

Password Reset PRO: Determining Licensed vs. Unlicensed User Accounts

Software version 3.x.x

This guide will help you to understand how “licensable” users are determined by Password Reset PRO.

We are using the standard Active Directory cataloging system to determine your “licensable” user accounts in AD that will require licenses and can use the self service Web Portal. Normal, password expiring user objects in AD have a userAccountControl identifier of “512” (0x200), and these are the only user accounts which require licenses / can access the Web Portal. We reference these licensable user objects in order of their AD creation date, from oldest to newest. If you go over your licensed amount, then only the *newest* AD accounts over your limit are excluded from access until you add more licenses to cover them. We can apply licensing to the entire domain, one OU only, or several OUs.

This type of licensing system is very cost effective will exclude any need to license your disabled user accounts, System AD accounts (IWAM, IUSR, \$ etc), and enabled user accounts set with “password never expires” on their account properties (typically your service / resource accounts). These other types of accounts have different userAccountControl identifier numbers and are excluded from access to the Web Portal automatically.

We also exclude the domain/administrator, domain/guest, domain/krbtgt, user accounts with an expired logon date or expired logon hours, user objects missing the UPN (universalPrincipalName) and user objects set with “can’t change password”.

Are “service” or “resource” or terminated employee accounts showing as “licensed users” and consuming licenses?

Keep in mind that a “service” or “resource” user account is still considered a *normal user object* by Active Directory standards, the same as an actual employee user account. It is very common to have a number of “resource / service” user accounts in AD that have been left unmanaged and with an expiring password. In this case, no one actually logs on with the account and it solely exists to run a calendar meeting room, phone system, etc. As far as AD (and our software) is concerned these are simply normal, password expiring user accounts, and will require a license by our software.

To remedy these accounts from taking up licenses, look through the Password Reset PRO Report Console tabs for “Licensed Users” and “Unlicensed Users”. Look for any obvious non-employee user accounts which may solely exist to run a “resource” or “service”. Open the Active Directory Users and Computers management console, go to the properties for each of these user accounts, and set them to “password never expires”. This will remove the accounts from requiring licenses for our software, and if you are presently over your licensed amount, it could help you get back below your licensing limit. The Report Console is located in the Master Service configuration application, on the “Report and Email Settings” tab. Also, take a look through the “Excluded Users” tab to see which if your enabled user accounts in AD are being excluded from licensing and from Web Portal access.

Ideally and from a compliance perspective, only your enabled employee-assigned user accounts should expire the password via policy. All other types of user accounts should be managed by disabling unused or “temp” accounts, and setting active “resource / service” accounts to “password never expires” in AD. The Report Console helps make this an easy task.

Tech Note: Terminated employee user accounts kept active for Exchange mailbox access should have the password changed, set with “password never expires” and “can’t change password” on the account in AD to secure them while they remain in use, and also exclude them from licensing.

We’re suggesting this according to current typical standards and requirements for PCI/DSS, Sarb-Ox, SaS 70, and HIPAA compliance, which our software is designed to help you enforce and maintain.

Have more questions? Contact our knowledgeable Sales & Support Teams

1-877-SYSOPTOOLS (USA) or +1-213-995-5060 (Direct & Int'l)

Support Team Hours: M-F 8am-6pm PST | Sales Team Hours: M-F 9am-6pm PST

Additional Resources:

 [Purchase Information](#) |

 [Reference Material and Knowledge Base](#)

 [Support Information](#) |

 [**>>Sign up and Download Password Reset PRO Software**](#)

SysOp Tools, Inc. is a privately held company located in Los Angeles, California – Software sales, support and development are handled by experienced in-house staff. We do not outsource any of our operations.