Configuring Server Profiles

Server Profiles

In Cisco Intersight, a Server Profile enables resource management by streamlining policy alignment, and server configuration. To view the Server Profiles table view, from the **Service Selector** drop-down list, choose **Infrastructure Service**. Navigate to **Configure** > **Profiles**. You can create Server Profiles using the Server Profile wizard or you can import the configuration details of C-series servers in standalone mode and FI-attached servers in Intersight Managed Mode (IMM), directly from Cisco IMC. You can create Server Profiles using the Server Profile wizard to provision servers, create policies to ensure smooth deployment of servers, and eliminate failures that are caused by inconsistent configuration. The Server Profiles wizard groups the server policies into the following four categories to provide a quick Summary View of the policies that are attached to a profile:

- **Compute Policies**—BIOS, Boot Order, and Virtual Media.
- **Network Policies**—Adapter Configuration, iSCSI Boot, LAN Connectivity, and SAN Connectivity policies.
  - The LAN Connectivity policy allows you to create Ethernet Network Policy, Ethernet Network Control Policy, Ethernet Network Group Policy, Ethernet Adapter Policy, or Ethernet QoS Policy. When you attach a LAN Connectivity policy to a server profile, the addresses of the MAC address Pool, or the static MAC address, are automatically assigned.

Note A LAN Connectivity policy that has a static MAC address can be attached to only one server profile.

  - The SAN Connectivity policy requires you to create Fibre Channel Network Policy, Fibre Channel Adapter Policy, or Fiber Channel QoS Policy. When you attach a SAN Connectivity policy to a server profile, the addresses of the WWPN and WWNN Pools, or the static WWPN and WWNN addresses, are automatically assigned.

Note A SAN Connectivity policy that has a static WWPN, or a static WWNN can be attached to only one server profile.

- **Storage Policies**—SD Card and Storage policies
- **Management Policies**—Device Connector, IPMI Over LAN, LDAP, Local User, Network Connectivity, SMTP, SNMP, SSH, Serial over LAN, Syslog, NTP, Certificate Management, and Virtual KVM policies

For more information and descriptions of the policies, see the **Server Policies** section. For an example of the policy creation workflow, see Creating Network Policies.

Server Profile List View

When you select **Profiles** > **UCS Server Profiles** in the Intersight UI, the UCS server profile list view is seen.

The list view shows the following details in a tabular format:

- Name – The name of the server profile.
- Status – The deployment status of the server profile.

  The **Status** of the profiles can have any of the following values:

  - **Not Assigned**—Policies are not assigned to the server profile.

Note
- Once you deploy policies to the server profile, the status changes automatically from *Not Assigned* to the new status depending on the outcome. You may need to refresh your screen to view the updated status.
- You must do the Power Cycle/Power ON after each profile deployment.

  - **OK**—Policies deployed successfully on the server profile
  - **In Progress**—Deployment of policies to the server profile is in progress
  - **Failed**—Server profile validation, configuration, or deployment has failed.
  - **Inconsistent**—Indicates that the policy configuration has changes that have not yet been deployed or activated. It may also indicate that the policy configuration at the endpoint is not in sync with the last deployed policy configuration in the server profile. If the endpoint settings are altered manually after a server profile is deployed, Intersight automatically detects the configuration changes and they will be shown on the server profile as **Inconsistent**. For more information, see the *Server Profile Drift* and the *Deploying and Activating a Server Profile* sections.

- Inconsistency Reason – The reason for the status being shown as *Inconsistent*. Example - Not Deployed, Not Activated, Out of Sync
- Target Platform – Indicates if the platform for which the profile is applicable is a Standalone UCS server or FI-attached UCS server.

- UCS Server Template – The template attached to the server profile or from which the profile has been derived.
- Server – The name of the server to which the profile is attached.
- Resource Pool – The pool to which the profile belongs.
- User Label – A user label is an identifier that helps in filtering the server profiles. It must be between 1 and 64 alphanumeric characters, containing only the following special characters: ! # $ % & * + , ( ) [ ] { } | / . ? @ _ : ; ~
- Last Update – The date on which the profile was last updated.
- Organization – The name of the organization.

Note Some of the columns are disabled by default, such as, **User Label**. To view such columns in the server profiles table view, you need to enable them while customizing the table view.

Server Profile Actions

After creating server profiles, actions that can be performed on a server profile are as follows:

- Deploy – Deploy the profile to the attached server
- Activate – Activate the profile on the attached server. The server gets power cycled on activation.
- Edit – Edit the profile
- Clone – Clone the profile
- Attach to Template – Attach the server profile to any of the available templates.

Note
- While template creation, if you toggle ON the **Attach UCS Server Profile to Profile Template** button, the selected profile gets attached to the template under creation.
- If you keep the toggle button OFF, the selected profile's properties are carried to the template but the profile does not get attached to it.

- Create a Template – A server profile can be used to create a template. This template can then be used to create multiple profiles with same configurations and deployed on multiple servers.
- Detach from Template – Detach the profile from the template.

Note

- **Create a Template** and **Attach to Template** actions can be performed only if a server profile is not attached to any template.
- A server profile can be attached to an existing template. This attachment overrides the config properties of the profile and replaces them with the template properties.
- A server profile attached to a template cannot be modified. The modifications can be done in the associated template.
- A server profile can be detached from a template and modified as per the requirements.
- A detached server profile can always be reattached to a template.

- Unassign Server – Unassign the server from the profile.
- Set User Label – You can also set, update, or delete user labels for each server profile through the **Set User Label** action.

Server Profile Details View

Clicking on a profile redirects to the **Server Profile Details View** that displays the configuration details of the profile under **General**, **Server**, and **Inventory** tabs.

Server Profile Drift

A server profile drift occurs when the policy configuration at the endpoint is not in sync with the last deployed policy configuration in the Server Profile.

Cisco Intersight supports Server Profile Drift detection for standalone servers and Intersight Managed Mode servers. For Intersight Managed Mode servers, the firmware versions required for drift detection are:

- For 4.2 release, the Cisco IMC version must be 4.2(1b) or above.
- For 4.1 release, the Cisco IMC versions must be:
    - For rack servers - 4.1(3d) or above
    - For blade servers - 4.1(33e) or above

The check to look up for any configuration change at the endpoint is performed every 30 min.

To see the policy configurations that have changed at the endpoint relative to the currently deployed policy configuration in Intersight, navigate to server profile details view and click **View Changes**. You can choose to view the **Changes Only** or **All** the policy configuration details.

Property	Essential Information
Saved Settings	Displays the policy settings in Intersight.
Last Deployed Settings	Displays the latest policy settings deployed on the server profile.

Property	Essential Information
Endpoint Settings	Displays the configuration at the endpoint.

To move the Server Profile status back to **OK**, you can either redeploy the profile or change the values at the endpoint. You can use the Device Connector Policy in Intersight to control configuration changes allowed from Cisco IMC. In the Device Connector Policy, choose **Configuration from Intersight only** to stop allowing configuration changes from Cisco IMC directly.

Limitations of Server Profile Drift - Standalone Servers

For standalone servers, configuration changes at the endpoint will not be detected for the following policies under the specified conditions:

Policy	Configuration at the endpoint
SD Card Policy	If an SD card is removed.
Storage Policy	• If Expand to Available is set for any of the virtual drives in the policy. • If the Power Cycle is not done after every deployment. • If there are additional drive groups that are not configured from Intersight
Boot Order Policy	If the Power Cycle is not done after every deployment. In SAN boot devices, Intersight does not detect drift for **Interface Name** and **Target WWPN** **Note** Cisco recommends using a SAN boot, because it offers the server profile mobility within the system. If you boot from the SAN when you move a server profile from one server to another, the new server boots from the same operating system image. Therefore, the new server appears as the same server to the network. To use a SAN boot, ensure that the following is configured: • The Cisco UCS domain must be able to communicate with the SAN storage device that hosts the operating system image. • A boot target LUN (Logical Unit Number) on the device where the operating system image is located.

Policy	Configuration at the endpoint
Local User, SNMP, LDAP, and IPMI over LAN Policy	If there are changes to the Password at the endpoint.
Virtual Media policy	If there are changes to the Password, Mount Options, or Authentication Protocols at the endpoint.
BIOS Policy	• BIOS token values configured as 'platform-default' are changed to the default value for that platform. Drift detection does not occur for such BIOS tokens. For more details, see Table 16 of the Creating a BIOS Policy section in Supported UCS Server Policies. • BIOS tokens whose values depend on other BIOS token values are not considered for drift detection. Drift may get reported for a BIOS token whose value is not supported by the server on which the policy is being deployed. For more details, see Cisco UCS Server BIOS Tokens.
IPMI over LAN policy	'Privilege Level’ field will not be considered.
Network Connectivity Policy	‘Preferred IPv6 DNS Server’ and ‘Alternate IPv6 DNS Server’ fields in the policy will not be considered. Server Profile may move to Out of Sync status temporarily.
Adapter Configuration Policy	This policy will not be considered for drift calculation.
Ethernet Adapter Policy	If a usNIC or VMMQ has a different Ethernet Adapter policy, then the configuration changes will not be calculated for usNIC or VMMQ attached Ethernet Adapter policy. Due to VMQ configuration restrictions, VMQ Number of Interrupts will override the value of Interrupts in Ethernet Adapter Policy, and VMQ Number of Virtual Machine Queues will override the value of Receive Queue Count, Transmit Queue Count, and Completion Queue Count (Receive+Transmit) of Ethernet Adapter Policy. Drift will not be detected for Number of Interrupts, Number of Virtual Machine Queues, Receive Queue Count, Transmit Queue Count, and Completion Queue Count. Intersight does not detect drift for `Number of Interrupts', 'Number of Virtual Machine Queues', 'Receive Queue Count', 'Transmit Queue Count', and 'Completion Queue Count'.
LAN Connectivity Policy	‘CDN’ field will not be considered.

Policy	Configuration at the endpoint
IMC Access Policy	If both In-Band IPv6 and IPv4 configurations are available, the IPv6 DNS configuration is prioritized.

Limitations of Server Profile Drift - Intersight Managed Mode Servers

For Intersight Managed Mode servers, server configuration changes at the endpoint will not be detected for the following policies under the specified conditions:

Note The Name field is not supported for any policy because Name is not an endpoint setting.

Note Drift detection is not supported for pools and IDs.

Policy	Configuration at the endpoint
SD Card Policy	Drift detection is not supported if an SD card is removed.
Storage Policy, Boot Order Policy, BIOS Policy, Virtual Media Policy	Drift detection is not supported for Storage policy, Boot Order Policy, BIOS Policy, and Virtual Media Policy on Intersight Managed Mode servers.
Local User Policy, SNMP Policy, Certificate Management Policy	Drift detection is not supported if there are changes to secure fields such as Password, Community Strings, and Private Key at the endpoint.

Policy	Configuration at the endpoint
LAN Connectivity Policy	Drift detection is not supported for: • VMQ connection • Number of interrupts • Number of Virtual Machine Queues • Consistent Device Naming (CDN) • Auto vNICs Placement IDs • Ethernet Adapter Policy • Interrupts Settings - Interrupts • Completion - Completion Queue Count, Completion Ring Size • VMMQ Adapter Policy • usNIC Adapter Policy **Note** Drift detection is supported only when the servers are powered on.
IMC Access Policy	Drift detection is not supported for Out-of-Band configuration.
SAN Connectivity Policy	Drift detection is not supported for Auto vNICs Placement IDs. **Note** Drift detection is supported only when the servers are powered on.
Power Policy	Drift detection is not supported for the Power Priority property.

Server Profile Import

Intersight provides the capability to import configuration details of C-series servers in standalone mode and FI-attached servers in Intersight Managed Mode (IMM), directly from Cisco IMC. The Server Profile import enables you to migrate the configuration of your existing servers to Intersight without having to create a profile and the policies manually. The Server Profile import operation creates a profile and the associated policies based on the server configuration. You can create a *golden* configuration profile and clone it and apply to another server already claimed in Intersight.

You can import a server profile configuration from the following locations in Intersight:

- **Servers** table view—Select a Cisco UCS C-Series Standalone server or any FI-attached server in Intersight Managed Mode (IMM) from the table view and click the ellipses (**...**) and select **Import Server Profile**.
- Click a C-series server in standalone mode or any FI-attached server in Intersight Managed Mode (IMM) in the Servers table view to access the Server details page. Click **Actions** on the top-right corner and

select **Import Server Profile**. This option is enabled only when no server profile is associated with the server.

Note A partially imported server profile cannot be attached to a template or cannot be used for creating a template.

For more information on how to import a Server Profile Import and about the detection of manual configuration changes at the endpoint, see Importing a Server Profile in Resources.

Estimate Impact

The Estimate Impact workflow, for standalone and Intersight Managed Mode servers, analyzes the disruptions that would be caused by the various policies attached to a server profile, when the server profile is deployed. The analyze impact workflow is triggered when a policy is attached, detached, or updated. The Disruption is indicated against each policy. The disruptions, which could be caused by the policies, are:

- Immediate reboot is required for standalone server policies such as Persistent Memory policy or Adapter policy. In such cases, the disruption indicated against the policy is **Immediate Reboot.**
- An Activate action on the server profile needs the server to reboot and activate the policy configuration on the server. In such cases, the disruption indicated against the policy is **Activate Requires Reboot**.
- Some policies, such as IMC Access policy, cause a brief outage of the server management network. In such cases, the disruption indicated against the policy is **Network Management Outage**.

Deploying and Activating a Server Profile

Deploy and **Activate** are two explicit actions that can be performed on server profiles. Policy configuration staging happens as a part of server profile deployment. Policy staging allows you to stage the policy configurations and get an idea of the pending actions for activating the policies. You can activate the policy by rebooting servers manually or using the **Activate** action of the Server Profile during a maintenance window. Policy activation failures are identified when the **Activate** action is triggered.

The **Status** widget in the Server Profiles table view shows the number of profiles in **Inconsistent** state. A server profile will be in the **Inconsistent** state when it has policy changes that have not yet been deployed or activated. The **Inconsistency Reason** widget shows the reason why a profile is in the **Inconsistent** state. A server profile could be in an **Inconsistent** state because:

- There are changes in the policies attached to the server profile assigned to the server.
- The policy configuration is out-of-sync with the configuration deployed in the endpoints.
- The policy is in **Not Activated** state.

You can use **Deploy** action to stage the configuration changes. During Deploy, you can choose to enable a toggle button to **Reboot Immediately**. If enabled, the server reboots and the server profile is activated immediately. If disabled, the policy configuration changes are activated at the next reboot.

The **Activate** action in the Server Profile details, reboots the server and activates the configuration on the server. You can trigger **Deploy** to stage the configuration changes and later trigger **Activate**, during the maintenance window, to activate the deployed configuration.

The **Update and Deploy** option in the policy edit page allows you to modify a policy configuration and deploy the changes on multiple server profiles to which the policy is attached.

Creating a UCS Server Profile

A server profile defines a server and its compute, storage, management, and network characteristics. When a server profile is deployed to a server, Cisco Intersight automatically configures the server and its connections to match the configuration specified in the server profile.

Note A Server profile can also be derived from Server Profile Templates. For more details, see Server Profile Templates

Step 1 Log in to Cisco Intersight with your Cisco ID and select admin role.

Step 2 Navigate to **Service Profiles** > **UCS Server Profiles** tab, and click **Create UCS Server Profile**.

Step 3 On the **General** page, enter the following information:

a) **Name** of your server profile.

b) **Target Platform** for which the profile is applicable. This can be **Standalone** servers or **FI Attached** servers.

A UCS server profile created for Standalone servers cannot be deployed on FI Attached servers. Similarly, a UCS server profile created for FI Attached servers cannot be deployed on Standalone servers.

c) (Optional) **Tag** for the profile. Tags must be in the key:value format. For example, Org: IT or Site: APJ.

d) (Optional) **Description** to help identify the profile.

Step 4 On the **Server Assignment** page, assign a server to the server profile. You can choose any of the following options for the server assignment:

- **Assign from a Specific Server**—Use this option for an immediate assignation of a server to the server profile.
- **Assign Server from a Resource Pool**—Use this option to assign a server from a resource pool to the server profile.
- **Assign by Chassis Slot Location**—Use this option to pre-assign a server to the server profile using the Domain Name, Chassis ID, and Slot ID.
- **Assign by Serial Number**—Use this option to pre-assign a server to the server profile using the Serial Number of the server.

  Note
  - Cisco UCS B-Series servers can be pre-assigned using **Chassis Slot Location** or **Serial Number**.
  - Cisco Intersight Managed Mode C-Series servers and Cisco UCS C-Series Standalone servers can be pre-assigned only using **Serial Number**.

- **Assign Later**—Use this option to assign a server to the server profile at a later time.

The server assignment table displays list of servers or resource pools and their details. You can use any of the following options to view the details:

- **Show All** to view all the servers or resource pool currently present
- **Show Selected** to view the current server or resource pool selected
- **Unselect** to remove the selection.

Step 5 Click **Next**.

Step 6 On the **Compute Configuration** page, do the following:

a) Choose the appropriate **UUID Assignment**:

- **Pool**—Allows UUID Pool association to the server.
- **Static**—Allows UUID association to the server using Static UUID address.

b) Select the existing policies or create new policies.

c) Click **Next**.

Step 7 On the **Management** page, attach the required policies to the **UCS Server Profile** and click **Next**.

Step 8 On the **Storage** page, attach the required policies to the **UCS Server Profile** and click **Next**.

Step 9 On the **Network Configuration** page, attach the required policies to the **UCS Server Profile** and click **Next**.

Step 10 On the **Summary** page, verify the details of the UCS Server Profile and the policies attached to it.

Step 11 Click **Deploy** to create the UCS Server Profile and deploy it to the assigned server.

Note

- For the **Assign Server from a Resource Pool** assignment type, if a resource is not available in the resource pool, the status of the Server Profile changes to **Waiting for Resources** . Similar behavior is observed for the pre-assignment of the Server Profile. When a server is added to the resource pool at a later time, the server gets automatically added to the server profile from the **Waiting for Resources** status.

  An alarm gets raised when the Server Profile is in the **Waiting** state. It gets auto-cleared when a server gets assigned to the Server Profile.

- Resource pool does not support dynamic selection of server. You can manually assign servers to a resource pool and can continue with the automated server profile assignment.
- The Server Profile pre-assignment is a one-time operation till the server is assigned. The Pre-assigned properties are lost once the server is assigned and continues to function as any other existing Server Profiles.
- For more information on creating a resource pool and viewing the resource pool details, see Resource Pools.
- For more information on creating a UUID pool and viewing the UUID pool details, see UUID Pools.

UCS Server Profile Details

The UCS Server Profile Details page displays details of the UCS Server profile and the server that it is assigned to. Navigate to the UCS Server Details from the UCS Server Profiles Table view. On this page, you can:

- Perform UCS Server profile **Actions**:
  - **Deploy**—Deploy the UCS Server profile on a Fabric Interconnect pair.

Note This action can be performed on a server profile that has servers assigned to it.

- **Unassign**—Unassign the UCS Server profile from the Fabric Interconnect pair.

Note This action can be performed on a server profile that has servers assigned to it.

- **Edit**—Edit the properties of the UCS Server Profile.
- **Clone**—Clone the UCS Server profile with properties similar to an existing UCS Server profile. The clones are associated with the same policies as on the original UCS Server profile.
- **Delete**—Delete the server profile.
- **Attach to template**—Attach the server profile to an existing server profile template.

Note This action can be performed on a server profile that is not attached to any template.

- **Create a template**—Create a new template using the properties of the server profile.

Note This action can be performed on a server profile that is not attached to any template.

- **Detach from template**—Detach the server profile from a template and modify its properties.

Note This action can be performed on a server profile that is attached to a server profile template.

- **Manage Tags**— Set a tag for a profile in the key:value format.

- View UCS Server profile **Details** in the **General** tab:

Property	Essential Information
Status	The status of deploying the UCS Server profile on a Fabric Interconnect pair. This could be: • **OK** • **Failed** • **Not Assigned** • **Not Deployed**
Name	The UCS Server profile name.
Server	The name of the associated server.

Property	Essential Information
Last Update	The date and time that the UCS Server profile was last updated.
Tags	The existing tags for the selected object are displayed by default. Click **Manage** to add new tags or modify the existing ones.

Displays the policies associated with the server profile. Click on the policy name to view details of the associated policy.

If you make changes to a policy attached to a Server Profile after it is deployed, or add a new policy to the profile, the Server Profile Table view displays Not Deployed Changes to reflect the edits to the profile or the referenced policies. The Server Profile Detail view highlights the referenced policies, and the View Changes window allows you to view the actual changes. You can also view the Configuration details from the Service Profiles table view.

- View the assigned server and its properties in the **Server** tab.
- View the inventory of the assigned server in the **Inventory** tab.