



ID Pools

This chapter includes the following sections:

- [ID Universe, page 1](#)
- [Server Pools, page 8](#)
- [Server Pool Qualification Policy, page 9](#)

ID Universe

The **ID Universe** displays the pools, collections of identities, or physical or logical resources, that are available in the system. All pools increase the flexibility of service profiles and allow you to centrally manage your system resources. Pools that are defined in Cisco UCS Central are called Global Pools and can be shared between Cisco UCS domains. Global Pools allow centralized ID management across Cisco UCS domains that are registered with Cisco UCS Central. By allocating ID pools from Cisco UCS Central to Cisco UCS Manager, you can track how and where the IDs are used, prevent conflicts, and be notified if a conflict occurs. Pools that are defined locally in Cisco UCS Manager are called Domain Pools.



Note

The same ID can exist in different pools, but can be assigned only once. Two blocks in the same pool cannot have the same ID.

You can pool identifying information, such as MAC addresses, to preassign ranges for servers that host specific applications. For example, you can configure all database servers across Cisco UCS domains within the same range of MAC addresses, UUIDs, and WWNs.

From the **ID Universe** page, you can view the total number IDs for each type of pool, and how many of the total are **Available**, **In Use**, or have a **Conflict**. If you click on a **Resource**, you can view detailed information about that ID and where it is used.

IP Pools

IP pools are a collection of IP addresses. You can use IP pools in Cisco UCS Central in one of the following ways:

- For external management of Cisco UCS Managerservers.
- For iSCSI boot initiators.

- For both external management and iSCSI boot initiators in Cisco UCS Manager.

**Note**

The IP pool must not contain any IP addresses that have been assigned as static IP addresses for a server or service profile.

A fault is raised if the same IP address is assigned to two different Cisco UCS domains. If you want to use the same IP address, you can use the **scope** property to specify whether the IP addresses in the block are public or private:

- **public**—The IP addresses in the block can be assigned to one and only one registered Cisco UCS domain.
- **private**—The IP addresses in the block can be assigned to multiple Cisco UCS domains.

Cisco UCS Central creates public IP pools by default.

Global IP pools should be used for similar geographic locations. If the IP addressing schemes are different, the same IP pool cannot be used for those sites.

Cisco UCS Central supports creating and deleting IPv4 and IPv6 blocks in IP pools. However, iSCSI boot initiators support only IPv4 blocks.

IQN Pools

An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs in a Cisco UCS domain. IQN pools created in Cisco UCS Central can be shared between Cisco UCS domains.

IQN pool members are of the form *prefix:suffix:number*, where you can specify the prefix, suffix, and a block (range) of numbers.

An IQN pool can contain more than one IQN block, with different number ranges and different suffixes, but share the same prefix.

MAC Pools

A MAC pool is a collection of network identities or MAC addresses that are unique in their layer 2 environment and are available to be assigned to vNICs on a server. MAC pools created in Cisco UCS Central can be shared between Cisco UCS domains. If you use MAC pools in service profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the service profile.

In a system that implements multi-tenancy, you can use the organizational hierarchy to ensure that MAC pools can only be used by specific applications or business services. Cisco UCS Central uses the name resolution policy to assign MAC addresses from the pool.

To assign a MAC address to a server, you must include the MAC pool in a vNIC policy. The vNIC policy is then included in the service profile assigned to that server.

You can specify your own MAC addresses or use a group of MAC addresses provided by Cisco.

UUID Suffix Pool

A UUID suffix pool is a collection of SMBIOS UUIDs that are available to be assigned to servers. The first number of digits that constitute the prefix of the UUID are fixed. The remaining digits, the UUID suffix, are variable values. A UUID suffix pool ensures that these variable values are unique for each server associated with a service profile which uses that particular pool to avoid conflicts.

If you use UUID suffix pools in service profiles, you do not have to manually configure the UUID of the server associated with the service profile. Assigning global UUID suffix pools from Cisco UCS Central to service profiles in Cisco UCS Central or Cisco UCS Manager allows them to be shared across Cisco UCS domains.

WWN Pools

A WWN pool is a collection of WWNs for use by the Fibre Channel vHBAs in a Cisco UCS domain. WWN pools created in Cisco UCS Central can be shared between Cisco UCS domain. You create separate pools for the following:

- WW node names assigned to the server
- WW port names assigned to the vHBA
- Both WW node names and WW port names



Important

A WWN pool can include only WWNNs or WWPNS in the ranges from 20:00:00:00:00:00:00:00 to 20:FF:FF:FF:FF:FF:FF:FF or from 50:00:00:00:00:00:00:00 to 5F:FF:FF:FF:FF:FF:FF:FF. All other WWN ranges are reserved. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNS in the SAN fabric, we recommend that you use the following WWN prefix for all blocks in a pool:
20:00:00:25:B5:XX:XX:XX

If you use WWN pools in service profiles, you do not have to manually configure the WWNs that will be used by the server associated with the service profile. In a system that implements multi-tenancy, you can use a WWN pool to control the WWNs used by each organization.

You assign WWNs to pools in blocks.

WWNN Pools

A World Wide Node Names (WWNN) pool is a WWN pool that contains only WW node names. If you include a pool of WWNNs in a service profile, the associated server is assigned a WWNN from that pool.

WWPN Pools

A World Wide Port Name (WWPN) pool is a WWN pool that contains only WW port names. If you include a pool of WWPNS in a service profile, the port on each vHBA of the associated server is assigned a WWPN from that pool.

WWxN Pools

A WWxN pool is a WWN pool that contains both WW node names and WW port names. You can specify how many ports per node are created with WWxN pools. The pool size for WWxN pools must be a multiple of $ports-per-node + 1$. For example, if there are 7 ports per node, the pool size must be a multiple of 8. If there are 63 ports per node, the pool size must be a multiple of 64.

All Pools

Display a complete list of ID pools in the system. You can use filter to sort by **Utilization Status**, **Org** or **ID Type** to view availability and usage.

Creating and Editing an IP Pool

After creating an IP pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected IP pool. To select an IP pool, go to **All Pools** page and select the IP pool that you want to edit. The page redirects you to the overall summary page of the selected IP pool.

-
- Step 1** In the Task bar, type **Create IP Pool** and press **Enter**. This launches the **Create IP Pool** dialog box.
- Step 2** In **Basic**, complete the following:
- From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an IP pool.
 - Enter the name and description of the pool.
- Step 3** Click the respective IP blocks to create a block of IP addresses (IPV4 or IPV6) and complete the following:
- Click the **Plus** sign to create one or more blocks of IP addresses in the selected pool.
 - In the respective IP block start column, enter the first IPv4 or IPv6 addresses in the block.
 - In the **Size** column, enter the total number of IP addresses in the pool.
- Step 4** Click the **Apply** icon. The page displays additional fields.
- Step 5** In **Basic**, complete the following fields:
- Enter the subnet mask associated with the IPv4 or IPv6 address in the block.
 - Enter the default gateway associated with the IPv4 or IPv6 address in the block.
 - Enter the primary DNS server that this block of IPv4 or IPv6 address should access.
 - Enter the secondary DNS server that this block of IPv4 or IPv6 address should access.
 - Select whether the IP addresses in the block can be assigned to one or more Cisco UCS domains registered with Cisco UCS Central. This can be one of the following:
 - **Public**—The IP addresses in the block can be assigned to one and only one registered Cisco UCS domain.
 - **Private**—The IP addresses in the block can be assigned to multiple Cisco UCS domains.
- Note** The scope for an IP address within the block cannot be changed after the block has been saved.
- Step 6** In **IPv4** or **IPv6** addresses, you can view a graphical representation of the number of IP addresses in the pool, the number of assigned IP addresses and the number of duplicated IP addresses.
- Step 7** In **Access Control**, select a policy to associate with this IP address block from the **ID Range Access Control Policy** drop-down list
- Step 8** Click **Create**.
-

What to Do Next

Creating and Editing an IQN Pool

**Note**

In most cases, the maximum iSCSI Qualified Name (IQN) size (prefix + suffix + additional characters) is 223 characters. When using the Cisco UCS NIC M51KR-B adapter, you must limit the IQN size to 128 characters.

After creating an IQN pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected IQN pool. To select an IQN pool, go to **All Pools** page and select the IQN pool that you want to edit. The page redirects you to the overall summary page of the selected IQN pool.

-
- Step 1** In the Task bar, type **Create IQN Pool** and press Enter. This launches the **Create IQN Pool** dialog box.
- Step 2** In **Basic**, complete the following:
- From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an IQN pool.
 - Enter name and description of the IQN pool.
 - Enter the prefix for any IQN blocks created for this pool.
- Step 3** In **Suffix Blocks**, complete the following:
- Click the **Plus** icon to create one or more blocks of IQN suffixes in the selected pool.
 - In the **Suffix Block** column, enter the suffix for this block of IQNs.
 - In the **Start** column, enter the first IQN suffix in the block.
 - In the **Size** column, enter the total number of IQN suffixes in the block.
- Step 4** Click the **Apply** icon.
- Step 5** Click **Create**.
-

What to Do Next

Include the IQN suffix pool in a service profile or a service profile template.

Creating and Editing a MAC Pool

After creating a MAC pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected MAC pool. To select a MAC pool, go to **All Pools** page and select the MAC pool that you want to edit. The page redirects you to the overall summary page of the selected MAC pool.

-
- Step 1** In the Task bar, type **Create MAC Pool** and press **Enter**. This launches the **Create MAC Pool** dialog box.

- Step 2** In **Basic**, complete the following:
- From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access a MAC pool.
 - Enter name and description of the pool.
- Step 3** In **MAC Blocks**, complete the following:
- Click the **Plus** icon to create a block of MAC addresses.
 - In the **MAC Block Start** column, enter the first MAC address in the block.
 - In the **Size** column, enter the number of MAC addresses in the block.
 - Click the **Apply** icon.
Additional fields related to the MAC pools are displayed.
 - In **MAC Addresses**, you can view a graphical representation of the number of MAC addresses in the pool, the number of assigned MAC addresses, duplicate MAC addresses, and MAC summary.
 - In **Access Control**, select the ID range access control policy to apply to this block. If you do not have a policy, you can create one by typing **Create ID Range Access Control Policy** in the task bar.
- Step 4** Click **Create**.
-

What to Do Next

Include the MAC pool in a vNIC template.

Creating and Editing a UUID Suffix Pool

After creating a UUID pool you can edit it by selecting the **Edit** icon on the overall summary page of the selected UUID pool. To select a UUID pool, go to **All Pools** page and select the UUID pool that you want to edit. The page redirects you to the overall summary page of the selected UUID pool.

- Step 1** In the Task bar, type **Create UUID Pool** and press **Enter**.
This launches the **Create UUID Pool** dialog box.
- Step 2** In **Basic**, complete the following:
- From the **Organization** drop-down list, select an organization or a sub-organization in which you want to create or access an UUID pool.
 - Enter name and description of the pool.
 - Enter the suffix for any UUID blocks created for this pool.
- Step 3** In **Suffix Blocks**, complete the following:
- Click the **Create** icon.
 - In the **Suffix Block** column, enter the suffix for this block of UUIDs.
 - In the **Start** column, enter the first UUID suffix in the block.
 - In the **Size** column, enter the total number of UUIDs in the block.
 - Click the **Apply** icon.
Additional fields related to UUID pools are displayed.

- f) In **UUIDs**, you can view a graphical representation of the number of UUID addresses in the pool, the number of assigned UUID addresses, duplicate UUID addresses, and UUID summary.
- g) In **Access Control**, select the ID range access control policy to apply to this block. If you do not have a policy, you can create one by typing **Create ID Range Access Control Policy** in the task bar.

Step 4 Click **Create**.

What to Do Next

Include the UUID suffix pool in a service profile or service profile template.

Creating and Editing a WWN Pool

After creating a WWN pool you can edit by selecting the **Edit** icon on the overall summary page of the selected WWN pool. To select a WWN pool, go to **All Pools** page and select the WWN pool that you want to edit. The page redirects you to the overall summary page of the selected WWN pool.

Step 1 In the Task bar, type **Create WWN Pool** and press **Enter**. This launches the **Create WWN Pool** dialog box.

Step 2 In **Basic**, complete the following:

- a) Click **Organization** and select the location in which you want to create the pool.
- b) Enter name and description of the WWN pool.
- c) In the **World Wide Name (WWN) Used For** area, select one of the following:
 - **Port (WWPN)**—The pool is used for both WWNNs and WWPNS.
 - **Node (WWNN)**—The pool is used for WWNNs.
 - **Both (WWxN)**—The pool is used for WWNNs.

Step 3 In **WWN Blocks**, complete the following:

- a) Click the **Create** icon.
- b) In the **WWN Block Start** column, enter the first WWN initiator in the block.
- c) In the **Size** column, enter the total number of WWN initiators in the pool.
- d) Click the **Apply** icon.
Additional fields related to WWN pools are displayed.
- e) Click the **WWNs** tab, you can view a graphical representation of the number of WWN addresses in the pool, the number of assigned WWN addresses, and the duplicate MAC addresses and WWN summary.
- f) In **Access Control**, select the ID range access control policy to apply to this block. If you do not have a policy, you can create one by typing **Create ID Range Access Control Policy** in the task bar.

Step 4 Click **Create**.

Note You must wait a minimum of 5 seconds before you create another pool.

What to Do Next

- Include the WWPN pool in a vHBA template.
- Include the WWNN pool in a service profile or service profile template.
- Include the WWxN pool in a service profile or service profile template.

Deleting a Pool

If you delete a pool, Cisco UCS Central does not reallocate any addresses (from that pool) that have been assigned to vNICs or vHBAs in Cisco UCS Manager. All assigned addresses from a deleted pool remain with the vNIC or vHBA to which they are assigned until one of the following occurs:

- The associated service profiles are deleted.
- The vNIC or vHBA to which the address is assigned is deleted.
- The vNIC or vHBA is assigned to a different pool.

Before You Begin

-
- Step 1** In the navigation bar, click the **Operations** icon and select **Pools**. This launches the **All Pools** dialog box.
- Step 2** In the **Pool name** column, select the pool that you want to delete. You can search for the pool in one of the following ways:
- Browse through the list of pool.
 - Click the **Search** icon and enter the pool name.
 - Select a pool type from the **Filter** column.
- Step 3** In the **Org** column, click the pool. This launches the overall summary page of the selected pool.
- Step 4** Click the **Delete** icon. If Cisco UCS Central GUI displays a confirmation dialog box, click **Yes**.
-

Server Pools

A server pool contains a set of servers. These servers typically share the same characteristics. Those characteristics can be their location in the chassis, or an attribute such as server type, amount of memory,

local storage, type of CPU, or local drive configuration. You can manually assign a server to a server pool, or use server pool policies and server pool policy qualifications to automate the assignment.

If your system implements multitenancy through organizations, you can designate one or more server pools to be used by a specific organization. For example, a pool that includes all servers with two CPUs could be assigned to the Marketing organization, while all servers with 64 GB memory could be assigned to the Finance organization.

A server pool can include servers from any chassis in the system. A given server can belong to multiple server pools.

When you select a specific server pool, you can view the individual details for that pool, including the number of servers included in the pool, and the associated qualification policies.

Creating or Editing a Server Pool

-
- Step 1** In the Task bar, type **Create Server Pool** and press Enter. This launches the **Create Server Pool** dialog box.
- Step 2** In **Basic**, click **Organization** and select the location in which you want to create the server pool.
- Step 3** Enter a **Name** and optional **Description**.
- Step 4** In **Qualification**, click **Add** to add new qualification policies, or **Delete** to remove existing ones. For more information, see [Creating or Editing a Server Pool Qualification Policy](#), on page 10.
- Step 5** In **Servers**, add the servers to be included in the pool.
- Step 6** Click **Create**.
-

Server Pool Qualification Policy

Server pool qualification policy qualifies servers based on the server inventory conducted during the discovery process. You can configure these qualifications or individual rules in the policy to determine whether a server meets the selection criteria. For example, you can create a rule that specifies the minimum memory capacity for servers in a data center pool.

Qualifications are used in other policies to place servers, not just by the server pool policies. For example, if a server meets the criteria in a qualification policy, it can be added to one or more server pools or have a service profile automatically associated with it.

You can use the server pool policy qualifications to qualify servers according to the following criteria:

- Adapter type
- Chassis location
- Memory type and configuration
- Power group
- CPU cores, type, and configuration

- Storage configuration and capacity
- Server model or server type
- Owner
- Site
- Address
- Domain group
- Domain name
- Product family

Depending upon the implementation, you might need to configure several policies with server pool policy qualifications including the following:

- Autoconfiguration policy
- Chassis discovery policy
- Server discovery policy
- Server inheritance policy
- Server pool policy

Creating or Editing a Server Pool Qualification Policy

-
- Step 1** In the Task bar, type **Create Server Pool Qualification Policy** and press Enter. This launches the **Create Server Pool Qualification Policy** dialog box.
- Step 2** In **Basic**, click **Organization** and select the location in which you want to create the server pool qualification policy.
- Step 3** Enter a **Name** and optional **Description** and **Server Model/PID**.
- Step 4** (Optional) In **Domain**, click the plus sign to add the **Domain Qualifier**. When you click **Domain Qualifier** the system displays available domain qualification options in tabs on the right pane. Click the appropriate tabs and add the qualification.
- Step 5** In **Hardware**, select the appropriate qualification if you enable any of the options such as processor, memory, storage, and adapter.
- Step 6** Click **Create**.
-