

# Secret Server User Guide

---

|   |           |
|---|-----------|
| <b>SECRET SERVER USER GUIDE .....</b>                                       | <b>1</b>  |
| <b>I. GETTING STARTED .....</b>   | <b>8</b>  |
| <b>1. INSTALLATION GUIDE – SEE SEPARATE DOCUMENT .....</b>                  | <b>8</b>  |
| <b>2. TERMINOLOGY .....</b>   | <b>8</b>  |
| <b>II. DASHBOARD SECTION .....</b>  | <b>9</b>  |
| <b>1. DASHBOARD .....</b>   | <b>10</b> |
| a. <i>Browse tab</i> .....  | 10        |
| b. <i>Search / Browse Widget</i> .....                                      | 10        |
| c. <i>Widgets</i> .....   | 10        |
| a. <i>Managing Widgets</i> .....  | 11        |
| b. <i>Custom Tabs</i> .....   | 11        |
| <b>III. SECRET SECTION .....</b>  | <b>12</b> |
| <b>1. SECRETS .....</b>   | <b>12</b> |
| a. <i>Creating a Secret</i> .....   | 12        |
| <b>NEW SECRET PAGE.....</b>   | <b>13</b> |
| b. <i>Viewing a Secret</i> .....  | 13        |
| c. <i>Editing and Deleting a Secret</i> .....                               | 15        |
| d. <i>Secret Sharing and Permissions</i> .....                              | 15        |
| <b>SHARING A SECRET.....</b>  | <b>16</b> |
| e. <i>Secret Copy</i> .....   | 17        |
| f. <i>Bulk Operations on Secrets</i> .....                                  | 17        |
| <b>2. FOLDERS.....</b>  | <b>17</b> |
| a. <i>Creating a Folder</i> .....   | 17        |
| <b>CREATING A FOLDER .....</b>  | <b>18</b> |
| <b>CHOOSING A FOLDER .....</b>  | <b>19</b> |
| <b>FOLDER TREE VIEW .....</b>   | <b>20</b> |
| b. <i>Folder Sharing and Permissions</i> .....                              | 20        |
| <b>EDITING FOLDER PERMISSIONS .....</b>                                     | <b>21</b> |
| c. <i>Folder Permissions – Adding and Moving Secrets</i> .....              | 22        |
| d. <i>Folder Permissions – Creating, Deleting, and Moving Folders</i> ..... | 22        |

|   |           |
|---|-----------|
| <b>SECRET TEMPLATES</b> .....   | <b>23</b> |
| e. <i>Creating or Editing a Secret Template</i> .....                     | 23        |
| f. <i>Using the Secret Template Designer</i> .....                        | 23        |
| <b>SECRET TEMPLATE DESIGNER</b> .....                                     | <b>23</b> |
| g. <i>Template Field Types</i> .....                                      | 25        |
| h. <i>Additional Changes to a Template</i> .....                          | 25        |
| i. <i>Activating / Inactivating Templates</i> .....                       | 25        |
| <b>BULK TEMPLATE ACTIVATION</b> .....                                     | <b>26</b> |
| j. <i>Character Sets</i> .....  | 27        |
| k. <i>Password Requirements</i> .....                                     | 27        |
| l. <i>Naming Patterns</i> .....   | 28        |
| <b>3. CONVERT SECRET TO NEW TEMPLATE</b> .....                            | <b>29</b> |
| <b>4. SECRET VIEW TABS</b> .....  | <b>29</b> |
| a. <i>Expiration Tab</i> .....  | 29        |
| b. <i>Personalized Tab</i> .....  | 29        |
| c. <i>Security Tab</i> .....  | 30        |
| d. <i>Launcher Tab</i> .....  | 30        |
| e. <i>Remote Password Changing Tab</i> .....                              | 31        |
| f. <i>Dependencies Tab</i> .....  | 31        |
| <b>5. LAUNCHER</b> .....  | <b>31</b> |
| <b>SUPPORTED LAUNCHER TYPES</b> .....                                     | <b>31</b> |
| a. <i>Enabling the Launcher</i> .....                                     | 31        |
| <b>REMOTE DESKTOP LAUNCHER</b> .....                                      | <b>32</b> |
| b. <i>Session Recording (Enterprise Plus - version 7.5.000000+)</i> ..... | 33        |
| c. <i>Custom Launcher</i> .....   | 33        |
| d. <i>Using the Launcher</i> .....  | 34        |
| <b>LAUNCHING RDP</b> .....  | <b>35</b> |
| <b>6. WEB LAUNCHER</b> .....  | <b>35</b> |
| a. <i>Configuring the Web Launcher for Secret</i> .....                   | 35        |
| b. <i>Creating a Configuration</i> .....                                  | 36        |
| c. <i>Using the Web Launcher</i> .....                                    | 36        |
| d. <i>Incompatible Sites</i> .....  | 37        |
| <b>7. SETTING UP PASSWORD MASKING</b> .....                               | <b>37</b> |
| <b>8. SECRET EXPIRATION</b> .....   | <b>38</b> |

|            |  |           |
|------------|--|-----------|
| a.         | <i>Setting up Secret Expiration for the Secret Template</i> .....          | 38        |
| b.         | <i>Setting up Secret Expiration for the Secret</i> .....                   | 38        |
| c.         | <i>Forcing Expiration</i> .....  | 38        |
| d.         | <i>Resetting an Expired Secret</i> .....                                   | 39        |
| <b>9.</b>  | <b>DOUBLELOCK (ENTERPRISE EDITION)</b> .....                               | <b>39</b> |
| a.         | <i>Creating a DoubleLock Password</i> .....                                | 39        |
| b.         | <i>Creating a DoubleLock</i> .....   | 39        |
| c.         | <i>Assigning a DoubleLock to a Secret</i> .....                            | 40        |
| d.         | <i>Changing a DoubleLock Password</i> .....                                | 40        |
| e.         | <i>Resetting a DoubleLock Password</i> .....                               | 40        |
| <b>10.</b> | <b>SECRET CHECK OUT (ENTERPRISE EDITION)</b> .....                         | <b>40</b> |
|            | <b>ENABLING CHECK OUT</b> .....  | <b>41</b> |
| a.         | <i>Configuring Check Out</i> .....   | 41        |
| b.         | <i>Checking Out Secrets</i> .....  | 42        |
|            | <b>CONFIGURING A SECRET FOR CHECK OUT</b> .....                            | <b>42</b> |
| <b>11.</b> | <b>REQUIRES APPROVAL FOR ACCESS (ENTERPRISE EDITION)</b> .....             | <b>44</b> |
| a.         | <i>Setting Up Access Request for a Secret</i> .....                        | 44        |
| b.         | <i>Requesting Access After Approval is Granted</i> .....                   | 45        |
| c.         | <i>Approving a Request</i> .....   | 45        |
| <b>12.</b> | <b>REMOTE PASSWORD CHANGING (PROFESSIONAL OR ENTERPRISE EDITION)</b> ..... | <b>45</b> |
| a.         | <i>Remote Accounts Supported</i> .....                                     | 46        |
| b.         | <i>Enabling Remote Password Changing in Secret Server</i> .....            | 46        |
| c.         | <i>Configuring a Secret for AutoChange</i> .....                           | 46        |
| d.         | <i>Privileged Accounts and Reset Secrets</i> .....                         | 47        |
| e.         | <i>Change Password Remotely</i> .....                                      | 47        |
| f.         | <i>Configuring Remote Password Changing - Mapping Account Fields</i> ..... | 47        |
|            | <b>CONFIGURE PASSWORD CHANGING MAPPING</b> .....                           | <b>48</b> |
| g.         | <i>AutoChange Schedule</i> .....   | 48        |
| h.         | <i>Remote Password Service Accounts (Enterprise Edition)</i> .....         | 49        |
|            | <b>DEPENDENCY SETTINGS AND INFORMATION</b> .....                           | <b>49</b> |
| <b>13.</b> | <b>CUSTOM PASSWORD CHANGERS (PROFESSIONAL OR ENTERPRISE EDITION)</b> ..... | <b>50</b> |
| a.         | <i>Accessing the Password Changers</i> .....                               | 50        |
| b.         | <i>Changing Ports and Line Endings</i> .....                               | 50        |
| c.         | <i>Editing a Custom Command</i> .....                                      | 50        |

|            |   |           |
|------------|---|-----------|
| d.         | <i>Creating a new Custom Command Password Changer</i> .....   | 51        |
| <b>14.</b> | <b>HEARTBEAT (PROFESSIONAL OR ENTERPRISE EDITION)</b> .....   | <b>52</b> |
| a.         | <i>Remote Accounts Supported – See the RPC section on Remote Accounts Supported.</i> .....          | 52        |
| b.         | <i>Enabling Heartbeat</i> .....   | 52        |
| c.         | <i>Configuring Heartbeat</i> .....  | 52        |
| d.         | <i>Using Heartbeat</i> .....  | 52        |
| e.         | <i>Alerts on Failure</i> .....  | 53        |
| <b>15.</b> | <b>REMOTE AGENTS (PROFESSIONAL OR ENTERPRISE EDITION)</b> .....                                     | <b>53</b> |
| a.         | <i>Enabling Remote Agents</i> .....   | 53        |
| b.         | <i>Create an Agent Installer</i> .....  | 53        |
| c.         | <i>Installing an Agent</i> .....  | 53        |
| d.         | <i>Assigning an Agent to a Secret</i> .....   | 53        |
| <b>16.</b> | <b>SEARCHING SECRETS</b> .....  | <b>54</b> |
|            | <b>SEARCHING SECRETS</b> .....  | <b>55</b> |
| a.         | <i>Search Indexer</i> .....   | 55        |
|            | <b>SEARCH INDEXER EDIT</b> .....  | <b>55</b> |
| b.         | <i>Search Indexer Administration</i> .....  | 55        |
|            | <b>SEARCH INDEXER ADMINISTRATION</b> .....  | <b>56</b> |
| <b>17.</b> | <b>SECRET IMPORT</b> .....  | <b>56</b> |
| a.         | <i>Configuring Data for Import</i> .....  | 57        |
|            | <b>IMPORTING SECRETS</b> .....  | <b>57</b> |
| b.         | <i>Secret Server Migration Tool</i> .....   | 58        |
| c.         | <i>Advanced XML Import</i> .....  | 58        |
| <b>18.</b> | <b>DISCOVERY (ENTERPRISE PLUS EDITION)</b> .....  | <b>58</b> |
| a.         | <i>Enabling Discovery</i> .....   | 58        |
| b.         | <i>Importing Local Accounts</i> .....   | 58        |
| <b>19.</b> | <b>WEBSERVICES</b> .....  | <b>59</b> |
| a.         | <i>Enabling Webservices</i> .....   | 59        |
| b.         | <i>Secret Webservices</i> .....   | 59        |
| c.         | <i>Folder Webservices</i> .....   | 60        |
| d.         | <i>Windows Integrated Authentication Webservice</i> .....   | 60        |
| e.         | <i>Java Console API for Accessing Secret Values Programmatically (Enterprise Plus Edition)</i> .... | 61        |
| <b>20.</b> | <b>FOLDER SYNCHRONIZATION (PROFESSIONAL OR ENTERPRISE EDITION)</b> .....                            | <b>62</b> |
| <b>IV.</b> | <b>USER SECTION</b> .....   | <b>62</b> |

|           |   |           |
|-----------|---|-----------|
| <b>1.</b> | <b>CREATING A USER .....</b>  | <b>62</b> |
| <b>2.</b> | <b>CONFIGURING THE USERS .....</b>  | <b>63</b> |
|           | a. <i>Login Settings.....</i>   | 64        |
|           | b. <i>Password Settings.....</i>  | 64        |
|           | c. <i>Restriction Settings.....</i>   | 65        |
| <b>3.</b> | <b>ACTIVE DIRECTORY SYNCHRONIZATION (PROFESSIONAL OR ENTERPRISE EDITION).....</b> | <b>66</b> |
|           | a. <i>Adding a Domain.....</i>  | 66        |
|           | b. <i>Setting Up a Synchronization Group .....</i>                                | 67        |
|           | c. <i>Configuring Active Directory.....</i>                                       | 67        |
|           | <b>ACTIVE DIRECTORY CONFIGURATION.....</b>  | <b>67</b> |
|           | d. <i>Creating an Active Directory User .....</i>                                 | 68        |
|           | <b>CREATING AN ACTIVE DIRECTORY USER .....</b>                                    | <b>69</b> |
|           | e. <i>Converting Local Users to Domain Users.....</i>                             | 69        |
|           | f. <i>Integrated Windows Authentication.....</i>                                  | 69        |
|           | g. <i>Unlocking Local Accounts .....</i>  | 70        |
| <b>4.</b> | <b>USER PREFERENCES .....</b>   | <b>70</b> |
|           | a. <i>General Tab .....</i>   | 70        |
|           | b. <i>Launcher tab .....</i>  | 71        |
| <b>5.</b> | <b>GROUPS .....</b>   | <b>71</b> |
|           | a. <i>Creating a Group .....</i>  | 71        |
|           | <b>GROUPS .....</b>   | <b>72</b> |
|           | b. <i>Adding Users to a Group .....</i>   | 72        |
|           | <b>GROUP PAGE.....</b>  | <b>73</b> |
|           | <b>GROUP ASSIGNMENT .....</b>   | <b>74</b> |
| <b>6.</b> | <b>ROLES .....</b>  | <b>74</b> |
|           | a. <i>Creating a Role.....</i>  | 75        |
|           | b. <i>Editing Permissions for a Role .....</i>                                    | 75        |
|           | <b>ROLE EDIT PAGE .....</b>   | <b>75</b> |
|           | c. <i>Assigning Roles to a User .....</i>   | 76        |
| <b>7.</b> | <b>IP ADDRESS RESTRICTIONS .....</b>  | <b>76</b> |
|           | a. <i>Creating an IP Address Range.....</i>                                       | 76        |
|           | b. <i>Editing and Deleting an IP Address Range .....</i>                          | 76        |
|           | c. <i>Assigning an IP Address Range.....</i>                                      | 76        |
| <b>V.</b> | <b>ADMINISTRATION.....</b>  | <b>77</b> |

|    |  |           |
|----|--|-----------|
| 1. | CONFIGURATION SETTINGS.....                                    | 77        |
|    | <b>THE SETTINGS ARE EXPLAINED BELOW. ....</b>                  | <b>77</b> |
|    | a. General Tab .....   | 77        |
|    | b. Security Tab .....  | 78        |
| 2. | ADMINISTRATOR AUDITING .....                                   | 79        |
|    | a. User Audit Report .....                                     | 79        |
|    | <b>USER AUDIT.....</b>   | <b>80</b> |
|    | b. Secret Audit .....  | 80        |
|    | <b>SECRET AUDIT.....</b>                                       | <b>81</b> |
|    | c. Report Auditing.....  | 81        |
| 3. | BACKUP / DISASTER RECOVERY .....                               | 84        |
|    | a. Configuring Backups .....                                   | 84        |
|    | <b>SETTINGS.....</b>   | <b>84</b> |
|    | b. Setting up Folder Permissions .....                         | 85        |
|    | c. Manual Backups .....  | 85        |
|    | d. Scheduled Backups (Professional or Enterprise Edition)..... | 85        |
|    | e. File Attachment Backups.....                                | 85        |
|    | f. Exporting Secrets: Configuring an Export.....               | 86        |
|    | <b>EXPORTS.....</b>  | <b>86</b> |
|    | g. Exported File Format.....                                   | 86        |
|    | h. Recovery .....  | 87        |
| 4. | UNLIMITED ADMINISTRATION MODE.....                             | 87        |
|    | a. Configuring Unlimited Administration Mode .....             | 87        |
|    | <b>UNLIMITED ADMINISTRATION .....</b>                          | <b>88</b> |
| 5. | SYSTEM LOG.....  | 88        |
| 6. | EVENT ENGINE (PROFESSIONAL OR ENTERPRISE EDITION) .....        | 88        |
|    | a. Subscription page .....                                     | 89        |
|    | <b>EVENT SUBSCRIPTION PAGE .....</b>                           | <b>89</b> |
|    | b. Creating an Event Subscription.....                         | 89        |
|    | c. Editing a Subscription .....                                | 90        |
|    | d. Deleting a Subscription .....                               | 90        |
|    | e. Viewing the Event Subscription Log .....                    | 90        |
|    | <b>EVENT SUBSCRIPTION USER LOG PAGE .....</b>                  | <b>91</b> |
| 7. | CEF / SIEM INTEGRATION (ENTERPRISE PLUS EDITION) .....         | 91        |

|            |   |            |
|------------|---|------------|
| a.         | Configuring CEF .....   | 91         |
| b.         | Testing CEF .....   | 92         |
| <b>8.</b>  | <b>LANGUAGE MAINTENANCE .....</b>                               | <b>92</b>  |
| <b>9.</b>  | <b>CUSTOMIZING THE LOOK.....</b>                                | <b>92</b>  |
|            | <b>THEMES .....</b>   | <b>93</b>  |
| a.         | Creating Themes .....   | 93         |
| b.         | Embedded Mode.....  | 93         |
| <b>10.</b> | <b>REPORTING IN SECRET SERVER.....</b>                          | <b>94</b>  |
| a.         | General Tab .....   | 94         |
|            | <b>REPORTS VIEW PAGE.....</b>                                   | <b>95</b>  |
|            | <b>REPORTS EDIT PAGE.....</b>                                   | <b>96</b>  |
| b.         | Security Hardening Tab .....                                    | 98         |
| c.         | User Audit Tab .....  | 100        |
| <b>11.</b> | <b>SERVER CLUSTERING (ENTERPRISE PLUS EDITION) .....</b>        | <b>100</b> |
| a.         | Setting up Clustering .....                                     | 100        |
| <b>12.</b> | <b>SECRET SERVER ENCRYPTION .....</b>                           | <b>100</b> |
| a.         | Advanced Encryption Standard .....                              | 100        |
| b.         | SHA-512 .....   | 101        |
| c.         | SSL Overview .....  | 101        |
| <b>13.</b> | <b>TWO FACTOR AUTHENTICATION LOGIN .....</b>                    | <b>102</b> |
| a.         | Email Two Factor Authentication .....                           | 102        |
|            | <b>USER EDIT PAGE .....</b>                                     | <b>103</b> |
|            | <b>CONFIRMATION CODE PROMPT .....</b>                           | <b>104</b> |
| b.         | RADIUS Authentication (Professional or Enterprise Edition)..... | 104        |
|            | <b>CONFIGURING RADIUS .....</b>                                 | <b>105</b> |
|            | <b>CONFIGURING RADIUS FOR THE USER .....</b>                    | <b>106</b> |
| <b>14.</b> | <b>CONFIGURING SMTP EMAIL SERVER.....</b>                       | <b>106</b> |
|            | <b>SMTP CONFIGURATION .....</b>                                 | <b>107</b> |
| <b>15.</b> | <b>FIPS COMPLIANCE (ENTERPRISE PLUS EDITION) .....</b>          | <b>107</b> |
| <b>16.</b> | <b>PCI DATACENTER COMPLIANCE .....</b>                          | <b>108</b> |
| <b>17.</b> | <b>UPGRADING SECRET SERVER.....</b>                             | <b>108</b> |
| <b>VI.</b> | <b>LICENSING .....</b>  | <b>109</b> |
| <b>1.</b>  | <b>PROFESSIONAL LICENSE.....</b>                                | <b>109</b> |
| <b>2.</b>  | <b>ENTERPRISE LICENSE .....</b>                                 | <b>109</b> |
| <b>3.</b>  | <b>ENTERPRISE PLUS LICENSE .....</b>                            | <b>110</b> |

|    |   |            |
|----|---|------------|
| 4. | INSTALLING NEW LICENSES.....            | 110        |
|    | <b>ADDING A LICENSE .....</b>           | <b>110</b> |
| 5. | CONVERTING FROM TRIAL LICENSES.....     | 111        |
| 6. | ACTIVATING LICENSES .....               | 111        |
| 7. | LIMITED MODE .....                      | 111        |
|    | <b>VII. EXTERNAL APPLICATIONS .....</b> | <b>111</b> |
| 1. | IPHONE APPLICATION .....                | 111        |
|    | <b>SETTING UP THE IPHONE .....</b>      | <b>112</b> |
| 2. | BLACKBERRY APPLICATION.....             | 113        |
|    | <b>SETTING UP THE BLACKBERRY .....</b>  | <b>114</b> |
| 3. | ANDROID APPLICATION (BETA) .....        | 115        |
|    | <b>VIII. APPENDIX .....</b>             | <b>116</b> |
| a. | <i>Technical Support .....</i>          | <i>116</i> |

## I. Getting Started

### 1. Installation Guide – see separate document

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

### 2. Terminology

Throughout this User Guide, certain terms are used to refer to specific features or concepts within Secret Server.

- **Administrator**

All the features within Secret Server can be separated out into different Roles. Administrator is one of the default Roles that comes installed with Secret Server. This Role can be customized to have different permissions. In this guide, 'Administrator' will be used when referring to the User(s) who manage the system. Administrators have control over the 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.

- **Secret**

Any sensitive piece of information that you would like to manage within Secret Server. Secrets are derived from customizable 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 info or even a Microsoft Word or Excel document.

- **Secret Template**

Used for creating Secrets, Secret Templates allow you to customize and format Secrets to meet your company's needs and standards. Examples include: Local Administrator Account, SQL Server Login, Oracle Login, Credit Card and Web site Logins. Templates can contain passwords, User names, notes, uploaded files, and drop-down list values. Templates can be customized and new Secret Templates can also be created.

- **Role Based Security**

Secret Server uses Role Based Access Control. All features in Secret Server map to permissions which can then be assigned to Roles. Users and Groups can then be given one or more Roles. Role Based Security provides Administrators the ability to set strict, granular permissions for each User.

- **Unlimited Administration Mode**

This is the emergency ("break-the-glass") feature. When this mode is enabled, Administrators are able to access all content within the system regardless of explicit permissions. Access to the Unlimited Administration Mode is controlled using Roles.

- **Remote Password Changing**

Secret Server can automatically change passwords on remote devices and various platforms including: Windows Accounts, various database logins, Active Directory accounts, UNIX/Linux/Mac accounts (including root passwords), network appliances/devices and more.

## II. Dashboard Section

# 1. Dashboard

Dashboard is the main screen for searching and viewing Secrets. For a visual demonstration of the Dashboard see <http://www.thycotic.com/movies/secretserver/welcome/>.

## a. Browse tab

The Browse tab is the first tab that users see when they start using Secret Server (no other tabs exist for new users). The initial layout for the Browse tab contains the Search / Browse widget, Favorite Secrets widget, Expired Secrets widget, Create New Secret widget, and the Recent Secrets widget. Note that the Browse tab cannot be deleted or renamed (it can be moved in the tab order). All Widgets except the Search / Browse widget can be added or removed from this tab.

## b. Search / Browse Widget

This Widget is created by dragging a folder from the folder tree view of another Search / Browse Widget (ie. Browse Tab) into the Tab region. At the start of the folder drag, the Tab region will be outlined. This Widget can be used to limit the Secret search results to a particular folder and its subfolders.

- i) Creating* – New Search / Browse Widgets are tied directly to custom Tabs, which are described further below. Only one Search / Browse widget is allowed per Tab. To create a new Search / Browse Widget you must drag a folder from an existing Search / Browse Widget. You can always find one on the Browse Tab as it always will contain a Search / Browse Widget based on the <Root> folder.
- ii) Deleting* – Search / Browse Widgets may be deleted from a Tab but cannot be added back to an existing Tab.
- iii) Rearranging* – Search / Browse Widgets cannot be rearranged and will always be located in the top left portion of the Tab.
- iv) Using the Widget* – The Search / Browse Widget will be one of your most frequently used Widgets under the Dashboard paradigm. Secrets may be filtered by selecting a folder on the left by either clicking it or by the search field above the folder tree. On the right portion of the Widget, Secrets may be further filtered by the search criteria in the top textbox. The advanced section allows you to filter by Secret Template, status, and whether or not you want to see Secrets contained in sub-folders. Please note that advanced criteria is only in effect while expanded (visible).
- v) Secret Views* – Secrets that are listed in the results grid may be managed / viewed based on the user's permissions. To view a Secret, click on the row and it will expand to display. Some of the features available include the viewing/unmasking of passwords, using the launcher, and viewing other pertinent details.

## c. Widgets

Widgets are what make Dashboard work. All widgets, except for the Search / Browse widget share similar UI functionality. Widgets may be created, deleted, and rearranged as you see fit.

**Create Secret Widget** – This Widget is used to create new Secrets. From the Create New drop down list, select the Secret Template that you wish to use. You will then be sent to the **New Secret** page. See the [Creating a Secret](#) section for the details on how to use this screen.

**Expired Secrets Widget** – This Widget displays all the Secrets that are Expired. To view a Secret, click on the Secret name and it will expand to display.

**Favorite Secrets Widget** – This Widget displays all the Secrets that are set as Favorites. To view a Secret, click on the Secret name and it will expand to display.

**Out-Of-Sync Secrets Widget** – This Widget displays all the Secrets that are Out-Of-Sync. For a definition of out-of-sync Secrets, see the [Configuring a Secret for AutoChange](#) section. To view a Secret, click on the Secret name and it will expand to display.

**Recent Secrets Widget** – This Widget displays all the recently viewed Secrets. To view a Secret, click on the Secret name and it will expand to display.

**Report Widget** – This Widget is used to display a Report. From the Create New drop down list, select the Report you wish to view. There can only be one Report per Widget. To navigate to the Report view page from the Widget, click the title of the Report. For details on Reports, see the [Reporting in Secret Server](#) section.

## a. Managing Widgets


### i) Adding Widgets

There are a few different draggable Widgets available. To create one of these Widgets, expand the Content area at the upper left of the screen and drag the widget to the content area below. The available Widgets actions are as follows:

### ii) Deleting a Widget

To delete a Widget, click the trash icon (  ) at the top of the Widget.

### iii) Refreshing a Widget

To refresh a Widget, click the refresh icon (  ) at the top right of the Widget. Not all Widgets will have this.

## b. Custom Tabs

### i) Creating a Tab

To create a tab the user can either drag a folder from the Browse / Search Widget to the Tab strip, or the user can click on the plus (+) tab in order to create a new empty tab.

### *ii) Editing a Tab*

If the user clicks on the edit icon (✎) on the tab, they will be able to enter a new name for the tab. The user can cancel their changes by pressing the Esc key.

### *iii) Deleting a Tab*

If the user clicks on the delete icon (✖) on the tab, they will be asked to confirm that they indeed mean to delete the tab. Once they confirm, the tab will be deleted from the dashboard.

## III. Secret Section

### 1. Secrets

Secrets are individually named sets of sensitive information created from Secret Templates. Flexibility in Templates allows Secrets to address a broad spectrum of secure data. Secret security can be centrally managed through **View/Edit** settings for each individual Secret. Additionally, the Folder structure allows one or more Secrets to inherit permissions from a parent Folder. All Secret field information is securely encrypted within the database with a detailed audit trail for access and history.

#### a. Creating a Secret

If using the **Dashboard**, see the [Dashboard section](#).

If using the **Home** screen, in the upper right corner, select the Secret Template from which to create the Secret. This Template contains all the relevant fields for a Secret. If there is not a suitable Template, custom ones can be created (see [Creating or Editing a Secret Template](#) section). Upon selecting a Template, you will be sent to the **New Secret** page.

The screenshot shows a 'New Secret Page' with the following fields:

- Secret Template:** RPC - Active Directory Account
- Secret Name:** \* RPC admin
- Domain:** \* production.acme.com
- Username:** \* admin
- Password:** \* \$UMhV\*t6t9\*Y
- Notes:** This is the password changer for "admin"

At the bottom right, there is a 'Click for fullscreen' button with a green icon.

### New Secret Page

For the basic Secret Templates, Secret creation is intuitive and straightforward. The more complex Secret Templates are discussed later in the User Guide. Keep in mind that the **Secret Name** field is the text used both for display purposes throughout the application as well as for search functions (other fields can be used as well; see the [Searching Secrets](#) section for more details).

The **Save and Share** button allows you to immediately set the **Sharing** settings on the newly created Secret. Sharing is discussed in more detail in the [Secret Sharing](#) section.

**Note:** It is possible to import data as Secrets. This topic is discussed in the [Secret Import](#) section.


### b. Viewing a Secret


If using the **Dashboard**, see the [Dashboard section](#).


To view the information contained in a Secret, you must navigate to the **Home** page. From there, click on the Secret name. For instructions on browsing your Secrets on the **Home** page, see the [Searching Secrets](#) section.


Only the **General** tab is discussed in this section. This page will be referred to as the **Secret View** page. For information on the other tabs, see the [Secret View Tabs](#) section.

The **Secret View** page displays the relevant information for a Secret. The **Password** fields of a Secret may be masked, depending on your settings (see the [Setting Up Password Masking](#) section).

To unmask a field, click on the **Lock** icon(). This will unmask the field for as long as you have the cursor over the Lock.

To see the history of changes to the field as well as the current setting, click on the History icon ().

To copy the field to the clipboard, click on the Copy To Clipboard icon(). You may need an add-on for this to function.

To view the field using the NATO phonetic alphabet, click on the NATO icon (). (This is helpful when needing to give the password over the phone).


Discussed below are the settings that are common to every Secret:

- The **Folder** field is the Folder that contains the Secret. You can make the Secret use the **Sharing** setup of this Folder by setting the **Default Secrets Inherit Permissions** setting in the Configuration. See [Sharing a Folder](#) section for further details on this setting.
- The **Favorite?** checkbox is used to group Secrets in the **Favorite Secrets** widget on the **Home** page.
- You can edit or delete a Secret by clicking the **Edit and Delete** button, respectively. For more details, see the [Edit and Delete a Secret](#) section.
- The **Share** button is used to set up the Sharing settings (permissions) for this Secret. For further information, see the [Secret Sharing](#) section.
- You can check which Users have accessed the Secret as well as the changes performed on the Secret by clicking **View Audit** button. For additional details, see the [Auditing](#) section.

Below are the buttons, fields, and icons that are specific to more advanced Secrets. They are discussed in detail under their relevant sections.

- The **Change Password Remotely** button is discussed further in the [Remote Password Changing](#) section.
- The **Expire Now** button is discussed further in the [Secret Expiration](#) section.
- The **AutoChange Schedule** button is discussed further in the [Remote Password Changing](#) section.
- The **AutoChange?** field is discussed further in the [Remote Password Changing](#) section.



- The **Launcher** icon (  ) is discussed further in the [Launcher](#) section.

### c. Editing and Deleting a Secret

If using the **Dashboard**, see the [Dashboard section](#).

To edit a Secret, navigate to its **Secret View** page. Click on the **Edit** button. All fields on the previous Secret View page will become editable

**Note:** **Password** fields will be unmasked.

For passwords, there is an ability to randomly create a password with the **Generate** button. This will generate a password according to the rules set in the Secret's Template (see [Secret Template](#) section).

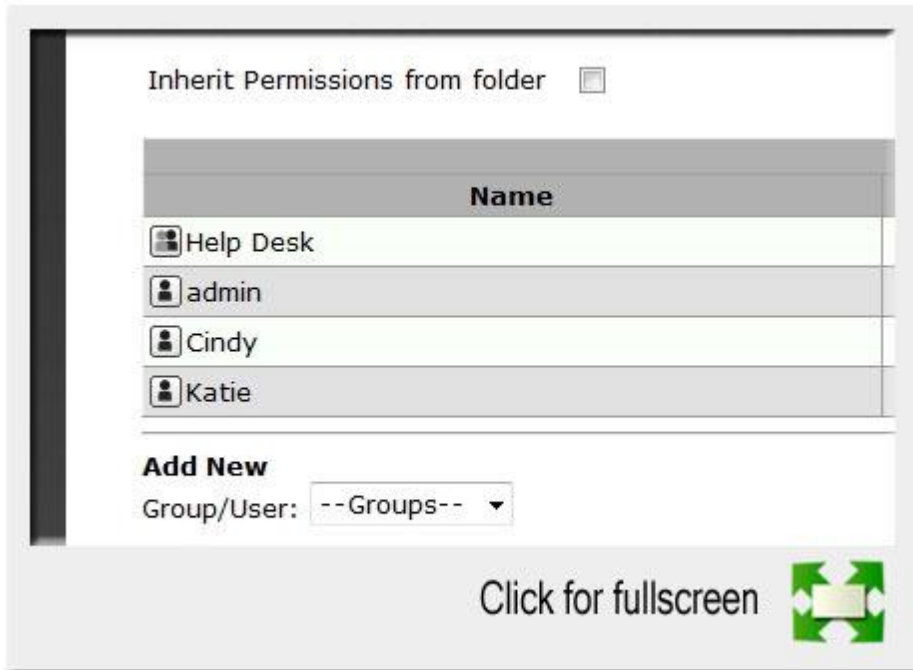
To delete a Secret, navigate to the **Secret View** page and click on the **Delete** button. The Secret will be logically deleted and hidden from Users who do not have a Role with the **View Deleted Secrets** permission. Secret Server uses "soft deletes" so that audit history for all data is maintained. This also prevents Denial of Service attacks where a disgruntled employee could delete all Secrets. However, deleted Secrets are still accessible by administrators (like a permanent Recycle Bin) – this is done to ensure the audit history is maintained and to support recovery.

Secrets can also be deleted in bulk. This is discussed in more detail in the [Bulk Operations on Secrets](#) section.

To undelete a Secret, navigate to the **Secret View** page and click the **Undelete** button. NOTE: The User must have the **View Deleted Secrets** permission (see [Roles](#) section) to access the **Secret View** page for this Secret, as well as Owner permission on the Secret.

### d. Secret Sharing and Permissions

Sharing passwords is crucial for information technology teams. Due to the sensitive nature of sharing secure information, Secret Server takes all necessary security measures to ensure that shared passwords are tracked and guarded.



### Sharing a Secret

There are three different levels of permission to choose from when sharing Secrets with another User or Group of Users: **View**, **Edit** and **Owner**.

**View** allows users to view the fields on a Secret and **Edit** allows users to change values of the fields. To perform more advanced features, such as configuring the password of a Secret to be automatically changed, you need the Owner permission.

**View** = Allows the user to see all data (fields – username, password, etc.) and metadata (permissions, auditing, history, security settings, etc.)

**Edit** = Allows the user to edit the data (username, password, etc.). Also allows users to move the Secret to another folder unless **Inherit Permissions from Folder** is turned on, in which case the user needs Owner permissions to move the Secret.

**Owner** = Allows the user to change all the metadata (permissions, security settings, etc.)

**Note:** **Password Fields** will not be visible if a Secret has a launcher and **Hide Launcher Password** is turned on or the user does not have the **View Launcher Password** role permission.

For example, Administrators need the **Edit** permission to the router password, but a contractor doing network upgrades might only need **View** (read only) access on that same Secret.

Secrets can be shared with either Groups or individual Users. The Secret Sharing section allows Secrets to be configured for access.

To add and remove **Sharing** from a Secret, navigate to the **Secret View** page for the Secret you wish to change. Click the **Share** button.

In this **Secret Share** page, existing Sharing settings for each User or Group are displayed on the grid. To edit Sharing for a Secret, click the **Edit** button. You can now add or remove Users or Groups from Sharing on the Secret. You can also add or remove specific Sharing settings to a User or Group that already has Sharing enabled for this Secret. If a User or Group is not displayed in the grid, then they do not have access to the Secret.

To further simplify the process of Sharing, Secrets can automatically inherit the settings from the Folder they are located within. By enabling the **Inherit Permissions from Folder** option in Configuration, a Secret will inherit all the parent Folder's Share permissions. For more on Folder security, see [Folders](#) section.

### e. Secret Copy

Secret Copy allows for rapid duplication of secrets. Any user with the Owner secret permission on a secret can click the **Copy Secret** button at the bottom of the View tab in order to create a new secret with information based on the original secret. Secret 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.

### f. Bulk Operations on Secrets

If using the **Dashboard**, see the [Dashboard section](#).

From the **Home** page, bulk operations can be performed on multiple Secrets. Select the Secret you wish to include by checking the checkbox next to the Secret's **Name**. To check them all, check the checkbox that is in the column headers. Then, select the operation from the dropdown list below the list of Secrets.

## 2. Folders

Folders allow you to create containers based on your individual needs. These Folders help organize your customers, computers, regions, branch offices, etc., into centralized areas. Folders can be nested within other Folders to create further sub-categories for each set of classifications. Secrets can be assigned to these Folders and sub-Folders. A benefit of Folders is customizing permissions at the Folder level and enabling **Inherit Permissions on Secrets** within the Folders. Setting permissions at the Folder level will ensure future Secrets in that Folder have the same assigned permissions, and simplify managing access across Users and Groups.

### a. Creating a Folder

To create a Folder, navigate to **Administration>Folders**.

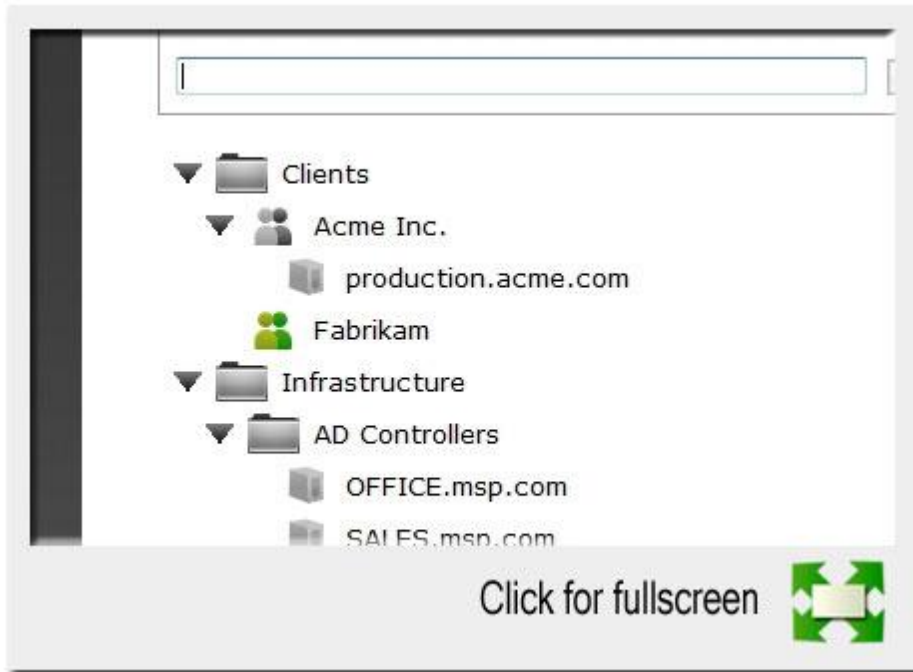
NOTE: To create Folders, you must have a Role assignment with **Administer Folder** permissions.



### Creating a Folder

By default, a new Folder will be created at the root level. If you wish to create a sub-Folder, select the parent Folder from the Folder tree before clicking the **New** button. To return to the root level, click the highlighted Folder to unselect it. To create a sub-Folder, you must have **Owner** permissions on the parent Folder.

The **Folder Name** field is the text used both for display purposes throughout the application as well as for search functions.



### Choosing a Folder

The Folder Template setting is used to display the specialized Folder icon in the Folder Tree views and advanced Folder searching. The Folder Templates are Folder (default), Customer, and Computer.



### Folder Tree View

#### b. Folder Sharing and Permissions

If the new Folder is a sub-Folder, then you can have it use the **Sharing** setting of its parent Folder by enabling the **Folder to Inherit Permissions from Parent** setting.

Folders have the same Sharing structure as Secrets: **Edit**, **View** and **Owner**. The **Save and Edit Permissions** button allows you to set Folder Sharing on the new Folder. Depending on your Configuration setup, these Sharing settings could affect the Sharing of the sub-Folders and Secrets that are contained in it. Folders are not visible to Users that do not have **View** permission (unless the configuration setting "Require View Permissions on Specific Folder for Visibility" is turned on). This allows Users to create and manage their own Folders without them being visible to all Users. The **Edit** permission is also necessary to add Secrets to a Folder.

**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 (will force “Inherit Permissions from Parent” to on for the new folder), move Secrets into that folder, and add new Secrets into that folder.

**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.

**Note:** If a User has been granted the **Owner** permission for a Folder, that User can then change permissions on that Folder. It does not matter that the User did not create the Folder.

| Name  | View                                |
|-------|-------------------------------------|
| admin | <input checked="" type="checkbox"/> |

### Editing Folder Permissions

Below are a few Folder-specific settings you may wish to use in your Secret Server configuration (go to **Administration>Configuration**):

- **Default Secrets Inherit Permissions** – When disabled, the Sharing settings on Secrets contained in Folders need to be explicitly set. They will not use the settings from the Folder.
- **Require View Permission on Specific Folder for Visibility** – When enabled, this hides Folders that the User does not have explicit View permission on. The Folders will not appear in the tree

view or allow search and browse. If disabled, the Users can see the Folders in the Folder tree but they will appear empty as the User does not have View permission to the Secrets.

- **Require Folder for Secrets** setting is used to force Users to always add Secrets to Folders.

**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 the [Folder Synchronization](#) section.

### c. Folder Permissions – Adding and Moving Secrets

To add a Secret to a folder, you must have Edit permission on that folder (either direct or through inheritance).

To 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 “Inherit Permissions from folder” then you must have Owner permission to move that Secret to a new folder (this also requires the “Share Secret” role permission in Secret Server 7.8.000002 but this requirement will be removed in the next release).

When a Secret is moved to a folder, it will automatically get “Inherit Permissions from folder” even if it had specific permissions before the move.

### d. Folder Permissions – Creating, Deleting, and Moving Folders

The “Administer Folders” role permission will allow a user to be able to create new folders and manage folders but specific folder permissions still apply.

Any user with “Administer Folders” role permission will be able to create new folders at the root level.

They will also be able to add new folders to any folders where they have Edit or Owner permission on that folder.

They must have Owner permission to be able to delete a folder.

They 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 will automatically “Inherit Permissions from parent” when it is moved (same as when Secrets are moved).

## Secret Templates

### e. Creating or Editing a Secret Template

Navigate to **Administration>Secret Templates**. On this screen, either select a Secret Template to edit or create a new one. If creating a new Secret Template, a prompt will appear to specify the name of the new Template. Enter the new name and proceed. The **Secret Template Designer** page provides all the options for configuring a Secret Template as well as which fields will appear on any Secret created from that Template.

### f. Using the Secret Template Designer

Expiration Enabled?

**Expiration Days** 90

**Expiration Field** Password


[Change](#)

| Field Name | Field Description         |
|------------|---------------------------|
| Password   | The Domain Users Password |

Click for fullscreen 

### Secret Template Designer

Below is a description of the various field settings and buttons:

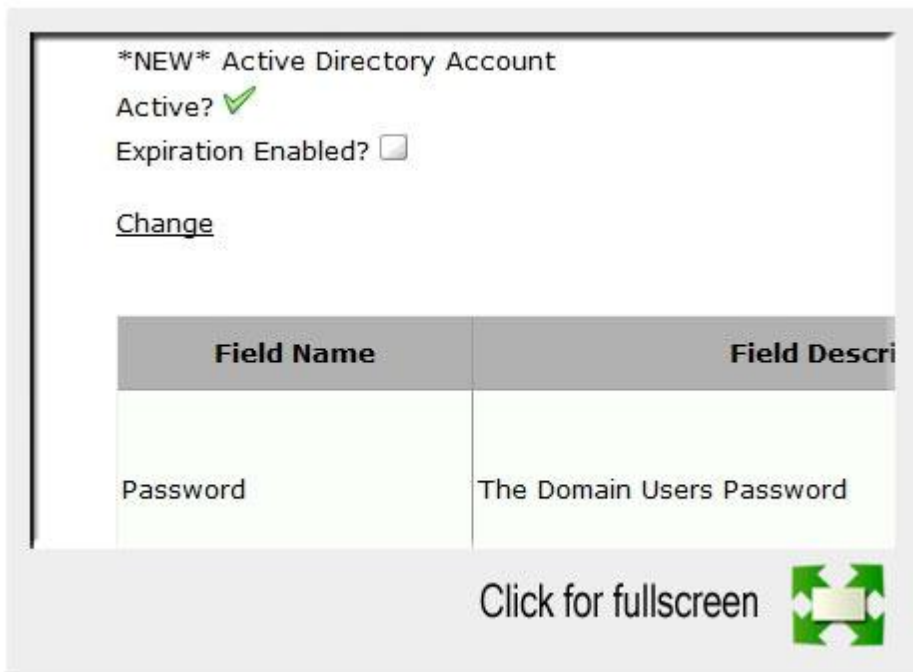
To add a field, fill out the values and click the Add button (.

- **Field Name** – The name of the field. This name will be used for the **Create New** drop-down list on either the Dashboard's **Create Secret Widget** or **Home** page.

- **Field Description** – The description of the field.
- **Field Type** – Selection of the type to use in the field. See below for a description of the different fields.
- **Is Required** - Specifies whether the field should require a value. These fields will be checked for correct content when the User attempts to create this Secret. A validation error will be displayed if not entered correctly.
- **History** - The number of values to keep in the field's history of values.
- **Searchable** - Whether that field should be indexed for searching. By default, passwords are not indexed. File attachments and history fields cannot be indexed for searching.


To delete a field, click the button (✕). There will be a confirmation dialog box before deletion takes place.

To edit a field, click the Edit button (✎). Click either the Save button (💾) to save or the Discard button (🗑️) to discard the changes.



### Secret Template Designer Edit

The order of appearance of the fields in the Template Designer grid is the order in which they will appear when the User views or edits a Secret created from this Template. The order can be modified through the up and down arrows on the grid.

Default values can be specified on each field by clicking the Edit Defaults button (). These added values will appear as a drop down list on any Secret created from this Template.

## g. Template Field Types

Template fields can be specified as one of several different types to enhance customization.

- **Text** - A single line text field.
- **Notes** - A multi-line text field.
- **URL** - A clickable hyperlink.
- **Password** - A password type field.
- **File** - A file attachment link. File attachments are stored in the Microsoft SQL Server database.
- **Edit Passwords** button – This button is only visible for templates that contain a field that is of 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 the [Editing and Deleting a Secret](#) for further details on password auto-generation).
- **Configure Password Changing** button – This button is used to enable Remote Password Changing on these Secrets. For further details, see the [Remote Password Changing](#) section.
- **Configure Launcher** button – This button is used to enable Remote Desktop or PUTTY Launcher or custom launchers on these Secrets. For further details, see the [Launcher](#) section.

## h. Additional Changes to a Template

For additional changes to a Secret Template, click the **Change** link on the **Secret Template Designer** page to navigate to the **Secret Template Edit** page.

## i. Activating / Inactivating 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.



### Bulk Template Activation

Templates can also be inactivated in bulk from the **Manage Secret Templates** screen. Click the **Active Templates** button to navigate to the **Set Active Secret Templates** screen. 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 will bring the Secret Templates into effect immediately. Note that inactivating a Secret Template will not inactivate any Secrets using that Secret Template – those Secrets will still exist but users won't be able to create new Secrets using an inactivated Secret Template.

- **Expiration Enabled? Setting** – Secret Templates allow expiration on certain fields. When the **Expiration Enabled?** option is turned on, an expiration time interval can be specified for a selected field using the drop down menu. With this option enabled and a time duration specified, Secret Server will begin providing alerts if the Secret field is not changed within the specified expiration requirements. See [Secret Expiration](#) section.
- **Keep Secret Name History? Setting** - If **Keep Secret Name History?** is enabled, Secret Server will keep the specified number of entries for viewing. This feature creates a record of every name used when a new Secret is created.

## j. 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](#) section. The 5 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.



## k. Password Requirements

Requirements can be set on a password field to validate user-entered passwords and/or make auto-generated passwords conform to certain specifications.

A Password Requirement is made up of a minimum and maximum length, a set of characters, and optional rules such as “At least 3 upper-case characters”. The default password requirement is 12 characters from the Default character set, with at least one upper-case, lower-case, numeric, and symbol character.

Password Requirements can be created or edited through the Password Requirements button on the **Administration>Secret Templates** page. Character sets can be created or deleted from the Character Sets button next to the Password Requirements button.

**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 will be displayed.

To set the password requirement for a field, click the Edit Passwords button on the **Secret Template Edit** page. Next, click the Edit button (  ), select the desired Password Requirement, and click the Save button (  ) to save the changes.

Validation of manually entered passwords can be turned on or off at the Secret Template level via the **Validate Password Requirements On Create** and **Validate Password Requirements On Edit** settings.

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.

## I. 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.

An example regular expression is `^w+\\w+$`, which would allow "NTDOMAIN01\USER3454" but not "USER3454 on NTDOMAIN01". Here the "^" symbolizes the beginning of the text. "w" specifies alphanumeric characters, plus the "\_" character, while "+" indicates one or more occurrences of the previous symbol. In this case "+" means one or more alpha-numeric characters ("w"). The "\\\" is used to denote a

single "\". In regular expressions special characters are escaped with a "\", so to try and match a single slash requires extra escape characters. Lastly the "\$" signals the end of the text.

### 3. Convert Secret to New Template

It is possible to convert Secrets from one Secret Template to a different Secret Template. To do this, view a Secret and click on the **Convert Template** button. Next, select the target Template from the Secret Template drop down list. You will then be able to map each field to a new field. To do this, go through each drop down list and select the target field for each source field on your Secret. If you want to remove the value for a field instead of converting it, then select the **< Remove >** option on the drop down list for that field. When you are done selecting, you can choose a folder and 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.

### 4. Secret View Tabs

#### a. Expiration Tab

Inside the **Expiration** tab is the settings for Secret Expiration. For further information, see the [Secret Expiration](#) section.

#### b. Personalized Tab

These settings will only be applied to the User who is editing the settings. They will not apply to the other Users who have **View/Edit/Owner** permission to the Secret.

To use the settings in this area, you must have email configured correctly in your **Configuration** settings (see [Configuring SMTP Email Server](#) section for details). You also need a valid email address set for each User who wishes to use these settings. This can be set in the **Administration>Users** section (see [Creating a User](#) section for details).

The **Send Email Alert When Viewed** setting is a User-level setting that will email the User when the Secret is viewed. The email will contain the name of the User who views the Secret.

The **Send Email Alert When Changed** setting is a User-level setting that will email the User when the Secret is edited. The email will contain the name of the User who edits the Secret.

### c. Security Tab

Inside the **Security** tab are various settings pertaining to the security of Secrets. Listed below are the settings. These may or may not be visible, depending on your configuration settings.

- **Require Check Out** – for more information on this, see the [Check Out](#) section.
- **Enable DoubleLock** – for more information, see the [DoubleLock](#) section.
- **Enable Requires Approval for Access** – for more information, see the [Requires Approval for Access](#) section.
- **Require Comment** – will require the user to enter a reason for viewing each time the Secret is accessed.

### d. Launcher Tab

Inside the Launcher tab there are different settings depending on which type of launcher is configured for the Secret. If the Launcher Type is **Remote Desktop** the following settings will be available.

- **Connect to Console** – If true the user will be logged in as a console login.
- **Allow Access to Printers** – If true the RDC will have access to the Local Printers
- **Allow Access to Drives** – If true the RDC will have access to the Local Computer's Drives
- **Allow Access to Clipboard** – If true the RDC will have access to the Local Computer's clipboard.

If the Launcher Type is **Web Launcher** the tab will display how the Web Launcher is configured to the Secret.

- The **Test Launcher** button allows the user to test the Web Launcher Configuration.
- The **Edit Fields** button allows the user to change which Secret Fields are configured to correspond to the HTML input controls on the target website.
- The **Reconfigure Web Launcher** button allows the user to reset the configuration. See the [Web Launcher](#) section for details.

## e. Remote Password Changing Tab

The settings inside the **Remote Password Changing** tab are used for Secrets that are Remote Password Changing- enabled. For more information see the [Remote Password Changing](#) section.

## f. Dependencies Tab

The settings inside the **Dependencies** tab are used for Secrets that are Remote Password Changing- enabled. For more information on Dependency checking, see the [Dependency Finder](#) section within [Remote Password Changing](#) section.

# 5. Launcher

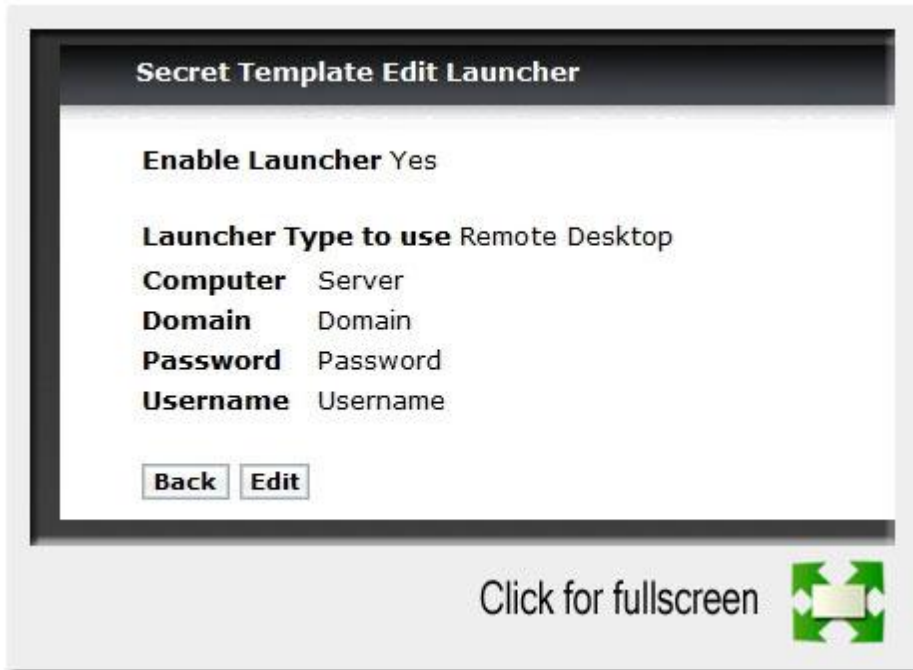
Secret Server's **Launcher** opens a connection to the remote computer or logs into a website using the Secret's credentials directly from the Web page. While this provides a convenient method of opening RDP and PUTTY connections, it also circumvents Users being required to know their passwords. A User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

Supported Launcher Types

- **Remote Desktop** - The RDP launcher will launch a Windows Remote Desktop session and automatically authenticate the User into the machine.
- **PUTTY** - The PUTTY launcher will open a PUTTY session and authenticate the User into Unix system.
- **Web Launcher** – The Web Launcher will open a new window in the browser and use the credentials to automatically log the user into a website. The [Web Launcher](#) section has more detailed information.

## a. Enabling the Launcher

By default, the Launcher will be enabled at the corresponding *Administration*>*Configuration* setting.



## Remote Desktop Launcher

### *i) FireFox Configuration*

Firefox requires a Helper Add-on application to run the RDP and PUTTY Launcher. The Microsoft .Net Framework Assistant add-on and .NET framework version 3.5 SP1 need to be installed.

### *ii) Chrome Configuration*

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.

### *iii) SSL Certificates*

SSL must be set up properly for the RDP launcher to work correctly. If Secret Server is using SSL certificates, they must be trusted at the User's computer. This will only be an issue with self-created certificates.

### *iv) Setting Up the Secret Template*

**Launcher** can be accessed from any Secret created from a properly configured Template. Secrets can be configured for the Launcher from within the Secret Template Designer page. **Configure Remote Desktop Launcher** displays the options for editing the launcher. The **Enable Remote Desktop Launcher** must be checked to allow editing of the Launcher mapping options. 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.

For a Remote Desktop Connection to work properly, Secret Server requires the appropriate logon information. The **Launcher** credentials are taken from the specified Secret fields. Fields must be assigned their corresponding credentials from the drop down list. In addition to the Secret Fields, the Domain can be mapped to **<blank>** which passes 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.

## b. Session Recording (Enterprise Plus - version 7.5.000000+)

Session recording provides an additional level of security by recording a user's actions after a launcher is used. Session Recording will work for any launcher, including Putty/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 the [Session Recording KB article](#). When a user launches a session with session recording enabled, a brief message is displayed to inform the user that their actions will be recorded.

## c. Custom Launcher

Secret Server has the ability to wire up a program to run when clicking the Launcher on a Secret. The Process Launchers can be customized to work with any command-line started application and will pass values from the Secret. In order for the process launchers to work, the client machine will need to have the program installed and typically needs the program folder in the PATH environment variable.

### i) *Creating a Custom Launcher*

In order to create a new Custom Launcher, navigate to Administration -> Secret Templates and click on the **Configure Launchers** button. Click on the **New** button.

- **Launcher Name** - The friendly name of the launcher that will be displayed to the user.
- **Active** – Whether or not the Launcher is active for use.
- **Process Name** – The name of the process that will be launched.
- **Process Arguments** – The process arguments depend on the process that is being launched. View the built in SQL Server Launcher for examples on how the fields are substituted.
- **Run Process As Secret Credentials** – If set to true, the process will authenticate as the credentials on the Secret instead of the client user that is using the launcher.
- **Use Additional Prompt** – If this setting is turned on, the user will be prompted for additional information when using the launcher.
- **Additional Prompt Field Name** – This is the name of the field that will be prompted for when the user uses the launcher. This value can be referenced in the **Process Arguments** with a \$ prefix.

### ii) *Default Launchers Requirements:*

- SQL Server Launcher - Requires SQL Server Management Studio installed. When installed the program will be automatically added to the PATH. (Default uses 2008)

- Powershell Launcher - Requires Powershell installed. When installed the program will be automatically added to the PATH.
- Sybase isql Launcher - Requires isql.exe installed. It may need to be added to the PATH if \$SYSBASE has not been added.

### *iii) How to add a Program Folder to the PATH?*

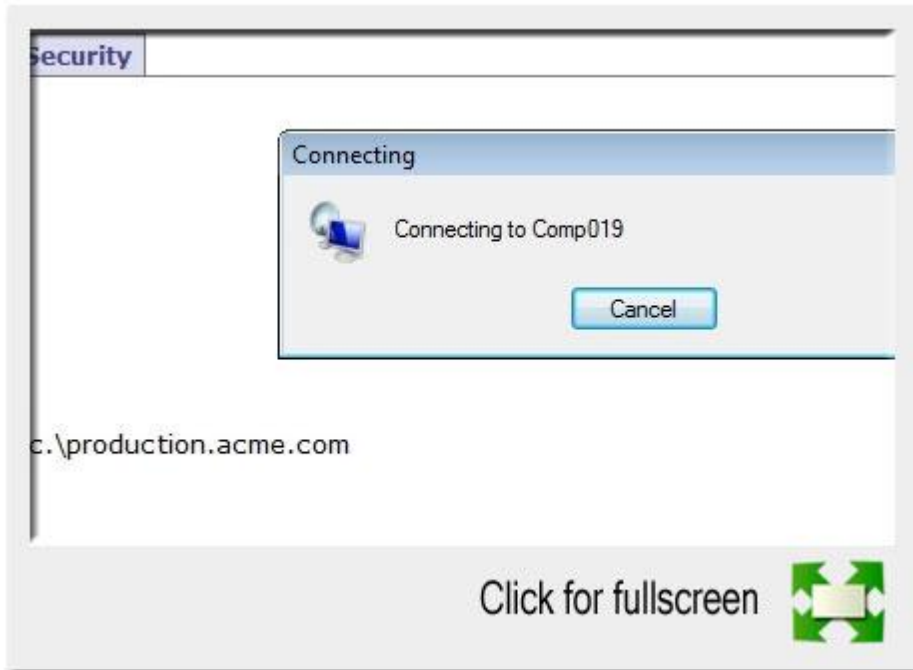
Right click on Computer and go to Properties. In the properties window click Advanced system settings. On the Advanced Tab, click the Environment Variables button. In the System Variables section scroll to Path. Click Edit then at the very end of the Textbox, paste the full path to the folder where the program file is located but make sure not to replace any existing entries. The list is semi-colon separated. Click Ok to close the dialogs.

### *iv) Common 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 will need 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.

## **d. Using the Launcher**

On the **Secret View** page, clicking the **Launcher** icon will launch the Remote Desktop, PUTTY session directly from the browser or log into the website. The mapped fields will be passed to the Launcher for automatic authentication. If the machine is set to **<user input>** for Remote Desktop, the console will launch and allow the machine to be specified from the RDP dialog. If the Host is set to **<user input>**, a prompt will ask for the specific machine before launching the PUTTY session. For certain browser security levels, the User will need to click **Allow** for the Launcher application to open.



### Launching RDP

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

The settings inside the [Launcher Tab](#) are used for Secrets that are Remote Desktop Launcher-enabled.

## 6. Web Launcher

The Web Launcher provides a convenient click to automatically log into websites. By default, the web launcher is enabled on the Secret Template Web Password, but can be enabled on custom templates as well as described in [Enabling the Launcher](#).

### a. Configuring the Web Launcher for Secret

Once enabled on the template, the Web Launcher will need to be configured for the Secret. Each website login is unique and will require the Secret fields to be mapped to the form controls. For a new Secret the Launcher icon will appear and clicking on it will take 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 will have 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 will check 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. See the [Configuration Settings](#) section for further details.

The drop down list will list all downloaded configurations and other Secrets' configuration for the same domain that the user has permission to view. Select one from the drop down list and click **Next** to create a copy of the settings for the Secret.

There is also an option to create a configuration which will allow the Web Launcher to be used on most websites and not rely on published configuration settings. In order to use this select the last item in the dropdown list and click **Next**. The next section will discuss the create process.

### ***b. Creating a Configuration***

**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 will automatically detect 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 will need 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 will be automatically obtained and this step will not be present.

**Choosing the Form** – The page will be read and the exact login form will need to be identified. The page forms will be listed in the drop down list with the most likely selected. If no forms or no likely forms are found, the user will need 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 will automatically wire up the Username and Password fields to the correct page controls. If not the user will complete the control mapping on the Launcher tab.

### **c. Using the Web Launcher**

The Web Launcher can be used by clicking the Launcher icon on the Secret View page. The Web Launcher will open a new window in the browser which will attempt 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 will create a dialog to offer troubleshooting help and means to upload the configuration to Thycotic.com. The uploaded configuration will be reviewed and published by Thycotic for all Secret Server customers to use with the [Check Online](#) feature.

**Note:** No Secret or identifiable information is uploaded to Thycotic.com. Only the website URL and control names are sent.

#### d. Incompatible Sites

A few websites prevent the ability to auto-login and will not work with the Web Launcher.

- Sites with a multi-screen login process
  - Most bank sites
- Cookie / Token based authentication to prevent auto-login
  - Google
  - Facebook
  - MSN/Microsoft

## 7. Setting Up Password Masking

Password Masking prevents over the shoulder viewing of your passwords by a casual observer (passwords show as \*\*\*\*\*). Note the number of asterisk does not relate to the length of the password for added security.

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

**Note:** The passwords will be unmasked when the User is editing the Secret.

There is also a User Preference setting which will force password masking on all Secret **Password** fields viewed by the User. This **Mask passwords when viewing Secrets** setting is found in the Tools>Preference section for each User. Note that if the Configuration setting discussed above is enabled, this User Preference setting will be overridden and cannot be disabled.

See the [Viewing the Secret](#) section for instructions on unmasking the password using the Lock icon.

## 8. Secret Expiration

A core feature of Secret Server is **Secret Expiration**. Any Template can be set to expire within a fixed time interval. For a Secret to expire, a 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 field every 90 days. If the password remains unchanged past the length of time specified, that Secret is considered expired and will appear 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 can assist in meeting compliance requirements that mandate certain passwords be changed on a regular basis. When expiration is combined with **Remote Password Changing**, Secret Server can completely automate the process of regularly changing entire sets of passwords to meet security needs.

### a. Setting up Secret Expiration for the Secret Template

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**, navigate to **Administration > Secret Templates**. In the **Manage Secret Templates** page, select the Template from the dropdown list and click the **Edit** button. In the **Secret Template Designer** page, click on the **Change** link. On this subsequent page, check the **Expiration Enabled?** checkbox. You can now enter the Expiration interval (every x number of days) as well as the field on the Secret you wish to expire and require to be changed. The interval setting can be overridden for each individual Secret (see below).

**Note:** Enabling **Expiration for a Template** will enable Expiration for all the Secrets that were created using this Template.

### b. Setting up Secret Expiration for the Secret

Now that Expiration has been enabled for the Template, Secret Expiration is enabled for the Secrets that were created using that Template as well as Secrets created in the future. The **Expiration** tab will appear on the Secret View page and requires the User to have Owner permission on the Secret. If you would prefer to set a custom expiration at the Secret level, you can adjust the interval of Expiration for the Secret by clicking the **Expiration** tab in the **Secret View** page. In the **Expiration** tab, you can set the Secret to expire using the Template settings (default), a custom interval, or a specific date in the future.

### c. Forcing Expiration

To force Expiration, navigate to the Secret View page. From there, click the **Expire Now** button. This will force the Secret to expire immediately regardless of the interval setting. The expiration date will read "Expiration Forced".

#### d. Resetting an Expired Secret

To reset an expired Secret, you will need to change the field that has expired and is required to change. For example, if the field set to expire is the Password field and the current Password is "asdf", then a change to "jklh" will reset the Expiration interval and thus remove the Expiration text on the Secret View page.

If you do not know which field is set to expire, you will need to go to the Secret Template that the Secret was created from. Navigate to Administration>Secret Template and select the Template. Click the Edit button and then on the next page, click the "Change" link. In the "Change Required On" textbox you will see the field that is set to expire.

## 9. DoubleLock *(Enterprise Edition)*

DoubleLock provides an additional layer of security by encrypting Secret data with a custom encryption key that is only accessible with an additional password, regardless of permissions or physical access to the machine running Secret Server. DoubleLock uses private/public key encryption technology to securely share access to the DoubleLock between Users when access is granted.

#### a. Creating a DoubleLock Password

Before creating a DoubleLock, you will need to create a DoubleLock password. This password will be used to generate DoubleLock keys that encrypt sensitive secrets.

**Note:** Any reference to a password while using DoubleLock will refer to this DoubleLock password, not the User's Secret Server login password.

#### b. Creating a DoubleLock

A DoubleLock is the entity key used to encrypt a given Secret and allow assigned Users access to the encrypted Secret.

As an Administrator, to use the DoubleLock functionality on your Secrets, you must first create a DoubleLock. To do that, navigate to **Administration>DoubleLock**. If you have not created a DoubleLock password yet, you will be prompted to create one.

Before creating a new DoubleLock, you may be prompted to enter your DoubleLock password. After DoubleLock creation, you can assign the DoubleLock to other Users who already have DoubleLock passwords. These other Users will be able to access the Secrets that use this DoubleLock. They will need to use their own DoubleLock password.

### c. Assigning a DoubleLock to a Secret

To assign a DoubleLock, navigate to the **Security** tab of the **Secret View** page for the Secret. In there, click the **Enable DoubleLock** checkbox. You can now select from a dropdown list the DoubleLock to assign to the Secret.

### d. Changing a DoubleLock Password

A User may change their DoubleLock password by going to **Tools>Change DoubleLock Password**. The change will update the encryption on the DoubleLock keys for that User and will not affect other Users assigned to a common DoubleLock.

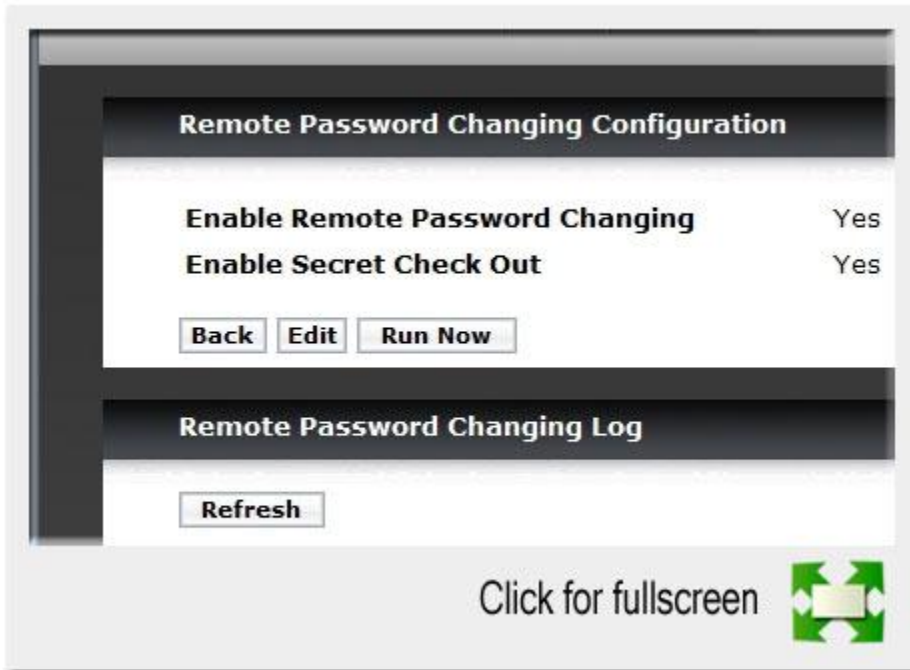
### e. Resetting a DoubleLock Password

In the event a User forgets their DoubleLock password, it can be reset by going to **Tools>Reset Double Lock Password**.

**Note:** This will result in the **loss of access** to existing DoubleLocked Secrets.

In the case the DoubleLocked Secret is only accessible by the User, the Secret will be **deleted** and the data **permanently** lost, as the password used to encrypt the Secret has been removed. Once the DoubleLock is reset, the other Users assigned to a DoubleLock will need to reassign the User who reset their password.

## 10. Secret Check Out *(Enterprise Edition)*



### Enabling Check Out

The **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 (see [Unlimited Administrator](#) section). 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.

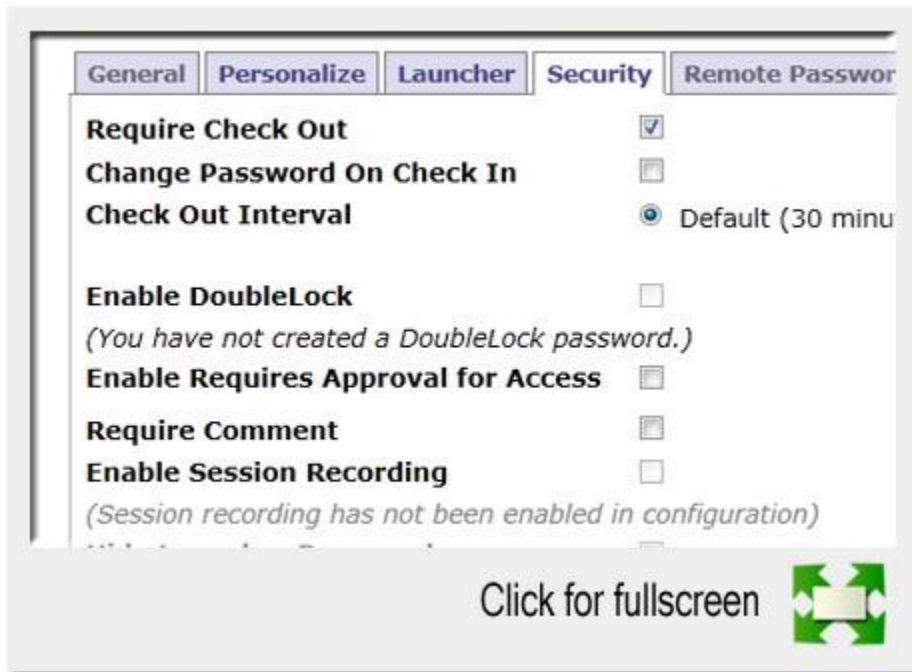
**Note:** The exception to the exclusive access rule is the assignment of **Unlimited Administrator**. If Unlimited Administration is enabled, Users with Unlimited Administrator Role permission can access checked out Secrets.

#### a. Configuring Check Out

To configure **Change Password on Check In** and **Check Out**, navigate to the **Remote Password Changing** administration page and set **Enable Secret Check Out**. If Remote Password Changing is turned off, it will need to be enabled before Check Out can be configured. Once Remote Password Changing and Check Out are enabled, certain Secrets can be configured for **Change Password on Check In** and **Check Out**. Optionally, you can also set a Check Out interval that specifies how long a user will have exclusive access to the Secret.

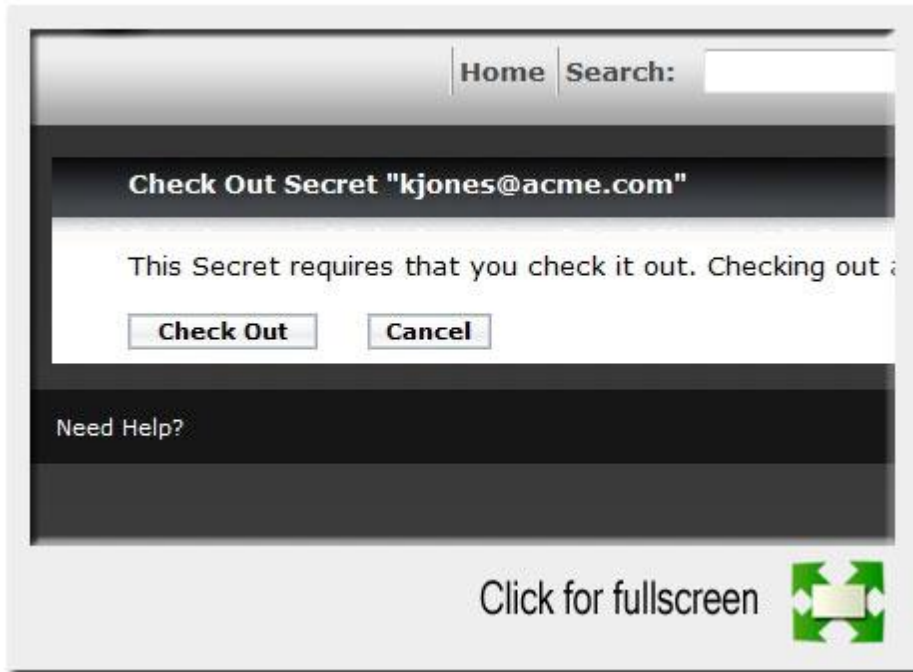
## b. Checking Out Secrets

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. The Secret needs to be configured for Remote Password Changing before **Change Password on Check In** can be set. Enable **Require Check Out** to force Users to check out the Secret before gaining access. And Enable **Change Password on Check In** to have the password change after the secret is "Checked in"



### Configuring a Secret for Check Out

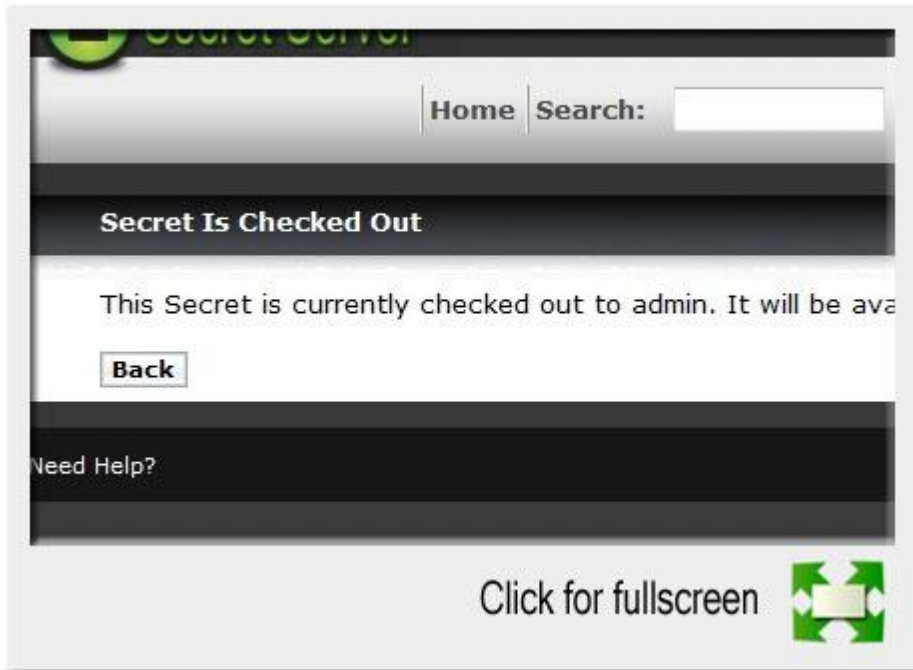
After **Require Check Out** is enabled, Users will be prompted for **Check Out** when attempting to view that Secret.



### Exclusive Access

Any User attempting to view a checked out Secret will be directed to a notification dialog informing them when the Secret will be 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.



## Exclusive Access

### 11. Requires Approval for Access *(Enterprise Edition)*

The Access Request feature allows a Secret to require approval prior to accessing the Secret. Establishing a workflow model, the User will have to request access from the approval group or groups. An email will be 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 will be granted for a set time period. If **Owners and Approvers also Require Approval** is enabled, then even users who are Owners or are in an approval group will need to request access.

#### a. Setting Up Access Request for a Secret

To enable **Access Request** for a Secret, navigate to the **Secret View** page for the Secret. Go into the **Security** tab and click the **Edit** button. You can then check the **Enable Requires Approval for Access** checkbox to enable the setting. Once enabled, you must then select Users or Groups as **Approvers** for the Secret. Unless the **Owners and Approvers also Require Approval option is turned on**, users with **Owner** share permission for the Secret, or Users that are members of the **Approvers** Group will not need to 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 will be unable to find the Secret with Search or Browse.

**Note:** The email configuration settings will need to be set up, as well as valid email addresses, for the Users in the Approval Group in order for the emailing functionality to work.

## b. 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 will then be sent to the **Request** page. In there, the User can explain the reason for the request and then click the **Request Access** button to submit the request.

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

## c. Approving a Request

Once a request for access to a Secret has been made, you can either click the link contained in the email that was received from the Approval Group or navigate to **Tools>Manage Secret Access Requests**. If choosing the latter, in the displayed grid, click the **Pending** text in the **Status** column. This will take you to the **Secret Access Request Approval** page. From here, you can **Accept** or **Deny** the request, as well as set an **Expiration** date. The requestor will have access to the Secret up to this date. Selecting the current date is the smallest window allowed and will grant access to the end of the day.

**Note:** This Expiration is not the same as Secret Expiration.

## 12. Remote Password Changing (*Professional or Enterprise Edition*)

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 will automatically generate 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 will appear notifying that there are Secrets out of sync.

## a. Remote Accounts Supported

- **Unix Accounts**
  - Both Telnet and SSH 2.0 connections to the remote host.
  - Includes Unix Root Accounts
- **SQL Server Accounts**
- **Windows User Accounts**
- **Active Directory Accounts**
  - Includes support for changing passwords on Windows Services, Scheduled Tasks, IIS Application Pools, and .ini/.config/text files
- **Sybase Account**
- **Oracle Account**
- **MySQL Accounts**
- **OpenLDAP Accounts**
- **DSEE Accounts**
- **VMWare ESX Accounts**
- **Juniper Accounts**
- **Enterasys Accounts**
- **WatchGuard Accounts**
- **Check Point Accounts**
- **Dell DRAC Accounts**
- **HP iLO Accounts**
- **Cisco Accounts**
  - Both legacy Telnet and SSH 2.0 connections to the remote host.
  - Includes Cisco Enable Secret

## b. Enabling Remote Password Changing in Secret Server

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 will be available to use RPC.

## c. Configuring a Secret for AutoChange

The **Remote Password Changing** tab contains the settings for configuring RPC on an individual Secret. Enabling AutoChange on a Secret will allow 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 field can be set or if left blank an auto-generated password will be used.

**Note:** If the password change fails, Secret Server will flag 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** will stop the Secret from being retried.

## d. Privileged Accounts and Reset Secrets

By default, RPC uses the **Credentials on Secret** option, indicating the credentials stored on the Secret are used to invoke a password change. For Windows Accounts and Active Directory Accounts, a privileged account can be used instead by selecting the **Privileged Account Credentials** option and then 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 be assigned for use in the Custom Commands. See section [Custom Command Sets \(Professional or Enterprise Edition\)](#) for more details on using the Reset 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 will see 'You do not have access to View this Secret' for the Secret name and on the Edit screen all fields mapped for RPC except the Password will be 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 fields mapped for RPC except Password is restricted to prevent changing the password on another account.

## e. Change Password Remotely

On the RPC tab there is a button called **Change Password Remotely** that allows the user 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 are able to enter in or generate the new password for the account. When the user clicks the **Change** button the secret will enter the queue for having its password changed. The RPC Log found on the Administration, Remote Password Changing page details the results of the password change attempts and can be used for debugging.

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

## f. Configuring Remote Password Changing - Mapping Account Fields

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 fields to be used for authenticating to the remote server. The Secret Fields will need to be mapped to the corresponding required fields based on the Password change type.

### Configure Password Changing Mapping

#### Required Ports

Secret Server makes use of the following list of ports to access the remote server. In order for RPC to work when the target computer is behind a firewall, verify that the correct ports are properly configured.

- **Unix SSH (22)**
- **Unix Telnet (23)**
- **Microsoft SQL Server (1433)**
- **Windows Kerberos (441)**
- **Windows NTLM (2640)**
- **Active Directory (389 or 636)**
- **Sybase (5000)**
- **Oracle (1521 or 1526)**

#### g. AutoChange Schedule

The AutoChange Schedule button will be 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 is allowed to be changed. This setting is useful for having the Remote Password Change occur during off-hours in order to prevent disruptions. By default, this setting will be **None**, which allows the Secret to be changed immediately. Note that regardless of the AutoChange Schedule, the password will still have to expire before being automatically changed.

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

## h. Remote Password Service Accounts (*Enterprise Edition*)

RPC can be performed on Service accounts where the dependent services will be automatically updated and restarted as the service account password is changed. Administrators will be notified if a dependency fails to restart. The support dependency types are IIS Application Pools, Schedule Tasks, Windows Services, and passwords embedded in .ini, .config, and other text files.

### i) *Configuring the Dependency Tab*

Dependencies are items that rely on the username and password stored in the Secret. By adding them to the dependencies tab, they will automatically be updated when the Secret's password is changed, ensuring they are up to date with the account on which they depend.

#### Dependency Settings and Information

- **Machine Name** - is the computer name or IP address on which the dependency is located.
- **Dependency Type** - specifies whether the Dependency is an IIS Application Pool, Scheduled Task, Windows Service, or Remote File.
- **Dependency Name** - is the name of the Dependency on the remote machine.
- **Privileged Account** - is the account Secret Server will authenticate as when changing the Dependency's credentials, so it must have privileges on the remote machine to edit the Dependency.
- **Status** - tells whether the Dependency was successfully updated during the last password change.
- **Active** - shows whether Secret Server will attempt to update the Dependency. An inactive Dependency will be ignored by Secret Server.
- **Description** – a description of the dependency for documentation purposes.
- **Regex** - for Remote File dependency types, the regular expression used to locate the password embedded in the file.
- **File Path** - for Remote File dependency types, the file path on the remote server where the embedded password exists.

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

**Note:** Due to security constraints, Dependencies other than Windows Services may not be changed if they are on the same machine as the Secret Server installation. Additionally, Scheduled Tasks require an Active Directory domain user as the Privileged Account.

### ii) *Manually Adding a Dependency*

To manually add a dependency, click on the plus icon next to **Create New Dependency** on the **Dependencies** tab. Then, choose your dependency type from the drop down list. Next, fill in the Dependency Name, Machine Name, and other information depending on the Dependency type.. 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 will be used. Click the OK button to finish adding the Dependency.

### iii) *Dependency Finder*

To automate adding all impacted Windows Services, the Dependency Finder can be used to search domain computers for services running under the credentials on the Secret. On the Dependency Tab, click the Find Dependency button, and then enter the domain and credentials to search for computers in Active Directory. The username and domain name will be saved for faster searching in the future. Entering **Computer Names** will limit the search to specific computers. When leaving **Computer Names** blank, the computer's screen will list all computers within the domain, and the User can choose the computers to be searched. Each computer search may take a while as the Windows Services are located. The next step of the Dependency Finder is to select the desired dependencies and then set the Privileged Account. The Dependency Finder will create and add service dependencies to the Secret. Dependency Finder will filter out dependencies already setup on the secret.

**Note:** The Dependency Finder is only available on for Active Directory accounts.

## 13. Custom Password Changers (*Professional or Enterprise Edition*)

There are a few Password changing types that allow the user to enter in specific commands that will be 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.

### a. Accessing the Password Changers

In order to access the custom commands and settings on password changers, go to the **Remote Password Changing** section of the Administration section. From there, click on **Configure Password Changers** and either edit an existing password changer or create a new one.

### b. Changing Ports and Line Endings

To change the port or line ending used on a password changer, click on the password changer on the **Configure Password Changers** page and then click the **Edit** button. 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.

### c. Editing a Custom Command

Not every password changer can be edited, only those with available custom commands. These include:

- Cisco Account Custom (SSH)
- Cisco Account Custom (Telnet)
- Cisco Enable Secret Custom (SSH)
- Cisco Enable Secret Custom (Telnet)
- Unix Account Custom (SSH)
- Unix Account Custom (Telnet)
- Unix Root Account Custom (SSH)

The **SSH** type changers use the **SSH** protocol to access the machine. This type only contains custom commands for the password reset functionality. 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.

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

Any Secret Field value can be substituted by prefacing the 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 Fields:

- \$USERNAME – The username field mapped in RPC on the Secret Template.
- \$CURRENTPASSWORD – The password field mapped in RPC on the Secret Template.
- \$NEWPASSWORD – The next password (filled in Next Password textbox or auto-generated).

Associated Reset Secrets:

- Adding the prefix \$[1] to any fields will target the associated Reset Secret with order 1.
- Ex. \$[1]\$USERNAME – The mapped username of the associated secret.
- Both the mapped fields and Secret Field names can be used.

Check Result Commands:

- \$\$CHECKFOR <text> - Checks that the response from the last command equals <text>
- \$\$CHECKCONTAINS <text> - Checks that the response from last command contains <text>
- If these conditions are not met the process fails and immediately returns a result.

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 will be displayed when using these test buttons.

#### d. Creating a new Custom Command Password Changer

You can create a new custom command by clicking on the **New** button on the password changers list screen. This will take you to a screen where you can enter the name of the new password changer and

choose the protocol and type (SSH vs. Telnet). Once **Save** is clicked, the password changer is created and you can modify the commands in the same way that you would in the edit screen.

## 14. Heartbeat (*Professional or Enterprise Edition*)

Heartbeat allows properly configured Secrets to have the entered credentials automatically tested for accuracy at a given interval. Using Heartbeat on Secrets will ensure the credentials stored in Secret Server 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.

**a. Remote Accounts Supported** – See the RPC section on [Remote Accounts Supported](#).

### b. Enabling Heartbeat

To enable Heartbeat, **Enable Heartbeat** must first be turned on in the Remote Password Changing Configuration page (navigate to **Administration>Remote Password Changing**). It must also be set on the Secret Template by enabling the **Enable Remote Password Changing Heartbeat** setting.

### c. Configuring Heartbeat

Heartbeat is configured from the Secret Template Designer. The Heartbeat interval will determine how often the Secret credentials will be tested. See the RPC Section on [Configuring Remote Password Changing - Mapping Account Fields](#).

### d. Using Heartbeat

Heartbeat will run in a background thread to check each Secret where it is enabled. If the credential test fails the Secret will be flagged as **Heartbeat Failed** and out of sync. To avoid locking out the account, Heartbeat will no longer run on that Secret until the Secret items are edited by the user. If the machine is determined to be Unavailable the Secret will be flagged as **Heartbeat Unable to Connect** and the Secret will continue to be checked on the Heartbeat interval.

To manually use Heartbeat to check the credentials the [Secret View](#) page has the **Heartbeat Now** button. The Heartbeat Now button will mark the password as **Heartbeat Pending**. The background thread will process the Secret in the next 10 Secrets and when the page is refreshed the **Heartbeat Status** will be updated.

**Note:** Heartbeat for Windows Accounts is not compatible for accounts on the server that is running Secret Server. These accounts will be flagged with a status of **Incompatible Host**.

## e. Alerts on Failure

On the [Preference](#) page, the **Send email alerts when Heartbeat fails for Secrets** setting can be enabled to email the user when Heartbeat fails for any Secret he has **View** access to.

## 15. Remote Agents *(Professional or Enterprise Edition)*

Remote Agents allow Remote Password Changing and Heartbeat to occur on networks that are not directly connected to the network that Secret Server is installed on.

### a. Enabling Remote Agents

In order to enable Remote Agent Support in Secret Server perform the following steps:

- Navigate to the Administration menu of Secret Server.
- Click the "Remote Password Changing" link.
- Click the "Agent Configuration" button.
- Click the "Edit" button to edit the "Remote Password Changing Agent Configuration".
- Check the "Enable Remote Agents" checkbox and click the save button.

### b. Create an Agent Installer

In order to create a Remote Agent installer, perform the following steps:

- Navigate to the Administration menu of Secret Server.
- Click the "Remote Password Changing" link.
- Click the "Download Agent Installer" button.

### c. Installing an Agent

- Extract the zip file that was created in previous section and run the "SecretServerAgentInstaller.msi" file from the remote computer that you are installing the Agent on.
- Follow the installation instructions in the installer and take note of the "Confirmation Code" that is displayed.
- Go back into Secret Server and click the "Manage Agents" button, your new installed Agent should be there (or will be in a minute or two).
- Click on the Agent name and then click on the "Activate" button if the Confirmation Code matches what was displayed when the Agent was installed.
- The Agent is now available to be used for Heartbeat and RPC.

### d. Assigning an Agent to a Secret

In order to use a Remote Agent to use RPC or perform a Heartbeat on a Secret, perform the following steps:

- Open the RPC-enabled Secret.
- Navigate to the "Remote Password Changing" tab.
- Click the "Edit" button.
- Choose the preferred Agent from the dropdown list and click the "Save" button.

That Secret will now use the selected Agent when a RPC or Heartbeat action is called on the Secret.

**Note:** For additional information on agents, please read the following KB article: [Remote Agent FAQ](#)

## 16. Searching Secrets

To search Secrets using Dashboard, see the [Dashboard section](#).

Searching Secrets is performed on the **Home** page from the **Search** tab. To make searches more precise, the results can be limited by way of the various parameters available on the tab. Searches will search for all fields that are set to **Searchable** (previously **Indexable**) on the Secret's Template if the **Search Indexer** is enabled. If the Search Indexer is not enabled, searches will only be performed on the **Secret Name** field.

The **Browse** tab is a quick way to view all active Secrets available regardless of Folders or search parameters.

The screenshot shows a dashboard interface with two tabs: "Search" and "Browse". The "Search" tab is active and contains the following controls:

- Search For:** A text input field containing "admin".
- By Secret Template:** A dropdown menu.
- By Status:** A dropdown menu set to "Active".
- Result Size:** A dropdown menu set to "15".
- Include Subfolders:** A checked checkbox.
- Folder:** A field containing "\\Clients\Acme Inc." with a "Clear" button next to it.

The "Browse" tab is partially visible on the right, showing a table with the following data:

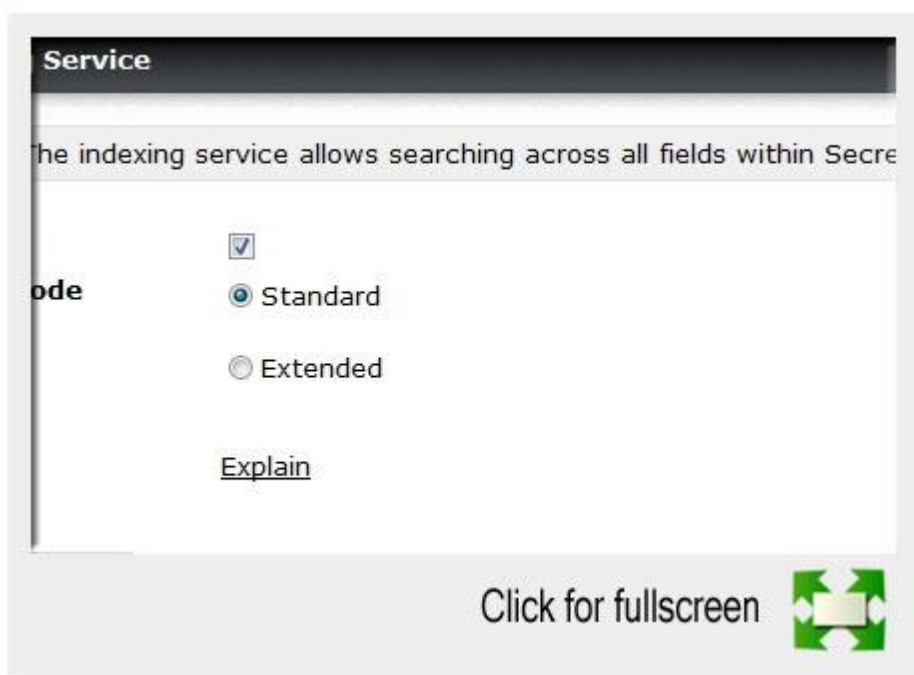
|                          | Name           | Temp                               |
|--------------------------|----------------|------------------------------------|
| <input type="checkbox"/> | Computer Lobby | *NEW<br>Active<br>Direct<br>Accou  |
| <input type="checkbox"/> | RPC admin      | RPC -<br>Active<br>Direct<br>Accou |

At the bottom of the interface, there is a "Click for fullscreen" button and a green fullscreen icon.

## Searching Secrets

### a. Search Indexer

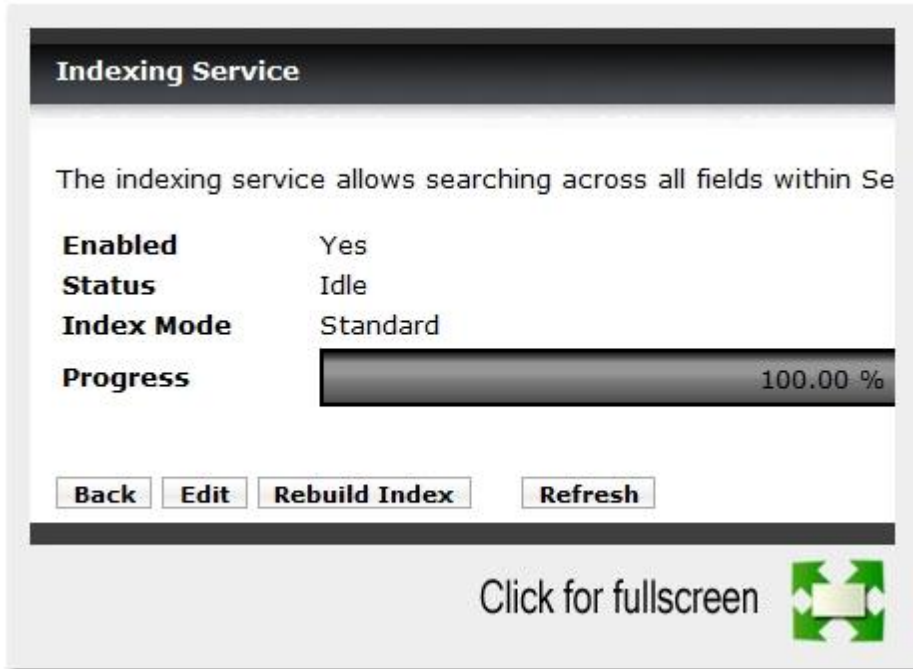
The **Search Indexer** allows searching on all fields set to **Searchable** (previously **Indexable**) on the Template. From the **Administration>Search** Indexer, click the **Edit** button to configure and enable the indexing service. Save any changes and the Indexer will start indexing all the Secrets. The progress is displayed on the **Search Indexer Administration** page and indexing may take some time depending on the size of the installation. The indexer runs in the background to avoid the undesirable effect of decreased performance caused by using full server resources.



### Search Indexer Edit

### b. Search Indexer Administration

**Standard Search** mode is the default search mode. Standard searching creates indexes on the values of each field set to **Searchable** (previously **Indexable**) on the Template. However, it will only search on whole words in these fields. For example, a Secret with a field value of "Thycotic" would only match a search for "Thycotic".



### Search Indexer Administration

**Extended Search** allows searching on both whole words and sections of words (minimum three letters). For example, the Secret with a field value of "Thycotic" would be returned on a search for "Thycotic" or "thy" or "cotic". This allows for more fine-grained search results, but may impact search performance as well as create a larger index table.

**Indexing Separators** are used to split the text 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** will require a full rebuild of the search index.

## 17. Secret Import

Secret Server's **Import** feature simplifies integration with legacy systems and allows Users to easily add large numbers of Secrets from an Excel or CSV/Tab delimited file. Secrets are batch imported by Template, so multiple types of input data will need to be imported in several batches. The Password Migration Tool supports easy addition of existing Secrets from other third party password storing applications.

## a. Configuring Data for Import

To get started, click **Import Secrets** from the **Tools** page. A Template corresponding to the type of data in the input file must then be selected; then **Continue** to add the Secrets.

Paste the Secrets for import directly into the text area in the **Import Secrets** dialog. The order of the fields being imported will be listed depending on the Template selected. A few items to note when importing Secrets:

- Do not include a header line.
- Secret Names must be included but others fields can be blank unless the **Secret Template** indicates that the field is required.
- Fields containing commas or tabs must be surrounded with double quotes.

There are two options for importing Secrets: **Ignore Duplicate Secrets** and **Import With Folder**. **Ignore Duplicate Secrets** will prevent the import of any Secrets with the same name of an already existing Secret. **Import With Folder** allows an additional field in the import text specifying a fully qualified Folder name for the Secret to be created in. Secret Server will display a preview of the new Secrets prior to being imported.



Importing Secrets

## b. 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:

- Password Corral
- KeePass
- Password Safe
- Password Manager Pro
  - This is done with another Export Tool that creates a single XML file. Please contact support for more details.

## c. Advanced XML Import

The Advanced Import will add 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 the Knowledge Base article [Advanced Import with XML](#).

## 18. Discovery (*Enterprise Plus Edition*)

As an alternative to manually creating or importing accounts, Secret Server has an automatic **Discovery** option for local Windows accounts. This allows administrators to quickly import accounts found by Secret Server on specified domains.

### a. Enabling Discovery

Discovery can be enabled at the Administration>Discovery page. First, Discovery must be enabled by clicking **Edit** and then checking the **Enable Discovery** checkbox. Additionally an interval can be selected for when Discovery runs on the network. Click the **Edit Domains** button to configure which domains Discovery should run on. On the domain edit page click the **Enable Discovery** checkbox to enable that domain for Discovery. Once a domain has been configured select the **Discovery Network View** button from the Discovery page.

**NOTE:** At this point Secret Server is scanning the domain for machines and accounts so the view may not be contain all domain data immediately.

### b. Importing Local Accounts

Once the domain has been scanned, the **Discovery Network View** page will display the OUs and machines on the domain and any local accounts found on those machines. To import accounts for a machine, select the OU from the network tree with the machine that has accounts to be imported. In the center grid select the accounts to import by checking the checkbox next to each row. Click the **Import Accounts** button and an import dialog will be presented with several options.

- **Secret Template** – Choose the Secret Template that these secrets will be imported as. The list of available templates is filtered by the templates that are valid for windows remote password changing.
- **Folder** – Choose the Secret Server folder that the Secrets will be imported into.

- **Secret Name** – Choose the Secret name that the secret will be imported as. The following keywords automatically substitute values in the Secret name
  - \$MACHINE
  - \$USERNAME
- **Password** – At this point there are two options, if the password of the account(s) is already known, choose the **Know Existing** option and enter the **Existing Password**. If the password is unknown, Secret Server can take over the account when **Take Over Account** is selected. When this option is selected Secret Server will use the **Privileged Account** selected and will change the password on the computer account. The new password can either be entered or Secret Server can randomly generate a new password for the account.

NOTE: If the **Take Over Account** option is selected, Secret Server will change the password for the account on the remote machine. The ports required for Discovery are documented in [this](#) KB article.

After completing the dialog, clicking the **OK** button will create a Secret for each selected account.

## 19. Webservices

Secret Server provides a suite of **Webservices** which can be used to retrieve and update Secrets, and Folders. The Webservices allow Secret Server to be accessed using the iPhone, BlackBerry, and Android (in development) apps, as well as custom built integrations. The Webservices are secure and require authentication in the same manner as regular access to Secret Server. All actions that involve data are also logged (Secret views, updates, adds, etc).

### a. Enabling Webservices

Webservices can be enabled at the Administration>Configuration general tab. Enabling Webservices simply makes the ASP.NET Webservices built into Secret Server available. They are found under /webservices/sswebservice.aspx in your Secret Server. They run on the same port as the web application. You can view them with a browser to see the functionality that is offered.

### b. Secret Webservices

- **Authenticate** - takes in the User credentials and returns an authentication token that must be used with the other calls.
- **AuthenticateRADIUS** - takes in the User credentials and RADIUS password and returns an authentication token that must be used with the other calls.
- **AddSecret** - adds the Secret to Secret Server.

- **DeactivateSecret** - deletes the Secret.
- **GeneratePassword** - generates for a given secret field and applies the Password Requirement rules and settings.
- **GetFavorites** - returns a list of secrets that the User has marked as a favorite.
- **GetSecret** - returns the given secret if the User has permission to it.
- **GetSecretTemplateFields** - returns the secret fields for the given Secret Template.
- **GetSecretTemplates** - returns a list of all the Secret Templates.
- **SearchSecrets** - returns the search result of the given term. A blank search term will return all secrets.
- **SearchWebPasswordsForURL** - searches all secrets of type URL to match the search term. This is used in Secret Assistant (deprecated) for retrieving secrets based on a URL.
- **UpdateFavorite** - marks the given secret as a favorite for the User.
- **UpdateSecret** - updates the fields of the given Secret. Requires Edit permission on the secret.
- **VersionGet** - returns the Secret Server version.

### c. Folder Webservices

- **FolderCreate** - adds the Folder to Secret Server.
- **FolderGet** - returns the Folder.
- **FolderGetAllChildren** - returns the child Folders for the given parent Folder.
- **FolderUpdate** - updates the name and type of a Folder.
- **SearchFolder** – returns the search result of the given term. A blank search term will return all folders.

### d. Windows Integrated Authentication Webservice

Secret Server also provides a webservice that use Integrated Windows Authentication instead of a user name 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](#)" Knowledge Base article at [support.thycotic.com](http://support.thycotic.com) for more advanced technical information on using this webservice.

### e. Java Console API for Accessing Secret Values Programmatically (Enterprise Plus Edition)

Secret Server has the ability to setup 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 will not allow it to access Secret Server. As a user in Secret Server, an admin can choose to 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.

#### i) Installing the Java Console

1. Create a local user account in Secret Server that will be used by the instance of Java Console API you are installing
  - i. Note: Since the hardware is used to secure the API to a specific account, a different user is required for each machine where the jconsole is installed.
2. Install Java 7 JRE on the machine available from [here](#).
3. Request the jar file from your Thycotic Account Manager at <http://thycotic.com/MyAccount.html>
4. Once the zip is received in an email, place the jar file in a folder you will access it from. Ex C:\SecretServerAPI\
5. Install the jar file using the -i command
  - a. C:\SecretServerAPI> C:\Program Files\java\jre7\java -jar secretserver-jconsole.jar -i (Username) (Password) (URL to Secret Server)
  - b. The URL does not include any pages.
    - i. Good example: http:\\mysecretserver.com\SecretServer\
    - ii. Bad example: http:\\mysecretserver.com\SecretServer\login.aspx
6. Once installed the password on the account is changed based on some encrypted items and the machine hardware
7. The secretserver-jconsole.jar can be called with -s or -v to retrieve Secret Field Values
  - a. Single Field => C:\SecretServerAPI> C:\Program Files\java\jre7\java -jar secretserver-jconsole.jar -s (SecretId) (FieldName)
  - b. Multiple Fields => C:\SecretServerAPI> C:\Program Files\java\jre7\java -jar secretserver-jconsole.jar -v (SecretId) (Seperator) (FieldName1) (FieldName2)
  - c. The SecretId can be found by going to SecretView.aspx and in the address bar the QueryString will have SecretId=# that can be used to load the Secret

#### ii) Security in the API

- No Password Stored - The credentials to Secret Server are calculated based on Hardware of the machine and encrypted files, so the password is not known by anyone.
- Obfuscation - The Java console is obfuscated to make reversing the encryption more difficult.
- Tied to Hardware - copying the files to another machine will not work to access Secret Server
- Password Expiration causes Automatic Change - when the local account password expires (based on configuration settings) the console will automatically change the password.

- Recommendation:
  - Locking down the secretserver-jconsole.jar and created config files through file permissions to grant only certain users access to calling the Java Console. This will allow only the allowed scripts or users to use the API.

## 20. Folder Synchronization *(Professional or Enterprise Edition)*

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 will require specifying the synchronization Interval in Days, Hours, and Minutes. The **Folder to Synchronize** is the parent Folder where you will be creating the Folder structure. 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.

**Note:** See the "[How to create a custom view for ConnectWise synchronization](#)" Knowledge Base article at [support.thycotic.com](http://support.thycotic.com) for more advanced technical information on setting up the **SQL View**.

## IV. User Section

### 1. Creating a User

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](#) section).

**Note:** Be aware that a new User will be assigned the Role called "User" by default. For more information on Roles, see the [Roles](#) section.

Below is a brief explanation of each field:

- **User Name** - The Login name for the User.
- **Display Name** - The text that is used throughout the User Interface.
- **Email Address** - The email address used for Request Access, Email Two Factor Authentication, etc.
- **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 field (and all the other fields) set is through Active Directory synchronization (see [Active Directory Synchronization](#) section).
- **Password** – This will be the Login password for the User. For the various Login settings, see [Login Settings](#) section.
- **Email Two Factor Authentication** – On a Login attempt the User will have an email sent to the email address entered above. This email will contain a Pin Code that the User will need to log into the account. See Email Two Factor Authentication for more details.
- **RADIUS Two Factor Authentication** - This field will only appear if RADIUS authentication is enabled in the configuration. On a Login attempt the User will need to enter the RADIUS token sent from the RADIUS server. See [RADIUS Authentication](#) section for more details.
  - **RADIUS User Name** – This field will only appear if the above **RADIUS Two Factor Authentication** setting is enabled. This is the Username the RADIUS server is expecting. See RADIUS Authentication Integration for more details.
- **Enabled** – Disabling this field will remove this User from the system. Effectively, this is the way to delete a User as Secret Server does not allow complete deleting of Users due to auditing requirements. To re-enable this User, navigate to the **Administration>Users** page. Check the **Show Inactive Users** checkbox just under the Users grid. All Inactive Users will then be visible in the grid. Click the **User Name** of the User you wish to edit.
- **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 checkbox. For more details on locking out Users, see [Maximum Login Failures](#) setting described in the Login Settings section.

## 2. Configuring the Users

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.

## a. Login Settings

The following settings are found in the **Administration>Configuration** page, inside the **Login** tab:

- **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 will be set in their browser. This will enable the User to revisit Secret Server without the need to Login. This cookie will no longer be valid when the **Remember Me** period has expired. They will then have to enter their Login information again. This option allows Users to remain logged in for up to a specific period of time (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 **Allow Remember Me** is enabled. This is the period of time that the **Remember Me** cookie mentioned above will be valid. For example: if set to one day, then Users taking advantage of **Remember Me** will have to Login at least once a day. To set a time value (Minutes, Hours, or Days), uncheck the **Unlimited** checkbox.

- **Allow AutoComplete** - AutoComplete is a feature provided by most web browsers to automatically remember and pre-fill 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.
- **Maximum Login Failures** - Set the number of Login attempts allowed before a User is locked out of their account. Once locked out, they will need a Secret Server administrator to reset their password and enable their account. For details on how to reset a locked account, see the [Creating a User](#) section.
- **Visual Encrypted Keyboard Enabled** – This setting will enable the Visual Keyboard for Logins.
- **Visual Encrypted Keyboard Required** – This setting will require the Visual Keyboard for Logins.
- **Enable RADIUS Integration** – This setting will allow for RADIUS server integration with your User Login authentication. Other RADIUS settings will appear upon enabling this option. These settings are discussed in the [RADIUS Authentication Integration](#) section.

## b. 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** – This setting will make the **Forgot your password?** link appear on all Users' Login screens. Clicking on this link will prompt 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 will be sent. Note that this only works for local user accounts and not for Active Directory accounts.

- **Symbols Required for Passwords** – This setting will force all User Secret Server Login passwords to contain at least one *symbol* (i.e., !@#%&^\*).
- **Lowercase Letters Required for Passwords** – This setting will force all User Secret Server Login passwords to contain at least one *lowercase letter*.
- **Uppercase Letters Required for Passwords** – This setting will force all User Secret Server Login passwords to contain at least one *uppercase letter*.
- **Numbers Required for Passwords** – This setting will force all User Secret Server Login passwords to contain at least one *number*.
- **Minimum Password Length** – This setting will force all User Secret Server Login passwords to contain at least this many characters.
- **Enable Local User Password Expiration** – This setting will force a password change for a User after a set interval elapses. After the interval time has elapsed, the next time the User attempts to log in, the User will be prompted for the old password, a new password, and a confirmation of the new password. The new password will be validated against all the password requirements (see the earlier settings – **Symbols Required for Passwords**, etc.).
- **Local User Password is valid for** – If **Enable Local User Password Expiration** is enabled, then this is the interval setting for it (see **Enable Local User Password Expiration** setting for details). If **Enable Local User Password Expiration** is disabled, the entered value will display as “Unlimited”.
- **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 will prevent a user from changing their password too frequently, which will allow them to quickly re-use old password.
- **Enable Local User Password History** - If enabled, this will prevent a user from reusing a password. For example, if set to “20 Passwords”, this will prevent the user from using a password they have used the previous 20 times. This in conjunction with **Enable Minimum Local Password Age** will help ensure that users are using a new and unique password frequently rather than recycling old passwords.

### c. Restriction Settings

- **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.

- **IP Restrictions (Professional or Enterprise Edition) -**

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 may 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. From here, click the **Login Policy Agreement** button.
  - **Enable Login Policy** – If enabled, this will simply display the agreement. To force the acceptance of the policy, also enable **Force Login Policy**.
  - **Force Login Policy** – This setting will force the checking of the **"I accept these terms"** checkbox before allowing the User to Login to Secret Server.

### 3. **Active Directory Synchronization (Professional or Enterprise Edition)**

Secret Server can integrate with Active Directory by allowing Users to use their Active Directory credentials to login to Secret Server. 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 periodic interval. Secret Server does not store the Domain user's passwords. Instead, it will pass 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 will use to replicate Users and membership. When a new user is pulled in from Active Directory, Secret Server will also replicate the email address.

#### a. **Adding a Domain**

Before synchronizing or creating Users, specify which domains Secret Server will be able to authenticate against. Secret Server can synchronize with any number of Domains. From the Active Directory Configuration page, click **Edit Domains** and then **Create New** to add a new Active Directory Domain. **Username** and **Password** are only required for connecting to the Domain when synchronizing Users. Note that a member of a parent or child domain can be used to synchronize if you enter the username in the **Domain\Username**.

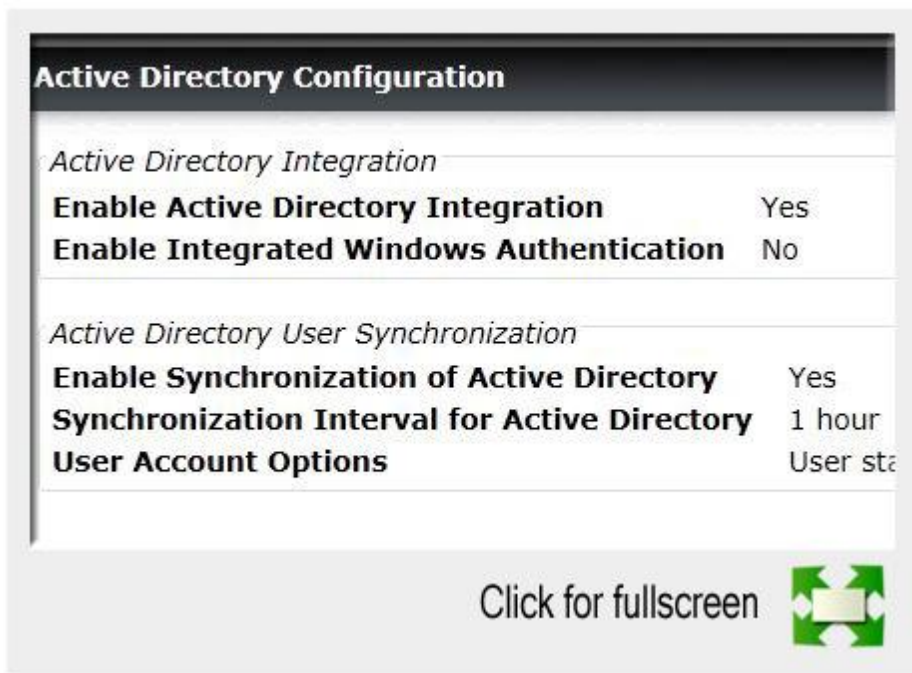
**Note:** the account entered will be used to synchronize Users and Groups, it will require permission to search and view the attributes of the Users and Groups. If you plan on using **Discovery**, the account will also need permissions to scan computers on the network for accounts.

## b. Setting Up a Synchronization Group

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.

## c. Configuring Active Directory

Active Directory configuration can be enabled by a User with the "Administer Active Directory" Role.



### Active Directory Configuration

The configuration screen offers several options:

- **Enable Active Directory Integration**

Enable or disable the Active Directory Integration 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 be using the Synchronization Group, do not enable this setting or manual Users can be locked out.

- **Enable Integrated Windows Authentication**

Enable or disable the [Windows Integrated Authentication](#) feature.

- **Synchronization Interval for Active Directory**

Set the interval that Secret Server will synchronize its Users and Groups with the Active Directory.

- **User Account Options**

- **Users are enabled by default (Manual)**

Secret Server users will automatically be enabled when they are pulled in as new users from Active Directory. If they were disabled explicitly in Secret Server, they will not be automatically re-enabled. If creating a new user will cause the user count to exceed your license limit, the user will be created as disabled.

- **Users are disabled by default (Manual)**

Secret Server users will automatically be disabled when they are pulled in as new users from Active Directory. If they were enabled explicitly in Secret Server, they will not be automatically re-enabled.

- **User status mirrors Active Directory (Automatic)**

When a new user is pulled in from Active Directory, they will be automatically enabled if active on the domain. The exception is when this will cause you to exceed your license count. For existing users, they will automatically be disabled if they are removed from all synchronization groups, deleted in AD, or disabled in AD. They will be automatically re-enabled when they are part of a synchronization group and are active in AD.

#### **d. Creating an Active Directory User**

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.

### Creating an Active Directory User

#### e. 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 be changed to match the Domain User throughout the system.

#### f. Integrated Windows Authentication

Windows Integrated Authentication allows Users to log into workstations and be automatically authenticated to Secret Server. A User's Active Directory credentials are automatically passed through to IIS, logging them into the site.

Setting up Windows Integrated Authentication requires additional configuration. A video demonstrating how to configure Secret Server and IIS can be found [here](#). Also see the “[Configuring Users to Log in using Windows Authentication](#)” Knowledge Base article. For further information, Microsoft has a [knowledge base](#) article troubleshooting some common client side issues with integrated authentication.

## g. Unlocking Local Accounts

If a User fails his login too many times (specified in the **Local User Passwords** section of the configuration page), their account will be locked out and they won't be able to log in. To unlock the account, log in as an administrator, click on **Administration**, then on **Users**, and then click on the users who is locked out. Next, click **Edit**, uncheck the **Locked Out** check box, and save.

## 4. User Preferences

Users can set their preferences by navigating to **Tools>User Preferences**.

### a. General Tab

Below is an explanation of the different settings:

**Mask passwords when viewing Secrets** – If enabled, this will mask the **Password** field for a Secret. There is a Configuration setting that will force this to be enabled for all Users. For details on password masking, see [Setting Up Password Masking](#) in the Secret section.

**Send email alerts when dependencies fail to update** – This setting will enable emails to be sent when dependencies fail to update. For further explanation of this, see the [Dependency Finder](#) section.

**Send email alerts when Secrets are changed** – This setting will enable 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 will be sent.

**Send email alerts when Secrets are viewed** – This setting will enable 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 will be sent.

**Send email alerts when Heartbeat fails for Secrets** - This setting can be enabled to email the user when Heartbeat fails for any Secret the User has View permission.

**Show the full folder path on search results** – This 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** – This enables the TreeView control for the Search tab on the **Legacy Home** screen. Note that this option does not apply to the **Dashboard**.

**Date Format** and **Time Format** – These settings are used to specify the date and time format displayed for a User in Secret Server.

**Language and My Theme** – These settings are used to customize the look of Secret Server on a per User basis. For details, see the [Customizing the Look](#) section.

## b. Launcher tab

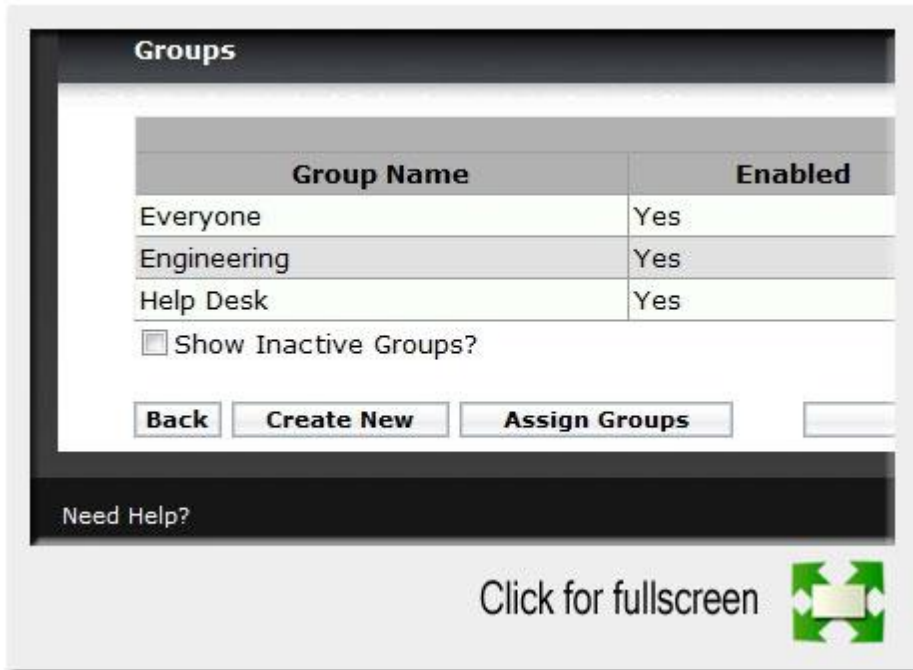
**Connect to Console** - This setting allows you to connect to remote machines using the Remote Desktop Launcher and will connect as an Administrator. This is the equivalent of using the /admin or /console switch when launching Remote Desktop.

**Allow Access to Printers, Allow Access to Drives, Allow Access to Clipboard** – These settings are used to allow the various items when using the Launcher. See the [Launcher](#) section for more details.

## 5. Groups

Secret Server allows administrators to manage Users through 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 various permissions and Roles that can be assigned to a User. Additionally, Groups can be synchronized with Active Directory to further simplify management.

### a. Creating a Group



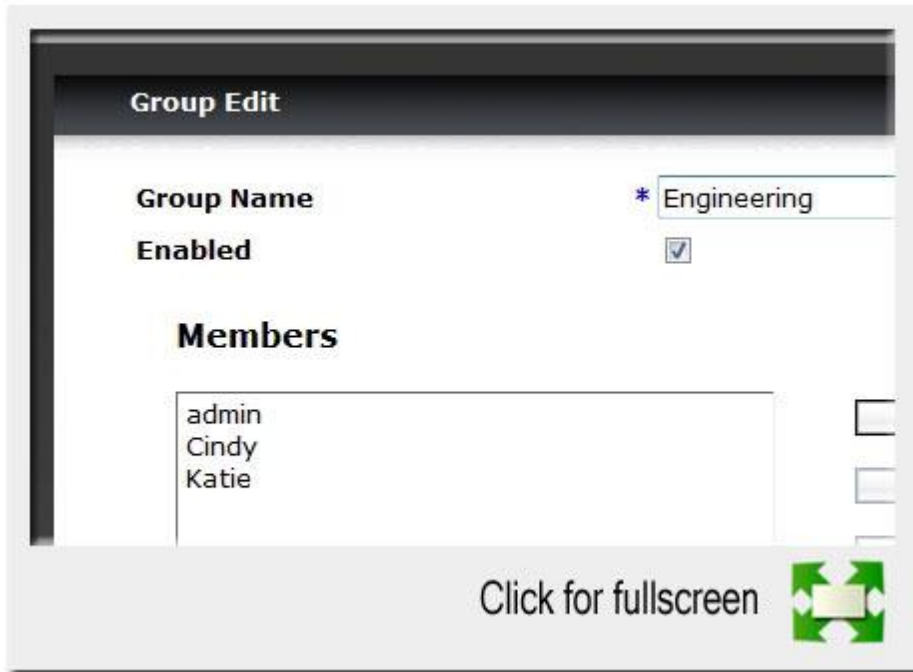
## Groups

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 the **Create New** button, 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](#) section).

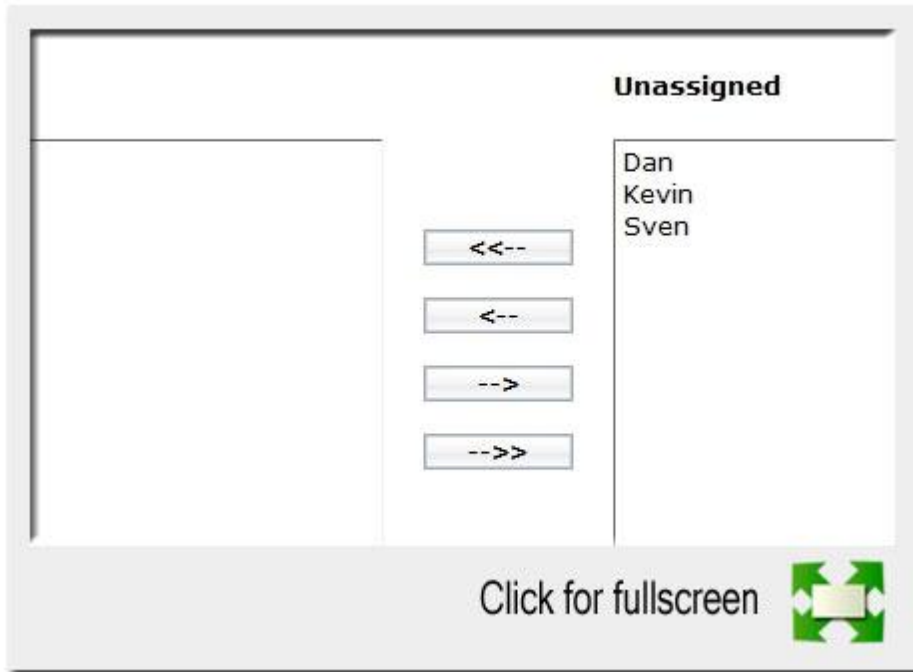
### b. Adding Users to a Group

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 the **Save** button and your new Group members will be added.



### Group Page

Alternatively, you can click the **Assign Groups** button on the main **Groups** page. This will allow you to select a Group from a drop-down list, and assign or unassign Users to the Group. In the **By User** tab, you can select a User from a drop-down list, and assign or unassign the User from the Groups in the selectable list boxes.



### Group Assignment

**Note:** that if the Group was created using Active Directory synchronization, this Group will not be editable. See the [Active Directory Synchronization](#) section for details on adding and removing Users using Active Directory synchronization.

## 6. Roles

Modeled after the Role Base Access Control mechanism (RBAC), 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 the following KB article: <http://updates.thycotic.net/link.ashx?SSRolePermissions>

Multiple permissions can be assigned to a Role. For example, you could assign Administrator Users, Edit Secret, Share 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 will allow the User to have Unlimited Administrator rights when Unlimited Administrator is enabled in the *Configuration*. By default, it is disabled. See the [Unlimited Administrator](#) section for more information.

### a. Creating a Role

You can create Roles from the *Roles* page. To get to the *Roles* page, navigate to *Administration>Roles*. Click the *Create New* button to add the Role.

### b. Editing Permissions for a Role

Navigate to *Administration>Roles*.



**Role Edit Page**

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 the *Edit* button. 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 the **Save** button to have the changes take effect.

### c. Assigning Roles to a User

To assign Roles to a User, click the **Assign Roles** button on the main **Roles** page. Depending on which tab is selected, this page will allow you either view the Roles that are assigned to Users or view the Users that are assigned to Roles. To change these settings, click the **Edit** button. Now select a Role from the drop-down 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 drop-down list, and assign or unassign Roles to them in the selectable list boxes.

## 7. IP Address Restrictions

IP Address Restrictions allow you to control which IP Address ranges users can use to log in to Secret Server.

### a. Creating an IP Address Range

To create an IP Address Range, go to the **IP Addresses** under **Administration**. Once there, click the **Create New** button. In the **IP Address/Network Name** text box, enter a descriptive name for your range. In the **IP Address Range** text box, enter an IP Address or IP Address range. Secret Server supports single IP Addresses (i.e., 10.0.0.4), a range separated by a hyphen (i.e., 10.0.0.1-10.0.0.255), and CIDR notation (i.e., 10.0.0.0/24). Finally, click **Save**.

### b. Editing and Deleting an IP Address Range

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 the **Delete** button.

### c. Assigning an IP Address Range

To assign a range to a user, go to the **Users** page under administration, click on a user name, 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 or ::1). This prevents total lockout from Secret Server.

## V. Administration

### 1. Configuration Settings

Secret Server is a highly customizable application. 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.

#### a. General Tab

- **Email Server** - Specify the domain name or IP address of your SMTP server. For example “smtp.yourcompany.com”.
- **From Email Address** - This is the *From* address for emails sent by Secret Server.
- **Allow automatic checks for software updates over internet** - 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 will be a link to the latest update. This feature is only available to those with Support licenses.
- **Enable Webservices** - Enable other applications to interact with Secret Server (still requires them to login as a Secret Server User).
- **Maximum Time for Offline Access on Mobile Devices** – This setting is used to set the amount of time that a mobile device can be disconnected from the server before it removes the cached Secret Server data off of the device.
- **Force Inactivity Timeout** – See [Configuring the Users](#) section.
- **Force Password Masking** - See [Setting Up Password Masking](#) section.
- 
- **Require Folder For Secrets** – See [Folders](#) section.

- **Prevent Application from Sleeping When Idle** – This setting prevents the application pool that Secret Server is running under from going to sleep.
- **Default Theme** – See [Customizing the Look](#) section.
- **Allow User to select theme** – Allows Users to customize the theme for Secret Server. This selected theme would only apply to their login. See [Customizing the Look](#) section for more details.
- **Enable Launcher** – This setting enables Remote Desktop Launcher capabilities for Secret Server. See the [Launcher](#) section for further details.
- **Allow Secret Server to Retrieve Website Content** – This setting enables the Web Launcher to retrieve the web site content in order to parse the form and find the login controls.
- **Allow Web Launcher Mappings to be Downloaded** – This setting enables the Web Launcher Configuration to download pre-approved website launcher settings from Thycotic.com.
- **Allow Web Launcher Mappings to be Uploaded Off-site** – This setting enables the user to upload successful Web Launcher Configurations to Thycotic.com where they will be approved and shared with other customers.

**Note:** There will not be any Secret data uploaded to Thycotic.com, only the website URL and control names are sent.

- 
- **Default Secrets Inherit Permissions** – See [Folders](#) section.
- **Require View Permission on Specific Folder for Visibility** – See [Folders](#) section.
- **Default Date Format** – This is the default Date format used for all Users. This setting can be overridden by each User. See [User Preferences](#) section for more details.
- **Default Time Format** - This is the default Time format used for all Users. This setting can be overridden by each User. See [User Preferences](#) section for more details.
- **Change Administration Mode** button – See the [Unlimited Administration](#) section.

## b. Security Tab

- **Force HTTPS/SSL** - By requiring HTTPS, Users will not be able to access Secret Server using HTTP.
- **Enable FIPS Compliance** – See [FIPS Compliance](#) section.

- **Encrypt Key using DPAPI** – This will encrypt 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 will be impossible if the server dies. After encrypting the key, an administrator of Secret Server will be able to decrypt it.

For details on the settings in the **Login** and **Local User Passwords** tab, see [Configuring the Users](#) in the Users section.

## 2. Administrator 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.

### a. User Audit Report

From the **Reports** page, on the **Reports - User Audit** dialog select a User and a date range to view, then **Search History** to view the User's audit trail.



## User Audit

The **Audit Search** displays results for all of the Secrets the selected User has viewed or edited during the selected time period. The administrator has the option of expiring all of the viewed Secrets, to notify Users to change sensitive information, or to force password changing (if the Remote Password Changing is configured).

To get a full view of the actions taken on a particular Secret, select that Secret from the results list. The Secret Audit displays the specific User actions for a Secret.

### b. Secret Audit

The audit log for a Secret can be accessed by clicking the **View Audit** button on **Secret View** page or navigating from the **User Audit Report**. The log will show the Date, the User Name, 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:

- View
- Update
- Editing Permissions
- Forced Expiration
- Check Out
- Set for Check-In
- Hide launcher password changes
- Adding, Updating and Removing Secret Dependencies

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 need to know exactly what was modified.

| Date               | Full Name |    |
|--------------------|-----------|----|
| 3/24/2010 09:34 PM | admin     | VI |
| 3/24/2010 07:35 PM | Dan       | VI |
| 3/24/2010 06:39 PM | Dan       | VI |
| 3/24/2010 06:39 PM | admin     | EE |
| 3/24/2010 06:38 PM | admin     | SE |
| 3/24/2010 06:38 PM | admin     | SE |
| 3/24/2010 06:35 PM | admin     | VI |
| 3/24/2010 06:28 PM | admin     | VI |
| 3/24/2010 04:59 PM | admin     | VI |
| 3/24/2010 11:56 AM | admin     | CI |

Click for fullscreen 

### Secret Audit

#### c. Report Auditing

In addition to the User Audit and individual Secret Audit, the **Reporting** feature provides a series of Activity, User, and Secret reports.

##### i) Legacy Reports

- **Secret Server Usage** - The Secret Server Usage report shows the number of Secret audit activity records (view, edit, sharing) by month over a period of time. This report is an indicator of overall usage of the system.

- **Secret Expiration Health** - The Secret Expiration Health report shows the number of Secrets in the system in various stages of expiration. This is a good indicator for the overall health of the Secrets in terms of age (frequently changed passwords are more secure).
- **Secret Template Distribution** - The Secret Template Distribution report shows the percentage and number of Secrets based on their Secret Template within the system. This typically indicates the types of information being stored.
- **Top Ten Viewers** - The Top Ten Viewers shows the ten Users who have viewed the most Secrets over a date period.

### ii) Secrets

- **What Secrets can all users see?** - Shows the Secrets that are viewable by all users. This report is useful from an auditing perspective to ensure that users are not able to access inappropriate Secrets.
- **What Secrets can a user see?** - Shows the Secrets that are viewable by a particular User (User has view permission). This report is useful from an auditing perspective to ensure that a User is not able to access inappropriate Secrets.
- **What Secrets have been accessed?** - Shows all the Secrets that have been accessed within the date range. This report shows the user and last accessed date for each Secret.
- **What Secrets have been accessed by a user?** - Shows all the Secrets that have been accessed within the date range for the user. This report shows the last accessed date for each Secret for the user.
- **What Secret permissions exist?** - Shows all the permissions on Secrets in the system along with where the Permission has been set. This report can be used to verify that all Secrets have the correct permissions.
- **What Secret permissions exist for a user?** - Shows all the permissions on Secrets for the user along with where the Permission has been set. This report can be used to verify that a user has the correct permissions on Secrets.

### iii) Folders

- **What folders can all users see?** - Shows the folders permissions for all users. This report is useful from an auditing perspective to ensure that users are not able to access inappropriate folders.
- **What folders can a user see?** - Shows the Folder's permissions for a particular User. This report is useful from an auditing perspective to ensure that a User is not able to access inappropriate Folders.
- **What folder permissions exist?** - Shows all the Folders in the system along with their assigned or inherited permissions. This report can be used to verify that all Folders have the correct permissions.

#### *iv) Groups*

- **Group Membership** - Shows the Role permissions for a particular User and where they are getting the Role permission from (Group, Role). This can be useful in diagnosing complex Role assignments.

#### *v) Roles and Permissions*

- **What role permissions does a user have?** - Shows the Roles and which Users have been assigned to the Role and how (directly or through a Group). This report can be used to quickly verify that all Users have been assigned to the correct Roles.
- **What role assignments exist?** - Shows the Roles and which Users have been assigned to the Role and how (directly or through a Group). This report can be used to quickly verify that all Users have been assigned to the correct Roles.
- **What role permission assignments exist?** - Shows the assignment of permissions to Users based on Role assignments and Group memberships. This report can be useful when auditing that permissions are assigned correctly.

#### *vi) User*

- **Failed login attempts** - Shows all failed login attempts to the Secret Server. This report can be used to show any attempts to compromise a User account.
- **Who hasn't logged in within the last 90 days?** - Shows User accounts that are not being used on a regular basis. Access by these Users should be re-evaluated to determine if they really need access to the system.

#### *vii) Activity*

- **Secret Activity** – Shows all Secret activity for a given date range. This report can be used to quickly verify Secret activity by all users.
- **Secret Activity Today** – Shows all Secret activity for today. This report can be used to quickly verify Secret activity by all users.

- **Secret Activity Yesterday** – Shows all Secret activity for yesterday. This report can be used to quickly verify Secret activity by all users.
- **Folder Activity** – Shows all folder activity for a given date range. This report can be used to quickly verify folder activity by all users.
- **Users Activity** – Shows all user activity for a given date range. This report can be used to quickly verify user activity by all users.
- **Custom Report Activity** - Shows all custom report activity for a given date range. This report can be used to quickly verify custom report activity by all users.

In addition to the packaged reports, a User can create their own. See [Creating Reports](#) section for more information.

### 3. Backup / 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 CVS spreadsheet.

#### a. Configuring Backups

##### Settings

- **Backup File Path** - This directory must exist on the web server and will store the zip file of the application directory.
- **Backup Database File Path** - This Folder must be accessible by the SQL server and will store the database.bak file.
- **Keep Number of Backups** – Number of previous backups to keep.

- **Notify Administrators on Backup Failure** – This will email all Users with the **Administer Backup** permission if the backup fails.
- **Enable Scheduled Backup** – Enables automatic backups at a set schedule.

## b. Setting up Folder Permissions

From the **Backup Administration** page, specify the correct directory paths for the IIS Secret Server file directory and the database backups to go. 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 place backups in them. The account that needs permissions will be displayed as an alert on the page.

## c. Manual Backups

On the **Backup Administration** page, the **Backup Now** button can be clicked to force an immediate backup. This is useful for testing the backup settings, and is recommended to be done before Upgrading.

## d. Scheduled Backups (*Professional or Enterprise Edition*)

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 who would be administrating a disaster recovery scenario, the database backup can either truncate the transaction log or keep it intact. The additional schedule settings will be available when the Enable Schedule Backup is enabled and the view page will indicate the time and date of the next scheduled backup.

## e. 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 will be inside the application backup file (the .zip file).

## f. Exporting Secrets: Configuring an Export

From within the **Administration>Export** page, select the Folder that needs to be exported. By default, all Secrets will be exported if a Folder is not selected. In the event that no particular Folder is selected, all Secrets will be 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 will be 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 need to be imported at a later date.

By default, the option to **Export Child Folders** is active. While this option is enabled, any export of a specified Folder will also export content located in Folders beneath the initial selection.



The screenshot shows a dialog box for configuring an export. At the top, it says "Please enter your password for security purposes." Below this, there are several fields and options:

- Folder:** A dropdown menu with a folder icon and the text "No Selected Folder".
- Password:** A text input field with a blue asterisk to its right.
- Export with folder path:** A checkbox that is checked.
- Export Child Folders:** A checkbox that is checked.

Below these options is a text area with the prompt "Enter any additional notes or explanations for the export." At the bottom of the dialog, there is a button labeled "Click for fullscreen" next to a green icon with four arrows pointing outwards.

### Exports

## g. Exported File Format

Secrets are exported as a comma separated file (csv) or as XML.

The csv file can be easily handled in Excel or other spreadsheet applications. The file is grouped by Secret Templates and each cluster of Secrets has a header row that contains the Template field names and is followed by all the exported Secrets of that Template.

The XML file follows the exact structure as 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. As long as exports are maintained, an installation of Secret Server can be completely reproduced on a separate instance by applying the exported file.

## h. 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 [“Restoring Secret Server from a backup”](#) KnowledgeBase article at support.thycotic.com

## 4. 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 situation where access to a particular 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.

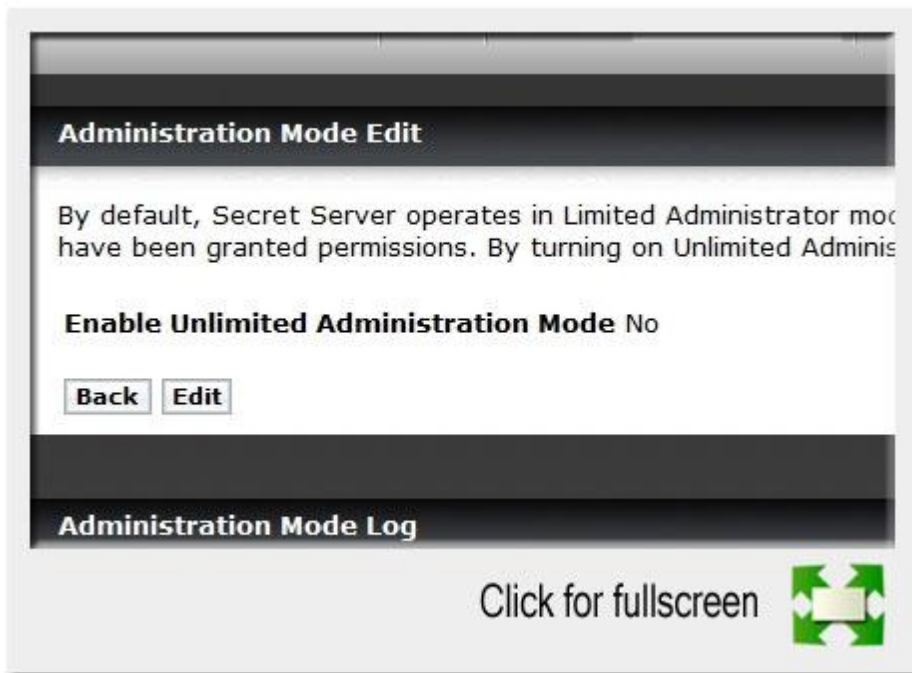
**Note:** An alert visible to all users will be displayed at the top of the Secret View page when Unlimited Administration Mode is enabled.

### a. Configuring Unlimited Administration Mode

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 set in **Configuration**.

To navigate to the Unlimited Administration section, you will need to go to the **Administration > Configuration** page, then click the **Change Administration Mode** button. It is recommended that Administrators have specific permissions to Folders and Secrets and this mode is only used temporarily to assign the correct permissions.

**Note:** Changes to Administration mode are logged in an audit grid. The grid shows the User, time of the change, and any notes made by the User.



## Unlimited Administration

### 5. 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.

- **Enable System Log** – This setting enables system logging.
- **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 **Administer System Log** assigned to it.
- **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 will be reduced by 25%.

To clear the System Log of all its records, click the **Clear** button.

### 6. Event Engine (*Professional or Enterprise Edition*)

## a. Subscription page

The screenshot shows a web interface for configuring an event subscription. It includes a text field for the subscription name, checkboxes for email alert settings, a table for subscribed users, an 'Add New' section with a dropdown menu, an 'Additional Email Recipients' text field, and a table for subscribed events. A 'Click for fullscreen' button with a green icon is located at the bottom right.

| Subscribed Users |   |
|------------------|---|
| Subscribers      |   |
| Help Desk        | X |

Add New --Groups--

| Subscribed Events |        |                      |   |
|-------------------|--------|----------------------|---|
| Entity            | Action | Condition            |   |
| Secret            | Create | In Folder: \Folder A | X |

### Event Subscription Page


- **Subscription Name** – This is the name for the Subscription.
- **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 Users** – This is a list of the Secret Server Users and Groups in this Subscription.
- **Additional Email Recipients** – The 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, User1's home email address.
- **Subscribed Events** – This is a list of the Events that are contained in this Subscription.

## b. Creating an Event Subscription

To add an Event Subscription, navigate to **Administration>Event Subscriptions**. In the **Event Subscriptions** page, click the **New** button.


In the **Subscription Name** field, enter a name for this new Event Subscription.


Add Users and Groups to this Subscription by selecting them from the **Add New** drop-down selector. They will be added to the **Subscribed Users** list above the **Add New** drop-down selector.

Add Events to this Subscription by adding rows to the **Subscribed Events** data grid. To do this, select an Entity type from the drop-down selector in the **Entity** column of the first row (Secret, User, Folder, etc.). After an Entity is chosen, you can now select an Action (Create, Delete, Edit Permissions, etc.). After an Action is selected, a condition may be available. Select the condition you wish to implement. Finally, to add this Event to the Subscription, click the add button (). This must be done before the **Save** button at the bottom of the page is clicked in order to add this Event to the Subscription.

### c. Editing a Subscription

To edit an Event Subscription, navigate to **Administration>Event Subscriptions**. On the **Event Subscriptions** page, click on the Subscription from the list of Subscription names. On the Subscription page, click the **Edit** button.

To remove a Subscribed User or Group, click the delete button () next to the entry in the **Subscribed Users** list.

To remove a Subscribed Event, click the delete button() next to the entry in the **Subscribed Event** list.

To add entries to either list, see the **Creating an Event Subscription** section above.

Click the **Save** button to save all changes.

### d. Deleting a Subscription

To edit an Event Subscription, navigate to **Administration>Event Subscriptions**. On the **Event Subscriptions** page, click on the Subscription from the list of Subscription names. On the subscription page, click the **Delete** button.


### e. Viewing the Event Subscription Log

**Event Subscription User Log**

Note: Only events that your user account is subscribed to will be shown, such as email group lists, that could be specified on the subscription settings page.

| Date                | Entity | Action | By User |   |
|---------------------|--------|--------|---------|---|
| 11/23/2010 04:56 PM | SECRET | CREATE | Katie   | [SecretServer] Event: [Secret] Account Container Name: Folder |

[Back](#) [Refresh](#)

[Click for fullscreen](#) 

### Event Subscription User Log Page

To view the Events that have been triggered in a Subscription, navigate to **Tools>View Event Subscription Log**. In the **Event Subscription User Log** list, the most recent Events to have been triggered will be on top of the list. **Note:** It may take a few seconds for the Events to make it into the Log.

## 7. CEF / SIEM Integration *(Enterprise Plus Edition)*

Secret Server can log to a 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.

### a. Configuring CEF

When in Administration -> Configuration, click the Edit button and check the **'Enable CEF Logging'** checkbox. When you do this, two additional text boxes will appear.

- **CEF Server** – The IP Address or name of the ArcSight or Syslog server
- **CEF Port** – The Port that the events will be sent to the server on

Once you have entered these values, click the **Save** Button.

### **b. 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.

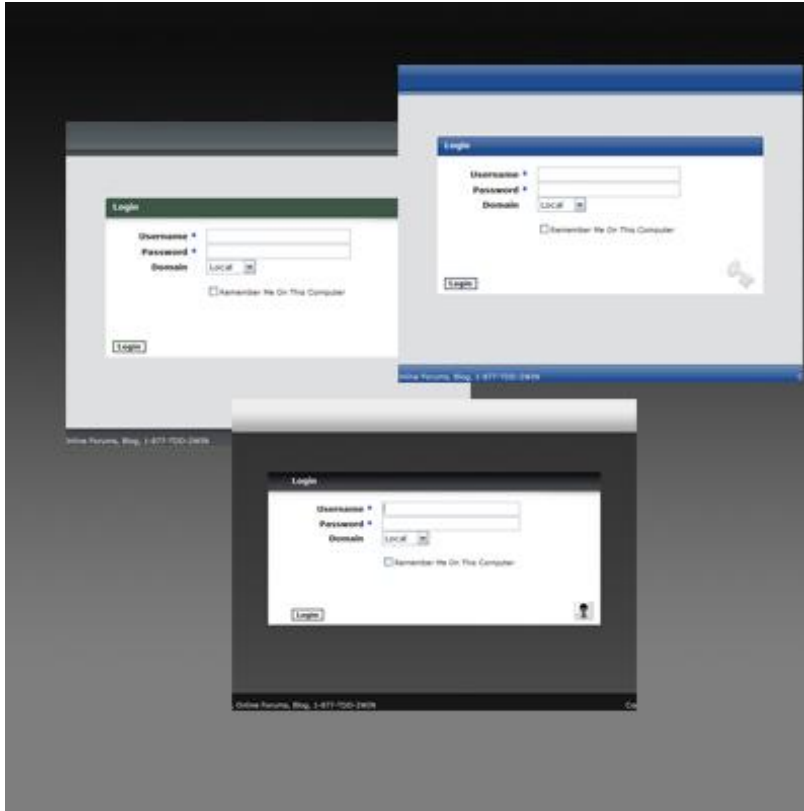
## **8. Language Maintenance**

The **Language Maintenance** page can be used to analyze the missing text from a custom language file. The Secret Server UI has been designed to be able to support any language using a resource file model. Secret Server ships with an English and Russian language file, but translating the English text to another language for a custom resource file is also possible. This page will compare the language resource files to the English one to identify all missing nodes. After an upgrade, the **Language Maintenance** page will illustrate the new nodes that need to be translated.

See the Knowledge Base article "[Translating Secret Server to Another Language](https://support.thycotic.com/knowledge-base/articles/translating-secret-server-to-another-language)" at support.thycotic.com for more technical information about creating another language file.

## **9. Customizing the Look**

By default Secret Server is set to a 'slate' theme unless specified within the Configuration settings. Secret Server comes with four other bundled themes: Classic, Corporate, Blue Chrome and ConnectWise. 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 theme** setting.



## Themes

### a. Creating Themes

Themes are controlled from style sheets and a central image directory within a theme directory. A guide for creating new themes is available in the form of a CSS document noting how each line affects specific aspects of Secret Server's appearance. CSS help, properties and tags are listed with examples at [www.w3schools.com](http://www.w3schools.com).

### b. Embedded Mode

**Embedded Mode** will remove 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 "http://myserver/Secretserver/login.aspx", then you can enable embedded mode by going to "http://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."

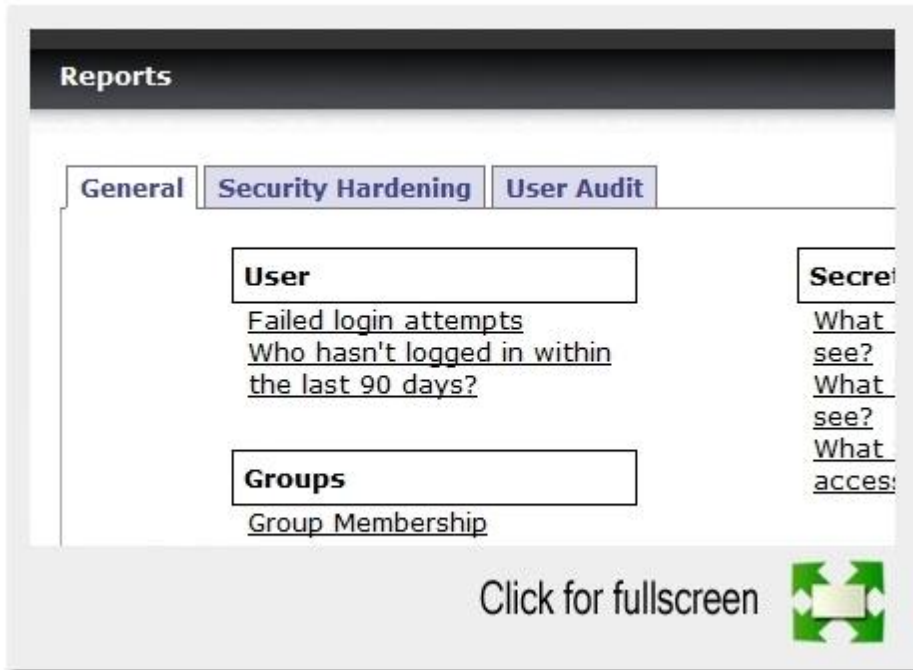
## 10. Reporting in Secret Server

The reporting interface comes with a set of Standard Reports. These Reports include a variety of 2D and 3D charting/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 (User, audit, permissions, Folders, etc). You can also 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.

The Security Hardening Report checks aspects of Secret Server to ensure security best practices are being implemented. While Secret Server will run with all of the items failing, administrators should be aware of possible security issues within an installation. For more details on this, see the [Security Hardening Tab](#) section below.

User Audit Reports show all Secrets accessed by a particular User during a specified period of time. For a more detailed explanation of this, see the [User Audit Reports](#) section below.

### a. General Tab



## Reports View Page

### i) Reports View Page

The Reports are listed under the Report Categories. To view a Report, click on the name. This will take 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 the [Auditing](#) section.

For details on the **Edit** button, see the [Configuring the Reports](#) section below.

The **Create it** link is a shortcut for creating a new Report. For further explanation, see the [Creating and Editing a Report](#) section.

### ii) Viewing a Report – Report View Page

On this page you will 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 will be visible and the text “There are no items” will be displayed in the **Show Data** section.

Some Reports use dynamic values like **User**, **Start Date**, **End Date**, etc. Adjust these values to generate the Report you need. Click the **Update Report** button to generate the new Report.

The **Edit** button allows you to alter the Report to fit your requirements. See the [Creating and Editing a Report](#) section below for details.

### iii) *Deleting or Undeleting a Report*

To delete a Report, click the **Delete** button.

To undelete a Report, you will need to navigate to the **Reports Edit** page (see the [Configuring the Reports](#) section) as deleted Reports are not visible on the Reports View page. On the Reports Edit page, click the **Show Deleted** button. This will display 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's name to go into its Report View page. In there, click the **Undelete Button**.

### iv) *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 on this, see the [Administrator Auditing](#) section.


### v) *Configuring the Reports – Reports Edit Page (Enterprise Edition)*

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 the **Edit** button on the Reports page.



## Reports Edit Page

- (1) Rearranging Report Categories and Reports

Any item with the  icon can be drag 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.

For details on the **Show Deleted** button, see [Undelete a Report](#) in the **Viewing a Report – Report View** page section.

## (2) Creating and Editing a Report

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 the **Edit** button.

**Note:** that the SQL script text cannot be edited for Standard Reports.

Below is an explanation of the different fields for the **Report Edit** page:

- **Report Name** – This is the name that is displayed on the Reports page. It is displayed as a link underneath its containing Reports Category.
- **Report Description** – This is the 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** – This is the selection for which Report Category to place the Report into.
- **Chart Type** – This is the Chart Type to use for displaying the results. If set to **None**, then a grid will be displayed.
- **3D Report** – This renders the Chart in the 3D style.
- **Page Size** – This is the page size limit setting for the data displayed in the grid.
- **Report SQL** – This is the actual SQL script used to generate the Report.

Reports support the embedding of certain parameters into the SQL in order 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](#)" Knowledge Base article.


Also available to aid the creation of custom Reports is the means to show Secret Server's SQL database information. By selecting the **SQL Table** from the drop down list, the details of the table's columns will be displayed in a grid. Click the **Show Secret Server SQL database information** link to see the **SQL Table** drop down list and **SQL Table Columns** grid.

Click the **Preview** button at the bottom of the page to see a preview of the chart. The resulting chart will display in the **Report Preview** section at the bottom of the page.


### (3) Creating a New Report Category

To create a new Report Category, click the **Create Report Category** button. The process is intuitive, but note that the **Report Description** entry is used as the tooltip for the Report Category on the Reports View page.

### (4) Deleting a Report Category

To delete a Report Category, click the  button next to the Report Category name. This will delete all the Reports contained in the Category. To undelete the Reports, see [Undelete a Report](#) in the Viewing a Report – Report View page section.

### (5) Editing a Report Category

To edit a Report Category, click the  button next to the Report Category name.

## b. Security Hardening Tab

The Security Hardening Report checks aspects of Secret Server to ensure security best practices are being implemented. While Secret Server will run with all of the items failing, administrators should be aware of possible security issues within an installation.

Below is an explanation of the different values:

- **Browser AutoComplete** - Browser AutoComplete allows web browsers to save the login credentials for the 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 (passwords show as \*\*\*\*\*). To activate this option, turn on the Force Password Masking option on the Configuration page.
- **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 particular User before that User's account is inactivated. A User with management permissions will then be required to reactivate 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 of time. Remember Me can be a security concern as it does not require re-entry of credentials to gain access to Secret Server. Turn Remember Me off to get a pass result. It must be set to be valid for 1 day or less to not get a fail result. Change the "Remember Me" settings on the Configuration page.
- **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, uppercase, 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" will give 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 page 19 of 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 on installing and configuring SSL certificates.

- **Using SSL** - 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.

**Note:** Use of SSL is highly recommended for Secret Server.

### c. User Audit Tab

User Audit Reports show all Secrets accessed by a particular User during a specified period of time. For a more detailed explanation of this, see [User Audit Reports](#) in the Audit section.

## 11. Server Clustering (*Enterprise Plus Edition*)

Secret Server has the ability to 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 will also allow users to load balance for better performance.

### a. Setting up Clustering

For instructions on enabling Clustering in Secret Server, see the "[Setting up Clustering](#)" Knowledge Base article.

## 12. Secret Server Encryption

### a. Advanced Encryption Standard

Secret Server uses different types of encryption to ensure data security. Every 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 level of security for sensitive data. The creation of AES was instigated by the National Institute of Standards and Technology (NIST) and the National Security

Agency (NSA) to find a replacement for the Data Encryption Standard (DES), which had numerous issues, namely small key size and efficiency.

**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.

To address concerns from the cryptographic community, the NIST embarked on a transparent selection process. During the selection process the 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.

For more information about the technical specifications of AES, please see the official standard.

## b. SHA-512

Secret Server User's passwords are hashed in the database using the **SHA 512** hashing function. A hash function differs from an encryption method such as AES because a hash function is practically impossible to reverse. Hashing algorithms are mathematical functions to replace inputted text values with numerical ones. If the input text is the same, the final hashed value will also be the same. The input text of "fox" will always produce the same hashed value. Minor changes in the input value will radically alter the hashed output, as shown in the examples below. In addition each password is hashed with a "Salt", which is just a random text. This guarantees that if two users use the same password, their hash in the database will not be the same, which prevents [Rainbow Table](#) attacks.

Example input text: "The quick brown fox jumps over the lazy dog".

Hashed value: 07e547d9 586f6a73 f73fbac0 435ed769 51218fb7 d0c8d788 a309d785 436bbb64  
2e93a252 a954f239 12547d1e 8a3b5ed6 e1bfd709 7821233f a0538f3d b854fee6

Example input text, with 'dog' changed to 'cog': "The quick brown fox jumps over the lazy cog".

Hashed value: 3eeee1d0 e11733ef 152a6c29 503b3ae2 0c4f1f3c da4cb26f 1bc1a41f 91c7fe4a  
b3bd8649 4049e201 c4bd5155 f31ecb7a 3c860684 3c4cc8df cab7da11 c8ae5045

## c. SSL Overview

Secret Server can be configured to run using Secure Sockets Layer (SSL) certificates. It is strongly recommended that Secret Server installations run using SSL. Not using SSL will significantly reduce the security of the contents of Secret Server since browsers viewing the site will not be using an encrypted connection.

## 13. Two Factor Authentication Login

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 is a method of strong authentication that requires two different forms of identification instead of the traditional single password.

### a. Email Two Factor Authentication


Secret Server uses this design by allowing Administrators to require Two Factor Authentication through a confirmation email for designated Users. For additional information on Two Factor Authentication please see [http://en.wikipedia.org/wiki/Two-factor\\_authentication](http://en.wikipedia.org/wiki/Two-factor_authentication).

#### *i) Configuring Two Factor for Users*

From the Users administration page, select a User to configure for Two Factor Authentication. Edit the selected User and enable the Two Factor Authentication option. Verify that the correct email address information is set, as that address is where the confirmation email will be sent.

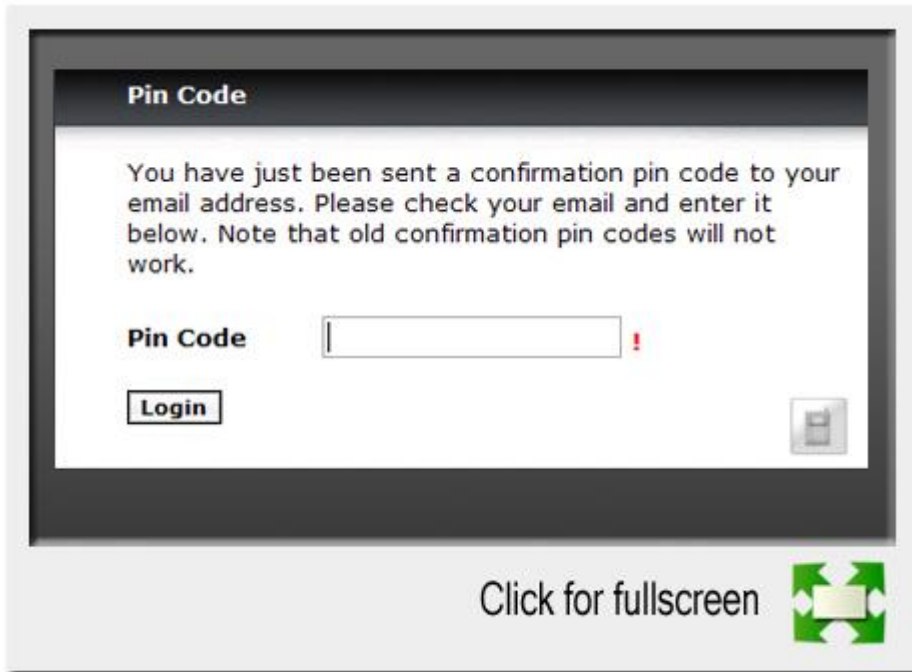
### Edit User

|  |                              |
|--|------------------------------|
| <b>User Name</b>                       | admin                        |
| <b>Display Name</b>                    | * admin <input type="text"/> |
| <b>Email Address</b>                   | <input type="text"/>         |
| <b>Domain</b>                          | Local                        |
| <b>Password</b>                        | <input type="text"/>         |
| <b>Confirm</b>                         | <input type="text"/>         |
| <b>Email Two Factor Authentication</b> | <input type="checkbox"/>     |

Click for fullscreen 

### User Edit Page

The next time that User attempts to login to the system, a unique confirmation code will be emailed to them. The User will then be required to enter a new confirmation code at each login.



**Confirmation Code Prompt**

### ***b. RADIUS Authentication (Professional or Enterprise Edition)***


Secret Server allows the use of 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.

#### ***i) Configuring RADIUS***

On the Login tab of the Configuration page, RADIUS can be setup, which requires enabling **RADIUS Integration**, specifying the server address, the ports, and the **RADIUS Shared Secret**. The RADIUS Shared Secret is a specific term for RADIUS clients and is not a reference to Secrets in Secret Server. The **RADIUS Login Explanation** can be customized to give Users detailed instructions for entering their RADIUS information. Once enabled, the **Test RADIUS Login** button **will appear 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 can't be accessed, the failover server will be used.

How do I integrate RADIUS with Secret Server?

|                                  |                                     |
|----------------------------------|-------------------------------------|
| <b>Enable RADIUS Integration</b> | <input checked="" type="checkbox"/> |
| <b>RADIUS Server IP</b>          | 127.168.99.196                      |
| <b>RADIUS Client Port</b>        | 1812                                |
| <b>RADIUS Server Port</b>        | 1812                                |
| <b>RADIUS Shared Secret</b>      | ••••••••                            |
| <b>RADIUS Login Explanation</b>  | Enter your RADIUS                   |


Click for fullscreen 

## Configuring RADIUS

### ii) *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, enter the **RADIUS User Name** for this User to match the RADIUS server.

|   |  |
|---|--|
| <b>Domain</b>                           | Local                                      |
| <b>Password</b>                         | <input type="text"/>                       |
| <b>Confirm</b>                          | <input type="text"/>                       |
| <b>Email Two Factor Authentication</b>  | <input type="checkbox"/>                   |
| <b>RADIUS Two Factor Authentication</b> | <input checked="" type="checkbox"/>        |
| <b>RADIUS User Name</b>                 | <input type="text" value="Administrator"/> |
| <b>Enabled</b>                          | <input checked="" type="checkbox"/>        |
| <b>Locked Out</b>                       | <input type="checkbox"/>                   |

Click for fullscreen 

### Configuring RADIUS for the User

## 14. Configuring SMTP Email Server

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 will be used to send notifications.



### SMTP Configuration

When configuring Secret Server to an SMTP server, the server's availability can be verified through Telnet.

In the command prompt run the following : "telnet servername 25", servername being the SMTP server, and 25 being the port Secret Server attempts to connect through. An example command would look like "telnet smtp.somesite.com 25".

If virus protection is running, a rule to allow aspnet\_wp.exe to send e-mails may be needed.

## 15. FIPS Compliance *(Enterprise Plus Edition)*

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 under environments which are FIPS compliant.

For instructions on enabling FIPS in Secret Server, see the [“Enabling FIPS Compliance in Secret Server”](#) Knowledge Base article.

## 16. PCI Datacenter Compliance

Secret Server can make it easier to comply with various PCI-DSS requirements.

Requirement 8 - Assign a unique ID to each person with computer access|

Requirement 10 - Track and monitor all access to network resources and cardholder data

Requirement 11 - Regularly test security systems and processes

Requirement 12 - Maintain a policy that addresses information security

Our solution will help 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.

As for Requirement 10, Secret Server is able to monitor all access to network resources. By employing Remote Password Changing to force password changes, Administrators are able to monitor and update network resources on a customized schedule. You can create a password changing schedule that best suits your environment.

Lastly, to help you comply with Requirement 12, our software’s global configuration and template driven data structure can be optimized to fit the requirements of your current information security policy or assist in creating a policy based around Secret Server.

Listed below are several of the configuration options available:

- Two-factor authentication
- Login password parameters (applies to local accounts only)
- Force HTTPS/SSL
- Require Folder for Secrets
- Enable Launcher
- Enable Webservices

## 17. Upgrading Secret Server

To upgrade Secret Server, you will need valid support licenses. To renew your support, please use our [online web form](#) or [contact sales](#). Once you have valid support licenses, follow the steps in this KB article to upgrade: [Upgrading Secret Server](#)

## VI. Licensing

Secret Server's licensing model allows for scalability and enhanced core functionality in the form of Edition enhancements (Professional and Enterprise) and User packs. Licenses can be purchased for these items:

**Users** - Secret Server ships with a free single User. Additional User licenses can be purchased through the Online Store ([www.thycotic.com/products\\_secretserver\\_buynow.html](http://www.thycotic.com/products_secretserver_buynow.html)) to expand an installation.

**Support** - Support licenses allow instances to receive all software updates. The number of Support licenses and User licenses must be equal in order to be eligible for upgrades.

Users must be supported in order to receive assistance from the Secret Server support team.

### 1. Professional License

The Professional license enables the following Secret Server capabilities:

- Folder Synchronization
- IP Restrictions
- Remote Password Changing
- RADIUS Integration
- Windows Integration, Active Directory Synchronization and Login
- Automated Backups

### 2. Enterprise License

The Enterprise license enables the following Secret Server capabilities:

- All the Professional license capabilities
- Secret Access Request
- DoubleLock
- Custom Reports
- Secret Check Out

- Managing Service Accounts

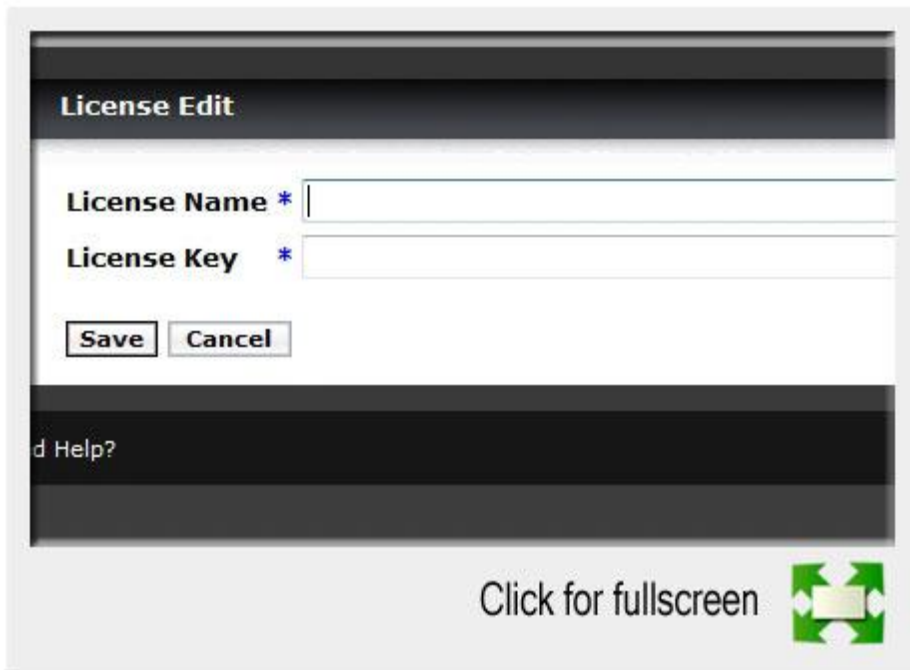
### 3. Enterprise Plus License

The Enterprise license enables the following Secret Server capabilities:

- All the Enterprise and Professional license capabilities
- FIPS enablement
- CEF / SIEM integration
- Server Clustering

### 4. Installing New Licenses

Once a license is obtained, it can be installed by copying the license name and code into the corresponding fields on a new **License** page.




**License Edit**

License Name \*

License Key \*

d Help?

Click for fullscreen 

**Adding a License**

## 5. Converting from Trial Licenses

If you previously had evaluation licenses and recently purchased, you will need to 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 will start getting “License has expired” error messages.

## 6. Activating Licenses

All non-evaluation licenses require activation after install. Activation is per license/web server combination. Therefore, if you bring up a new web server, it will need to be activated even if your previous web server was already activated. After installing each license, you will be prompted to activate. Follow the on-screen prompts for online or offline activation. The activation process gathers the name, email, and phone of the individual activating for internal purposes only. No other personal information will be sent to Thycotic.

## 7. Limited Mode

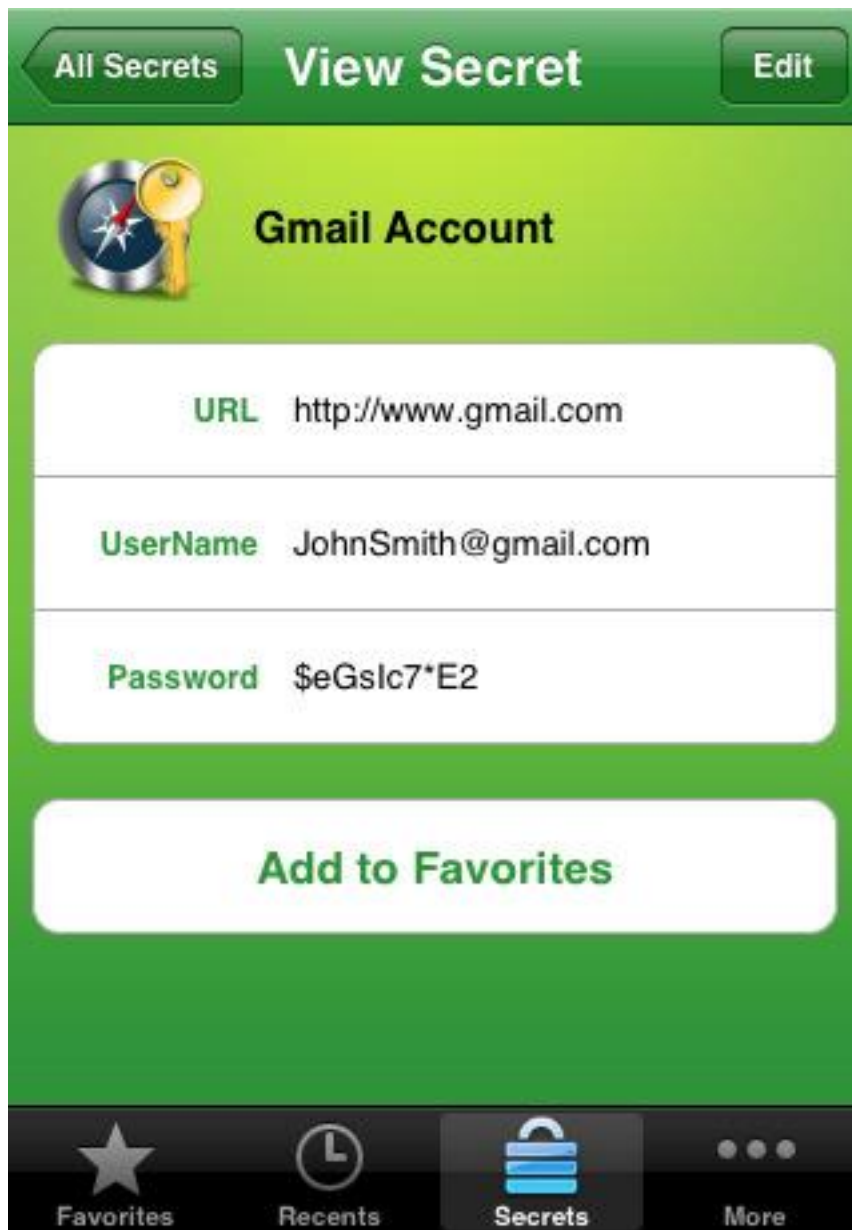
If you fail to activate, your system will be placed in limited mode, which will prevent the following actions:

- Creating and Editing Secrets
- Importing Secrets
- Active Directory Sync
- Web Services (Mobile applications)
- Manual RPC

# VII. External Applications

## 1. iPhone Application

The Password Manager Secret Server is available for free from the iTunes App Store for the iPhone, iPod Touch, and iPad. This great app features an intuitive Apple User interface making it easy to store, access, and organize passwords, and other private data. The app offers a portable method for access Secret Server while maintaining the strict security and permission based access.



## Setting Up the iPhone

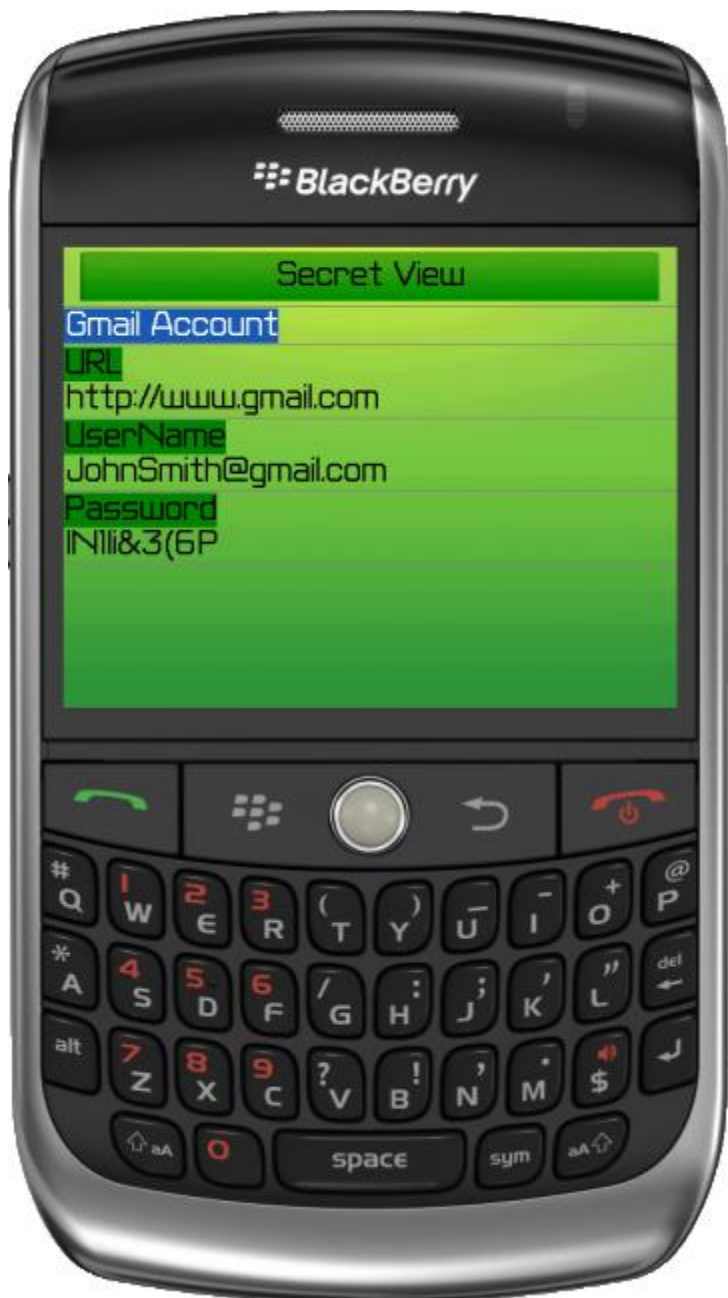
Once the application is installed on the iPhone, select **Existing Installed Account** to access your Secret Server instance. Enter the URL, Username, Domain, and Password to setup the Account. For local Users the Domain will be left blank. Once the account is set up, you can access and edit your Secrets from the

application. You will be required to login again when your token expires based on the length of the **Allow Remember Me** settings. It is recommended that you also set up the **Pin Lock** feature to prevent possession of the phone from giving access to your Secrets.



## 2. BlackBerry Application

The Secret Server BlackBerry application is available for free through the Blackberry App World. The app offers a portable method for access to Secret Server while maintaining the strict security and permission based access.



## Setting Up the BlackBerry

Once the application is installed on the BlackBerry, select **Existing Installed Account** to access your Secret Server instance. Enter the URL, Username, Domain, and Password to setup the Account. For local Users the Domain will be left blank. Once the account is set up, you can access your Secrets from the application. You will be required to login again when your token expires based on the length of the

**Allow Remember Me** settings. It is recommended that you also set up the **Passcode Lock** feature to prevent possession of the phone from giving access to your Secrets.



### 3. Android Application (beta)



The Secret Server Android application is available as a beta at Thycotic.com. Sign up for to receive the beta at ([http://www.thycotic.com/beta\\_android.html](http://www.thycotic.com/beta_android.html)). The app offers a portable method for access to Secret Server while maintaining the strict security and permission based access.

## VIII. Appendix

### a. Technical Support

To be supported, a customer must have an equal number of User support licenses as their number of User licenses and the User support licenses must not have expired. All support licenses expire 365 days after they are issued.

*i) What can be requested from Technical Support?*

Technical assistance is provided for all issues/bugs/questions related with Secret Server. We do not support software from other vendors except where Secret Server functionality is specifically affected. For instance, we do provide support if Windows Authentication to Microsoft SQL Server is working for other applications but not Secret Server. We do not provide support if Windows Authentication for Microsoft SQL Server is not functioning correctly - in such cases, support must be sought from the specific vendor.

*ii) How do I access Technical Support?*

Web: <http://thycotic.com/support.html>

Email: [support@thycotic.com](mailto:support@thycotic.com)

Phone: +1-877-833-2946 / +1-703-752-6113

Hours: 9am - 4:30pm ET

Technical assistance is provided through telephone, email, and remote assistance. Remote Assistance sessions are also offered when necessary using our preferred remote support vendor (currently <http://www.copilot.com>).

*iii) What response time can I expect?*

Phone calls will be answered immediately or may go to voicemail depending on call volume. Voicemails and support requests through email will receive a response within 24 hours during business hours.

*iv) What about upgrades?*

Customers that are supported have access to all new releases (both minor and major releases).

*v) Can I request new features?*

Customers with active support licensing are encouraged to participate on **Wishlist**. **Wishlist** allows for discussion and voting on new features. Also, feature requests can be sent directly from **Wishlist** at [http://www.thycotic.com/products\\_secretserver\\_wishlist.html](http://www.thycotic.com/products_secretserver_wishlist.html).