Passwordstate

Enterprise Password Management

Local Logins to Active Directory Migration

Table of Contents

1 Introduction

This document will describe the steps required to convert to Local accounts to Active Directory accounts within Passwordstate.

These steps are primarily required due to the way the UserID field is encrypted throughout the database, with the format being different for both types of authentication.

These instructions are for valid for any version of Passwordstate with build number **9960** or above.

2 Configure new Active Directory Account with Full Access

1. Go to the screen **Administration** -> **Email Templates**, and disable all templates

2. Now go to the screen **Administration** -> **Privileged Account Credentials**, and specify a domain account which has read access to Active Directory for the account '**Read Active Directory Security Groups and User Accounts**'. Typically, making this account a member of the Security Group "**Domain Users**" will provide read access to your Active Directory environment.

3. Go to the screen **Administration** -> **Active Directory Domains**, and add in the new domain information and set it as the default domain. Select the Privileged Account you created in step 2 above when adding in this domain.

4. Go to the screen **Administration** -> **User Accounts**, and click the **Add From AD** button. Search for your own account in Active Directory and add it into Passwordstate – if you don't have enough licenses for this, you can disable any one of the existing user accounts as disabled accounts don't count against licensing

5. With this new account, go to the screen **Administration** -> **Security Administrators**, and grant the account access to all Roles – If this option is greyed out, please see this forum post for more information about how to enable this: Using Emergency Access to Grant new Security Administrator Roles - General FAQs - Click Studios Community

6. Now log out of Passwordstate, and then try logging back in with this new account.

7. If the login with the new account was successfully, then move on to **Section 3** below.

3 Cloning Permissions for Users and Security Groups

1. Depending on how many available free licenses you have, you may need to disable some users so that you can create new accounts for them in the new domain. Go to the screen **Administration** -> **User Accounts**, and disable accounts as required

2. On this same User Accounts page, add in the new accounts you need for the new domain by using the '**Add from AD**' button (If you have a large number of accounts, you can instead add an Active Directory Security Group that contains all the users. Adding a Security Group will sync all those users into the system. This can be performed under **Administration -> Security Groups**)

3. While still on the User Accounts screen, click on the '**Clone User Permissions**' button, and clone permissions between the domain accounts as appropriate (note this will clone permissions only, not any of the user's Preferences settings). If you have a large number of users, you can use the "**Bulk Clone**" feature on this page. This requires you to generate and populate a .csv file, and reimport it back into Passwordstate.

   When cloning permissions for user accounts, there is a feature that can be unlocked which will allow you to move any Private Password Lists from the old user account to the new user account. By default, this feature is not visible and you will need to send an unlock code to Click Studios' support to gain access to this feature.

   To unlock this feature, go to **Administration** -> **Feature Access** -> **Restricted Features** tab, and generate a code for the "**When cloning user permissions, allow moving of Private Password Lists from source user to destination user**:" restricted feature. Send this unlock code to Click Studios' Support, and they will reply with an unlock code.

   Once unlocked, you will see an option when cloning users called **"Do you wish to move any Private Password Lists from the Source User to the Destination User"**. Setting this to **Yes** will move any Private Password List across to the new user account as part of the cloning process.

   The restricted feature can be reversed, if you wish to lock it back down again.

4. If you are using Security Groups at all for applying permissions, go to the screen **Administration** -> **Security Groups**, add the appropriate Security Groups from the Active Directory domain.

5. Whilst still on the same page, clone permissions between the old local security groups, and the new AD security groups by clicking the **Clone Permissions** button on this page. **Note:** This step is not required if you prefer to continue using "Local" security groups, as opposed to domain groups

6. Once you have finished adding the new users, cloning permissions and changing ownership of Private Lists, you can delete the old user accounts and the old security groups from the system.

7. Go to the Screen **Administration** -> **Email Templates**, and enable all templates

8. Restart the **Passwordstate Windows Service** on your web server, and move on to **Section 4** below

4 Final Considerations

There may be a few other things you need to check as well i.e.

1. On the screen **Administration** -> **Backups and Upgrades**. If you're using this feature, you may need to change the account here which is used to perform the backups
2. If you are using SAML for authentication into Passwordstate, this feature works by matching a specific attribute on the account in Passwordstate with the account in the SAML provider. You will need to ensure that attribute on the new Active Directory accounts you have added in as part of this guide are exactly the same as they were on the old local account. An example of this matching attribute is "**Email Address**". Users will not be able to login with their new domain accounts, if these attributes are not set correctly and you are using SAML to authenticate.