Change device credentials from Cisco Catalyst Center for wired and wireless devices for both SDA and Non-SDA network scenarios

Contents

Introduction

This document describes the steps of the credential change procedure from Cisco Catalyst Center (formerly Cisco DNA Center) for wired and wireless devices for both fabric and non-fabric network scenarios.

Background Information

This document also applies to sites with Dynamic Network Access Control (Cisco Catalyst Center) managed or unmanaged Authentication, Authorization and Accounting (AAA).

Synopsis

This document discusses the situation where there is a network requirement of updating the credentials used by Cisco Catalyst Center for automation. Managed devices are discovered by Cisco Catalyst Center with a username and password, and those same credentials are used by Cisco Catalyst Center for SSH connections to the managed devices (for automation/inventory collection and so on). This document covers the best practices to change the password for managed devices after they are discovered by Cisco Catalyst Center.

Solution (Best Practice)

Requirements

1. For sites with Cisco Catalyst Center managed AAA

- Requirement is to change the user’s password (no change to the enable password).
- Requirement is to change the user’s password and the enable password.

2. For sites with Cisco Catalyst Center unmanaged AAA

- Requirement is to change the user’s password (no change to the enable password).
- Requirement is to change the user’s password and the enable password.

Pre-requisites

- Ensure that AAA is not configured in Cisco Catalyst Center for all non-SDA sites.
- Use a Python script to validate whether all the Catalyst 9k switches (SDA or non-SDA) use RADIUS to ISE for SSH logins to VTY lines. Fix any devices that use local credentials.
- For extended Nodes
    - To update lines vty 0 to 4 use these configuration commands (this can be the very first step for extended nodes).

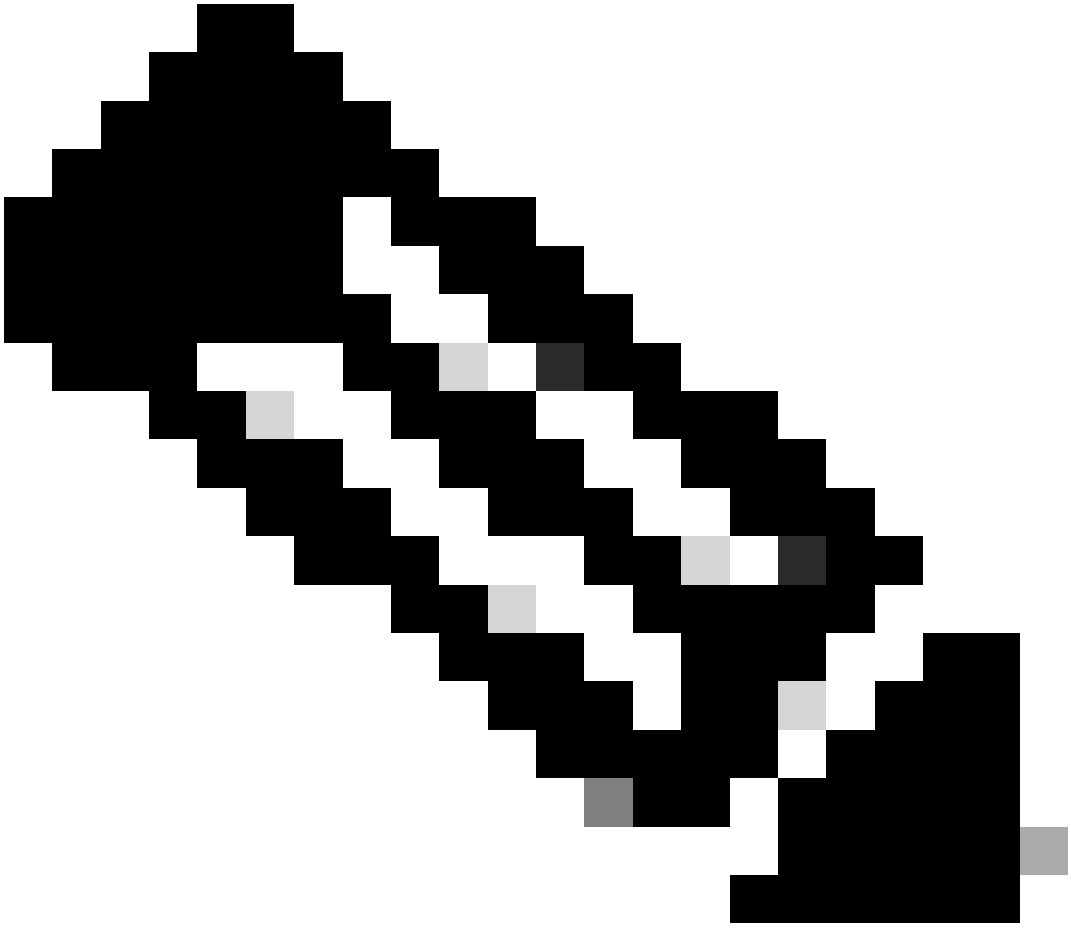
```
line vty 0 4
authorization exec VTY_author
login authentication VTY_authen
```

Procedure for Credential Change from Cisco Catalyst Center

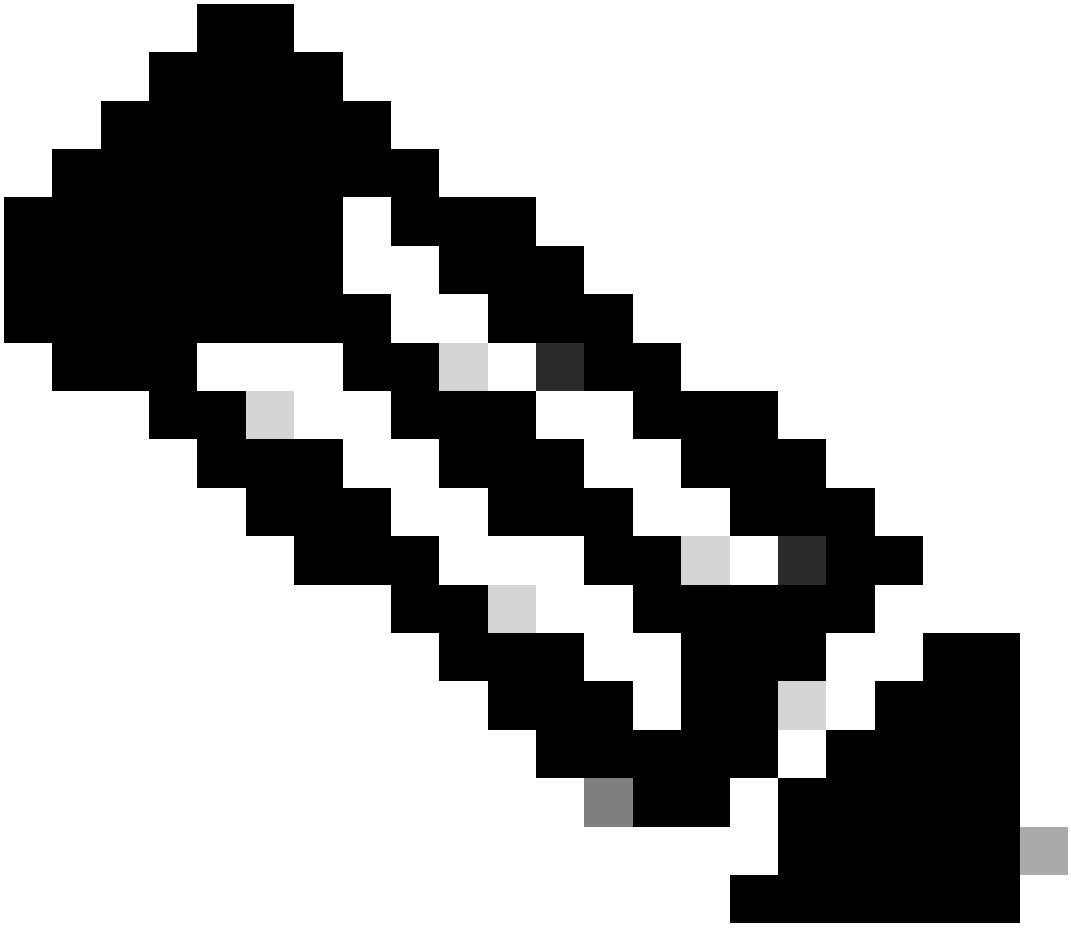
Sites with Cisco Catalyst Center Managed AAA

Requirement is to change the user’s password (no change to the enable password)

1. First update the credentials (password for the relevant username) in ISE. This will cause inventory collection failure and the managed device inventory states will change to Unreachable, Partial Collection Failure or Wrong Credentials.
2. On the Provision > Inventory page, select one or multiple devices and select Actions > Inventory > Edit Device > Credentials tab. Next, update the “Add device specific credential” with the new username and/or password (keep the same enable password). At this point Cisco Catalyst Center will be able to login to devices with the updated credentials and the device inventory states will come back to Managed.
3. The local credentials of the devices can be updated as a fallback in order to ensure that Cisco Catalyst Center is able to login to devices when the external AAA server is unreachable. The local credentials can be updated by using Cisco Catalyst Center's Template Editor, a custom Python script, or manually.
4. The last step is to update those same credentials on the Global Credentials page. This ensures that newly discovered devices or devices that are added that using LAN Automation will use the updated credentials from the Design page > Network Settings > Device Credentials > CLI Credentials > edit the username > update the user’s password without changing the enable password.



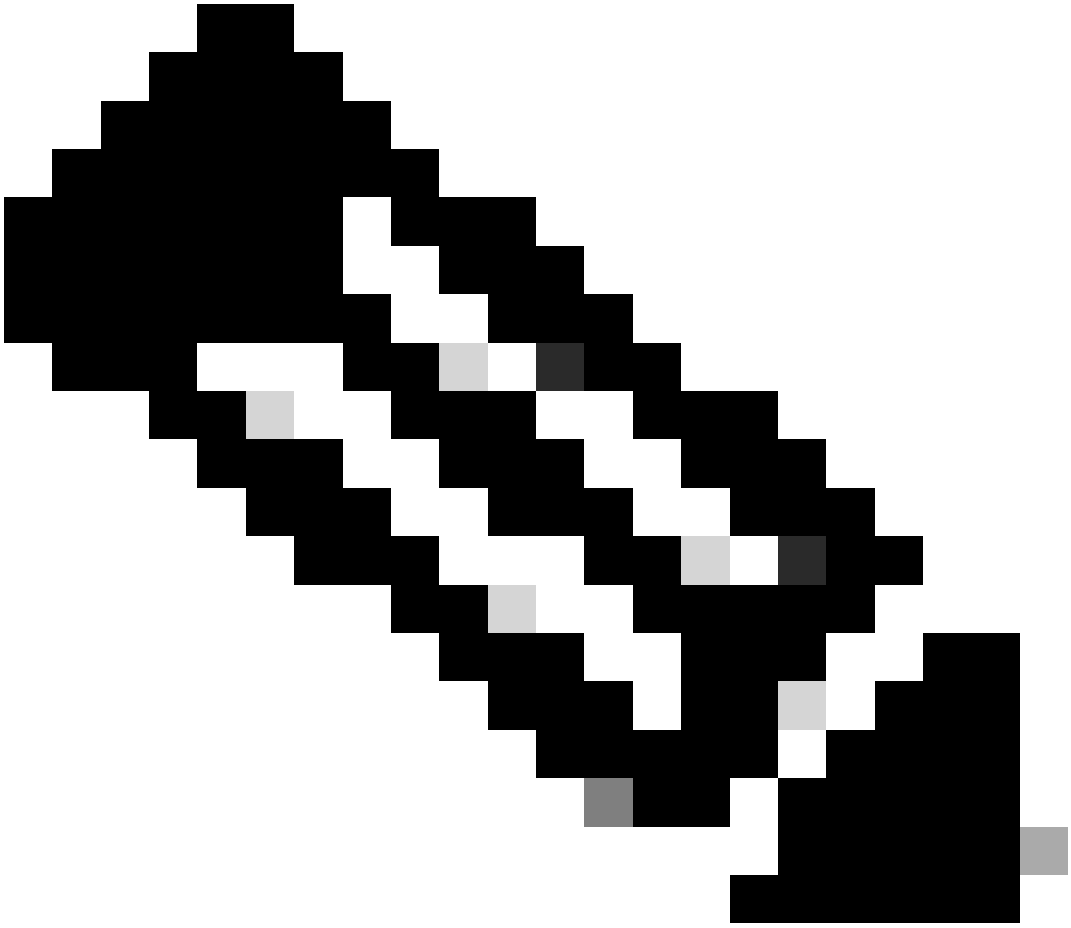
Note: The SSH/Telnet login is authenticated by the external AAA server. Local device credentials are not updated.



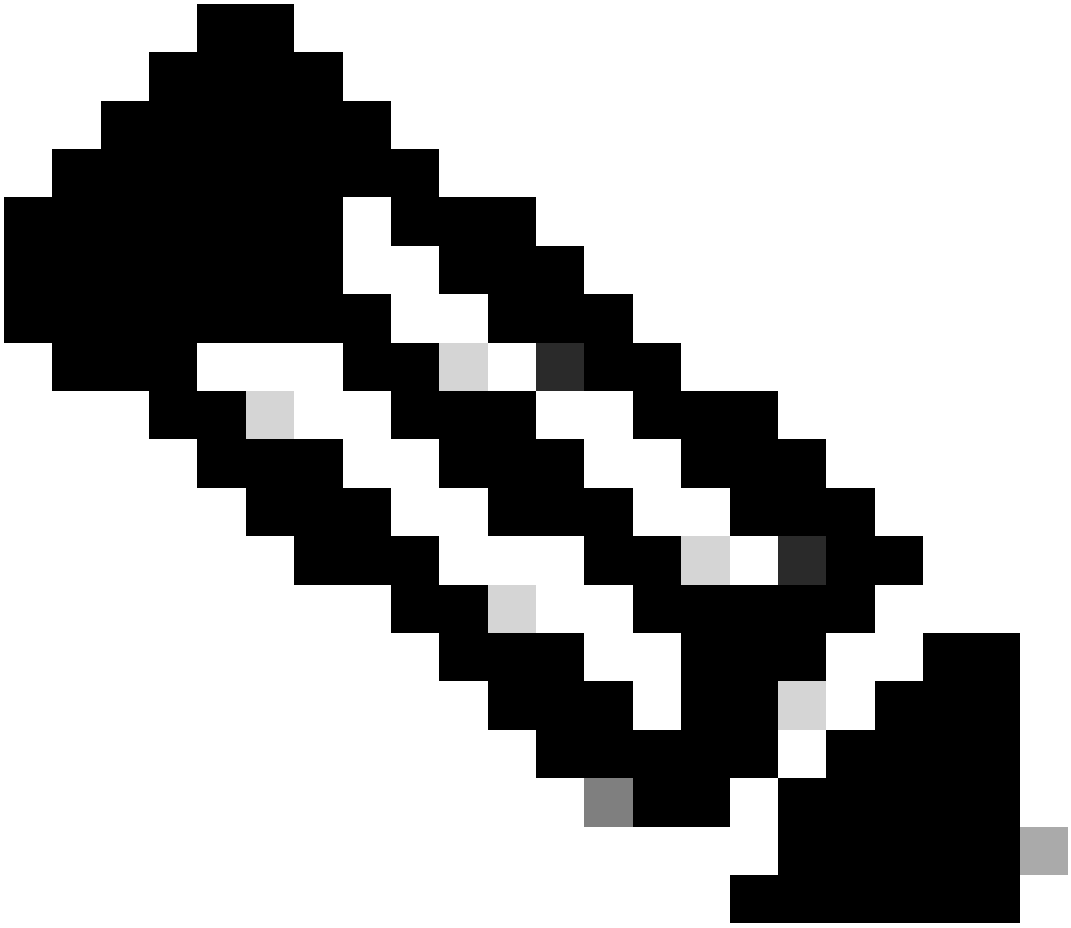
Note: When an external AAA server is configured on Cisco Catalyst Center's Design page for a site, Cisco Catalyst Center does not take any action on managed devices or ISE when you change/modify the credentials on the Global Credentials page.

Requirement is to change the user's password and the enable password

1. First update the credentials (password for the relevant username) in ISE. This will cause inventory collection failure and the managed device inventory states will change to Unreachable, Partial Collection Failure or Wrong Credentials.
2. On the Provision > Inventory page, select one or multiple devices and select Actions > Inventory > Edit Device > Credentials tab. Next, update the "Add device specific credential" with the new username and/or password as well as the enable password. At this point Cisco Catalyst Center will be able to login to devices with the updated credentials and the device inventory states will come back to Managed.
3. The last step is to update those same credentials on the Global Credentials page. This ensures that newly discovered devices or devices that are added that using LAN Automation will use the updated credentials from the Design page > Network Settings > Device Credentials > CLI Credentials > edit the username > update the user's password and the enable password.



Note: When the external AAA server is reachable, the username and password get authenticated by the external AAA server and the enable password gets authenticated locally by the managed device.

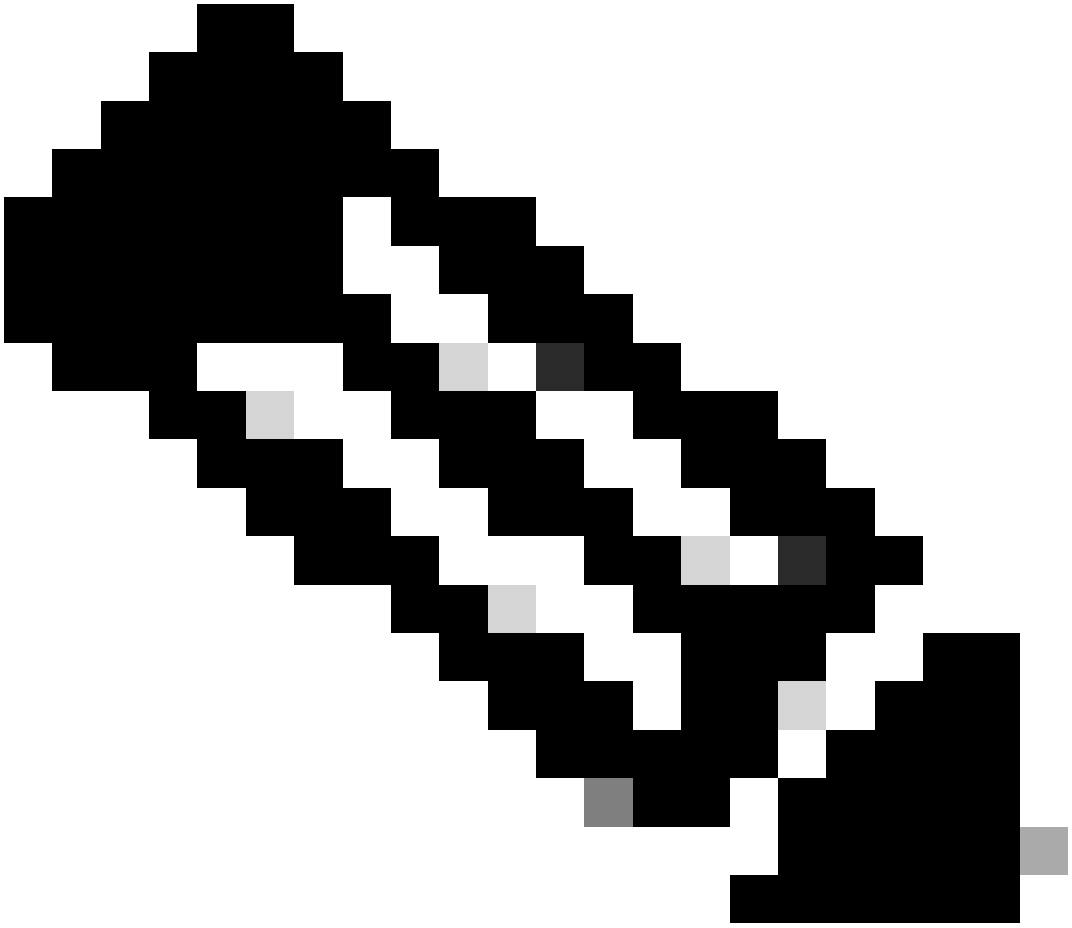


Note: When an external AAA server is configured on Cisco Catalyst Center's Design page for a site, Cisco Catalyst Center does not take any action on devices or ISE when you change or modify the credentials on the Global Credentials page.

Sites with Cisco Catalyst Center Unmanaged AAA

Requirement is to change the user’s password (no change to the enable password)

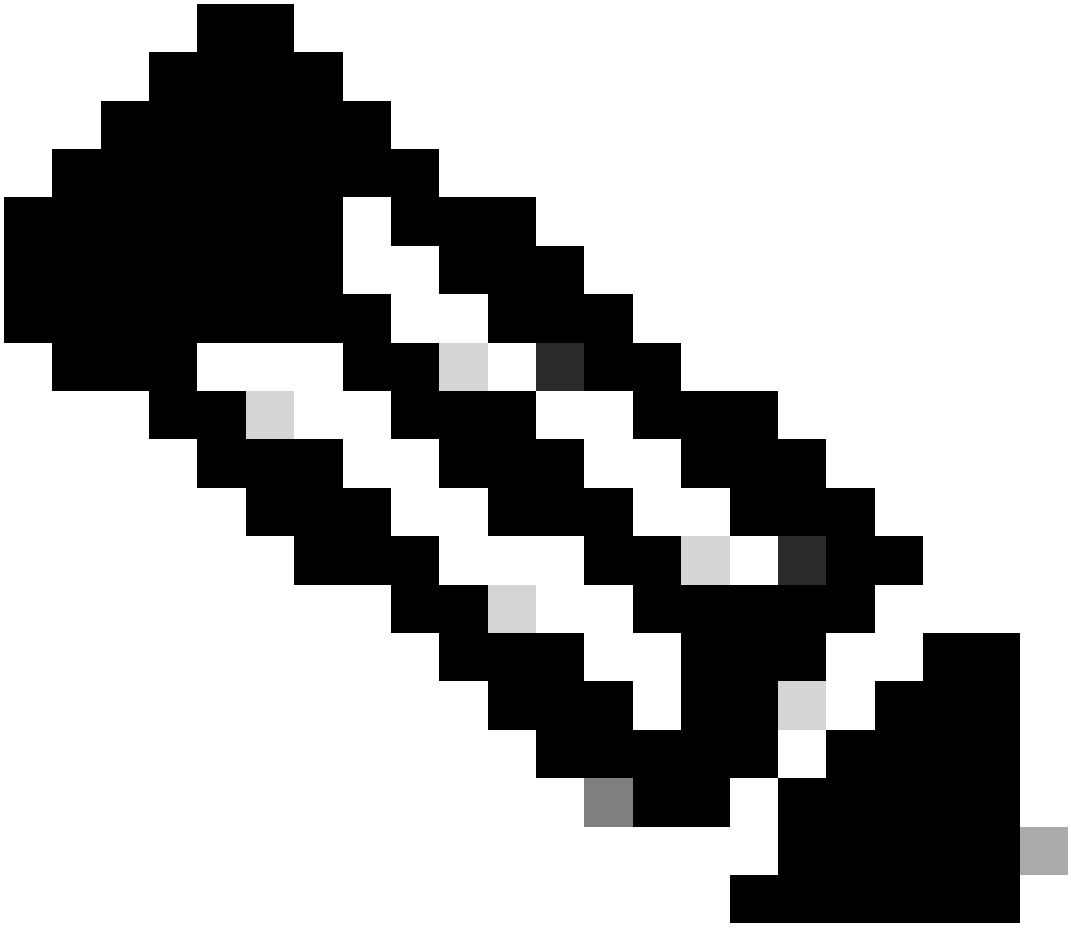
1. Update the credentials on the Global Credentials page at Design > Network Settings > Device Credentials > CLI Credentials > edit the username > update the user’s password without changing the enable password.
2. Once the credentials are modified on the Global Credentials page, the managed devices at the sites where Cisco Catalyst Center does not manage the AAA can be reconfigured with the updated credentials. Cisco Catalyst Center can push a temporary EEM script to validate the credentials. If the login is successful the configuration can be preserved.



Note: For the managed devices at the sites where Cisco Catalyst Center does not manage the AAA configuration, Cisco Catalyst Center does not have any knowledge as to whether or not managed devices are manually configured with the external AAA server or if the managed devices use only local credentials so ensure that the password is updated on the external AAA server if it is configured on the effected managed devices before proceeding with these steps.

Requirement is to change the user's password and the enable password

1. Update the credentials on the Global Credentials page at Design > Network Settings > Device Credentials > CLI Credentials > edit the username > update the user's password along with the enable password..
2. Once the credentials are modified on the Global Credentials page, the managed devices at the sites where Cisco Catalyst Center does not manage the AAA can be reconfigured with the updated credentials. Cisco Catalyst Center can push a temporary EEM script to validate the credentials. If the login is successful the configuration can be preserved.



Note: For the managed devices at the sites where Cisco Catalyst Center does not manage the AAA configuration, Cisco Catalyst Center does not have any knowledge as to whether or not managed devices are manually configured with the external AAA server or if the managed devices use only local credentials so ensure that the password is updated on the external AAA server if it is configured on the effected managed devices before proceeding with these steps.