



Active Directory Password Resets Using Cimitra

Table of Contents

Scenario Explanation	1
Before Cimitra - Student Password Reset Process	2
After Cimitra - Student Password Reset Process	2
Technical Overview	2
Active Directory Structure	2
Security Considerations	3
Technical Challenges	3
Technical Procedures Overview	3
Create A Special Purpose Active Directory User	4
Delegate Control To The Special Purpose Active Directory User	6
Install The Cimitra Agent	9
Install The PowerShell Script for Resetting Active Directory Passwords	11
Script Integration Into Cimitra	11
Share The Cimitra App	14
Conclusion	15

Scenario Explanation

Allowing a bigger group of people to reset passwords is one of the most popular use case requests for Cimitra. This solution explains how to reset Microsoft Active Directory passwords with a PowerShell script behind-the-scenes of a Cimitra App. Similar concepts could be applied to other solutions.

This document is based upon a real-world example from a university in the United States. The university has all students and staff registered in **Microsoft Active Directory (MAD)**. MAD gives access to workstations and applications provided by the university.

The Information Technology Services department is comprised of 3 different types of staff members.

1. Student Help Desk
2. Main Help Desk
3. IT Specialists

Utilizing Student Help Desk staff helps to manage the workload of having to service thousands of students. However, the need to reset a student's password, which happens often, took the following **8 steps** which might take **over a day** to accomplish. With Cimitra there are only **3 steps** that can be performed in a matter of **2 minutes**.

Before Cimitra - Student Password Reset Process

1. Student contacts Student Help Desk
2. Student Help Desk determines that a password reset event is required
3. Student Help Desk escalates to the Main Help Desk
4. Main Help Desk escalates a service ticket to an IT person who has sufficient rights in MAD to reset the student's password
5. The IT person resets the student's password
6. The IT person communicates back to the Main Help Desk that the password was reset
7. The Main Help Desk communicates back to the Student Help Desk that the password was reset.
8. The Student Help Desk informs the student that their password was reset

After Cimitra - Student Password Reset Process

1. Student contacts Student Help Desk
2. Student Help Desk determines that a password reset event is required
3. Student Help Desk personnel resets the student's password with Cimitra

Technical Overview

Active Directory Structure

Every person at the university is registered in MAD. In this scenario, Student Help Desk personnel should only be able to change the MAD passwords for students, and that is it!

All of the students are contained in one Organizational Unit (**OU**) in MAD called “**STU**”. This organizational structure greatly helps this solution.

Security Considerations

The procedure outlined in this document will take into account the following security requirements:

1. Student Help Desk personnel should only be able to reset the passwords for users in the **STU** Organizational Unit (**OU**) in Microsoft Active Directory (**MAD**).
2. Ever password reset should be auditable.

Technical Challenges

There are thousands of students in the **STU** Organizational Unit (**OU**). Many students have duplicate names. As such, the student’s need to be identified in the Cimitra Password Reset App by their “**Userid**” which in reality in Microsoft Active Directory (**MAD**) is an attribute called **sAMAccountName**. The following method is the PowerShell method for how a password is reset in MAD using the **sAMAccountName** to positively identify exactly whose password needs to be reset:

```
Set-ADAccountPassword -Identity $sAMAccountName . . .
```

The **Set-ADAccountPassword -Identity \$sAMAccountName** has one stubborn limitation, there is **no way to limit the scope** in which the command will work. Said a different way, using the method **Set-ADAccountPassword -Identity \$sAMAccountName** allows the password change of **any** person in MAD no matter why they are in the MAD tree.

Coming back to our example scenario, the following needs to be accomplished

1. **Allow** Student Help Desk to change passwords for MAD users in the **STU** OU only.
2. **Not Allow** Student Help Desk to change passwords in any other OU in MAD.

Technical Procedures Overview

This is a simple list showing an overview of the steps required to set up this solution.

1. Create an Active Directory user that does not exist in the **STU** OU
2. Delegate rights to the **STU** OU to the user which was created in Step #1

3. Determine the Windows Server that will host the Cimitra Agent, such as the Active Directory Domain Controller (DC).
4. Create a Cimitra Agent that will be specially created for this function
5. Define the Cimitra Agent as a very specific service on the Windows Server
6. Enable the Cimitra Agent to run as the user created in Step #1
7. Deploy the [SetUserPasswordSamAccountName.ps1](#) script to the server identified in Step #3.
8. Define a Cimitra App using the Cimitra Agent defined in Step #4. Link the Cimitra App to the script in Step #7.
9. Share the Cimitra App with users who should be enabled to reset passwords.

Create A Special Purpose Active Directory User


1. **Create** a new user in a **different** OU from the OU with users who will have password management via Cimitra. For example, a user called **AD_CIMITRA_ADMIN**.

The screenshot shows the 'New Object - User' dialog box in Active Directory. The dialog is titled 'New Object - User' and has a close button (X) in the top right corner. Below the title bar, there is a user icon and the text 'Create in: cimitrademo.com/CIMITRA'. The main area contains several input fields:

- First name: Cimitra
- Initials: (empty)
- Last name: Admin
- Full name: Cimitra Admin
- User logon name: AD_CIMITRA_ADMIN
- User logon name (pre-Windows 2000): CIMITRADEMO\AD_CIMITRA_ADMIN

At the bottom of the dialog, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'Next >' button is highlighted with a blue border.

New Object - User ✕

 Create in: cimitrademo.com/CIMITRA

Password:

Confirm password:


User must change password at next logon

User cannot change password

Password never expires

Account is disabled

New Object - User ✕

 Create in: cimitrademo.com/CIMITRA

When you click Finish, the following object will be created:

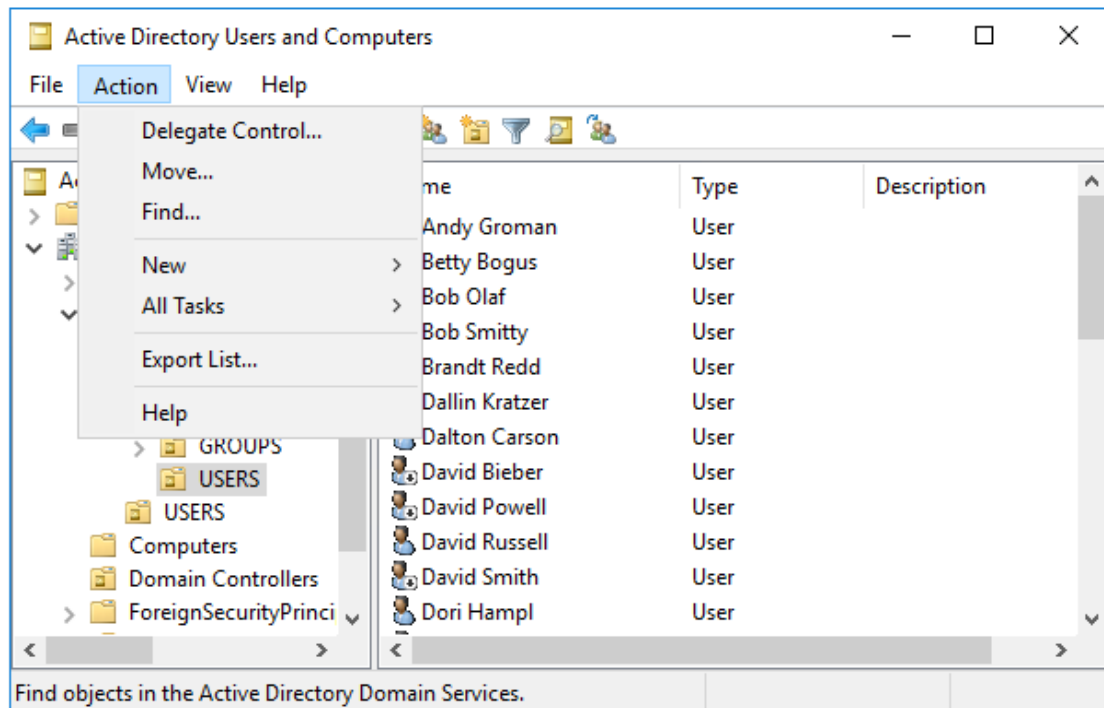
Full name: Cimitra Admin

User logon name: AD_CIMITRA_ADMIN@cimitrademo.com


The user cannot change the password.
The password never expires.

Delegate Control To The Special Purpose Active Directory User

2. **Delegate** rights to the OU in which you want to manage users in from Cimitra, to the user you created in step #1. To do this, highlight the OU that contains the users to be managed, and select **Action | Delegate Control**. Give the rights to **Reset user passwords and force password change at next logon**.



Delegation of Control Wizard ✕




Welcome to the Delegation of Control Wizard

This wizard helps you delegate control of Active Directory objects. You can grant users permission to manage users, groups, computers, organizational units, and other objects stored in Active Directory Domain Services.

To continue, click Next.

< Back Next > Cancel Help

Delegation of Control Wizard ✕

Users or Groups 

Select one or more users or groups to whom you want to delegate control.

Select Users, Computers, or Groups ✕

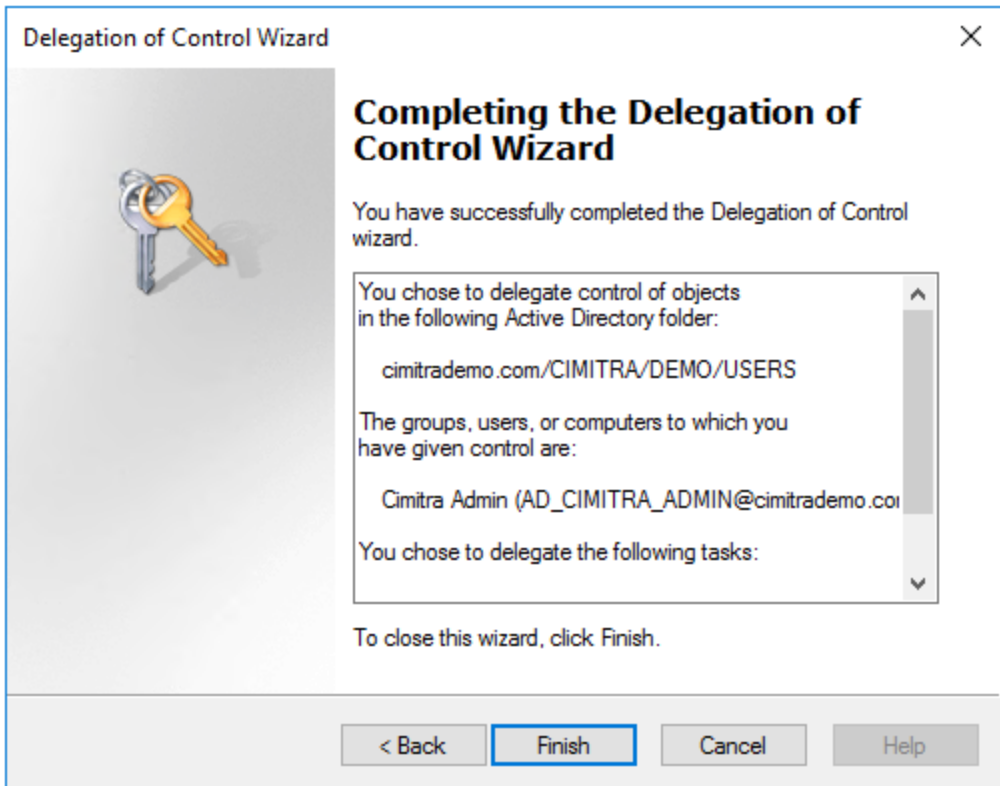
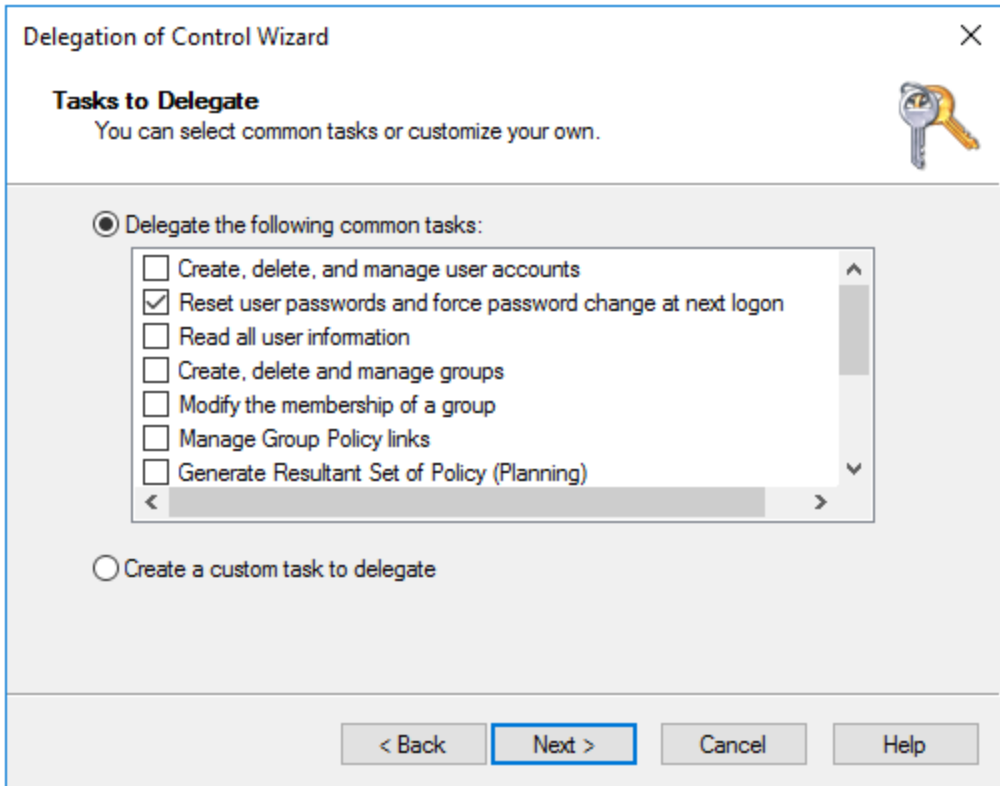
Select this object type:
 Object Types...

From this location:
 Locations...

Enter the object names to select ([examples](#)):
 Check Names

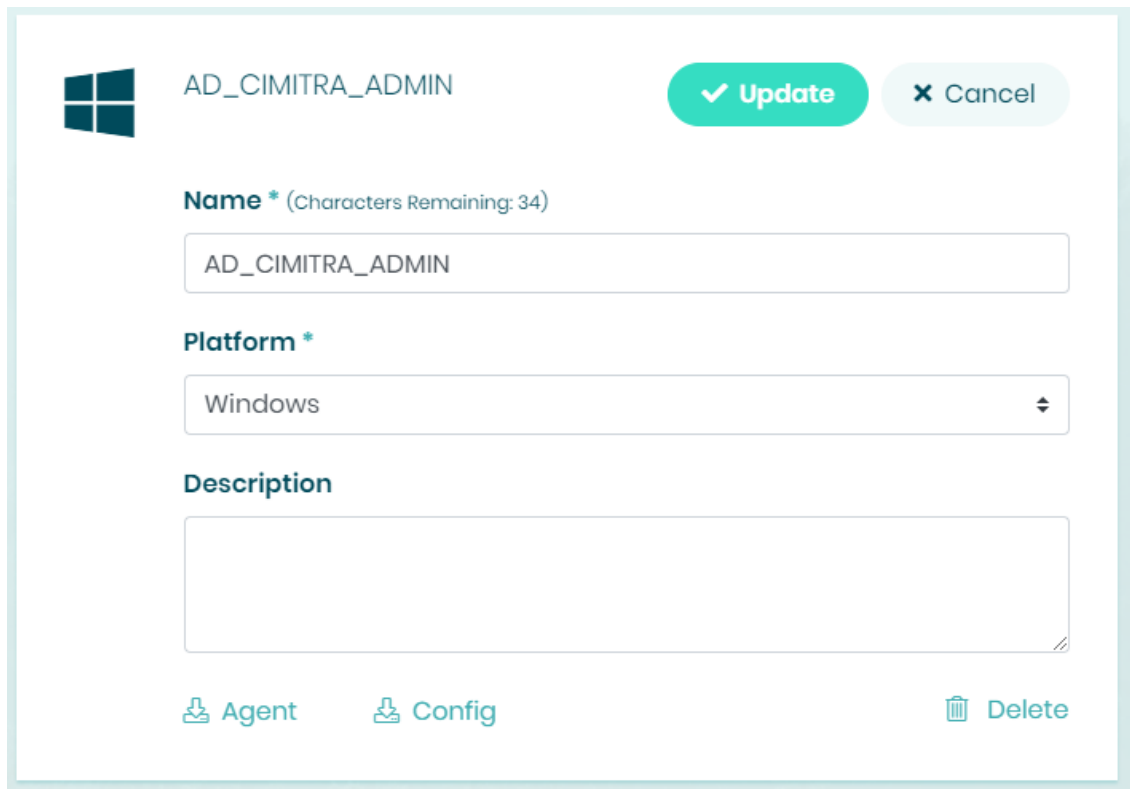
Advanced...OKCancel

< Back Next > Cancel Help



Install The Cimitra Agent

3. Determine a Windows Server that will host the Cimitra Agent, for example, the Domain Controller.
4. Create a new Cimitra Agent in Cimitra Administration. You may want to call it: **AD_CIMITRA_ADMIN** that's just a suggestion to keep things clearer.



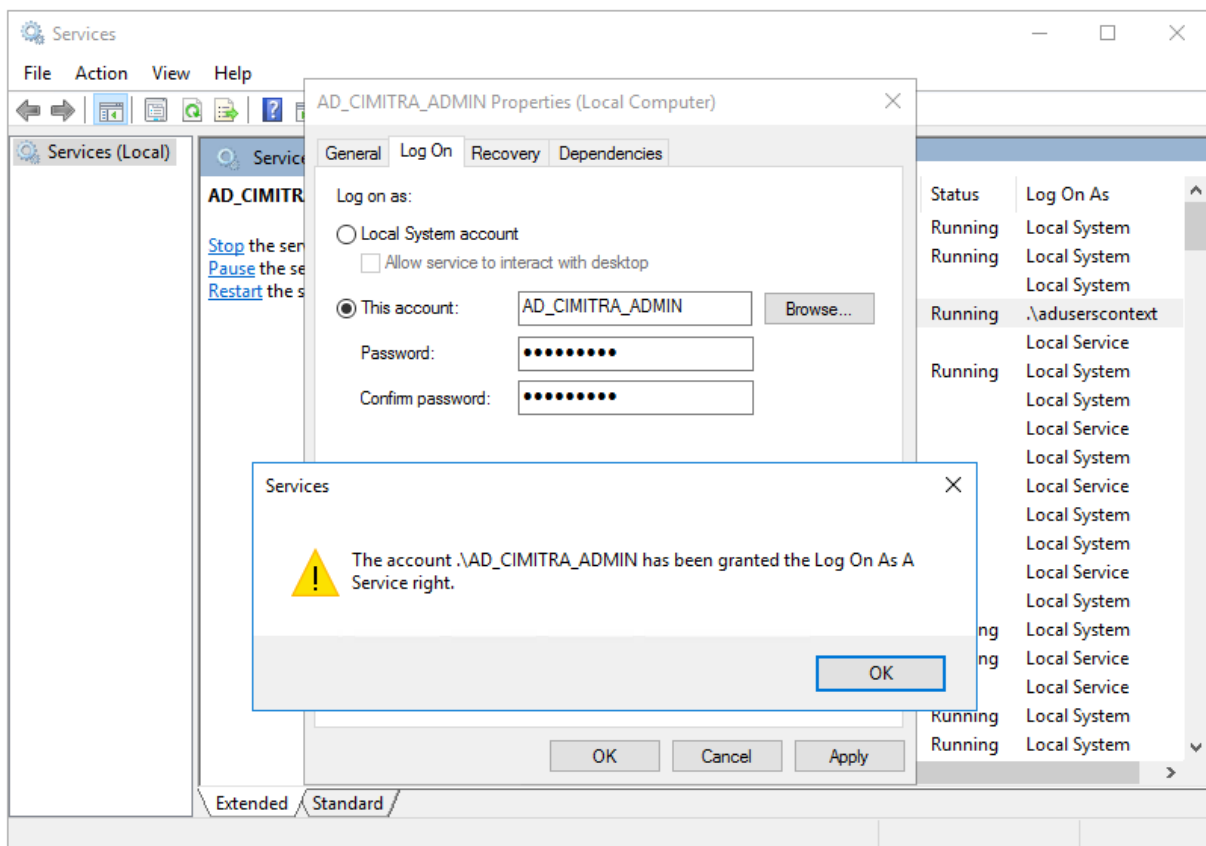
The screenshot shows a configuration window for a Cimitra Agent. At the top left is a Windows logo icon. The title of the window is "AD_CIMITRA_ADMIN". On the top right, there are two buttons: a green "Update" button with a checkmark and a grey "Cancel" button with an 'X'. Below the title, there is a "Name *" field with a character count "(Characters Remaining: 34)". The text "AD_CIMITRA_ADMIN" is entered in this field. Below that is a "Platform *" dropdown menu with "Windows" selected. Underneath is a "Description" text area which is currently empty. At the bottom of the window, there are three icons: "Agent" (a person icon), "Config" (a gear icon), and "Delete" (a trash can icon).

5. Install the Cimitra Agent as a service on the Windows Server using this documentation:

However, rather than letting the Cimitra Windows service be called by its default name: **"Cimitra"** it may be easier to correlate the Windows Service to the Cimitra Agent for this specific purpose if you call the Windows Service: **AD_CIMITRA_ADMIN**. See the section of Cimitra Agent for Windows documentation titled: **Advanced Installation | Additional Cimitra Agent Instances**. Using this approach of a different name for the Windows service, allows you to install a different instance of the Cimitra Agent that you

would use for a different set of scripts, that don't need restrictions to a particular OU in Active Directory.

6. After defining the **AD_CIMITRA_ADMIN** service go into the **Windows Services** utility and indicate that the user that runs the Cimitra Services is "**AD_CIMITRA_ADMIN**".



Install The PowerShell Script for Resetting Active Directory Passwords

7. Deploy the script [SetUserPasswordSamAccountName.ps1](#) to the Windows Server that is running the **AD_CIMITRA_ADMIN** Cimitra Agent.

Script Integration Into Cimitra

8. Define the Cimitra App that references the **AD_CIMITRA_ADMIN** Cimitra Agent and the path to the [SetUserPasswordSamAccountName.ps1](#) script along with the 2 parameters as follows.

CIMITRA APP PROPERTIES

Property	Value
Platform	Windows
Agent	AD_CIMITRA_ADMIN
Name	SET PASSWORD - Userid
Interpreter	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Script/Command	SetUserPasswordSamAccountName.ps1
User Defined Switches/Parameters	Click the “+Add Switch” option two times for switches as shown below. These switches correlate with the two command-line parameters we programmed into the script.

USERID SWITCH

Flag:	<LEAVE THIS FIELD BLANK>
Parameter Name:	USERID
Validating Regex:	/^[A-Za-z.-_]+\$
Allow: Letters, Periods, Dashes and Underscores	

PASSWORD SWITCH

Flag:	<LEAVE THIS FIELD BLANK>
Parameter Name:	PASSWORD
Validating Regex: Allow: Letters, numbers, dashes, and Underscores	/^[A-Za-z0-9_]+\$/
Example:	(Letters, Numbers, Dash "-", Underscores "_")
Mask: (Like a password)	ENABLE THIS

INFORMATION FIELD

NOTE: The password should be 8 characters long, and include a number and an underscore or dash and one uppercase letter.

[← Back](#)

▶ **SET PASSWORD - Userid**

Platform *

Agent *

Name * (Characters Remaining: 29)

Interpreter


Script/Command *

Switches

Switches

User Defined Switches / Parameters

[+ Add Switch](#)

USERID 


Flag:

Parameter Name:

Validating Regex:

Example:

Mask: (Like a password)

PASSWORD 

Flag:

Parameter Name:

Validating Regex:

Example:



Mask: (Like a password)

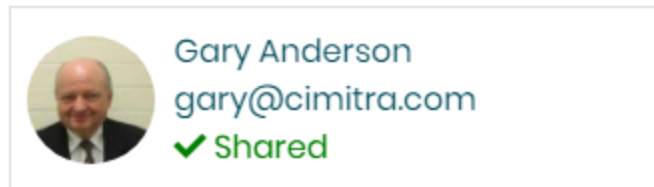
Information

Share The Cimitra App

9. Share the Cimitra Application with the people you want to be able to reset passwords.
 - a. Sharing an App requires that the App is placed into a Folder in Cimitra. You can drag and drop the Cimitra App to the Folder you want to place it into.



- b. Share the folder with the people who you want to have access to the Cimitra App to reset user passwords. Do this by going into the folder clicking the **pencil icon**  next to the folder name.
- c. Then select the **Sharing** option  **Sharing**
- d. Click on users that you want to have access to the Cimitra Folder with the Password Reset Application in it.



Conclusion

The setup of this script was very technical, primarily to meet the security requirements that the Student Help Desk should only be able to reset passwords in the STU context. The procedure for setting up most Cimitra Scripts is generally not as lengthy. The PowerShell command **Set-ADAccountPassword** is simply too powerful in its scope so the procedures in this documentation helped to reign in the power and scope of the PowerShell **Set-ADAccountPassword** command.