Recast

Automating password rotation

Last Modified on 2026-09-24

Keeping passwords secure and up to date is a critical part of maintaining software security. Manual password changes can be time-consuming and prone to oversight, especially in environments where credentials need to be rotated regularly. Application Workspace Powershell Module in combination with Application Workspace provides built-in tools that make this automation process straightforward.

This article offers you some basic examples of scripts which you can run at regular intervals by using scheduled tasks within Application Workspace or other tools like Windows Task Scheduler. These scripts cover for all the indentity sources types available in Application Workspace, connectors and SMTP and Microsoft Graph mail servers.

Examples

Application Workspace connector

```
$connector = Get-LiquitConnector -Name "AW Test"
$settings = $connector.Settings
$settings.password = "abcdefghijk123"
Set-LiquitConnector -Connector $connector -Settings $settings
```

Microsoft Graph mail server

```
$mailServer = Get-LiquitMailServer -Search "Test MS Graph Mail"
Set-LiquitMailServer -MailServer $mailServer -ClientSecret "abcdefg"
```

SMTP mail server

```
$mailServer = Get-LiquitMailServer -Name "SMTP Mail Test"
$password = ConvertTo-SecureString "abcdefg" -AsPlainText -Force
$credential = New-Object System.Management.Automation.PSCredential ($mailServer.Username, $password)
Set-LiquitMailServer -MailServer $mailServer -Credential $credential
```

LDAP identity source

```
$idSource = Get-LiquitIdentitySource -Name "LDAP Test"
Set-LiquitIdentitySource -IdentitySource $idSource -Password "abcdefgh"
```

Microsoft Entra ID (Azure AD) identity source

```
$idSource = Get-LiquitIdentitySource -Name "Entra ID Test "
Set-LiquitIdentitySource -IdentitySource $idSource -ClientSecret "abcdef12345"
```