Passly (AuthAnvil)

User Guide

Version R95

English

November 10, 2021

Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contents

Contents

Passly (Authanvil) Overview

Kaseya introduces a new addon module with this release, integrating Passly (AuthAnvil) identity and access management (IAM) solution with the Kaseya VSA. Integration with the VSA comprises a suite of three services called collectively **AuthAnvil Password Solutions**.

- **Two Factor Authentication** - Installed and configured as a separate website instance.
- **Password Server** - Installed and configured as a separate website instance.
- **Single Sign On** - Configured using a dedicated tab on the Two Factor Authentication website.

Important Note: In the case where a user account or IP address is whitelisted in the AuthAnvil two-factor module, the same user account and/or IP address will be subject to Kaseya's native two-factor authentication.

Two Factor Authentication

Integration enables two factor authentication for:

- Users logging into the VSA
- Users logging into Kaseya agent managed Windows servers and workstations
- Remote control sessions started from within the VSA
- Live Connect sessions, set independently from other types of remote control sessions

Alerts and logging are provided for all two factor authentication activity. Active Directory integration is supported. You can optionally enable endpoints with a "queue" of passcodes to support authentication when endpoints cannot connect to a network, for example laptops out in the field.

Password Server

The same AuthAnvil module includes integration with Password Server. Password Server is used to configure and store all the credentials VSA administrators are required to work with, on behalf of multiple customers. Password Server includes the ability to set policies for credentials, control user access to each credential using personal, private and shared vaults, schedule password updates, and maintain logs of credentials usage. Password Server supports both SAML-enabled logons that allow immediate access and logons that require a business workflow to complete the logon. Password Server can optionally include the two factor authentication credentials you've created using the Two Factor Authentication service.

Note: Password Server is not supported in SaaS environments.

Single Sign On

A credential, with or without two factor authentication, can be added as a "menu app" item to the Single Sign On service. Once the Single Sign On menu is configured, the VSA user only needs to authenticate once—typically using two factor authentication—to gain access to this menu. Clicking any app in the menu provides instant access to any other resource without having to re-authenticate. The three services, integrated with the VSA, handle all authentications entirely behind the scenes, providing immediate, highly- secure access to all the machines you manage.

One of the applications you can add to your Single Sign On menu is an app to logon to the VSA. That means the Single Single On menu becomes the front end for user access to both the VSA and all other authentications VSA users require to perform their daily tasks.

You can also add Password Service itself as an app to the Single Sign On menu.

Agent Procedure Approvals using Two Factor Authentication

Instead of signing and then approving agent procedures using two different VSA users, you can now sign and **approve your own agent procedures using your own 2FA passcode** *(page xiii)*, if Two

Factor Authentication has been enabled for your VSA user.

Installation

The AuthAnvil integration addon module for VSA is installed by default at no charge when you upgrade to R91. AuthAnvil is purchased separately. All three AuthAnvil services must be installed on a separate system from the KServer. Usually all three services are installed on the same system, along with the database server used by the AuthAnvil services.

- See AuthAnvil Password Solutions **System Requirements https://help.scorpionsoft.com/entries/25881456-System-Requirements**.

Integrating Passly *(AuthAnvil)* with the VSA

Note: In SaaS environments, the wizard described below does not display. Instead use the Configure Kaseya Logon (page vii) page to specify the Passly (AuthAnvil) instance you are integrating. Password Server is not supported in SaaS environments.

Before Running the Setup Wizard

Navigating to an unconfigured Passly (AuthAnvil) module displays a one time setup wizard. *Before running the one time setup wizard* the following Passly (AuthAnvil) services need to be installed separately from the system hosting the Kaseya Server. This includes:

- **Two Factor Authentication** - required
- **Password Server** - optional
- **Single Sign On** - optional

Running the Setup Wizard

For Two Factor Authentication, the one time setup wizard prompts you to provide the following information:

- **The Two Factor Auth SAS URL** - For example: `http://<yourwebsite>/AuthAnvil/sas.asmx`
- **The Two Factor Auth Server Site ID** - Defaults to 1. A different number applies only if your Two Factor Authentication service is running in multi-tenant mode.
- **Define a White listed User that will not be required to use AuthAnvil Two Factor Authentication** - Defines a white-listed user that will not be required to use AuthAnvil Two Factor Authentication. Users will continue to be subject to Native Two Factor requirement(s), when applicable. Delimit VSA usernames with commas.

You can optionally integrate Password Server with the VSA. If you elect to do this, the wizard prompts you to upload two files while running the wizard: These files are typically located here:

```
C:\Program Files\Scorpion Software\AuthAnvil Password Server\AAPS\web.config
C:\Program Files\Scorpion Software\AuthAnvil Password Server\AAPS\SyncAgent Setup Package.zip
```

You are are also asked to provide the web service URL for your Password Server instance. For example:

```
https://<yourwebsite>/AAPS/AAPS.svc
```

After Running the Setup Wizard

Once the setup wizard completes, you will see a Two Facto Auth menu. If you elected to add integrate Password Server, a Password Server menu also displays.

Mapping User Records

When creating users in the VSA, Two Factor Authentication and Password Server, **ensure that each user is defined using matching usernames and email addresses.** Single Sign On runs as a part of Two Factor Authentication and does not maintain a separate list of users.

Enabling 2FA for VSA Logons

Use this procedure to enable two factor authentication (2FA) for VSA users logging into the VSA.

> **Note:** When creating users in the VSA, Two Factor Authentication and Password Server, **ensure that each user is defined using matching usernames and email addresses.** Single Sign On runs as a part of Two Factor Authentication and does not maintain a separate list of users.

1. Select the AuthAnvil > Two Factor Auth > **Configure Kaseya Logon** option. After running AuthAnvil setup wizard, you should see the following settings already populated.
   - **AuthAnvil SAS URL** - The 2FA server you are integrating with the VSA.
   - **Whitelist Users** - As a safeguard, one or more "senior admins", delimited by commas. These users are NOT required to use AuthAnvil Two Factor Authentication to logon. Users will continue to be subject to Native Two Factor requirement(s), when applicable. Delimit VSA usernames with commas.
   - **Whitelisted IPS** - Defaults to blank. Optionally includes a range of user IP addresses that are allowed to log into the VSA.
   - **Whitelisted User Configuration** - Defaults to 'Required AuthAnvil Two Factor Authentication for All users except those in the whitelist'.
2. Uncheck the **Kaseya Logon Configuration** checkbox. This means all VSA users must logon using 2FA except your whitelisted "senior admins".
3. Test logging into the VSA. You can view a log of 2FA Kaseya logons on the **View Logons to Kaseya** *(page xiv)* page.

Enabling 2FA for End User Machine Logons

Use this procedure to require two factor authentication (2FA) for any user logging on to any machine managed by a Kaseya agent. The feature requires deploying an additional agent—called an **AuthAnvil agent**—to a Kaseya agent machine.

1. Navigate to the **Two Factor Auth** module.
2. On the **Manage Agent Groups** *(page ix)* page.
   - Click **Add Group** to create a new AuthAnvil agent group.
   - Add machines to the new AuthAnvil agent group by moving them to the **Machines in Group** list.
   - Click the **Show Advanced** button to **Enable Authentication for KLC**
3. On AuthAnvil > **Deploy Agents** *(page x)* page:
   - Select the **AuthAnvil Agent Group** to deploy.
   - Select machines in the **Select the endpoints that you wish to deploy AuthAnvil to** list.
   - Select **AuthAnvil Server Settings**.
     - ✓ This identifies the specific **Two Factor Authentication** server and **Site ID** you will use to authenticate user passcodes for a given set of machines. Each customer organization may have its own **Two Factor Authentication** server to manage its own set of user passcodes.

- Optionally configure a second **Two Factor Authentication** server for redundancy.
- Enter **Override Settings**.
  - ✓ This ensures the VSA administrator still has access to the machine if the 2FA passcode cannot be used.
  - ✓ Optionally set **Advanced Settings**.
  - ✓ You can modify override settings using the **Change Override Password** *(page xii)* page.
- Click **Deploy**.
  - ✓ You can modify agent settings after you deploy them using the **Modify Agent Settings** *(page xi)* page.

4. Confirm AuthAnvil agents have been successfully deployed using the **Discover Agents** *(page xi)* page.
5. View the results of **Discover Agents** query on the **View AuthAnvil Agent Info** *(page xiv)* page.
6. Test that AuthAnvil managed machines now require 2FA user logons.

Enabling 2FA for Remote Control from the VSA

You can require VSA users enter a 2FA passcode before launching a remote control session from within the VSA console. Entering this 2FA passcode is independent of whether the machine itself requires 2FA to logon.

- See **Remote Control Authentication** *(page ix)*

Note: 2FA for **Live Connect** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#4796.htm)* sessions are set separately from other remote control sessions. They are configured using the **Manage Agent Groups** *(page ix)* page.

Enabling 2FA for Live Connect

Enabling 2FA for **Live Connect** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#33845.htm)* sessions is configured using the **Manage Agent Groups** *(page ix)* page. After adding an AuthAnvil agent group, click the **Show Advanced** button to **Enable Authentication for KLC** - If checked, a user must use 2FA to use **Live Connect** on a machine.

- 2FA for **Live Connect** sessions are set separately from **other remote control sessions** *(page iv)*.
- Once enabled, you can use the **View KLC Audit Logs** *(page xv)* page to view Live Connect 2FA logon activity.
- For 9.3 the **Remote Control Authentication** *(page ix)* page only applies if you are using Live Connect (Classic). Live Connect (Classic) can be enabled by setting the **Use new Live Connect when clicking the Live Connect button in Quickview** option to `No` in System > Default Settings.

Enabling 2FA for Agent Procedures Approval

The **Agent Procedure Approval** *(page xiii)* page enables VSA users to approve *their own* agent procedures using two factor authentication (2FA).

If signing and approval of agent procedures is enabled *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#9332.htm)*, new or saved agent procedures must be approved before they can be run. Without 2FA, a standard user must have a *second user* approve a

new agent procedure before it can be run, using the Agent Procedure > **Pending Approvals** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#17981.htm)* page.

Monitoring Module Alerts

There are two categories of AuthAnvil alerts.

- AuthAnvil *server* alerts
- AuthAnvil *agent* alerts

AuthAnvil Server Alerts

1. Select the AuthAnvil servers you want to monitor using the **Define AuthAnvil Server(s)** *(page viii)* page.
2. Configure server alert settings using the **Configure Server Alert Settings** *(page ix)* page. *These settings apply globally to all AuthAnvil server machines you are monitoring in the VSA*.
3. View AuthAnvil alarms on the **View AuthAnvil Alarms** *(page xiii)* page and the Monitor > Alarm Summary page.

AuthAnvil Agent Alerts

1. Select the machines you want to install AuthAnvil agents on, using the **Manage Agent Groups** *(page ix)* and **Deploy Agents** *(page x)* pages.
2. Select the types of actions you want to take in response to triggered AuthAnvil agent alerts using the **Configure Agent Alert Settings** *(page xii)* page. *These settings apply globally to all machines in all AuthAnvil agent groups in the VSA*.
3. View AuthAnvil alarms on the **View AuthAnvil Alarms** *(page xiii)* page and the Monitor > Alarm Summary page.

Using Single Sign On to Logon to the VSA

One of the applications you can add to each VSA user's Single Sign On menu is an app to logon to the VSA. This means the Single Single On menu provides immediate, secure access to the VSA as well as all other resources VSA users require to perform their daily tasks.

Configuration

1. Logon to your Two Factor Authentication web server instance and use the Single Sign On tab to manually create a `Kaseya Logon` app.

   > See **Adding the Virtual System Administrator (VSA) for Single Sign On https://support.idagent.com/hc/en-us/articles/360009148537-Adding-the-Virtual-System-Administrator-VSA-for-Single-Sign-On.**

2. Download the public key certificate *(*.cer)* associated with the Kaseya Logon app from the Two Factor Authentication Manager > Single Sign On > Applications > `Kaseya Logon` > Certificate Authority page.
3. Enable access to the VSA using Single Sign On using the VSA > AuthAnvil > **Configure Kaseya Logon** *(page vii)* page. You are required to upload the certificate you downloaded in step 2.

Logon using Passly (Authanvil) On Demand

Virtual System Administrator™ supports single sign-on integration with Passly (Authanvil) On Demand, a cloud-based identity and access management web service.

1. A user initially logs into Passly (Authanvil) On Demand using *multi-factor authentication*, a strengthened method of user identification. This is the only time the user authenticates to access many different applications, hence the name 'single sign-on'.
2. Inside Passly (Authanvil) On Demand the user is shown a page of single sign-on apps. This can include a single sign-on app for the Virtual System Administrator™.
3. The user clicks any app's icon to immediately access that application. Passly (Authanvil) On Demand manages the specific logon requirements for each app, including periodic password changes if necessary, without the user's involvement.

Note: For more information, see **Passly (Authanvil) On Demand** *(https://help.authanvil.com/hc/en-us)*.

Prerequisites

- Access to Passly (Authanvil) On Demand.
- Access to Virtual System Administrator™.

Configuring the Passly (Authanvil) On Demand Kaseya App

1. Log into Passly (Authanvil) On Demand.
2. Select **SSO Manager**.
3. Click the add icon, then the book icon to select the `Kaseya` app template icon.
4. Click the **Application Configuration** tab.
   - **Change Image** - Optionally upload an icon for your new application.
   - **Application is Enabled** - Check to enable this application.
   - **Give your application a name** - Enter a name for your new application. You may wish to identify the specific VSA being accessed in the name.
   - **Authentication Policy** - Select an authentication policy.
5. Click the **Protocol Setup** tab.
   - **Protocol Type** - Select `SAML SP-init`.
   - **Reply to URL** - Replace the string `kaseyamachine` with your VSA domain name. For example change `http://kaseyamachine/vsapres/web20/core/ssologin.aspx` with `http://yourVSAname/vsapres/web20/core/ssologin.aspx`
6. Select **Advance Settings** on the same tab.
   - **Signing Algorithm** - Select `SHA-256` for stronger encryption.
7. Select the **Attribute Transformation** tab.
   - Confirm the `User.EmailAddress` custom attribute mapping displays.
   - This setting matches the email address of the Passly (Authanvil) On Demand user with a *VSA username formatted as the same email address* to access the VSA.
8. Click the **Permissions** tab.
   - Click **Add Groups** to add the user groups that will have access to your new application.
   - Note the email addresses of all users assigned the `Kaseya` app. You will need to know this when configuring the VSA.
9. Click the **Signing and Encryption** tab.
   - Click **Download**.
   - A `*.cer` file is downloaded to your local machine.

Configuring the VSA

1. Log into the VSA.
2. On the System > **Users** page, for each VSA user who will be accessing the VSA from Passly (Authanvil) On Demand:
   - Create or rename the username formatted as the user's email address.
   - Each VSA user's username must match the email address of the Passly (Authanvil) On Demand user assigned the `Kaseya` app.

   > **Note:** VSA users can still log on manually using their VSA username and password. Passly (Authanvil) On Demand provides an alternate method of logging in that ignores the VSA password.
3. On the Auth Anvil > **Configure Kaseya Logon** page:
   - **Select Certificate** - Click to display additional options.
   - **Choose File** - Click to select the `*.cer` file you downloaded from Passly (Authanvil) On Demand.
   - **Import Certificate** - Click to upload the `*.cer` file.
   - **Reply to URL** - Enter the following URL, replacing the `<yourVSAname>` with your VSA name. This should match step 5 in *Configuring the Passly (Authanvil) On Demand Kaseya App* above.

   `http://<yourVSAname>/vsapres/web20/core/ssologin.aspx`
   - **Enable Single Sign On to Kaseya** - Check this checkbox.
   - **Disable Two Factor Auth during Kaseya server logons** - Ensure this is checked. Passly (Authanvil) On Demand is being used instead.

Using the Kaseya Server App in Passly (Authanvil) On Demand

1. Logon to Passly (Authanvil) On Demand as any user in a user group assigned the `Kaseya` single sign-on app.
   - The new `Kaseya` app displays on the user's **My Apps** page.
2. Click the `Kaseya` single-sign-on app.
   - You are automatically logged into the VSA.

Two Factor Authentication

Configure Kaseya Logon

Passly (AuthAnvil) > Two Factor Auth > Configure Kaseya Logon

The **Configure Kaseya Logon** pages enables or disables two factor authentication (2FA) for users logging into the VSA. You can optionally limit VSA logons to those initiated from whitelisted IP addresses. Once configured, you view a log of 2FA Kaseya logons on the **View Logons to Kaseya** *(page xiv)* page.

> **Note:** *See* **Enabling Two Factor Authentication for VSA Logons** *(page iii).*

Kaseya Two Factor Auth Settings

- **AuthAnvil SAS URL** - The **Two Factor Authentication** server you are integrating with the VSA.
- **Site ID** - Accept the default value of 1. A different site ID number is only required if the **Two Factor Authentication** website your are integrating with is operating in multi-tenant mode.

- **Whitelist Users** - Optionally enter the usernames of one or more VSA users, *delimited by commas.* These users will be required or excluded from using 2FA logons, depending on the option you set in the **Whitelisted User Configuration**.
- **Whitelisted IPs** - Optionally include a range of IP addresses that VSA users must initiate a browser session from to log into the VSA. Delimit IP ranges by commas.
- **Whitelisted User Configuration** - Select how the **Whitelist Users** field is interpreted.
  - **Required Two Factor Auth for All users except those in the whitelist**
  - **Required Two Factor Auth only for users in the whitelist**
- **Kaseya Logon Configuration** - Uncheck the **Disable the Two Factor Auth during Kaseya server logons**. This means all VSA users must logon using AuthAnvil 2FA except your whitelisted users and whitelist IP addresses. Users will continue to be subject to Native Two Factor requirement(s), when applicable. Delimit VSA usernames with commas.

Kaseya Single Sign On Configuration

You can also use this page to add a logon app for the VSA itself. The app is then added to each VSA user's Single Sign On menu. This means the Single Single On menu provides immediate, secure access to the VSA as well as all other resources VSA users require to perform their daily tasks.

> **Note:** *See* **Using Single Sign On to Logon to the VSA** *(page v).*

- **Single Sign On** - If checked, enables the VSA to accept logons initiated by clicking a Kaseya app displayed on a user's Single Sign On menu.
- **Reply To URL** - The URL the VSA uses to accept Single Sign On requests. Example: `http://<YourKaseyaServerName>/vsapres/web20/core/ssologin.aspx`
- **Certificate Information** - The certificate the VSA uses to certify the identity of the Single Sign On server. Download the certificate from the Two Factor Authentication Manager > Single Sign On > Applications > `Kaseya Logon` > Certificate Authority page.

  > **Note:** The `Kaseya Logon` application must already be added as an SSO application in Two Factor Authentication before you can download its *public* certificate (*.cer) and upload it into the VSA here.

- **Certificate Expiry** - The certificate's expiration date.
- **Select Certificate** - Selects a certificate to import into the VSA.

Define AuthAnvil Server(s)

`Passly (AuthAnvil) > Two Factor Auth > Define AuthAnvil Server(s)`

The **Define AuthAnvil Server(s)** page selects one or more machines hosting AuthAnvil servers that you may wish to monitor. Hosted AuthAnvil servers can include:

- **Two Factor Authentication**
- **Password Server**
- **Single Sign Server**
- Any separate database server providing database services to an AuthAnvil product.

Use the **Configure Server Alert Settings** *(page ix)* page to configure alerts for AuthAnvil servers.

Configure Server Alert Settings

Passly (AuthAnvil) > Two Factor Auth > Configure Server Alert Settings

The **Configure Server Alert Settings** *(page ix)* page configures alert actions for monitored AuthAnvil servers. An alert is triggered when an AuthAnvil web service is down.

- **Monitor AuthAnvil Web Server** - If checked, AuthAnvil servers specified using the **Define AuthAnvil Server(s)** *(page viii)* page are monitored.
  - **Create Alarm** - If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reporting > Reports > Logs > Alarm Log.
  - **Create Ticket** - If checked and an alert condition is encountered, a ticket is created.
  - **Run Script** - If checked and an alert condition is encountered, an agent procedure is run. You must click the **select agent procedure** link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking **this machine ID** link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.
  - **Email Recipients** - If checked and an alert condition is encountered, emails are sent to the specified email addresses. Email is sent directly from the VSA to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Remote Control Authentication

Passly (AuthAnvil) > Two Factor Auth > Remote Control Authentication

You can require VSA users enter a 2FA passcode **within the VSA console** before starting a remote control session.

- Once enabled for a selected machine *any* VSA user must have a corresponding passcode provided by the **Two Factor Authentication server managing Kaseya logons** *(page vii)* to start any kind of remote control session from the VSA to that selected machine.
- Entering this 2FA passcode is independent of whether the **machine itself requires 2FA to logon** *(page iii)*. If both are enabled, then the VSA user will be required to enter the passcode twice.

Move agents to the **Agents requiring authentication** list to require 2FA authentication within the VSA console when remote control sessions are started.

> **Note:** If agents are not showing on this page, enable the System > **Configure** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#248.htm)* > **Enable VSA API Web Service** option in an on premises VSA. SAAS tenant users should contact Kaseya support to have this option enabled.

Manage Agent Groups

Passly (AuthAnvil) > Two Factor Auth > Manage Agent Groups

Use the **Manage Agent Groups** page create AuthAnvil agent groups and add Kaseya agent machines to those groups. This is one step in **Enabling 2FA for End User Machine Logons** *(page iii)*.

AuthAnvil Agent Groups

- **Add Group** - Create a new AuthAnvil agent group. Click the *down arrow* on a AuthAnvil group to:
  - Move machines from the **Available Machines** list to the Machines **Machines in Group** list.

- Click the **Show Advanced** button to **Enable Authentication for KLC** - If checked, a user must use 2FA to use **LiveConnect** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#33845.htm)* on a machine.
  - ✓ **Use logged on user** - If selected, the user initiating the LiveConnect session must enter his or her 2FA passcode.
  - ✓ **Specify user** - If selected, the user initiating the LiveConnect session must enter the 2FA passcode for a specified user.
  - ✓ **AuthAnvil SAS URL** - The **Two Factor Authentication** server to authenticate this user.
  - ✓ **Site ID** - Accept the default value of 1. A different site ID number is only required if the **Two Factor Authentication** website is operating in multi-tenant mode.
  - ✓ **Note** - Enter a note about this record.
- **Delete Group** - Delete a selected AuthAnvil agent group.

Ungrouped AuthAnvil Agents

Select the group that you wish to move agents to:

- **Machine ID**
- **Agent Type**
- **Agent Version**
- **Last Scanned**

Deploy Agents

Passly (AuthAnvil) > Two Factor Auth > Deploy Agents

Use the **Deploy Agents** *(page x)* page to deploy AuthAnvil agents to a selected **AuthAnvil group** *(page ix)* of machines. This is one step in **Enabling 2FA for End User Machine Logons** *(page iii)*.

Procedure

1. Select the **AuthAnvil Agent Group** to deploy.
2. Select machines in the **Select the endpoints that you wish to deploy AuthAnvil to** list.
3. Select **AuthAnvil Server Settings**.
   - This identifies the specific **Two Factor Authentication** server and **Site ID** you will use to authenticate user passcodes for a given set of machines. Each customer organization may have its own **Two Factor Authentication** server to manage its own set of user passcodes.
4. Optionally configure a second **Two Factor Authentication** server for redundancy.
5. Enter **Override Settings**.
   - Enter a password in the **Password** and **Confirm** fields to ensure the VSA administrator still has access to the machine if the 2FA passcode cannot be used.
   - For the **Group** field enter the name of a Windows security group. Whenever members of this Windows security group logon to machines that are members of this AuthAnvil group, AuthAnvil can generate two types of alerts, enabled using the **Configure Agent Alert Settings** *(page xii)* page:
     - ✓ `Monitor AuthAnvil Override Group Membership Changed`
     - ✓ `Monitor AuthAnvil Override Group Member Logged On`
   - You can modify override settings using the **Change Override Password** *(page xii)* page.
6. Optionally set **Advanced Settings**.

- **Install config tool to Control Panel** - If checked, a **AuthAnvil Logon Configuration** tool is installed on the machine. This tool enables configuration of **Two Factor Authentication** logon settings for a single machine directly. You can use the tool to change the **Server URL**, **Site ID** and **Override Group**. You can also **Enable offline caching mode**.
- **Enable offline caching mode** - If checked, a small number of one time passwords (OTPs) are cached on the machine. The number is specified on the Two Factor Authentication server. This enables user logon even if the machine cannot connect to the server. For example, a laptop in the field may not be able to establish a network connection.
- **Set installation password** - If specified, this password is required to manually uninstall the AuthAnvil agent from a machine. It is also required to open the **AuthAnvil Logon Configuration** tool on a machine.

7. Click **Deploy**.
   - You can modify agent settings after you deploy them using the **Modify Agent Settings** *(page xi)* page.
   - Confirm AuthAnvil agents have been successfully deployed using the **Discover Agents** *(page xi)* page.
   - View the results of **Discover Agents** query on the **View AuthAnvil Agent Info** *(page xiv)* page.

Discover Agents

Passly (AuthAnvil) > Two Factor Auth > Discover Agents

Use the **Discover Agents** page to confirm which machines have AuthAnvil agents deployed on them. View the results of your **Discover Agents** query using the **View AuthAnvil Agent Info** *(page xiv)* page. You can search by:

- Search by AuthAnvil Agent Group
- Search by Kaseya Machine Group

Typically, you do not have to run this function that often. It's helpful if you are migrating existing AuthAnvil agents from one AuthAnvil instance to another AuthAnvil instance. If you have removed a machine from an AuthAnvil agent group using the **Manage Agent Groups** *(page ix)* page, the machine will still have the AuthAnvil agent installed on it, but no longer be a member of any AuthAnvil agent group. In this case, the **Discover Agents** page is helpful for identifying the ungrouped AuthAnvil agents. Use the **Manage Agent Groups** page to reassign them to an existing group.

Modify Agent Settings

Passly (AuthAnvil) > Two Factor Auth > Modify Agent Settings

Use the **Modify Agent Settings** page to update the settings of AuthAnvil agents on selected machines in a selected **AuthAnvil group** *(page ix)*. These settings are similar to the ones available on the **Deploy Agents** *(page x)* page, with some exceptions.

Procedure

1. Select the **AuthAnvil Agent Group** to update..
2. Select machines in the **Select the endpoints that you wish to deploy new settings to** list.
3. Select **AuthAnvil Server Settings**.
   - This identifies the specific **Two Factor Authentication** server and **Site ID** you will use to authenticate user passcodes for a given set of machines.

- Each customer organization may have its own **Two Factor Authentication** server to manage its own set of user passcodes.
- The **Site ID** identifies the partition of a Two Factor Authentication server you are using. By default this is 1.

4. Optionally configure a second **Two Factor Authentication** server for redundancy.
5. Enter **Override Settings**.
   - This ensures the VSA administrator still has access to the machine if the 2FA passcode cannot be used.
   - You can modify override settings using the **Change Override Password** *(page xii)* page.
6. Optionally set **Advanced Settings**.
   - **Enable offline caching mode** - If checked, a small number of passcodes are cached on the machine. The number is specified on the Two Factor Authentication server. This enables two factor authentication of a user logon even if the machine cannot connect to the server. For example, a laptop in the field may not be able to establish a network connection.
7. Click **Deploy**.
   - You can modify agent settings after you deploy them using the **Modify Agent Settings** *(page xi)* page.
   - Confirm AuthAnvil agents have been successfully deployed using the **Discover Agents** *(page xi)* page.
   - View the results of a **Discover Agents** query using the **View AuthAnvil Agent Info** *(page xiv)* page.

Change Override Password

Passly (AuthAnvil) > Two Factor Auth > Change Override Password

Use the **Change Override Password** page to change the override password for selected machines in an AuthAnvil agent group. Only agents with an AuthAnvil logon agent installed can be selected.

1. Select the **AuthAnvil Agent Group.**
2. Select machines from the **Select endpoints that you wish to change the password on** list.
3. In **Override Settings** enter matching values in the **Password** and **Confirm** fields.

Configure Agent Alert Settings

Passly (AuthAnvil) > Two Factor Auth > Configure Agent Alert Settings

The **Configure Agent Alert Settings** page configures alerts for all **Auth Anvil agent machines** *(page x)*. This includes:

- **Monitor AuthAnvil Override Group Membership Changed** - Requires a Windows security group be specified on the **Deploy Agents** *(page x)* page.
- **Monitor Failed AuthAnvil Logons**
- **Monitor AuthAnvil Override Password Used** - Requires an override password be specified on the **Deploy Agents** *(page x)* page.
- **Monitor AuthAnvil Override Group Member Logged On** - Requires a Windows security group be specified on the **Deploy Agents** *(page x)* page.
- **Monitor Against AuthAnvil Agent Tampering**

For all type of alerts, the following options can be set:

- **Create Alarm** - If checked and an alert condition is encountered, an alarm is created. Alarms are displayed in Monitor > Dashboard List, Monitor > Alarm Summary and Info Center > Reporting > Reports > Logs > Alarm Log.
- **Create Ticket** - If checked and an alert condition is encountered, a ticket is created.
- **Run Script** - If checked and an alert condition is encountered, an agent procedure is run. You must click the select agent procedure link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking this machine ID link. These specified machine IDs do not have to match the machine ID that encountered the alert condition.
- **Email Recipients** - If checked and an alert condition is encountered, emails are sent to the specified email addresses. Email is sent directly from the VSA to the email address specified in the alert. Set the **From Address** using System > Outbound Email.

Agent Procedures Approval

Passly (AuthAnvil) > Two Factor Auth > Agent Procedure Approval

The **Agent Procedure Approval** page enables a VSA standard user to approve his or her *own* agent procedures using two factor authentication (2FA).

If signing and approval of agent procedures is enabled *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#9332.htm)*, new or saved agent procedures must be approved before they can be run. Without 2FA, a standard user must have a *second user* approve a new agent procedure before it can be run, using the Agent Procedure > **Pending Approvals** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#17981.htm)* page.

Procedure

1. Add a single VSA user to the AuthAnvil > Two Factor Auth > **Agent Procedure Approval** page. This VSA user must be configured to use 2FA to log into the VSA.
2. Check the **AuthAnvil user (or grouped user) that will be used for approval requests** checkbox.
3. The VSA user specified in step 1 creates a new agent procedure or saves an existing agent procedure using the Agent Procedures > **Schedule / Create** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#2845.htm)* page.
4. The same VSA user then clicks the Agent Procedures > **Schedule / Create** *(http://help.kaseya.com/webhelp/EN/VSA/9050000/index.asp#2845.htm)* > **Approve using AuthAnvil** button to enter his or her 2FA passcode to approve the agent procedure.

View AuthAnvil Alarms

Passly (AuthAnvil) > Two Factor Auth > View AuthAnvil Alarms

The **View AuthAnvil Alarms** page displays a log of <AAPS1> module activity by:

- **Timestamp**
- **Event**
- **User**
- **Message**

View Logons to Kaseya

Passly (AuthAnvil) > Two Factor Auth > View Logons to Kaseya

The **View Logons to Kaseya** page displays a log of Kaseya logon activity by:

- **Timestamp**
- **Event**
  - OPU - Override password used
  - Override Group Membership Changed
  - Failed AuthAnvil Logons
  - Override Group Member Logged On
  - Agent Tampering
- **User**
- **Message**

View AuthAnvil Agent Info

Passly (AuthAnvil) > Two Factor Auth > View AuthAnvil Agent Info

The **View AuthAnvil Agent Info** page displays all AuthAnvil agent settings currently used by each machine that belongs to an **AuthAnvil agent group** *(page ix)*. If information has changed or been removed unexpectedly, check this page to determine what settings may have been involved.

- Machine ID
- Agent Type
- Agent Version
- Last Scanned
- SAS URL
- Site ID
- Failover SAS URL
- Failover Site ID
- Override Group
- Offline Caching Enabled

View Audit Logs

Passly (AuthAnvil) > Two Factor Auth > View Audit Logs

The **View Audit Logs** page displays a log of <AAPS1> module activity by:

- **Timestamp**
- **Event**
- **User**
- **Message**

View KLC Audit Logs

Passly (AuthAnvil) > Two Factor Auth > View KLC Audit Logs

The **View KLC Audit Logs** page displays a log of Kaseya logon activity by:

- **Timestamp**
- **User**
- **IP**
- **Message**
- **Agent**
- **Type**

Authentication for LiveConnect (KLC) sessions are enabled by **AuthAnvil Agent Group** *(page ix)*.

Additional Resources

Passly (AuthAnvil) > Two Factor Auth

- **Documentation** - Opens the **AuthAnvil Documentation Center** *(http://www.scorpionsoft.com/docs/authanvil/)* in a new window.
- **Training Videos** - Opens an **AuthAnvil training videos** *(http://www.scorpionsoft.com/docs/aak2/index.html)* page in a new window.
- **Contact Support** - Opens the **AuthAnvil Help Center** *(https://help.scorpionsoft.com/home)* and knowledge base in a new window.
- **Visit the Online Store** - Opens the **AuthAnvil Online Store** *(http://www.scorpionsoft.com/pricing)* in a new window.

Password Server

Note: Password Server is not supported in SaaS environments.

Configure Web Server

Passly (AuthAnvil) > Password Server > Configure Web Server

Note: Password Server is not supported in SaaS environments.

The **Configure Web Server** page enables a logon app for the Password Server to be added the Single Sign On server. This means the Single Single On menu provides immediate, highly secure access to the Password Server, independently of the VSA, as well as all other resources VSA users require to perform their daily tasks.

- **Enable SSO Authentication** - If checked, enables user to access Password Server by clicking an app from their Single Sign On menu of apps.
- **Single Sign On** - The URL Password Server should send an SSO request. Example: `http://scorpionlabs.local/AAPS/ssologon.asmx`
- **Reply To URL** - The URL an SSO server should send replies to. Example: `http://scorpionlabs.local/aaps/ssologin.aspx`

- **Verify** - Verifies the URLs to ensure you have a connection.

Dashboard

Passly (AuthAnvil) > Password Server > Dashboard

The **Dashboard** page provides a brief introduction to **Password Server** and displays counts for significant **System Health** issues. Click any category to jump to that category immediately.

- **Expiring Passwords**
- **Sync Issues**
- **Agent Tasks**
- **Catalog Updates**
- **Pending Requests**

Review Tasks and Issues

You can also click the **Review Tasks and Issues** link to review tasks that might exist for you to complete. Tasks might include updating passwords or reviewing password requests.

Favorite Passwords

If you have any passwords marked as **favorites** *(page xxi)*, they are listed on the left side of the **Dashboard** page. Each passwords shows its sync status and when it was last used. Click the **manage** link for any password to update its settings immediately.

Users

Passly (AuthAnvil) > Password Server > Users

The **Users** page specifies the users who can log into **Password Server**.

Users table

The **Users** table displays properties for existing users.

- **Display Name** - Click a display name to edit settings for that user. These settings are described below.
- **Email Address** - A unique email address within Password Server.
- **Enabled** - If ■, the user is enabled.
- **Locked Out** - If ■, the user is locked out.
- **Requires 2FA** - If ■, the user requires two factor authentication.
- **Last Logon** - The last time the user logged on.
- **Last Logon Failure** - The last time the user failed to log on.

Adding Users

Click the **Actions > Add User** option to add a new user using three different tabs.

General Settings tab

- **Email Address** - A unique email address within **Password Server**. This email is used for logging in as well as for user notifications, such as password expiration, requesting access, and permission approval.
- **Display Name** - A unique username within **Password Server**.
- **Password** / **Confirm Password** - Enter a matching password in both fields.
- **Account Status** - `Enabled` or `Disabled`.

- **Requires two-factor authentication to login** - If checked, the user does not use a password, instead using AuthAnvil Two-Factor Auth to log in.
- **Allowed to maintain a Private Vault** - If checked, the user is allowed to maintain a private vault, where they can keep private passwords. See the section on **Private Vaults** for more details.
- **Allowed to create Shared Vaults** - If checked, the user is allowed to create and manage new shared vaults. This permission implies the **Allowed to own Shared Vaults** permission.
- **Allowed to own Vaults and create Personal Vaults** - If checked, the user is allowed to be assigned the "owner" permission for shared vaults so that they can manage them. They are also able to manage their own personal **vaults** *(page xvii)*.
- **Organization Administrator** - If checked, the user is an organization administrator, allowed to manage users, settings, and sync agents, and run reports. If the administrator is also assigned the **Allowed to own Shared Vaults** permission, they can **seize control of shared vaults** *(page xix)*.

AuthAnvil Two Factor Auth tab

This tab specifies the **Two Factor Authentication** server processing 2FA requests for this user.

> **Note:** The **Requires two-factor authentication to login** checkbox on the first tab must be checked to access to this tab's settings.

- **Use Organization SAS Settings** - If checked, use the default **Two Factor Authentication** server to process 2FA requests for this user. The default **Two Factor Authentication** server is set on the **Settings** *(page xxvii)* page. If unchecked, enter values for the following:
  - **AuthAnvil SAS URL** - Specifies the **Two Factor Authentication** server used to process 2FA requests for this user.
  - **Site ID** - Accept the default value of 1. A different site ID number is only required if the **Two Factor Authentication** server being connected to is operating in multi-tenant mode.

Roles tab

This tab assigns one or more roles to a user. Roles enable **scope** *(page xxx)* and **vault permissions** *(page xviii)* to be assigned to all members of the same role.

- A user must be assigned to at least one role.
- By default all users are assigned to the `Default Role` initially.
- When multiple roles are assigned to a user, permissions are added to each other.

Vaults

Passly (AuthAnvil) > Password Server > Vaults

Vaults store passwords. A password may or may not specify a corresponding username. Each vault—and each type of vault—determines who can access its passwords, how those passwords are shared, and how those passwords are used by the logon apps of multiple users managed by the **Single Sign On** server.

Vault Types and tabs

- **Shared Vaults** - Shared vaults allow policies and access to be controlled and shared by users and/or roles. This type of vault can be used by a **Single Sign On** server.
- **Personal Vaults** - Personal vaults allow policies and access only for its owner. This type of vault can be used by a **Single Sign On** server.
- **Private Vaults** - Private vaults are separately encrypted vaults managed by each user to store personal passwords. This type of vault cannot be used by **Single Sign On** server.

> **Note:** A private vault is individually encrypted with a password only you know. *If you lose that password, you cannot unencrypt, recover or access your private passwords.*

- **Personal Vaults - Admin** - Provides a list of all **Personal Vaults** in an **organization** *(page xxxi)*. If you are not the owner of a given vault, you can request the owner to grant you access. This creates a task for them to review your request.

Adding Vaults

Passly (AuthAnvil) > Password Server > Vaults > (vault type)

Click the **Add Vault** button displayed on the **Shared Vaults**, **Personal Vaults** or **Private Vault** tabs.

General Settings tab

- **Name** - The name of the vault.
- **Description** - A description of the vault.
- **Scope** - *Displays for shared vaults only.* The **scope** *(page xxx)* assigned to this vault. Users can only see vaults that are assigned to scopes they are a member of. *The scope cannot be changed after the vault is created*. Scopes are created using the **Settings** *(page xxvii)* page.

Vault Password Policy tab

Sets password policies for all passwords in this vault. Values default from the **Settings** *(page xxvii)* page.

- **Minimum Length** - The minimum length of a password. Must be greater than 3.
- **Maximum Length** - The maximum length of a password. Must be less than 65.
- **Days to Expiration** - Days before the password expires and must be changed. Set to 0 to never expire.
- **Enable automatic rekey of Vault** - If checked, the vault is automatically rekeyed on a schedule. Rekeying changes the encryption key that is used to protect the passwords for each user in the vault. This is a cryptographically complex operation and can take some time, and should not be done on a frequent basis and may impact performance of the server.
- **Automatically rekey the Vault after** - The number of days to automatically rekey the vault.
- Optionally check the following for passwords in this vault:
  - **Require English uppercase characters (A through Z)**
  - **Require English lowercase characters (a through z)**
  - **Require base 10 digits (0 through 9)**
  - **Require non-alphabetic characters (for example, !, $, #, %)**
- **Save Password History** - If checked, keep a record of historical passwords for each password in the vault.
- **Enforce Password History** - If checked, stop users from re-using passwords from their historical password list.
- **Keep Password History For** - Sets the number of passwords kept in the historical password list for each password.

Vault Members tab (visible when adding or editing Shared Vaults only)

Adds the users who are members of a *shared vault* and assigns user permissions for that vault.

- **Add** - Adds a user to the shared vault.
- **Display Name** - The unique username of the user.
- **Email Address** - The unique email address of the users.

There are several **vault permissions** available for each user.

- **Owner** - The user has full control over the vault, and can set password policy, add and delete users, and even delete the vault itself. This permission level also implies all of the other

permission levels, including Audit, and has all of their privileges. A user can only be assigned the **Owner** permission if they have the **Allowed to Own Shared Vaults** *(page xvi)* permission assigned to their user account.

- **Create** - The user has permissions to import, create, and delete passwords within the vault. It implies the read and modify permissions.
- **Read** - The user can read and export existing passwords from the vault.
- **Modify** - The user has permissions to modify the existing passwords within the vault. It implies the **Read** permission.
- **Launch** - The user can launch one-click applications from the **Single Sign On** server. Available for both Windows passwords (RDP launch) and web passwords.
- **Audit** - The user can run vault-specific reports from the reports tab.
- **Requires Approval** - This permission can be combined with the **Read** and **Modify** permissions. The user must request permission from an administrator before being allowed to view or modify the password for a set period of time. The user can also be assigned the **Audit** permission while this permission is active.

Managing Vaults

Passly (AuthAnvil) > Password Server > Vaults > (vault type) > (vault)

Editing Vaults

Click the **manage** link in any vault list to edit vault properties. These are the same properties using when **adding vaults** *(page xviii)*. Editing displays two additional options.

- **Delete Vault** - Delete the vault and all of the passwords contained inside it.
- **Rekey Vault** - Re-encrypt the vault data with new encryption keys immediately.

Requesting Access to Vaults

If a user does not have permissions to access a vault, but it belongs to a **scope** *(page xxx)* that they are a member of, then they can request to join the vault.

1. Click on the vault name and click **Request Membership**.
2. The vault owners will receive an email with the request. If they want to give the user permissions to the vault, they can click on the link in the email and can choose what level of permissions to assign the user.

Seizing Vaults

If an administrator does not have permissions to access a vault that is in a **scope** *(page xxx)* that they are a member of, and they have the **Allowed to own shared vaults** permission, they can request to join the vault or seize the vault. If they need to seize the vault, they click on the vault name and click the seize vault button. This will send an email message to every member of the vault, informing them which administrator has seized the vault, and that they are now an owner of that vault.

Adding Passwords

Passly (AuthAnvil) > Password Server > Vaults > (vault type) > (vault)

Once a vault has been created, click the folder name of the vault in a vault list to open it. You can now add and edit passwords.

Actions

- **Add Password** - Select to **add a password** *(page xix)*. There are five property tabs for each password you create.
  - **General Settings** - Described below.

- **Password History** - A history of previously used passwords displays if **Save Password History** has been enabled for the vault and the **Allow previous password history to be shown** setting is set at the **organizational** *(page xxxi)* level.
- **Synchronization** - See **Synchronizing Passwords** *(page xxii)*
- **Associations** - See **Associations** *(page xxiv)*
- **Remote Connection Policy** - See **Remote Desktop Connections** *(page xxiii)*

- **Manage Vault** - **Edits vault properties** *(page xix)*.
- **Import Passwords** - Imports passwords from a CSV file. See **Importing and Exporting Vaults http://blog.scorpionsoft.com/blog/2012/02/password-vault-feature-focus-importing-and-exporting-vaults.html**.

General Settings tab

This is the first of the five property tabs for each password.

- **Password Name** - A friendly name for the password. This does not have to be the same as the **Username**.
- **Description** - A description of the password.
- **Password Type** - The category of password. If none of the password types apply, set it as a `General Password`. Most password types are informational, meaning they do not have a special affect on the password. Windows and Web password types—for example, `Active Directory Windows Password`—provide additional functionality or fields.
- **Days to Expire** - The number of days before this password expires and must be changed. If 0, this password never expires.
- **Expire X Minutes After Access** - After a user reveals or copies this password, wait this many minutes to automatically rotate this password or flag it for manual expiration. This also applies to passwords accessed through RDP or Web Launch icons. If 0, this password never expires.
- **Password Id** – A unique ID assigned to this password. Cannot be changed.
- **Vault ID** – The vault ID associated with this password. Cannot be changed.
- **Enable for Trusted Third Party Access** – If checked, this password can be used by third party. See **Third Party Certificates** *(page xxxiii)*.
- **Username** - The username associated with the password. This field is not displayed for password types that do not have usernames. If you have a `General Password` that does not have a username, just leave it blank.
- **Domain** - The Active Directory domain name associated with this password. This field is only displayed for the `Active Directory Windows Password` type.
- **Machine Name** - The name of the machine associated with this password. This field is only displayed for Windows password types.
- **Password** -Enter a password manually, or click **Generate** to generate a password for you.
- **Optional: Choose an alternate Password Policy** - Click this drop-down list to select a different password policy for this password than the one set for this vault. Once selected, the alternate policy applies to the password whether it is manually or automatically changed. To unassign a password policy from a record, select **Optional: Choose a Password Policy** from the policy dropdown list. You can create your own password policies on the **Setting** *(page xxvii)*s tab at the bottom of the page.
- **Ignore the Vault Password Policy for this Password** - Allows the password to be saved, even if it does not meet the necessary complexity requirements.
- **Do not include this Password in the 'Passwords not attached to an Association' report** - Excludes this password from a special report that looks up all passwords not tied to an association.
- **Notes** - Any additional notes needing to be stored with the password data. This could be special information about the connection or account. All **Notes** information displays when the password is revealed on screen.

Managing Passwords

Passly (AuthAnvil) > Password Server > Vaults > (vault type) > (vault) > (password)

Viewing a Password

You must have **Read** permissions or better to open a vault.

1. Select a password in vault.
2. Click the **Reveal Password** button for the selected password.

> **Note:** Users that have the **Requires Approval** permission set must follow the instructions in *Requesting Access to Passwords*, described below.

Editing a Password

A user with **Modify** permissions or better can click on the password's name to edit it. The following tabs are available:

- **General Settings** - Edits the same properties as **Adding Passwords** *(page xix)*.
- **Password History** - A history of previously used passwords displays if **Save Password History** has been enabled for the vault and the **Allow previous password history to be shown** setting is set at the **organizational** *(page xxxi)* level.
- **Synchronization** - See **Synchronizing Passwords** *(page xxii)*
- **Associations** - See **Associations** *(page xxiv)*
- **Remote Connection Policy** - See **Remote Desktop Connections** *(page xxiii)*

Deleting a Password

Select a password then click **Delete Password**. The password's history, if enabled, is also deleted from the vault. *This operation cannot be reversed.*

Setting Favorite Passwords

Click on the grey star under the **Favorite** column and this password will be flagged as a favorite. Favorites are marked with blue stars. You can configure up to 10 passwords this way.

Requesting Access to Passwords

1. If a user is assigned the **Requires Approval** permission, they must request approval to access a password in the vault, and an administrator must approve the request before they can see the password. The requires approval workflow goes as follows:
2. The user logs into the vault and clicks the **Request Approval** button beside the password. This sends an approval request to the vault owners.
3. When the owner logs into the vault, they will have a task in their task list letting them know that a password request is pending and that they have to review it. The admin then clicks **View Password Request**.
4. The administrator can then either approve or deny the request. If they decide to approve it, they can set an expiry date for the user's access, have the option to change the password before approval, expire the approval when the password expires, and can have the system automatically generate a new password when the approval expires—if the password is synchronized—then click **Accept**.
5. If the administrator approves the request, the system sends an email to the user letting them know that their request was approved.
6. The user can then log in to the vault and view or modify the password as their permission level allows.

Synchronizing Passwords

Passly (AuthAnvil) > Password Server > Vaults > (vault type) > (vault) > (password) > Synchronization tab

The **Synchronization** tab configures a selected **sync agent** *(page xxv)* with a password.

1. Install a sync agent on a target machine if you have not already done so.
2. Add or edit the password for the target machine you wish to synchronize.
3. Click the **Synchronization** tab.
4. Click **Enable Synchronization**. Fields on this page display if at least one sync agent is installed.
   - **Automatically generate a new random password and change it when it expires**
   - **Sync Agent** - Select a sync agent. If this is a Windows password, select a sync agent on the same network or domain. For web passwords, make sure the sync agent has internet access.
   - **Add another link in this sync chain that will be updated when this password changes** - You can add additional items to sync as a part of sync chain. The `Default Sync` link is always the first password in a sync chain, and represents the synchronization against the target specified in the **General Settings** tab.

Sync Chains

Sync chains allow a user to define a series of passwords that need to be kept in sync. A common example is when you change a password for an administrative user account. If that user account has scheduled tasks that run using its credentials, the stored credentials used by the scheduled task must also be updated when the password is synchronized. That's where sync chains come in.

To set up a sync chain, you enable synchronization for a password and choose a sync agent to synchronize against. You can then add links to the sync chain. The `Default Sync` link is always the first password in a sync chain, and represents the synchronization against the target specified in the **General Settings** tab. Other links are processed in order and represent various local passwords, domain passwords, remote passwords, task passwords and service passwords. Depending on the link, you will have to specify the relevant information, such as the username of the user to synchronize and machine, domain, device, or task-specific information.

For example, in a computer lab where each machine is domain joined, you may want to synchronize all of the local administrator accounts to a single password. This is the perfect scenario for a sync chain. You would install a sync agent on one of the machines in the lab and set up a Standalone Windows Password for the local Administrator account on that machine. Then, in the sync chain, you would set up a Remote Password link for each machine in the lab, specifying the machine name and the username to synchronize. The vault will test to make sure that the passwords are initially in sync, and then synchronize all of them against the same password each time it changes in the vault.

> Note: Remote Windows Passwords, Task Passwords, and Service Passwords require a linked credential be configured for the **sync agent** *(page xxv)*.

Sync States

Every password has a status to let users know how the password is being synchronized. This tells the user whether the password is synced or not, if it can be synced, or if it is in the process of being synced. A sync state can be found under the **Sync Status** column for a password. Here is a list of sync states and their meanings:

- **Not Synced** – A password that has not been configured for synchronization.
- **Pending Sync** – A sync agent is in the process of either testing the password or changing it to a new value.
- **In Sync** – The current password is synchronized and tested against the target login.
- **Out of Sync** – The current password was unable to be validated, or did not log in correctly.

- **Unsyncable** – The Web Workflow on this password has no validation steps, so it cannot be verified as the proper password. Launch permissions can still be configured for Single Sign On access to this application.
- **Change not Configured** – This web password was changed, but there are no workflow steps to update this password on the website. It will have to be manually updated on the website, then you can retry the sync.

Out of Sync Passwords

Occasionally, a password gets out of sync with its vault. This can happen because of an incorrect password stored in Password Server, or a changed password on the Windows / website level, or a failed change due to a bad connection or password complexity. Password Server alerts vault owners with an email that the password needs an administrative override. When the vault owner logs in, they will see a task in their task list that a password sync has failed and that administrative override is required to force the sync.

You can see passwords `Sync Issues` in your task list on the **Dashboard** *(page xvi)* page. The vault owner must enter administrative credentials for the target machine, along with a new password for the account, and click the **Approve** button. This instructs **Password Server** to bring the password back into sync. Users can also click the **Retest Sync** button to send the sync instruction again. This is useful if the target machine was temporarily unavailable during the last synchronization attempt.

Remote Desktop Connections

Passly (AuthAnvil) > Password Server > Vaults > (vault type) > (vault) > (password) > Remote Desktop Connections tab

The **Remote Desktop Connections** tab configures Windows passwords to launch RDP sessions. Any Windows password stored in a vault can be RDP-enabled. Once configured, you can click the desktop icon displayed by an RDP-enabled password to launch the RDP session. You can also set various policies to restrict the actions allowed during an RDP connection.

> **Note:** For more information, see **How do I configure Remote Desktop Connections with AuthAnvil Password Server?** *(https://help.scorpionsoft.com/entries/26219267-How-do-I-configure-Remote-Desktop-Connections-with-AuthAnvil-Password-Server-)*

Creating an RDP Password

1. Select or create a password set to any of the three 'Windows' password types.
2. Click the password's **Remote Connection Policy** tab.
3. Check the **Enable Remote Desktop Policy** checkbox.
4. Select a policy: `High`, `Medium`, `Low`

   > **Note:** Create a new RDP connection policy using the Admin > External Settings > **RDP Connection Policies** *(page xxxv)* tab.

5. Optionally select an **RDP Image**. An icon used to classify the type of RDP session that will be launched when an RDP-enabled password is clicked in a vault's password list. For example, by client or server type.
6. Optionally check the **Use RD Gateway Server** to securely use the RD gateway to connect to machines you don't have direct access to when working remotely.
   - **Server Name** - Enter a FQDN name for the remote desktop gateway server. The username and password specified for this password record serves as the credential for accessing the RD gateway server *and* the target machine. The machine you are connecting to is specified in the **Machine Name** of this password record.

- **Use a Linked Credential for RD Gateway Access** - If checked, requires you to specify a *different* password record to provide access to an RD gateway.
  - ✓ **Vault**
  - ✓ **Credential** - A password record.

7. Return to the list of passwords in a vault. Click the desktop icon for an RDP-enabled password to launch the remote desktop session.

Associations

Passly (AuthAnvil) > Password Server > Associations

Associations represent devices or sites within an **organization** *(page xxxi)*. Once you associate passwords with a device or site, you only have to click the association to see all the passwords used to manage that resource. Use the Vaults > (vault) > (password) > **Associations** tab to link a password with an association. Each password can be linked to multiple associations.

Adding Associations

Once added, an association can be deleted or edited.

General Settings tab

- **Name** - The friendly name of a device or site.
- **Address** - The machine name or web address of the device or site.
- **Guid** - A GUID to uniquely identify this association. This value is used when dealing with external applications.
- **Association Type** - The type of device or site. Used for search lookups when selecting associations.

Scopes tab

Select one or more scopes to assign to the association. A **scope** *(page xxx)* assigned to an association must match the scope of a vault before a vault member can add the association to a password.

Roles

Passly (AuthAnvil) > Password Server > Roles

Managing access to vaults and passwords by role enables you to quickly update permissions for entire sets of users simultaneously.

All users in a role have access to vaults using scopes that are assigned to that role. A **scope** *(page xxxi)* is a collection of one or more vaults. For example, multiple users can be added to a named role—like Technician or Auditor. The role is then assigned to one or more scopes.

A user has access to vaults and passwords based on their combined role and user permissions. A user is always given the best combined permissions of both their role and user permissions.

Adding Roles

Once added, a role can be deleted or edited.

General Settings tab

- **Role Name** - A short name for a role.
- **Description** - A longer description of the role.

Scopes tab

Toggle a scope tile to add or remove it from the role. You can select or removed all scopes.

Role Members tab

Toggle a user tile to add or remove it from the role.

Sync Agents

Passly (AuthAnvil) > Password Server > Sync Agents

Sync Agents are deployed to machines. They communicate with **Password Server** to synchronize the passwords stored in vaults with the passwords stored on the machines, based on vault policy. Each day **Password Server** verifies that all synchronized password records are still in sync with respective Windows user accounts.

Sync agents are configured to work with four general categories of passwords:

- Web Passwords on Forms-Based Websites
- Windows Passwords
- Windows Task Scheduler Passwords
- Windows Service Accounts Passwords

Additional guidelines:

- See **Sync Scenarios** *(http://www.scorpionsoft.com/docs/pwv/sync-scenario-v20)* for more details about synchronizing types of passwords.
- Passwords for Windows Scheduled Tasks and Windows Services can also be synchronized using Sync Chains.
- Sync agents should be installed on domain member servers rather than domain controllers.
- If installing in a non-domain environment, installing on a server with full network visibility is sufficient.
- For Standalone Windows Passwords, the sync agent must be on the same machine as the password being synchronized.
- For Remote Windows Passwords, the sync agent simply has to be on the same network as the target machine, but it requires an elevated Linked Credential to connect to the target machine. Active Directory Windows Passwords just need to be on a domain member machine.
- For Remote Windows Passwords, the target machine's firewall must have the appropriate ports open for remote management via WMI, as described in this MSDN article and, if it is running Windows Vista or later, must have the LocalAccountTokenFilterPolicy set as described in **this Microsoft KB article** *(https://support.microsoft.com/en-us/kb/942817)*.
- For Windows Service Passwords, you must use the *Service Name* of the service rather than the *Display Name*. Right-click the service and go to Properties to verify the Service Name.
- For any sync agents that synchronize passwords on remote machines, the machines must be online and available on the network. Otherwise the sync test will fail, and the password will be marked as Out of Sync.

Deployment

1. Download the Sync Agent install zip from the **Sync Agents** page.
2. Copy the zip to the target machine you want to install it on.
3. Extract the contents of the zip.

4. Run the `.msi` in the same directory as your unique configuration file.
5. Follow the on-screen instructions, and complete the installation.
6. Run the **Sync Agent Configuration** form with elevated privileges.
   - Confirm your Password Server URL.
   - Make note of the **Trust Verification Code (TVC)**
   - Save the settings to start the service.

> **Note:** For more information, see How do I deploy a Sync Agent.

Approval

1. Use the **Sync Agents** page to approve sync agents in the **Pending** list.
2. Confirm the TVC code to ensure you only approve authorized sync agents.
3. Provide the agent a name and select its scopes.

You can now navigate to the Vaults > (vault) > (password) > **Synchronize** *(page xxii)* tab to select the sync agent and assign it to a password.

Reports

Passly (AuthAnvil) > Password Server > Reports

Select any of the pre-defined reports on the **Reports** tab run it immediately. Once run you can export the report to CSV file.

Top 10 Reports

- Top 10 passwords accessed in the last 30 days
- Last 10 passwords accessed
- Top 10 users in the last 30 days

User Reports

- What passwords can a user see?
- What passwords has a user seen?
- What passwords does a user still know?
- What has a user been doing lately?

Vault Reports

- What vaults have been created recently?
- What vault settings have changed recently?
- Which vaults have been exported recently?
- What permissions have been granted for a vault?

Password Reports

- What passwords aren't mapped to an Association?
- What passwords are about to expire?
- What passwords are out of sync?
- What passwords are not being synced?
- What passwords have been accessed?
- What passwords are overriding Vault Policy?

Permission Reports

- What permissions does a user have?
- What permissions have changed recently?
- Who received password approval recently?
- Who was denied password approval recently?
- What permissions does a role have?

Activity Reports

- When have passwords been revealed lately?
- Which accounts seem to be inactive?
- Which accounts have failed to logon recently?
- What administrative activity has gone on lately?

Settings

Passly (AuthAnvil) > Password Server > Settings

The **Settings** page manages **organization** *(page xxxi)* settings. There are 8 settings tabs.

In This Section

General Settings

Passly (AuthAnvil) > Password Server > Settings > General Settings

This tab sets **General Settings** for an **organization** *(page xxxi)*.

- **Lockout Threshold (attempt)** - Determines how many failures are allowed before a user is prevented from logging into this organization in **Password Server**. A value of 0 means that the Password Server should never lockout a user. A typical value of 5 attempts allows a user to recover for an input error while preventing an attacker from probing the server in too much depth.
- **Lockout Duration (minutes)** - Determines how many minutes a user is locked out before the user can log into this organization again in **Password Server**. A value of 0 means that Password Server should never unlock the user, requiring an administrator to unlock the user manually. A typical value of 15 minutes allows a user to recover from a failure while preventing an attacker from probing the server in too much depth.
- **Base URL** - Defines the first part of the domain URL path string sent in server email messages. You can use internal domain names if the emails are expected to be within the local network only. If you expect emails to be also sent externally, you should provide a fully qualified domain name. Internal example: `yourdomain.local`. External example: `yourdomain.com`.
- **Allow the use of Private Vaults** - If checked, users in this organization can be assigned the **Allowed to maintain a private vault** permission. *Users that already have private vaults assigned will lose access to them if this setting is unset.* Losing access to private vaults does not delete the passwords in these private vaults. Users will regain access to their private vaults when this permission is re-enabled.
- **Allow Vault members who can Read to export content to CSV (in clear text)** - If checked, users with the **Read** permission are allowed to export the contents of the vault into a clear-text CSV file. Even if checked, users with **Requires Approval Assigned** cannot export vaults.
- **Allow previous password history to be shown** - If checked and a vault is configured to keep a password history, users with the **Modify** permission can see a list of previous passwords when they view a password history. If this option is turned off, a password history is still kept as per the vault settings. Users just aren't able to see it.

Mail Settings

Passly (AuthAnvil) > Password Server > Settings > Mail Settings

This tab sets **Mail Settings** for an **organization** *(page xxxi)*.

Mail Settings

- **Email Address used to send message (From field)** - The "From" email address used by this organization in outgoing email messages. *Administrative messages are sent to this same email address*.
- **SMTP Server name or IP Address** - The SMTP (mail) server used by this organization to relay outgoing email messages.
- **Use SSL if supported by SMTP server** - If checked, uses SSL to communicate with the mail server.
- **Advanced SMTP Settings**
  - **Server Port** - The port that the SMTP server is listening on.
  - **SMTP Server Requires Authentication** - If checked, authentication is required.
  - **Username** - The username of the SMTP user.
  - **Password** - The password for the SMTP user.
- **Test Saved SMTP Settings** - Verifies outgoing email can be sent successfully.

AuthAnvil Two Factor Auth Settings

Passly (AuthAnvil) > Password Server > Settings > AuthAnvil Two Factor Auth Settings

This tab sets **AuthAnvil Two Factor Auth Settings** for an **organization** *(page xxxi)* in Password Server.

- **AuthAnvil SAS URL** - The SAS URL of the AuthAnvil Two Factor Auth server used to authenticate users by default if the **Requires Two-Factor Authentication** setting is set for the user. This setting can be changed on a per user basis. Example: `http://(yourdomain)/AuthAnvil/SAS.asmx`
- **Site ID** - The Site ID of the AuthAnvil Two Factor Auth server used to authenticate users by default if the **Requires Two-Factor Authentication** setting is set for the user. This setting can be changed on a per user basis.
- **Require all users to sign in with an AuthAnvil strong two-factor authentication credential, or use Single Sign-On** - If checked, disables the use of passwords for logon to Password Server for this organization. Users that currently have passwords will be allowed to use them until an administrator switches them over to use Two-Factor Authentication. While waiting to be switched over, users are not able to change their password.
- **Test AuthAnvil settings** - Click to test the connection to the Two-Factor Authentication server only.
- **Single Sign-On Settings** - Click to display/hide the following settings.
  - **Enable Single Sign-On** - Enable SSO for Password Server via SAML. This feature works with any identity provider supporting SAML 2.0.
  - **SAML Version: 2.0 Issuer** - Allows you to specify the issuer of the certificate used for SSO.
  - **Identity Provider Login URL** - The URL of the SAML identity provider's login page.
  - **Identity Provider Logout URL** - The URL of the SAML identity provider's logout page.
  - **Import New SSO Certificate** - Import a new SSO certificate. This is the certificate the Password Server instance uses to certify the identity of the SSO service provided by the Two Factor Authentication instance.

Scopes

Passly (AuthAnvil) > Password Server > Settings > Scopes

This tab adds and removes **Scopes** for an **organization** *(page xxxi)*.

A scope is a grouping of vaults.

- A shared vault can only be assigned one scope and the scope assignment cannot be changed after the shared vault is created.
- Visibility of a shared vault by a user has two conditions: the user—or a role the user is member of—must be assigned the same scope as the vault and the user must be added as a member of the vault using the **Vault Members** tab.
- A scope assigned to an association must match the scope of a vault before a vault member can add the association to a password.
- A scope assigned a sync agent must match the scope of a vault before a vault member can add the sync agent to a password.
- Scopes can only be deleted if they have no vaults as members, and have no users exclusively assigned to them.

If a user does not have permissions to access a shared vault, but it belongs to a scope that they are a member of, then they can request to join the vault.

1. Click on the shared vault name and click **Request Membership**.
2. The shared vault owner will receive an email with the request. If the vault owner wants to give the user permissions to the vault, they can click on the link in the email and can choose what level of permissions to assign the user.

Default Password Policy

Passly (AuthAnvil) > Password Server > Settings > Default Password Policy

This tab sets the **Default Password Policy** for new vaults in an **organization** *(page xxxi)*.

- **Minimum Length** - The minimum length of a password. Must be greater than 3.
- **Maximum Length** - The maximum length of a password. Must be less than 65.
- **Days to Expiration** - Days before the password expires and must be changed. Set to 0 to never expire.
- Optionally check the following for passwords in this organization:
  - **Require English uppercase characters (A through Z)**
  - **Require English lowercase characters (a through z)**
  - **Require base 10 digits (0 through 9)**
  - **Require non-alphabetic characters (for example, !, $, #, %)**
- **Save Password History** - If checked, keep a record of historical passwords for each password.
- **Enforce Password History** - If checked, stop users from re-using passwords from their historical password list.
- **Number of Passwords to keep** - Sets the number of passwords kept in the historical password list for each password.
- **Enable automatic rekey of Vault** - If checked, the vault is automatically rekeyed on a schedule. Rekeying changes the encryption key that is used to protect the passwords for each user in the vault. This is a cryptographically complex operation and can take some time, and should not be done on a frequent basis and may impact performance of the server.
- **Days between Automatic rekeys** - The number of days to automatically rekey the vault.

Licensing

Passly (AuthAnvil) > Password Server > Settings > Licensing

- Only visible when logged into the first organization.

This tab sets **Licensing** information for Password Server.

- **Subscription Username** - The username for your subscription account in the Scorpion Software customer portal.
- **Subscription Key -** The subscription key associated with your subscription account in the Scorpion Software customer portal.

Organizations

Passly (AuthAnvil) > Password Server > Settings > Organizations

- Only visible when logged into the first organization.

This tab creates new **Organizations** in Password Server. In Password Server, each organization is a logically distinct grouping with its own users, vaults, scopes, and settings. Only administrators from the first organization can create new organizations. After they are created, you will see a dropdown on the login page, allowing users to select which organization to log in to.

- **New Organization Name**
- **New Organization Description**
- **New Organization Administrator Email Address**
- **New Organization Administrator Name**
- **New Administrator Password**
- **New Administrator Password Confirm**

Password Policies

Passly (AuthAnvil) > Password Server > Settings > Password Policies

The **Password Policies** page allows you to create customized password policy templates to control the complexity requirements for your passwords. Many websites have specific requirements or limitations on how long or short a password can be, as well as what characters are acceptable. Password Policies allow you to define the specific complexity requirements for each password to make sure they stay within the boundaries of your user account. Rotating passwords tied to a policy will also automatically generate based on those constraints to properly adhere to the security policy for the account.

- **Policy Name** – The title of your password policy
- **Length** - minimum / maximum
- **Allows**
  - **Lower** - lowercase (`abc`)
  - **Upper** - uppercase (`ABC`)
  - **Numeric** - numbers (`123`)
- **Special Characters** - Allow special characters (no spaces). Example: `!#$%^&*()_-+={}[]`

Policy	Length	Allows	Special Characters	Delete
Numeric	4 - 8	Lower: ■ Upper: ■ Numeric: ■		Delete Policy
Simple	6 - 12	Lower: ■ Upper: ■ Numeric: ■		Delete Policy
Simple with Common Chars	6 - 12	Lower: ■ Upper: ■ Numeric: ■	!@#$%^&*()-=_+	Delete Policy
Simple with Extended Chars	6 - 12	Lower: ■ Upper: ■ Numeric: ■	!@#$%^&*()-=_+[]\{}|;:,./<>?	Delete Policy
Enhanced	12 - 16	Lower: ■ Upper: ■ Numeric: ■		Delete Policy

External Settings

Passly (AuthAnvil) > Password Server > External Settings

The **External Settings** page manages external connections for an **organization** *(page xxxi)* settings. There are 3 settings tabs.

In This Section

Third Party Certificates

Passly (AuthAnvil) > Password Server > External Settings > Third Party Certificates

Password Server can expose a subset of information to third party applications if you provide them with a *third party certificate* created by Password Server. This ensures only third party applications you trust have access to this instance of Password Server. This requires additional integration using code. Please check out the **Developer Center** *(http://www.scorpionsoft.com/devcenter)* for more information.

Adding Third Party Certificates

1. Navigate to the External Settings > **Third Party Certificates** page.
   - Click **Add Third Party Certificate**.
   - Enter a unique identifier for the certificate.
   - Select one of the following:
     - ✓ `Third Party Certificate` - The default.
     - ✓ `AuthAnvil SSO Certificate` - For single sign on identity providers.
   - Click **Create Certificate**.
   - Click the name of the certificate to download it.
2. Email the certificate to the appropriate person representing the third party application.
3. To enable any password for third party access:
   - Check the Password Server > Vaults > (vault type) > (vault) > (password> > General Settings > **Enable this Password for Trusted Third Part Access** checkbox.

Delegated Trust Certificates

Passly (AuthAnvil) > Password Server > External Settings > Delegated Trust Certificates

There may be times when you wish to delegate trust from one appliance or application to your Password Server. When used, it allows a trusted application to access credential information on behalf of a user it has already authenticated. An example where this might be used is to allow an RMM tool or remote access application to collect the credentials to inject during a login without prompting the user to enter their credentials to the Password Server if they have already authenticated elsewhere.

> **Warning:** Use this feature with care. If you are not careful, it becomes possible to misuse this feature without validating the identity of the caller. If in doubt, do NOT enable this feature, and ask your security team to review your needs.

Setting up delegated trust

Trust is established by the use of digital certificates. You will need to maintain a full *X.509 certificate* which holds the *public* and *private* key on your application/server, in a non-exportable form within the Windows Certificate Store. You will also need to import the equivalent *public* certificate into Password Server so it knows to trust your application/server.

Create the X.509 certificate for the Application/Server

The steps below rely on Microsoft's `makecert.exe` cmd line tool. This is generally available in any of Microsoft's SDKs. If you currently maintain your own Certificate Authority (CA) and have the ability to generate and issue your own certificates, you can do so instead of using tools like `makecert`. What follows is guidance for IT teams who may not have such infrastructure and need to generate their own self-signed certificates.

1. Create a self-signed X509 cert. It is important that the hostname be resolvable via DNS as the "caller" to AuthAnvil.

```
makecert -ss My -sky Exchange -pe -n "CN=hostname"
```

2. Open up *MMC* as a standard user
3. Select *File* > *Add/Remove Snapin*.
4. Choose *Certificates*, click *Add*, then *OK*.
5. Choose *Personal* > *Certificates*. You should see the certificate you generated there.
6. Right click the certificate and select *All Tasks* > *Export*.
7. Click *Next*, and select *Yes, export the private key.*
8. Click *Next* twice. When prompted, select the *Password* checkbox and enter a password.
9. Browse to store the PFX somewhere safe. Name it something like `myPrivateDTcert.pfx.`
10. Continue to the end of the wizard and click *Finish*.

> **Warning:** This is your PUBLIC/PRIVATE keypair for the application/server. KEEP IT SAFE.

11. Run the export wizard again. But this time select *No, do not export the private key*.
12. Save the export as a *Base64-encoded X.509 cert*. Name it something like `myPublicDTcert.cer`.

> **Warning:** This is your PUBLIC key certificate used by Password Server.

Installing your private key into the Windows Certificate Store of the Application/Server

1. Open up mmc as an administrator
2. Select *File* > *Add/Remove Snapin*.
3. Choose *Certificates*, and click *Add*. When prompted, select *Computer account*, and complete adding the snapin.
4. Expand *Trusted Root Certificate Authorities*.
5. Right click the *Certificates* folder in the left pane and select *All tasks* > *Import*.
6. When prompted, browser for the PFX file. You may need to change the file type to see it.
7. Click *Next*. Enter the password you used during the export. Make sure the *Mark this key as exportable* checkbox is turned OFF.
8. Click *Next* several times until you get to the end of the wizard and click *Finish*. You have now imported your keypair.

Installing your public key into the Password Server

1. Login to Password Server as an administrator.
2. Navigate to the External Settings > **Delegate Trust Certificates** tab.
3. Click the **Add Delegated Trust Certificate** button.
4. Browse to select the PUBLIC certificate you previously created (*.cer).
5. Click **Install Certificate**.

At this point you can now call into the delegated SOAP/XML web services using `dtLogon()` to establish trust, and then request credentials as appropriate. Please see the Scorpion Software Developer Center for more information.

At this point, your instance of Password Server can now accept requests via web services from your trusted host, using the certificate as the authenticator. This certificate must have a Common Name (CN) that matches both a forward and reverse lookup name resolution on the AuthAnvil system. In other words, if your DNS name for the system resolves to `yourapp.contoso.com`, then the CN should be `CN=yourapp.contoso.com`. Using the configured digital thumbprint of the certificate and its public key, AuthAnvil validates all requests and encrypts all responses using asymmetric encryption from that certificate.

RDP Connection Policies

Passly (AuthAnvil) > Password Server > External Settings > RDP Connection Policies

Through **RDP Connection Policies** you can limit console access, mounting drives, and even copy/paste functionality within RDPs sessions that are launched from Password Service. Three pre-defined policies are provided, featuring `High`, `Medium`, and `Low` security settings. You can also create new RDP connection policies. Once added, the new policy can be selected on any password's **Remote Desktop Connections** *(page xxiii)* tab.

Adding an RDP Connection Policy

1. Navigate to the External Settings > **RDP Connection Policies** tab.
2. Click **Add RDP Policy**.
3. Enter a policy **Name**.
4. Check one or more of the following options.
   - **Allow Console Connection**
   - **Allow Mounting Drives**
   - **Allow Copy and Paste**
   - **Force the Use of specified machine name**

Admin Tools

Passly (AuthAnvil) > Password Server > Admin Tools

Organization *(page xxxi)* administrators have access to special import and export tools to manage their data in Password Server.

Import Tools

- **Master Import Tool** - Imports XML files generated using the Admin Tools > Complete Exports > **Export Total** option.
- **Bulk User Creation** - Automatically populates users and roles through a form builder. This tool can also import XML files generated using the Admin Tools > Complete Exports > **Export Users & Roles** option.
- **Bulk Vault Creation** - Automatically populate vaults through a form builder. This tool can import XML files generated using the Admin Tools > Complete Exports > **Export Vaults** option. All vaults created using the form builder use the **Default Password Policy** *(page xxxi)*. Any user that creates a vault is automatically assigned with **Owner** permissions for full access.
- **Bulk Password Creation** - Imports XML files generated by **Bulk Password Export**.

Bulk Password Export

- Exports all shared password data in clear text. Includes all of the details in the password record as well as the name of the vault containing it.

Complete Exports

> **Note:** All exports that affect passwords will notify all of the owners of each respective vault via email that the data has been exported.

- **Export Vaults** - Exports all of the password data in CLEAR TEXT. Includes all of the details in the password record as well as the name of the vault containing it.

- **Export Users & Roles** - Exports all user and role data mapped to specific scopes. Data can be re-imported using the Admin Tools > Import Tools > **Bulk User Creation** option.
- **Export Total** - Exports the following data: users, roles, scopes, permissions, shared vaults, and CLEARTEXT passwords. It does not export private or personal vault data, sync agent data, or audit reports.

User Control Panel

Passly (AuthAnvil) > Password Server > User Control Panel

The **User Control Panel** displays information about the currently logged in user. This includes:

- User properties
- Assigned vaults and vault permissions
- Assigned roles
- Favorite passwords

If you use a password to login to Password Server—instead of two factor authentication—you can also reset your password here.

Search Passwords

Passly (AuthAnvil) > Search Passwords

Enter a partial string in the **Password Search** field to find all matching password names and descriptions in all vaults you have permissions to access.

Index