Passwordstate
Enterprise Password Management

Active Directory to Local Logins Migration

Table of Contents

1   Introduction

This document will describe the steps required to convert to Local Account based authentication from Active Directory authentication. 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.

2   Migration Process

Step 1:

1. Upgrade Passwordstate to the latest build available, using this document as a guide: https://www.clickstudios.com.au/downloads/version9/Upgrade_Instructions.pdf. If you are running Passwordstate build 9435 or higher, this step is not required.

Step 2:

1. Got to the screen **Administration** -> **Email Templates**, and disable all templates
2. Now go to the screen **Administration** -> **User Accounts**, and create a new account for yourself – 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. Your new username can be the same as your domain account if desired. For example, if your domain username is '**contoso\jbloggs**', simply create your new user name as '**jbloggs**'
3. 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
4. Now log out of Passwordstate, and then try logging in with this new account
5. If the login with the new account was successful, then move on to Step 3 below

Step 3:

1. Go to the screen **Administration** -> **User Accounts**, and disable all the other Active Directory accounts – Active Directory accounts will be in the format of **domain\username** and you can disable these from the **Actions Menu** for each account, of if you have multiple accounts you can tick the check box next to their names and select **Process Selected Items** -> **Toggle Status**
2. Now create the new accounts you need. You can create these one-by-one, or you can use the '**Import**' button which will ask you to populate and import a csv file with all your new users.
3. While still on the User Accounts screen, click on the '**Clone User Permissions**' button, and clone permissions from the old Domain Accounts to the new Local Account based 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, we have introduced a "**Bulk Clone**" feature as of Build 8215. This can be found on the "**Clone User Permissions**" screen and requires you to generate and populate a .csv file, and reimport it back into Passwordstate. Ensure when cloning each user, you select the '**Move any Private Password Lists from the Source user to the Destination user**'
4. Once this is done, if you are using Security Groups at all for applying permissions, you now go to the screen **Administration** -> **Security Groups**, add one Local Security Group for each AD Security Group you have in the system. Then clone permissions between the security groups by clicking the '**Clone Permissions**' button on this page.
5. Now you can delete any old User Accounts or Security Groups from the system
6. Got to the Screen **Administration** -> **Email Templates**, and enable all templates
7. Restart the Passwordstate Windows Service

Step 4:

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

1. Screen **Administration** -> **System Settings** -> **Email Alerts & Options**. Possibly your email server settings may need changing
2. 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