Secret Rotation

- Secret Rotation, on page 1
- Rotating Secrets of Cisco Nexus Top of Rack Switch, on page 2
- Rotating Secrets of Cisco UCS manager, on page 2

Secret Rotation

Azure Stack Hub uses internal and external secrets to maintain secure communication between the Azure Stack Hub infrastructure resources and services. For more information on Azure Stack Hub specific secret rotation, see https://docs.microsoft.com/en-us/azure-stack/operator/azure-stack-rotate-secrets?view=azs-2002.

Cisco recommends using strong passwords for all the user accounts. This chapter covers the instructions to rotate the secrets of hardware management user accounts.

Cisco Azure Stack Hub has the following default user accounts created during the installation. The user accounts are configured with the customer provided password during the installation.

Device	Account	Purpose
Cisco UCS	admin	Default administrator account with the administrator role on Cisco UCS manager
	UCSAzSAdmin	Additional administrator account with the administrator role on UCS manager
	IpmiUser	Baseboard management controller (BMC) user account.
Nexus	admin	Default administrator account with the network-administrator role
	azsadmin-<5 character random string>	Additional administrator account with the network-administrator role

Rotating Secrets of Cisco Nexus Top of Rack Switch

To rotate passwords for each user account in Cisco Nexus Top of Rack switch, run the following command:

```
n9k-1# conf t
n9k-1(config)# username <username> password <new password>
```

Note Cisco Nexus Top of Rack switches are setup to allow only strong passwords. Ensure that you replace an existing password with a strong password which meets the requirements documented at the Enabling Password-Strength Checking section in the Cisco Nexus 9000 Series NX-OS Security Configuration Guide.

Rotating Secrets of Cisco UCS manager

Cisco UCS Manager is the control center for the UCS server infrastructure. Cisco UCS manager can be accessed using supported browser on any computer which has access to the out-of-band management network of Azure Stack Hub.

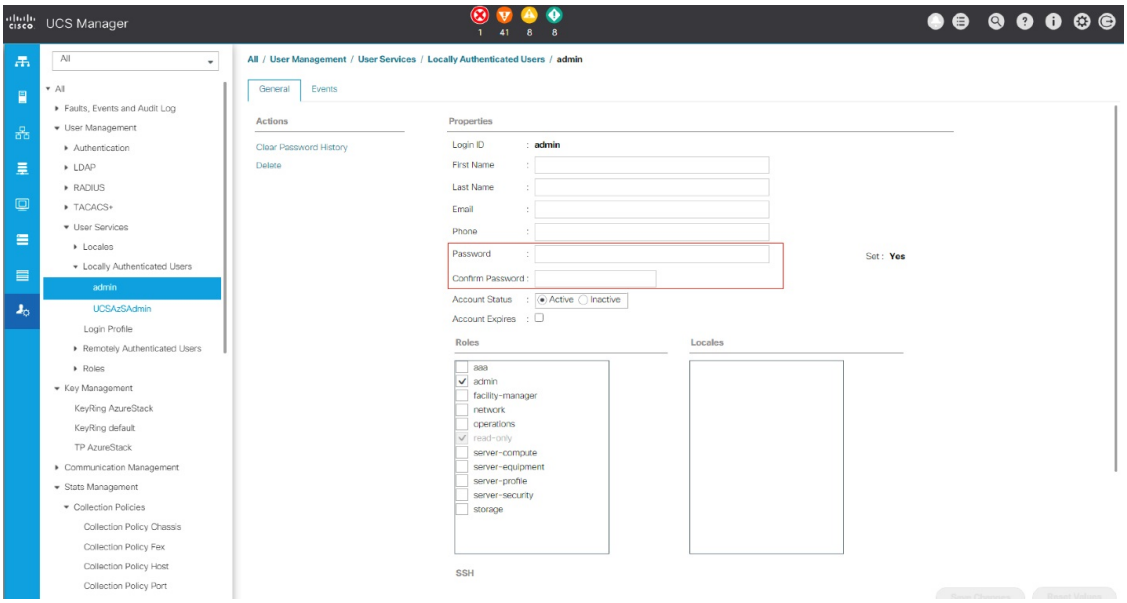
Note Never reboot any servers or other components using Cisco UCS manager, unless requested by Cisco support technician. Any reboot operation from Cisco UCS manager can result in the temporary or permanent data loss.

As described in the Table, Cisco UCS manager has three user accounts. To change the passwords on the user accounts, perform the following tasks:

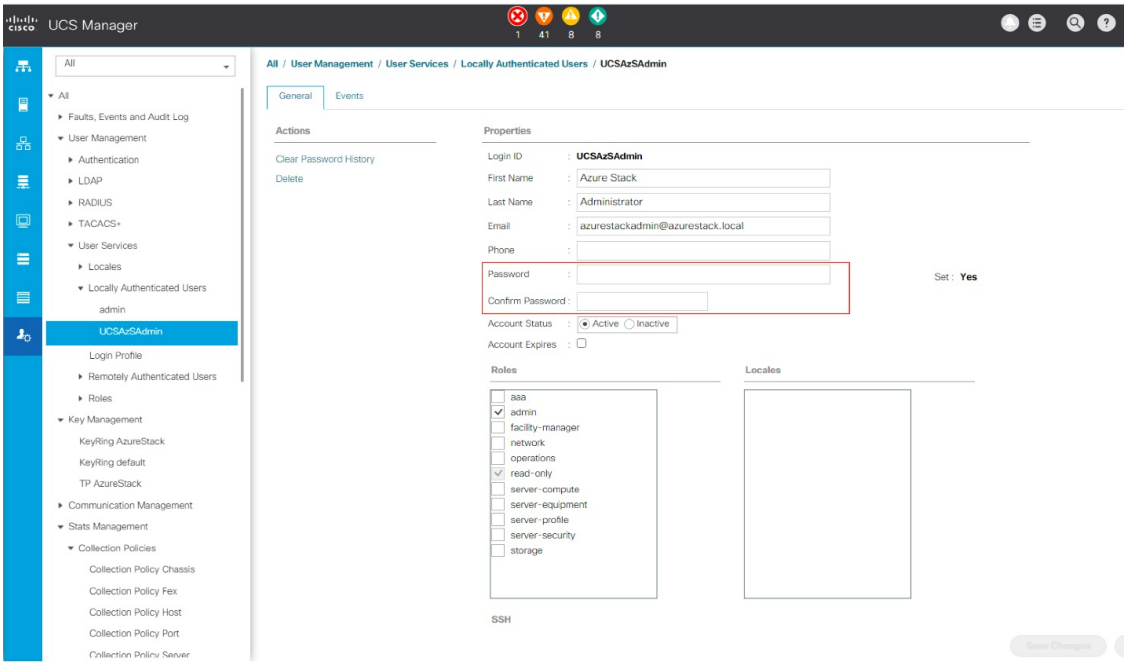
Procedure

Step 1 In any supported browser, enter `https://<UCS Manager IP>` and log into Cisco UCS manager using admin credentials.

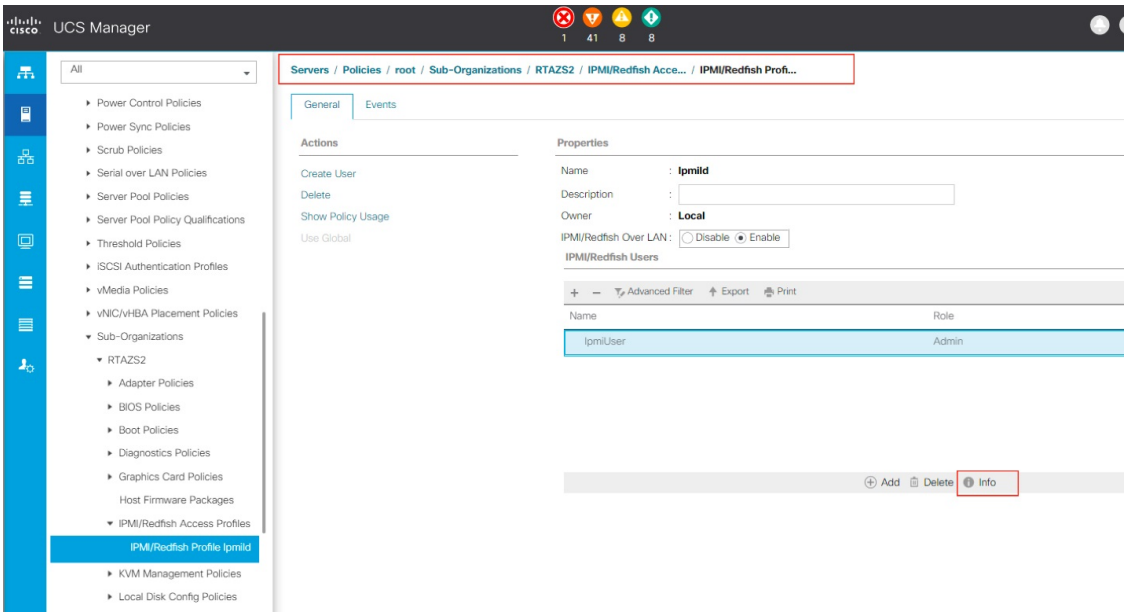
Step 2 In the **Navigation** pane, click **Admin**. Expand **All** > **User Management** > **User Services** > **Locally Authenticated Users** and then select **admin** user. In the **Properties** area on the right, enter the new password in the **Password** and **Confirm Password** fields. Click **Save Changes** to complete the password change.



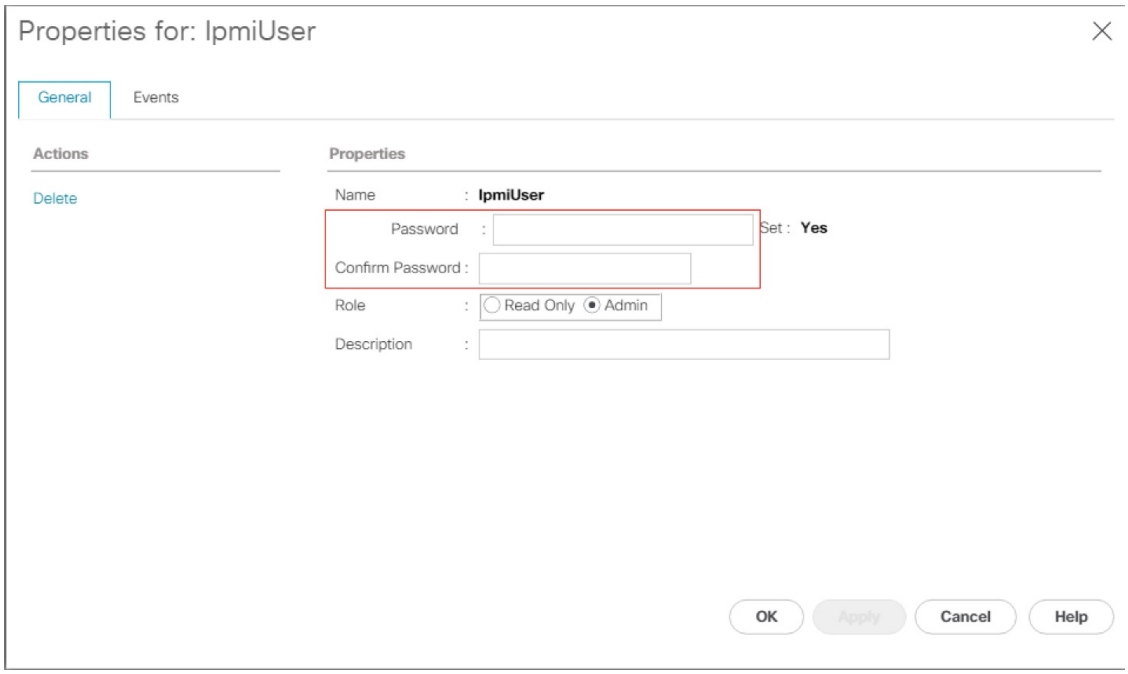
Step 3 Under **All** > **User Management** > **User Services** > **Locally Authenticated Users** , select **UCSAzSadmin** user. In the **Properties** area on the right, enter the new password in the **Password** and **Confirm Password** fields. Click **Save Changes** to complete the password change.



Step 4 In the **Navigation** pane, click **Servers**. Expand **Servers** > **Policies** > **root** > **Sub-Organizations** > **[Organization name provided during the deployment]** > **IPMI/Redfish Access Profiles** and then select **IPMI/Redfish profile IpmiId**. In the **Properties** area on the right, under the **IPMI/Redfish Users** sub-area, select **IpmiUser** and click **info**.



Step 5 Enter the new password in the **Password** and **Confirm Password** fields. Click **Save Changes** to complete the password change.



Step 6 Open an Elevated PowerShell window and connect to the Azure Stack Hub Emergency Recovery console using a “Cloudadmin” account. Update the baseboard management controller (BMC) credential by running the `set-bmccredential` command with the `-BypassBMCUpdate` flag.

Note The order should be first update BMC credentials on each server from Cisco UCS Manager (Step 4 and 5) and then run the `set-bmccredential` command (Step 6). For more information, refer to Microsoft documentation.

In the generic Azure Stack Hub, the `set-bmccredential` command is capable of updating BMC credentials on the BMC controller of each server along with the update to its internal credential store. But, in Cisco Azure Stack Hub, the credentials update on each server is not possible as the server BMC controllers are controlled using Cisco UCS Manager. Hence, set the new credentials on the BMC controller using Cisco UCS manager and then use the `set-bmccredential` command to update the internal credential store on Azure Stack Hub.