

IBM Security Secret Server
Version 10.7

Getting Started Guide

Contents

Getting Started Wizard	1
Security	2
Local Admin Account	2
HTTPS/SSL	2
Backups	3
Active Directory Integration	4
Add a Domain	4
Enable Active Directory Integration	4
Add a User	4
Add a Group	4
Enable Active Directory Synchronization	4
Choose Synchronization Groups	5
Run Active Directory Synchronization	6
Enable/Disable Active Directory Users	6
Synchronize and Authenticate AD Users via Distributed Engine	6
Secrets	7
Create a Secret	7
Heartbeat	9
Enable Heartbeat	9
Run Heartbeat for a Secret	9
Heartbeat Status Codes	10
Remote Password Changing	11
Enable Remote Password Changing	11
Perform a manual password change	11
Common Remote Password Changing Error Codes	12
Appendix	13
Licenses	13
Activate Licenses	13

Getting Started Wizard

At the end of the initial installation of Secret Server, you are prompted with the Getting Started Wizard, which will walk you through adding license keys, setting up your email server, and creating your first group. If you're not immediately routed to the Getting Started Wizard after your first login, you can also access the wizard by going to **Help | Getting Started**.

If you would like to reference information on how to administer licenses without going through the Getting Started Wizard, see the [Appendix](#).

Security

As you begin to use Secret Server, there are a few standard security settings we recommend configuring. While these are optional, it's strongly suggested that you configure these settings as best practice.

LOCAL ADMIN ACCOUNT

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

- ❑ Store the credentials in a secure location that you can access even if you were to lose all other access to Secret Server.
- ❑ Enable **Allow Users to Reset Forgotten Passwords** to provide a way of resetting the password, should the account be locked out or if the password is forgotten. Select **Configuration** from the **ADMIN** menu, and go to the **Local User Passwords** tab to find this setting. Note that this requires having an [SMTP server configured](#) (KB).
- ❑ Configure the **Local User Passwords** settings to enforce password requirements, expiration, password history, and other password policy settings.

HTTPS/SSL

As best practice, it's recommended to force HTTPS/SSL access to Secret Server. This requires setting up an SSL certificate for the website. Using a domain certificate is recommended. However, if you don't have a certificate already in mind, one option is [Installing a Self-Signed Certificate](#) (KB). Once you have your certificate:

- ❑ Configure the HTTPS binding for your Secret Server website using the certificate you choose (instructions for this are included in the KB article [here](#)).
- ❑ Ensure your certificate is trusted on the machines of those who will be accessing Secret Server. See [Trusting an SSL Certificate on a Client Machine](#) (KB) for instructions.
- ❑ Enable **Force HTTPS/SSL** on the **Security** tab of the Secret Server **Configuration** settings.

Backups

Configure backups to avoid losing your data. Secret Server provides the option to automatically take a backup on the interval you specify, sending the backups to a local or network location. There are two components of an entire backup of Secret Server: the web application files and the database. Find these settings by selecting **Backup** from the **ADMIN** menu.

For details around configuring the backup paths, see [Backup Configuration File Path Settings](#) (KB).

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

Active Directory Integration

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

ADD A DOMAIN

1. From the **ADMIN** menu, select **Active Directory**.
2. Click **Edit Domains** and then **Create New**.
3. Fill in the domain information and the username and password that will be used for connecting to the domain and synchronizing users and groups.
4. Click **Save and Validate**.

ENABLE ACTIVE DIRECTORY INTEGRATION

1. From the **Active Directory** page, click **Edit**.
2. Select the **Enable Active Directory Integration** check box and click **Save**.

Now you are ready to add individual users or groups of users for access to Secret Server using their Active Directory credentials. See the relevant section below for instructions.

ADD A USER

You can now add an individual AD user. If you prefer to sync users by group, see the Add a Group section below. To add an individual user:

1. From the **ADMIN** menu, select **Users**.
2. Click **Create New**, then select your domain from the **Domain** drop-down menu.
3. Fill in the user's Active Directory **User Name**, a **Display Name** that will be shown in Secret Server. The user's email address will be synced from Active Directory, if available, so it isn't necessary to fill that in.
4. Click **Save**.

ADD A GROUP

Secret Server can sync with security groups from Active Directory to automatically add, enable, and disable users. This can streamline the process of managing which users are enabled, which means they are counting toward your Secret Server user licensing.

Enable Active Directory Synchronization

1. From the **Active Directory** page, click **Edit**.
2. Select the **Enable Synchronization of Active Directory** check box. Additional settings will appear.
3. Choose how often you want Secret Server to sync with Active Directory by configuring the **Synchronization Interval**. The default value is 1 day.

4. Choose a **User Account Options** setting. See the following page for a detailed description of each option. **Users are disabled by default (Manual)** is recommended for initial testing.
5. Click **Save**.

Edit Active Directory Configuration

Active Directory Integration

Enable Active Directory Integration

Enable Integrated Windows Authentication *Requires advanced IIS settings (See [KB Article](#))*

Active Directory User Synchronization

Enable Synchronization of Active Directory *Enable to synchronize users by Active Directory Group. Once saved set the group with Edit Synchronization button.*

Synchronization Interval for Active Directory

Days

Hours

Minutes

User Account Options User status mirrors Active Directory (Automatic) ▾

Save Cancel

User Account Options

- ✓ **Users are enabled by default (Manual)** Secret Server users will automatically be enabled when they are synced 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-disabled.
- ✓ **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.

Choose Synchronization Groups

Now you will choose the security groups from Active Directory you want to sync with Secret Server:

1. From the **Active Directory** page, click **Edit Synchronization**.
2. Choose your domain from the drop-down menu. More options will appear.

3. Click **Search**. Select the group(s) you would like to sync from the **Available Groups** list, then click the single left arrow < to add them to **Synchronized Groups**.
4. Click **Save**.

Run Active Directory Synchronization

From the **Active Directory** page, click **Synchronize Now** to run a sync. You can click **Refresh** to monitor the logs until you see the message **Completed Domain synchronization for all domains**.

Enable/Disable Active Directory Users

If you selected a Manual setting for **User Account Options**, you can now enable or disable your AD users' access to Secret Server by going to the **ADMIN** menu and selecting **Users**. To enable users, select the **Show Inactive Users** check box, then select the box beside the user(s) to enable and choose **Enable Users** from the Bulk Operation drop-down menu. To disable users, use the same process, selecting **Disable Users** from the Bulk Operation menu.

Synchronize and Authenticate AD Users via Distributed Engine

In addition to syncing Active Directory with Secret Server via your local site, Secret Server can also synchronize and authenticate users from Distributed Engine. An Engine can be installed in a remote site, allowing all users to use the same Secret Server with their Active Directory Credentials. This feature allows organizations with users in different locations to easily get access to Secret Server and now organizations with Secret Server running in the cloud can use local Active Directory credentials for Authenticating. To setup Active Directory to Synchronize from Distributed Engine:

Secrets

New Secrets can be created from Dashboard. Click **HOME** to reach Dashboard from any page within Secret Server.



CREATE A SECRET

1. From Dashboard, find the **Create Secret** widget.
2. Select a template from the drop-down menu. For this example, we'll use **Active Directory Account**.
3. After selecting a template, you will be taken to a page where you can enter the information you would like to store and manage. Enter a name for the Secret in the **Secret Name** field (Figure A).
4. Enter information in the rest of the fields (fields with an asterisk * are required).
5. If you would like to place the Secret in a specific folder, click **No Selected Folder** or the folder name already listed to select another location (Figure B). Otherwise, click **Clear** to store the Secret at the root level.
6. Click **Save** to save your settings and view the new Secret.

The image is a screenshot of the "New" secret creation form in the Secret Server interface. The form has a dark header with the word "New" in white. Below the header, there is a "General" tab. The form contains several fields: "Secret Template" is a dropdown menu set to "Active Directory Account"; "Secret Name" is a text field containing "MYDOMAIN\svc_sqlserver"; "Domain" is a text field containing "mydomain.local"; "Username" is a text field containing "svc_sqlserver"; "Password" is a text field with masked characters "*****", a "Generate" button, and a strength indicator "Strong" with a checkmark; "Notes" is a text area containing "SQL Server service account"; and "Folder" is a dropdown menu set to "No Selected Folder".

Figure A Enter the Secret information and select a folder location

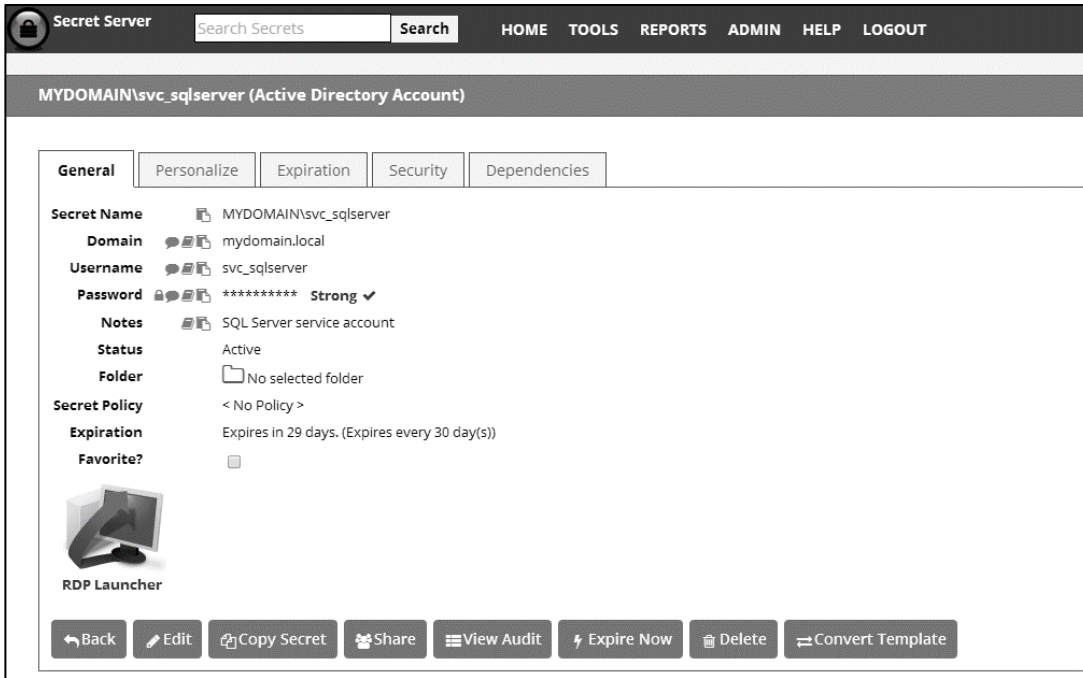


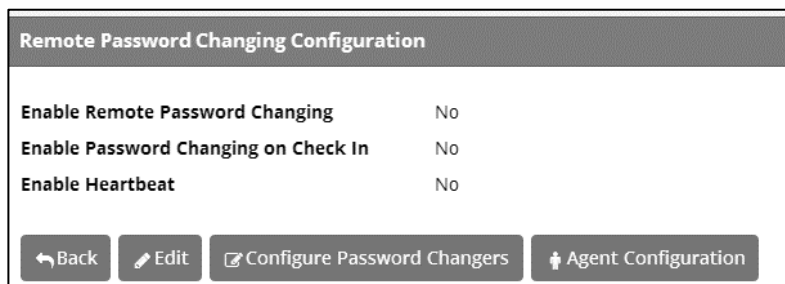
Figure B Newly created Secret

Heartbeat

Heartbeat allows you to determine from Secret Server whether the credentials in a Secret authenticate successfully with their target system. By default, Heartbeat is turned off in Secret Server.

ENABLE HEARTBEAT

1. From the **ADMIN** menu, select **Remote Password Changing**.
2. Click **Edit**, select the **Enable Heartbeat** check box, and then click **Save**.



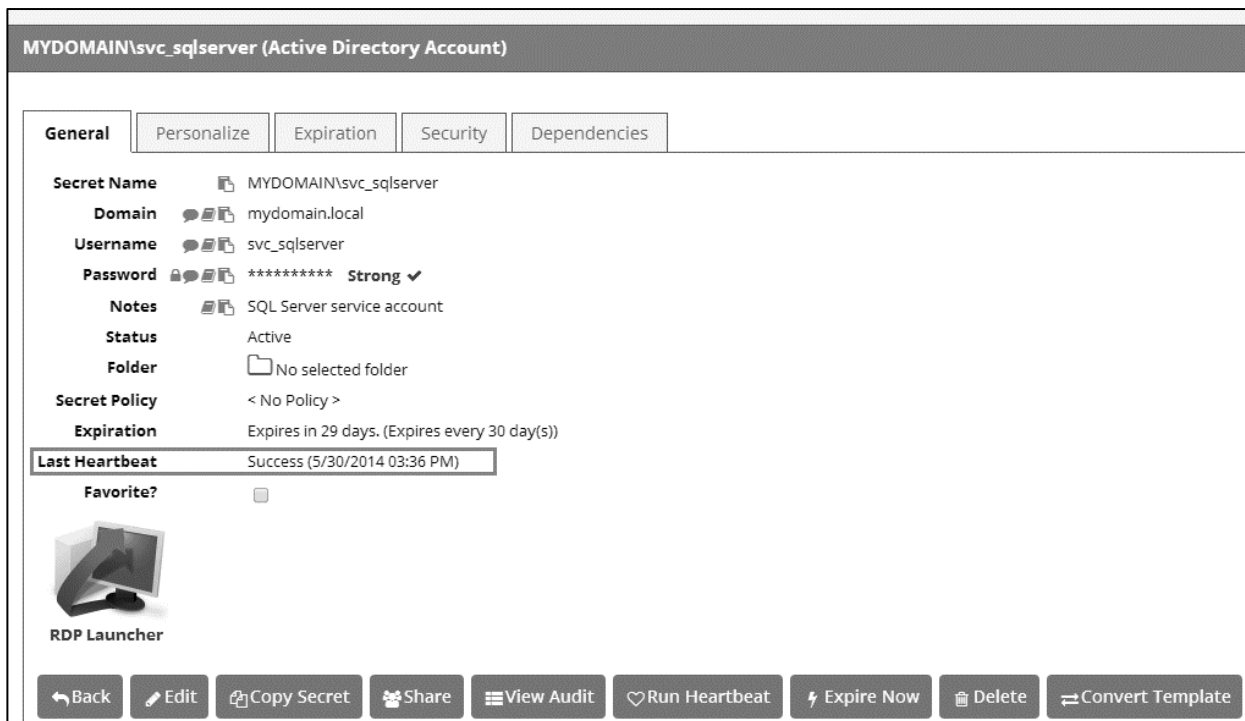
Remote Password Changing Configuration

Enable Remote Password Changing	No
Enable Password Changing on Check In	No
Enable Heartbeat	No

← Back Edit Configure Password Changers Agent Configuration

RUN HEARTBEAT FOR A SECRET

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



MYDOMAIN\svc_sqlserver (Active Directory Account)

General Personalize Expiration Security Dependencies

Secret Name MYDOMAIN\svc_sqlserver
Domain mydomain.local
Username svc_sqlserver
Password ***** Strong ✓
Notes SQL Server service account
Status Active
Folder No selected folder
Secret Policy < No Policy >
Expiration Expires in 29 days. (Expires every 30 day(s))
Last Heartbeat Success (5/30/2014 03:36 PM)
Favorite?

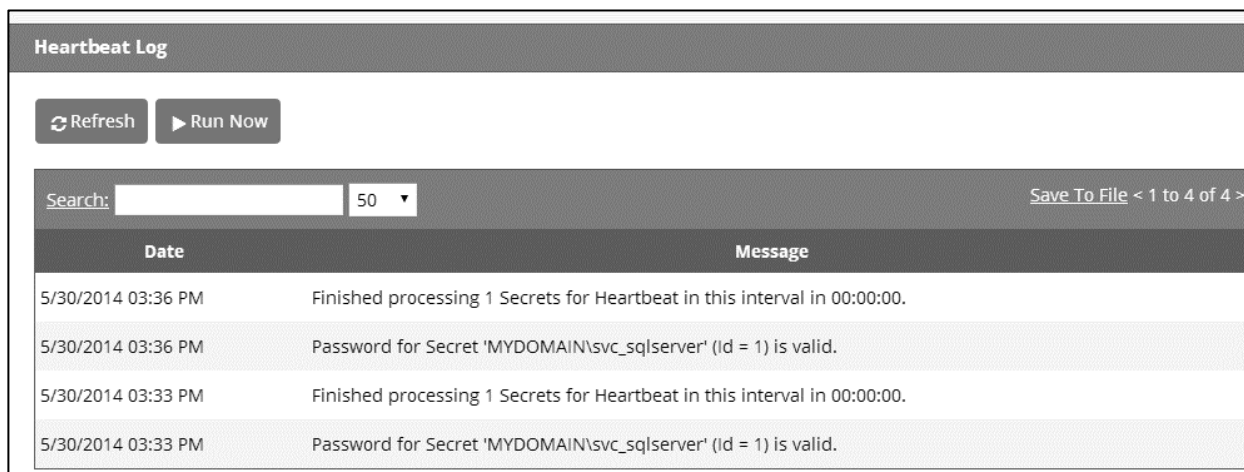
RDP Launcher

← Back Edit Copy Secret Share View Audit Run Heartbeat Expire Now Delete Convert Template

HEARTBEAT STATUS CODES

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

If you receive any Heartbeat status code aside from Success, you can check the Heartbeat log for details. To view the entry, select **Remote Password Changing** from the **ADMIN** menu and then search for the Secret name in the **Search** field of the **Heartbeat Log**.



The screenshot shows the 'Heartbeat Log' interface. At the top, there are 'Refresh' and 'Run Now' buttons. Below them is a search bar with a 'Search:' label, a text input field, and a dropdown menu set to '50'. To the right of the search bar is a 'Save To File < 1 to 4 of 4 >' link. The main part of the interface is a table with two columns: 'Date' and 'Message'.

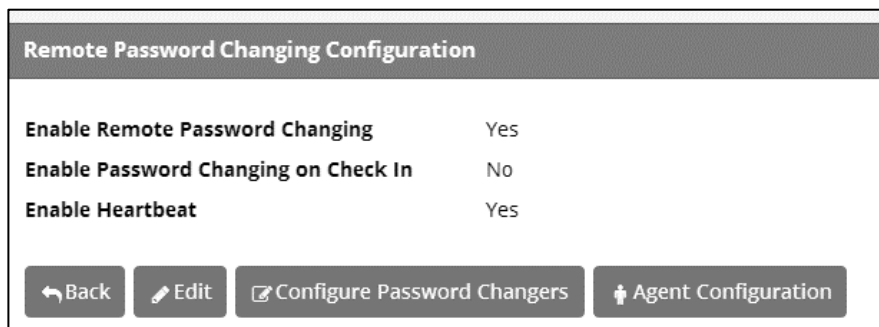
Date	Message
5/30/2014 03:36 PM	Finished processing 1 Secrets for Heartbeat in this interval in 00:00:00.
5/30/2014 03:36 PM	Password for Secret 'MYDOMAIN\svc_sqlserver' (Id = 1) is valid.
5/30/2014 03:33 PM	Finished processing 1 Secrets for Heartbeat in this interval in 00:00:00.
5/30/2014 03:33 PM	Password for Secret 'MYDOMAIN\svc_sqlserver' (Id = 1) is valid.

Remote Password Changing

Secret Server provides the ability to either kick off a password change manually or schedule automatic password changes to occur at a regular interval.

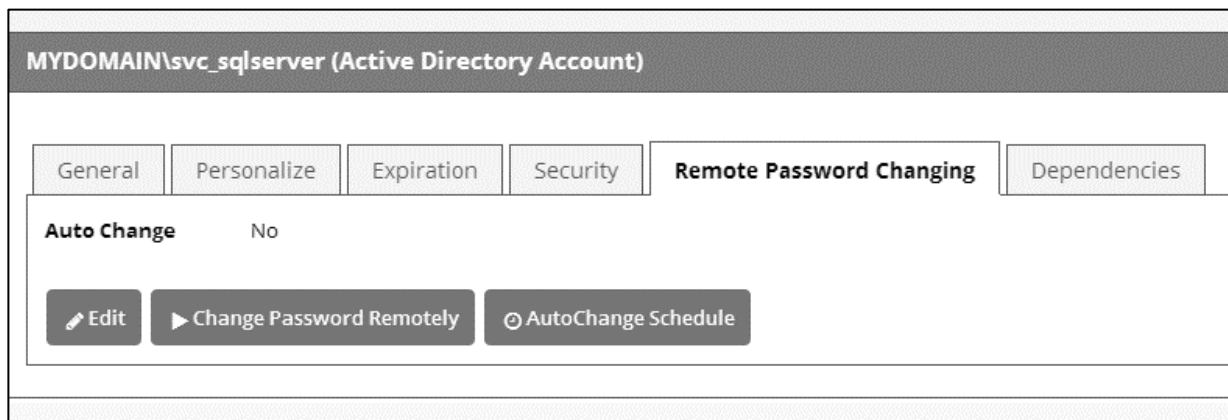
ENABLE REMOTE PASSWORD CHANGING

1. From the **ADMIN** menu, select **Remote Password Changing**.
2. Click **Edit**, select the **Enable Remote Password Changing** check box, and then click **Save**.



PERFORM A MANUAL PASSWORD CHANGE

1. From **Dashboard**, click the Secret you would like to test and then click **View**.
2. Click the **Remote Password Changing** tab, and then click **Change Password Remotely**.
3. Either provide a new password by typing it in the **Next Password** field, or click **Generate** to generate a random password.
4. Click **Change** to queue the Secret for a password change. Click **Back** and then the **General** tab to return to the Secret view.
5. You can verify that the password change completed either by unmasking the password on this screen (click the lock icon beside the password field) or by looking at the **Remote Password Changing** log. You can find the Remote Password Changing log by selecting **Remote Password Changing** from the **ADMIN** menu.



Change Password Remotely

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

Secret Name MYDOMAIN\svc_sqlserver

Next Password *

COMMON REMOTE PASSWORD CHANGING ERROR CODES

NERR_PasswordPolicySettings The password Secret Server is trying to set is a repeating password, or password that doesn't meet domain password policy standards. A common reason is minimum password age, which is often defaulted to 24 hours.

ERROR_ACCESS_DENIED The user account could be set to Not Able to Change Password or logon was denied.

ERROR_INVALID_PASSWORD Either the user does not exist (ensure the usernames match) or the password is not correct.

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

Appendix

LICENSES

After installation, the first thing we recommend doing is entering your licenses. You can do this in the Getting Started Wizard or from the Licenses administration page (instructions below). This will not only allow you to add more users but also will enable additional features in Secret Server.

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

Activate Licenses

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