THINMANAGER®
A ROCKWELL AUTOMATION TECHNOLOGY

LEARNING PAPERS:

ThinManager & Active Directory

ThinManager supports Active Directory integration to the platform.

ThinManager 8 and above supports Active Directory integration to the platform.

Terminal Users

Each Terminal needs a unique Windows account. The current Active Directory integration allows the ThinManager administrator to connect to the Active Directory, search for users, and reference an AD account as its Windows account. This can speed configuration and cut down on naming errors.

Location Users

Relevance uses Locations to deploy applications to the user. The Windows account is applied to the Location and not the terminal. The ThinManager Active Directory integration allows the administrator to connect to the Active Directory, search for users, and reference an AD account as its Windows account to speed configuration and eliminate naming errors.

Relevance User Services (formerly TermSecure)

Remote Desktop Services makes maintenance easier. Because the applications are Relevance User Services, formerly TermSecure, is an additional layer of security provided by ThinManager. There are two modes for Relevance User Services.

It can hide applications from users unless they log in with the correct access permission.

It can be used to apply an application(s) to a user where ever a user logs in, essentially making the application follow the user.

Relevance Users need a unique Windows account if they have an application tied to it. You can create the Relevance User with any name and tie it to an AD account, or use the Active Directory to create Relevance Users that match the AD account.

You can also create a Relevance User Services group by directly importing the users from an Active Directory Organizational Unit or Security Group. Users added to the AD OU or Security Group get automatically added as Relevance Users, and users deleted from the AD OU get deleted from ThinManager.

Continued on next page »

Password Management

ThinManager has added Password Management integration with Active Directory.

For handling AD passwords there are two basic modes:

No password stored. In this mode ThinManager does not keep or store the AD user's password. The user is prompted to enter the password when needed. (This applies to Relevance users only)

ThinManager can store the password. This allows you to use a badge or fingerprint scan and not need to enter a password after the scan.

You can use ThinManager to generate a new password and rotate the password in AD according to a set password policy. This allows you to match your standard password policy with ThinManager.

Requirements

Active Directory integration requires that the ThinManager Server be a member of a domain. Since Microsoft recommends that Server 2012 be run in a domain, the new Active Directory integration is helpful moving forward in the Microsoft environment.

The ThinManager administrator does not need to be a domain administrator, they just need to know the password of each account they reference.

Summary

ThinManager 8 introduced Active Directory integration. You can reference Active Directory users for use with ThinManager Terminal user accounts, Location user accounts, and Relevance User accounts.

Active Directory Organizational Units (OUs) can be used to create Relevance User Groups. Once connected, the ThinManager database will automatically synchronize the Active Directory Organizational Unit users with the Relevance User Group. Users added to AD will be added to the ThinManager tree, users deleted from AD will be removed from the ThinManager tree.