few seconds for the events to make it into the log.

## ALERT NOTIFICATION CENTER (INBOX)

The *Alert Notification Center* page shows event subscriptions, access requests, and other configuration alerts in a single interface. You can access the alert notification center by clicking the **Inbox** button on the main menu.



Event subscriptions disappear from the notification center after you view them. System alerts and access requests stay active until resolved.

## CEF AND SIEM INTEGRATION

Secret Server can log to a Comment Event Format (CEF) or Syslog listener. When this is configured, all event engine events and important system log entries are sent to the CEF or Syslog server that is entered in the configuration. The written events contain data such as user information, time, IP address, and any other important details about the event.

### Configuring CEF

1. To configure CEF:

2. Navigate to Administration > Configuration.
3. Click **Edit**.
4. Check the **Enable Syslog/CEF Logging** check box. When you do this, three additional text boxes or lists appear:
  - **Syslog/CEF Server:** IP address or name of the server.
  - **Syslog/CEF Protocol:** Either UDP or TCP, the protocol used by your server.
  - **Syslog/CEF Port:** Server port for sent events.
5. Complete or configure those controls.
6. Click **Save**.

## Testing CEF

After enabling CEF, your server should start to receive messages right away if you entered the data correctly. In order to force an event to happen, perform a log out and then log back in. If the event does not appear on your CEF server soon after, there is something wrong with your configuration.

# Customizing Secret Server's Appearance

By default, Secret Server is set to a default theme unless specified within the Configuration settings. Secret Server comes with three other bundled themes: Blue, Dark, and Green. The default theme can be set at **Administration > Configuration** on the general tab. Theming differences can be allowed by individual users with the **Allow User to Select Themes** permission.

## CREATING THEMES

Themes are controlled from the Theme Roller. To create a custom theme, go to Admin | More | Themes. For detailed instructions on using the Theme Roller please see this KB guide.

## EMBEDDED MODE

*Embedded mode* removes the header and footer to allow Secret Server to be more easily placed within a frame. To activate embedded mode for the session, add an `embedded=true` query string parameter to the URL when accessing Secret Server. For example, if you normally access Secret Server by going to:

<https://myserver/secretserver/login.aspx>,

then you can enable embedded mode by going to:

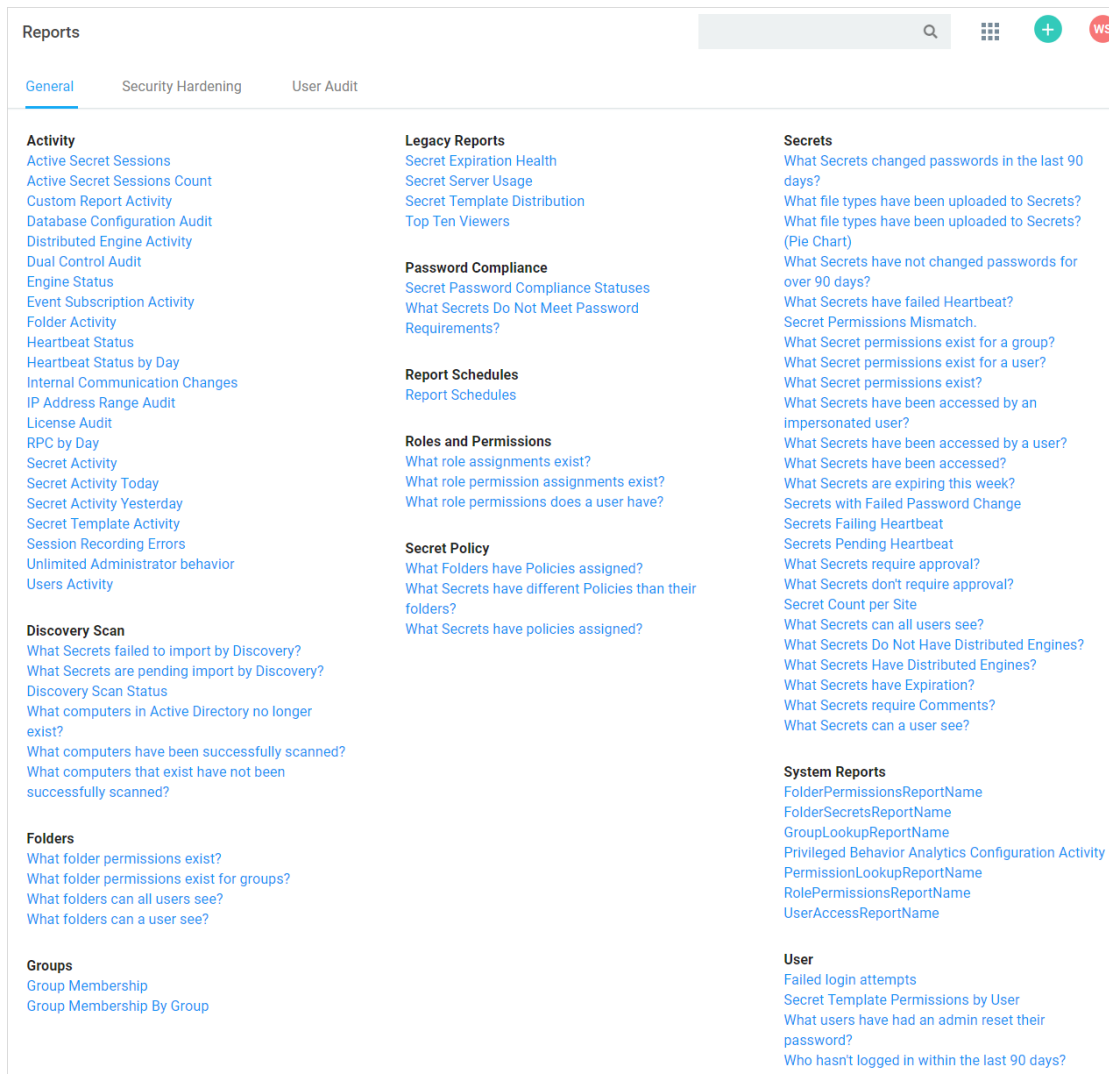
<https://myserver/secretserver/login.aspx?embedded=true>.

This parameter can be added to the URL on any page in Secret Server. To disable embedded mode simply change the query string to `embedded=false`.

# Secret Server Reports

The reporting interface comes with a set of standard reports. These reports include a variety of 2D and 3D charting and graphing components and a full grid of data. Some of the reports are purely data detailed and have no charts. You can also create your own reports based on any Secret Server data, such as user, audit, permissions, and folders. You can create report categories to aid in the organization of your reports. Reports can be arranged to provide access to auditors and meet compliance requirements. These reports can be accessed in the **General** tab on the **Reports** page.

**Figure:** Reports Page



The *Security Hardening Report* checks aspects of Secret Server to ensure security best practices are being implemented. While Secret Server runs with all the items failing,

administrators should be aware of possible security issues within an installation. For details on this, see [Reports Security Hardening Tab](#).

The User Audit Report shows all secrets accessed by a user during a specified period. For a detailed explanation of this, see [User Audit Report](#).

## REPORTS GENERAL TAB

See [Built-In Reports](#) (KB) for the most up-to-date list of reports included.

The reports are listed under the report categories. To view a report, click on its name. This takes you to the **Report View** page.

You can view a record of all the actions performed on reports by clicking on the **View Audit** button. For more information on this, see [Administration Auditing](#).

For details on **Edit**, see [Creating and Editing Reports](#).

The **Create it** link is a shortcut for creating a new report.

You can adjust the look of the Reports View page. The report categories as well as the reports can be rearranged on the page. To do this, click **Edit** on the Reports page.

## Modifying Report Categories

For details on the Show Deleted button, see [Deleting or Undeleting Reports](#).

- **Rearrange:** Any item with the icon can be dragged and dropped to a new location. Report categories can be moved anywhere within the page. Reports can be moved from one report category to another.
- **Create New:** Click **Create Report Category** and specify a category name and description on the following page. Note that the Report Category Description is used as the tooltip for the report category on the Reports View page.
- **Delete:** Click the icon next to the report category name. This deletes all the reports in the category. To undelete the reports, see [Deleting or Undeleting Reports..](#)
- **Edit:** Click the icon next to the report category name to change the name or description of the category.

## Creating and Editing Reports

There are two ways to create a Report. From the Reports Edit page, click the **Add New** link at the bottom of a Report Category. Or alternatively, from the Reports View page, click the **Create it** link at the bottom of that page.

To edit a Report, navigate to the Report View page and click **Edit**.

**Note:** The SQL script text cannot be edited for standard reports.



Below is an explanation of the different text-entry fields for the Report Edit page:

- **Report Name:** Name that is displayed on the Reports page as a link underneath its containing category.
- **Report Description:** Description for the Report. This is displayed in the Report View page. It is also used as the Tooltip for the Report name on the Reports page.
- **Report Category:** Selection for which Report Category to place the Report into.
- **Chart Type:** Type of chart to use for displaying the results. If set to None, a grid displays.
- **3D Report:** Specify a 3D style to render the chart in.
- **Page Size:** Page size limit setting for the data displayed in the grid.
- **Report SQL:** SQL script that is used to generate the report.

Reports support the embedding of certain parameters into the SQL to give the user the ability to dynamically change the resulting data set. Another option available for custom reports is to apply a different color to returned rows dependent on certain conditions. For more information as well as examples, see the [Using Dynamic Parameters in Reports](#) KB article.

You can show Secret Server's SQL database information to assist with creating custom reports. By selecting the SQL Table from the list, the details of the table's columns display in a grid. Click the **Show Secret Server SQL database information** link to see the SQL Table list and SQL Table Columns grid. Click **Preview** at the bottom of the page to see a preview of the chart. The resulting chart displays in the Report Preview section at the bottom of the page.

## REPORT PAGE

### Viewing Reports

On this page you see the graph, chart, grid, etc. for the report. To see a grid representation of the report, click the **Show Data** link to expand that area. If there is no data, then no graph is visible and the text "There are no items" displays in the Show Data section.

Some reports use dynamic values like user, start date, and end date. Adjust these values to generate the report you need. Click the **Update Report** button to generate the new report.

**Edit** allows you to alter the report to fit your requirements. See the Creating and Editing a Report section below for details.

### Deleting or Undeleting Reports

To delete or undelete a report.

- **Delete:** To delete a report, click **Delete**.

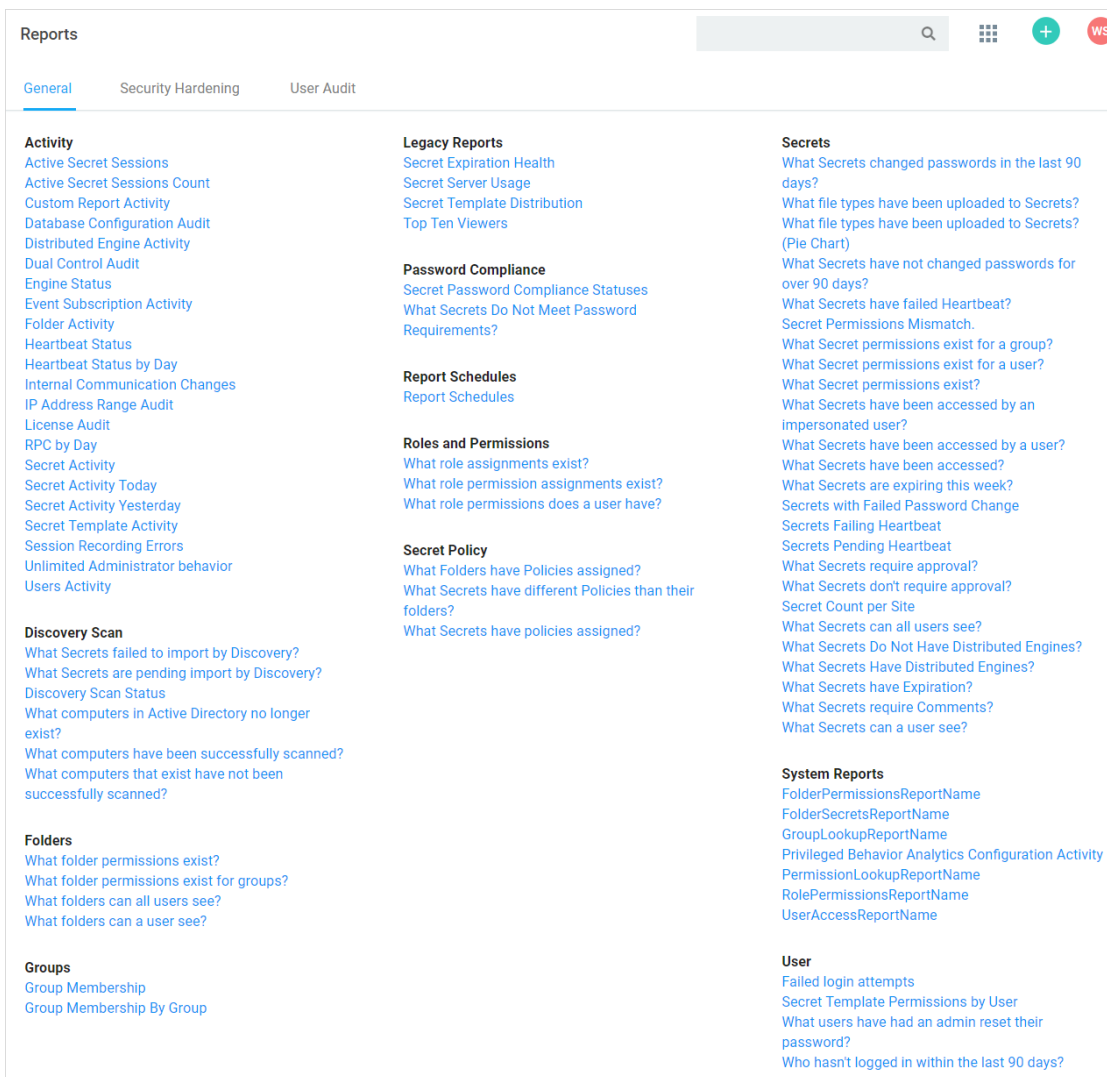
- **Undelete:** To undelete a report, you must navigate to the Reports Edit page as deleted reports are not visible on the Reports View page. On the Reports Edit page, click the **Show Deleted** button. This displays a Deleted Report category, which contains all the deleted reports. Either drag the report to a report category that is not deleted or click the report name to go into its Report View page. In there, click the **Undelete** button.

## Viewing Auditing for a Report

You can view a record of all the actions performed on a report by clicking on the View Audit button. For more information, see [Administration Auditing](#).

## Saving Reports to File

1. Click the **Reports** menu item. The Reports page appears:



2. Click the link for the desired report. Its page appears:



## Export

Please enter your password for security purposes.

Folder

 [No Selected Folder](#)

Password

\*

Export with Folder Path

Export Child Folders

Export Format

CSV  XML

Enter any additional notes or explanations for the export.

 **Export**

4. Click the **No Selected Folder** link to choose a folder.
5. Type your Secret Server password to ensure "you" are you.
6. Click the **Export with Folder Path** check box to recreate the secret folder hierarchy in the OS folder.
7. Similarly, click the **Export Child Folders** check box to include any child folders.
8. Click the **Export Format** option button to select an output folder type.
9. Type any notes in the unlabeled note text box.
10. Click the **Export** button.

## SCHEDULED REPORTS

### Creating New Schedules for Reports

1. To create a schedule for a report, click **Schedule** on the **Report View** page. The Custom Report Schedules page appears.
2. Click the **Create New** button.

### Viewing Existing Report Schedules

1. To view existing schedules for a report, click **Schedule** on the Report View screen. A list of existing schedules for the report appear in the grid.
2. To view the details of a schedule, click the schedule name in the grid.
3. (Optional) Deleted schedules can be made visible by checking the **Show Deleted** box at the bottom of the grid.
4. Click the **View** link in the History column of the grid to view the history of all generated reports for that schedule.

### Editing Schedule Settings

When viewing a report, click Schedule and then the name of the report schedule to modify it. The following configuration options are available:

- **Schedule Name:** This is the name of the schedule for the report. This name must be unique to the Secret Server installation.
- **Health Check:** This sends an email notification only when the report contains data.
- **Recurrence Schedule:** This specifies the schedule runs every X number of days, weeks, or months, with the option to specify days of the week or month as well. The date and time that the report schedule is effective can be specified in this section as well.

- **Save Generated Reports:** This saves the history of generated reports in the database for later viewing. Enabling this setting also allows you to specify the number of generated reports to save.
- **Send Email:** Secret Server sends an email containing the generated report every time the schedule runs. Enabling this setting also allows you to specify whether the email is sent with the high priority flag and a list of Secret Server users or groups that receive the generated report email. Add additional email recipients in the text box below the subscribers, separating recipients with a semi-colon.

The following configuration options appear if the report being scheduled contains at least one dynamic parameter in the SQL of the report:

- **User Parameter Value:** Value of the #USER parameter to set in the report when it is generated.
- **Group Parameter Value:** Value of the #GROUP parameter to set in the report when it is generated.
- **Start Date Parameter Value:** Value of the #STARTDATE parameter to set in the report when it is generated.
- **End Date Parameter Value:** Value of the #ENDDATE parameter to set in the report when it is generated.

## REPORTS SECURITY HARDENING TAB

The Security Hardening Tab configures aspects of Secret Server to ensure security best practices are being implemented. While Secret Server runs with all the items failing, administrators should be aware of possible security issues within an installation. Below is an explanation of the different features:

- **Browser AutoComplete:** Browser AutoComplete allows Web browsers to save the login credentials for the Secret Server login screen. These credentials are often kept by the Web browser in an insecure manner on the user's workstation. Allowing AutoComplete also interferes with the security policy of your Secret Server by not requiring the user to re-enter their login credentials on your desired schedule. To prevent the AutoComplete feature, disable the Allow AutoComplete option on the Configuration page.
- **Force Password Masking:** Password masking prevents over-the-shoulder viewing of your passwords by a casual observer (when masked, passwords show as \*). To activate this option, click to select the **Force Password Masking** option on the **Configuration** page.
- **Frame Blocking:** Frame blocking prevents the Secret Server site from being placed in an iFrame. This is to prevent clickjacking attacks. There may be legitimate reasons for placing Secret Server in a frame, such as embedding the UI in another site. To turn frame blocking on, enable the setting under the Security tab in Configuration.

- **Login Password Requirements:** Login passwords can be strengthened by requiring a minimum length and the use of various character sets. A minimum password length of 8 characters or longer is recommended. In addition, all character sets (lowercase, uppercase, numbers and symbols) are required to get a pass result. Turn on these login password settings on the Configuration page.
- **Maximum Login Failures:** The maximum number of login failures is the number of attempts that can be made to login to Secret Server as a user before that user's account is locked. A user with user administration permissions is then required to unlock the user's account. The maximum failures allowed should be set to 5 or less to get a pass result. Change the "Maximum Login Failures" settings on the Configuration page.
- **Remember Me:** Remember Me is a convenience option that allows users to remain logged in for up to a specific period. This setting can be a security concern as it does not require re-entry of credentials to gain access to Secret Server. Turn Remember Me off on the Configuration page to get a pass result. It must be set to be valid for 1 day or less to not get a fail result.
- **SQL Server Authentication Password Strength:** SQL Server authentication requires a username and password. The password must be a strong password to get a pass result. Strong passwords are 8 characters or longer and contain lowercase and uppercase letters, numbers and symbols. The SQL Server authentication credentials in use can be changed by going to the installer (installer.aspx) and changing them on Step 3. A pass result is also given if Windows authentication is used to authenticate to SQL Server.
- **SQL Server Authentication Username:** The SQL Server authentication username should not be obvious. The use of "sa", "ss" or "secretserver" triggers a fail result. The SQL Server authentication credentials in use can be changed by going to the installer (installer.aspx) and changing them on Step 3. A pass result is also given if Windows authentication is used to authenticate to SQL Server.
- **Windows Authentication:** Windows authentication takes advantage of Windows security to provide secure authentication to SQL Server. The SQL Server authentication options can be changed by going to the installer (installer.aspx) and changing them on Step 3. Please see the [Installation Guide](#) for instructions on configuring Windows authentication to SQL Server.
- **Require SSL:** Secure Sockets Layer (SSL) is required to ensure that all communication between the Web browser and Secret Server is encrypted and secure. Once the SSL certificate is installed, Force HTTPS/SSL in Configuration to get a pass result. Please see the [Installing a Self-Signed SSL/HTTPS Certificate](#) Knowledge Base article for instructions.

**Note:** SSL needs to be running with at least a 128-bit key size to get a pass result. A warning result indicates your key size is less than 128 bits. A fail result indicates you are not using SSL.

## REPORTS USER AUDIT TAB

User Audit Reports show all secrets accessed by a user during a specified period. For a more detailed explanation, see [User Audit Report](#).

## REPORTING AND DUAL CONTROLS

If there are requirements around protecting potentially personally identifying information when running reports or viewing recorded sessions, you can enforce that another user has authorized you by enabling dual control for a secret or Report. You can configure Dual Controls by clicking **Admin** and then **Dual Controls**.

**Note:** Dual Controls is not in the **Admin** dropdown and must be accessed from the full administration menu.

When enabled a user in the approver group must enter in their credentials before a report or session can be viewed:

Once the approver has entered their credentials, the resource can be accessed. The following resources can have dual control applied.

- **Access Report:** Protects any report from the General tab of the Reports view.
- **Access User Audit Report:** Protects the user audit report for any user.
- **Create Report:** Requires dual control for anytime a user creates a custom report.
- **Secret Session Access:** Requires dual control for any recorded or live sessions for a secret



## Server Clustering

Secret Server can run with multiple front-end Web servers. For a critical instance, clustering offers a redundant system to limit potential down time from a single point of failure. Clustering also allows users to load balance for better performance. For instructions on enabling clustering in Secret Server, see [Setting up Clustering](#).

# General Encryption and Security

## ADVANCED ENCRYPTION STANDARD

Secret Server uses different types of encryption to ensure data security. Every text-entry field, except name, on a secret is encrypted at the database level with the Advanced Encryption Standard (AES) 256-bit algorithm. Database encryption prevents unauthorized access of sensitive data on the server.

The AES encryption algorithm provides a high security level for sensitive data. The National Institute of Standards and Technology (NIST) and National Security Agency (NSA) search for a replacement for the Data Encryption Standard (DES), which had numerous issues, namely small key size and efficiency, and finally settled on AES.

**Note:** Encryption algorithms use keys to obfuscate the data. While DES only had a key size of 56 bits, AES can have a key size of 128, 192 or 256 bits. Larger keys provide more security as their size makes brute force attacks infeasible.

**Note:** To address concerns from the cryptographic community, NIST embarked on a transparent selection process. During the selection process NIST solicited designs from the global cryptographic community and voted for a winner from within fifteen finalists. The eventual winner was a team of Belgian cryptographers with their submission of the Rijndael encryption method, which became AES. For more information about the technical specifications of AES, please see the official standard.

## SSL CERTIFICATES

Secret Server can be configured to run using Secure Sockets Layer (SSL) certificates. We strongly recommend that Secret Server installations run using SSL. Not using SSL significantly reduces the security of the contents of Secret Server since browsers viewing the site are not using an encrypted connection.

## SECURITY COMPLIANCE STANDARDS

### FIPS Compliance

The Federal Information Processing Standard 140-1 (FIPS 140-1) and its successor (FIPS 140-2) are United States Government standards that provide a benchmark for implementing cryptographic software. Secret Server has been tested within environments that are FIPS compliant. For instructions to enabling FIPS in Secret Server, see the [Enabling FIPS Compliance in Secret Server](#) KB article.

### PCI Datacenter Compliance

Secret Server can make it easier to comply with PCI-DSS requirements:

- **Requirement 8:** Assign a unique ID to each person with computer access: Secret Server helps you comply with Requirement 8 by providing a secure repository for you to maintain

an automated password changing schedule, forcing each user to have a unique, secured password. Secret Server's Web-based access makes it easy to access these passwords.

- **Requirement 10:** Track and monitor all access to network resources and cardholder data: Secret Server can monitor all access to network resources. By employing remote password changing to force password changes, administrators can monitor and update network resources on a customized scheduled. You can create a password changing schedule that best suits your environment.
- **Requirement 11:** Regularly test security systems and processes.
- **Requirement 12:** Maintain a policy that addresses information security: You can optimize Secret Server's software's global configuration and template-driven data structure to fit the requirements of your current information security policy or assist in creating a policy based on Secret Server. Configuration options include:
  - Applying two-factor authentication
  - Enabling launchers
  - Enabling Web services
  - Enforcing local-user password requirements
  - Forcing HTTPS/SSL
  - Requiring folders for secrets (for uniform permissions)

## HSM INTEGRATION

You can configure Secret Server to use a Hardware Security Module (HSM). The HSM is a hardware device which handles the encryption and decryption in hardware. Because the encryption keys are stored within the hardware device itself (and never leave the device), an HSM increases the security of the encrypted data. Supported HSMs include SafeNet, Thales PCI, or Network HSMs. You also use paired PCI HSMs for failover. SafeNet and Thales HSM's are FIPS 140-2 certified and are the type of HSM most typically used by government and military customers.

Secret Server does not require an HSM to function, but it is available as an option for environments that require the highest levels of security. For information about configuring an HSM with Secret Server see the [HSM Integration Guide](#).

## KEY ROTATION

*Key rotation* is the process where the encryption key used for securing secret data is changed and secret data is re-encrypted. Each secret receives a new, unique AES-256 key. Secret key rotation can be used to meet compliance requirements that mandate encryption keys be changed on a regular basis. Secret Key Rotation requires the Rotate Encryption Keys role permission.

To perform secret key rotation:

1. Go to the **Admin** menu and select **Configuration**.
2. Click the **Security** tab.
3. Under the **Key Rotation** section, click **Rotate Secret Keys**.

Secret key rotation begins as soon as Secret Server enters Maintenance Mode. Because Maintenance Mode disables some functions, we recommend running secret key rotation during off-peak or non-business hours. To learn more about Maintenance Mode, see the Maintenance Mode KB article. For further details about the processing time for key rotation, see The Secret Key Rotation KB article.

# Two-Factor Authentication

Users who access Secret Server from laptops or other mobile devices are more vulnerable to having a device stolen. Requiring multiple forms of authentication provides additional security against theft or attempts to crack a user's password.

*Two-factor authentication* (2FA) is a method of strong authentication that requires two different forms of identification instead of the traditional single password. The types of two-factor authentication supported by Secret Server include the following:

- **Email:** A one-time pin code is emailed to the user. For further information, see [Email Two-Factor Authentication](#).
- **RADIUS:** Users are prompted for their RADIUS password or token as second factor of authentication.
- **Mobile Application or Soft Token:** Users are prompted to configure their mobile app or soft token using either Duo Security or TOTP RFC6238, such as Google Authenticator or Microsoft Authenticator.
- **Duo:** A Duo notification is sent to a Duo app on the approver's phone.

## EMAIL TWO-FACTOR AUTHENTICATION

Secret Server uses this design by allowing administrators to require two-factor authentication through a confirmation email for designated users.

To configure email two-factor authentication:

1. From the Users administration page select a user to configure.
2. Click **Edit**.
3. Click to select the Email Two Factor Authentication box.
4. Click **Save**.
5. Verify that the correct email address information is set, as that address is where the confirmation email is sent:
6. The next time that user attempts to login to the system, a unique confirmation code is emailed to them.
7. The user is then required to enter a new confirmation code at each login:

## RADIUS AUTHENTICATION

Secret Server allows the use of *Remote Authentication Dial-In User Service* (RADIUS) two-factor authentication on top of the normal authentication process for additional security needs.

Secret Server acts as a RADIUS client that can communicate with any server implementing the RADIUS protocol.

## Configuring RADIUS

Set up RADIUS on the **Login** tab of the **Configuration** page. This requires enabling RADIUS Integration, specifying the server address, the ports, and the RADIUS shared secret. The shared secret is a specific term for RADIUS clients and is not a reference to secrets in Secret Server.

You can customize the RADIUS "Login Explanation" to give users detailed instructions for entering their RADIUS information.

Once enabled, the **Test RADIUS Login** button appears on the **Login** tab for testing the communication with the RADIUS Server. If you have a failover RADIUS Server, you can specify it by clicking the **Enable RADIUS Failover** checkbox and entering the required information. If the primary RADIUS server cannot be accessed, the failover server is be used.

## Enabling RADIUS for a User

After enabling RADIUS on your Secret Server, you must enable RADIUS two-factor authentication for each user on a per-user basis. On the **User Edit** page, type the **RADIUS User Name** for this user to match the RADIUS server. RADIUS can be enabled for new users by domain, see [Adding Domains](#).

## TOTP TWO-FACTOR AUTHENTICATION

Secret Server supports using any type of soft token or mobile app authentication using the *Time-Based One-Time* (TOTP) RFC6238 algorithm. This includes Google Authenticator and Microsoft Authenticator. See instructions for setup below:

### Enabling TOTP Two-Factor Authentication

1. From the **Admin** menu, select **Users**.
2. Select the check box beside each user to enable two-factor authentication for.
3. From the **< Select Bulk Operation >** drop-down menu, select **Enable Google Auth Two Factor**.
4. Click **OK** in the dialog that appears, confirming the operation.
5. The user(s) are now required to complete the soft token setup with a mobile device the next time they log into Secret Server. See **User Setup of Soft Token Two-Factor Authentication** for details on the account and mobile app setup that follow.

## Disabling TOTP Two-Factor Authentication

To disable soft token two-factor authentication, follow almost the same process as enabling soft token two-factor authentication for a user, select **Disable Google Auth Two Factor** from the bulk operation drop-down menu instead of **Enable Google Auth Two Factor**.

## Resetting TOTP Two-Factor Authentication

1. From the **Admin** menu, select **Users**.
2. Select the check box beside the user to reset two-factor authentication for.
3. Click select **Reset Google Auth Two Factor** from on the **< Select Bulk Operation >** drop-down menu.
4. Click **OK** in the dialog that appears, confirming the operation.
5. The user is now required to complete the soft token setup with a mobile device the next time they log into Secret Server. See **User Setup of Soft Token Two-Factor Authentication** for further details on the account and mobile app setup that follow.

## Setting up TOTP Two-Factor Authentication (User)

1. Log into the main Secret Server login screen.
2. After successful authentication, a new screen appears with instructions.
3. Follow the instructions to configure the mobile device for soft token authentication. To enter the key manually rather than scanning the QR code, click the **Manual Setup** link (see image below).
4. Click **Next** to continue and enter the token in your mobile app to complete the setup.

**Note:** If you experience errors while setting up soft token authentication with a mobile device, see [Troubleshooting Google Authenticator](#) for more information.

## DUO SECURITY AUTHENTICATION

**Note:** Using this method of two-factor authentication requires that you have an active account for Duo Security.

**Note:** Secret Server supports using Duo Security as a second factor of authentication. See below for setup instructions:

### Enabling Duo (Admin)

1. From the **Admin** menu, select **Configuration**.
2. Click the **Login** tab, and then click **Edit**.
3. Select the **Enable Duo Integration** check box.

4. Enter the **API Hostname**, **Integration Key**, and **Secret Key** values (obtain these by logging into your account at duosecurity.com). See [Configuring Duo for Two-Factor Authentication](#) for details.
5. Click **Save**.
6. See **User Setup of Duo Two-Factor Authentication** for further details on the procedure that the user follows.

## Setting up Duo (User)

1. Log into Secret Server.
2. After successful authentication, a new screen appears with the option to select a method to authenticate with.
3. Select one of the options (**Duo Push**, **Send SMS**, or **Phone**), depending on your setup with Duo) and complete the selected authentication process to log in.

## FIDO2 (YUBIKEY) TWO-FACTOR AUTHENTICATION CONFIGURATION

### Overview

#### FIDO2

FIDO2 (Fast Identity Online, second edition) is an open authentication standard that uses physical devices for authentication. Thycotic uses it for two factor authentication (2FA) with FIDO2 providing the second authentication after a normal password entry—any FIDO2-enabled user attempting access to a Secret Server account **must** have a FIDO2 device in hand. The device eliminates many password-related issues, such as phishing and man-in-the-middle attacks. It also speeds up the long on process over callback or texting 2FA.

#### YubiKey

YubiKey is a FIDO2-compliant product series from Yubico, a commercial company. We recommend two of their devices--YubiKey 5 Series and Security Key by Yubico.

### Configuration

See [FIDO2 \(YubiKey\) Two-Factor Authentication Configuration](#) for details.

## SMTP CONFIGURATION FOR TWO-FACTOR AUTHENTICATION

Secret Server requires that a connection to a SMTP server be properly configured to send out confirmation code emails. Enter the SMTP server information and an email address that is used to send notifications:

1. Click **Admin > Configuration**.
2. Click the **Email** tab.



3. Verify SMTP server availability with telnet using the command `telnet <your server name> 25`.

**Note:** If virus protection is running, you may must add a firewall rule to allow `aspnet_wp.exe` to send e-mails.

## Upgrading Secret Server

To upgrade Secret Server, you need valid support licenses. To renew your support, contact sales. Once you have valid support licenses, see [Upgrading Secret Server](#).

# Licensing

## Installing New Licenses

Once a license is obtained, it can be installed by copying the license name and code into the corresponding text-entry fields to a new license page. To access this page:

1. Select **Licenses** from the **Administration** menu.
2. Click **Install New License**.

## Converting from Trial Licenses

If you previously had evaluation licenses and recently purchased Secret Server, you must remove all evaluation licenses and install your purchased licenses. Normal trial licenses expire one month after issue. If the new licenses are not installed, users see "License has expired" error messages.

## Activating Licenses

All non-evaluation licenses require activation after install. Activation is per license and Web server combination. Therefore, if you bring up a new Web server, it needs activation, even if your previous Web server was already activated. After installing each license, you are prompted to activate. Follow the on-screen prompts for online or offline activation. The activation process gathers the name, email, and phone number of the individual activating for internal purposes only. No other personal information is sent to Thycotic.

## Licensing Limited Mode

If you fail to activate, your system is be placed in limited mode, which prevents the following actions:

- AD sync
- Creating and editing secrets
- Importing secrets
- Manual RPC
- Web services (mobile applications)