



Configuring Pools

- [Pools, on page 1](#)
- [Identity \(ID\) Pools, on page 1](#)
- [Pool Allocation, on page 2](#)
- [Deleting Pools, on page 2](#)
- [Identity Retention, on page 3](#)
- [IP Pools, on page 4](#)
- [MAC Pools, on page 7](#)
- [UUID Pools, on page 9](#)
- [WWN Pools, on page 11](#)
- [IQN Pools, on page 14](#)
- [Resource Pools, on page 17](#)
- [Virtual Routing and Forwarding, on page 20](#)

Pools

Pools are the basic building blocks for uniquely identifying hardware resources. They form the foundation of the UCS management model, enabling the association of Server Profiles with blade servers while maintaining the same ID and presentation to the upstream LAN or SAN.

Pools are classified into Resource Pools and Identity (ID) Pools.

Using the Pools Table View, you can monitor the utilization of Server Pools, track *Available* and *Used* identifiers, and make informed decisions regarding pool capacity and allocation.

Identity (ID) Pools

ID Pools are further classified into the following categories:

- **IP pool:** Provides the flexibility of dynamically assigning IP addresses to services running on a network element.
- **MAC address pool:** Provides unique IDs for network interface ports.
- **UUID pool:** Provides unique IDs for each server associated with the server profile.

- **WWNN and WWPN pool:** Provides unique IDs for Fibre Channel resources on a server (Fibre Channel nodes and ports).
- **IQN pool:** Provides a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs.

Pool Allocation

To ensure consistent and repeatable ID allocation across multiple allocation iterations, the smallest available ID is allocated sequentially during pool allocation iterations.

For example, consider a pool with a range of 1 to 20 IDs. The following table describes the ID allocation and reallocation iterations.

Use Case	Behavior
5 IDs are requested from the pool	IDs 1 to 5 are allocated
1-5 IDs are released	IDs 1 to 5 are released
5 IDs are requested from the pool	IDs 1 to 5 are allocated

You can have overlapping pools, where some IDs are shared between different pools across organizations. Since IDs are unique across the account, whether they are used in different organizations or not, if an ID is consumed in one pool, it will also be marked as **Used** in all pools where it is used. The Pools Table View provides a summary of allocated IDs, providing the capability to track ID usage in Pools across Organizations. The Source column in the Pools Table View indicates the pool from which the ID is being allocated. If the ID is being allocated from the current pool, the Source column will be marked as **Self**. If the ID is allocated from another pool, the Source column will be marked as **Other**.

Deleting Pools

You can delete a pool or address block in an Organization where none of the IDs are allocated. It will not impact allocations in any pool in another Organization.

-
- Step 1** Check if the ID is not currently associated with a Server Profile:
- In the **Pools Table View**, review the **Source** column to analyze the pool usage.
 - If **Source** is marked as **Other**, you can proceed to delete the ID as it is allocated from some other overlapping pool.
 - Do not attempt to delete pools marked as **Source = Self** as it is not allowed since they are in use in one of the profiles.
- Step 2** Click **Delete**.
-

Identity Retention

IP Addresses, MAC addresses, IQNs, UUIDs, WWNNs, and WWPNS are the typical identifiers that a physical server gets from a Server Profile.

Intersight uses best efforts to retain the LAN Connectivity Policy (LCP) identifiers, such as MAC, IQN, and iSCSI IP, as well as the SAN Connectivity Policy (SCP) identifiers, such as WWPNS and WWNN, when modifying policies, profiles or templates.

If you change the LCP or SCP to a new policy that accesses different Pools with non-overlapping IDs, then expect all the IDs to change. Furthermore, expect changes if the new Pool does not have the exact ID available.

In the following scenarios, you can expect ID retention during edits or changes:

- When adding a vNIC or vHBA to an LCP or SCP.
- When changing policy LCP1/SCP1 to LCP2/SCP2 that uses the same Pool Reference.
- When changing policy LCP1/SCP1 to LCP2/SCP2 that uses a different Pool Reference, but with the same IDs available.
- When changing policy LCP1/SCP1 that uses Static Identifiers to LCP2/SCP2 that uses a Pool Reference with the same IDs available.
- When detaching a Server Profile from Template T1 and attaching the Server Profile to Template T2 with the same IDs available.
- When editing a Server Profile Template and changing LCP1/SCP1 to LCP2/SCP2 as above.
- When editing an existing LCP/SCP Policy and changing the Identifier Reference from Static to a Pool with the same IDs available.

Identity Reservation

Identities can be reserved prior to allocation to allow selecting a specific value from a pool, for purposes such as migration across environments. For example, Cisco UCSM to IMM.

Reserved Identifiers Guidelines

- The identifiers can be reserved only via the [IMM Transition Tool](#) or by using available pool Reservation APIs, such as <https://intersight.com/apidocs/apirefs/macpool/Reservations/model/>.
- The reservation of the identifiers can be done only for Fabric Interconnect-attached servers.
- Reserved identifiers are meant for one-time use and are removed from the reservation pool once consumed.

The reserved ID gets consumed either when a policy (with the reserved identifier) is attached to a server profile, or when the server profile is deployed.

The **Reserved Identifiers** tab shows the list of reserved identifier values, their type, and the corresponding Pool membership. The Pool membership appears blank when the allocation type is Static. You can select and delete any reserved identifier.

IP Pools

An IP Pool can contain one or more blocks of IPs that will get consumed in sequential order, beginning with the lowest block. IP pools support both IPv4 and IPv6 addresses.

Subnet Configuration in an IP Pool

You can create IP pools with either common subnet configurations for all IP blocks (pool-level) or different subnet configurations for each IP block (block-level).

After defining a pool with subnet configuration at the block level, you can migrate it to pool-level subnet configuration and vice versa. When migrating from a pool-level to a block-level subnet configuration, the subnet configuration will be replicated across each existing IP block. When migrating from block-level to pool-level subnet configuration, you need to reconfigure the common subnet settings at the pool-level.

If an IP block already has existing leases, migration is allowed only in the following scenarios:

- **Migrating from Pool-Level to Block-Level Configuration with Existing Leases:**

When you migrate from pool-level to block-level configuration with existing leases, the subnet configuration is moved to block-level without any changes. This means that the same subnet configuration previously set at the pool level is copied to each block. In such cases, the migration is allowed even if there are existing leases. After migration, if you observe that you cannot modify the subnet configuration of any block, it could be because it has existing active leases. Note that you cannot change the subnet configuration of any block if it already has active leases.

- **Migrating from Block-Level to Pool-Level Configuration with Existing Leases:**

When you migrate from block-level to pool-level configuration with existing leases, you must specify the subnet configuration at the pool level. If all the previous block-level subnet configurations are the same as the new pool-level subnet configuration, the migration is allowed. In this scenario, the migration is permitted even if there are existing leases.

Creating an IP Pool

IP Pools represent a collection of IP addresses that can be allocated to configuration entities such as server profiles. You can create IPv4 pool or IPv6 pool or both.

Step 1 From the left navigation panel, click **Create Pools > IP > Start**.

The **IP Pool** wizard appears.

Step 2 Add the following information on the **General** page:

- **Organization**—The organization of the IP pool.
- **Name**—Name of the IP pool.
- **Add Tag**—The tag to identify and search for the IP pool.
- **Description**—The description the IP pool.
- **Configure Subnet at Block Level**—Select the checkbox to enable subnet configurations for each IP block within IPv4 and IPv6 pools.

Step 3 Click **Next**.

Step 4 [Optional] Configure IPv4 pools:

- a) Use the **Configure IPv4 Pool** toggle button to enable IPv4 pool configuration. By default, it is enabled. You can opt to configure the IPv4 pool later.
- b) If you have opted to configure the **Netmask**, **Gateway**, **Primary DNS**, and **Secondary DNS** fields at the pool-level, enter these details under **Configuration**. If you have opted to configure these fields at the block-level, enter these details while configuring the IP block.
- c) Under **IP Blocks**, configure one or more IP blocks:
 1. Click **Add IP Blocks** to add an IP block.
 2. Enter the following parameters for the IP block:

Note You can configure the Netmask, Gateway, Primary DNS, and Secondary DNS fields at the pool-level or the block-level.

- **From**—Starting IP address of the IP pool.
- **Size**—Number of IP addresses allocated for the IP pool.
- **Netmask**—the netmask associated with the IP pool.
- **Gateway**—The IP address of the gateway for the IP pool.

Note If the IP Pool is to be used for an IMC Access policy, ensure that the gateway IP address specified in the IP Pool has connectivity to Cisco IMC.

- **Primary DNS**—the primary DNS server that this block of IP addresses should access.
- **Secondary DNS**—the secondary DNS server that this block of IP addresses should access.

Step 5 [Optional] Configure IPv6 pools:

- a) Use the **Configure IPv6 Pool** toggle button to enable IPv6 pool configuration. By default, it is enabled. You can also opt to configure an IPv6 pool later.
- b) If you have opted to configure the **Prefix**, **Gateway**, **Primary DNS**, and **Secondary DNS** fields at the pool level, enter these details under **Configuration**. If you have opted to configure these fields at the block level, enter these details while configuring the IP block.
- c) Under **IP Blocks**, configure one or more IP blocks:
 1. Click **Add IP Blocks** to add an IP block.
 2. Enter the following parameters for the IP block:

Note You can configure the Prefix, Gateway, Primary DNS, and Secondary DNS fields at the pool-level or the block-level.

- **From**—Starting IP address of the IP pool.
- **Size**—Number of IP addresses allocated for the IP pool.
- **Prefix**: The prefix associated with the IP pool.
- **Gateway**: The IP address of the gateway for the IP pool.

Note If the IP Pool is to be used for an IMC Access policy, ensure that the gateway IP address specified in the IP Pool has connectivity to Cisco IMC.

- **Primary DNS**—the primary DNS server that this block of IP addresses should access.
- **Secondary DNS**—the secondary DNS server that this block of IP addresses should access.

Step 6 Click **Create**.

The newly created IP pool appears in the list of IP pools.

IP Pool Details

Details

Displays the list of IP pools.

Property	Essential Information
Details	
Name	Displays the name of the IP pool
Type	Displays the type of the pool.
Size	Displays the total number of identifiers the IP pool contains.
Used	Displays the total number of identifiers in the IP pool that are in use and are no longer available.
Reserved	Displays the total number of identifiers in the IP pool that are reserved for later use.
Available	Displays the total number of identifiers in the IP pool that are available for use.
Description	A description of the IP pool.
Last Update	The date and time when the IP pool was last updated.
Organization	Users in a Default Organization automatically has access to all the resources available for the user account.
Configuration	
IPv4	Displays the IPv4 configuration of the pool, such as subnet mask, default gateway, primary DNS, and secondary DNS, when the subnet is configured at the pool level.
IPv6	Displays the IPv6 configuration of the pool, such as prefix, default gateway, primary DNS, and secondary DNS, when the subnet is configured at the pool level.

Property	Essential Information
From	Displays the starting IP of the pool. Note Cisco Intersight selects the identity in sequential manner, that is, the lowest available identity from the pool.
To	Displays the range of the block size. Note This value is dependent on the IP pool size property.
Size	Displays the IP pool size
Eye symbol	Displays the configuration of the pool, such as subnet mask, prefix, default gateway, primary DNS, and secondary DNS, when the subnet is configured at the block level.
Usage	
IP, VRFs, Status, Server Profile, and Source	Displays the IP address, VRF instances, status of usage (Reserved or Used) and associated server profiles. Source can be Self or Other , where Self is ID used or reserved by this pool and Other is ID used or reserved statically or by another pool.
Actions	
Edit	Allows to add or modify the configuration details of the IP pool.
Delete	Allows to delete the IP pool.

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. If you use MAC pools in server profiles, you do not have to manually configure the MAC addresses to be used by the server associated with the server profile.

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

Creating a MAC Pool

MAC Pools represent a collection of MAC addresses that can be allocated to vNICs of a server profile.

-
- Step 1** From the left navigation panel, click **Pools > MAC > Create MAC Pool**.
The **MAC Pool** wizard appears.
- Step 2** Add the following information on the **General** page:
- **Name**—Name of the MAC pool
 - **Description**—An optional description of the MAC pool.
 - **Organization**—The organization to which the MAC pool belongs.
 - **Add Tag**—An optional tag to identify and search for the MAC pool.
- Step 3** Click **Next**. The **Pool Details** page appears.
- Step 4** Add the following configuration information in the **MAC Blocks** area:
- **From**—Indicates the first MAC address in the block.
 - **Size**—Indicates the number of MAC addresses in the block.
- Step 5** To add more blocks, click + and then add the starting MAC address and total number of MAC addresses in the new block.
- Step 6** Click **Create**.
-

The newly created MAC pool appears in the list of MAC pools.

MAC Pool Details

Details

Displays the list of MAC pools.

Property	Essential Information
Name	The name of the MAC pool.
Size	The number of MAC addresses in the pool.
Used	The number of MAC addresses in the pool that have been used, and are no longer available.
Reserved	Displays the total number of identifiers in the MAC pool that have been reserved to be used later.
Available	Displays the total number of identifiers in the MAC pool that are available to be used.
Description	A description of the MAC pool.
Last Update	When the MAC pool was last updated.
Configuration	

Property	Essential Information
From	Displays the MAC prefix value of the pool. Note Cisco Intersight selects the identity in sequential manner, that is, the lowest available identity from the pool.
To	Displays the MAC suffix value of the pool.
Size	Displays the MAC pool size
Usage	
MAC address, Status, Server Profile, and Source	Displays the MAC address, status of usage (Reserved or Used) and associated server profiles. Source can be Self or Other , where Self is ID used or reserved by this pool and Other is ID used or reserved statically or by another pool.
Actions	
Edit	Allows to add or modify the configuration details of the MAC pool.
Delete	Allows to delete the MAC pool.

UUID Pools

A Universally Unique Identifier (UUID) pool is a collection of UUIDs that are assigned to servers. The prefix and suffix of the UUID are variable values. A UUID pool ensures that these variable values are unique for each server associated with a server profile that uses a particular pool to avoid conflicts.



- Note**
- The supported servers and its minimum firmware or Cisco IMC versions required for UUID pool are mentioned below:

Servers	Minimum firmware versions
Cisco UCS-B200-M5, UCS-B480-M5, Cisco UCS UCS-B200-M6	4.2(1b)
Cisco UCS-C220-M6, UCS-C240-M6	4.2(1b)
Cisco UCS-C225-M6, UCS-C245-M6	4.2(1i)
Cisco UCSX-210C-M6	5.0(1a)

- For more information on the server profile association using UUID pool, see [Configuring Server Profiles](#).

Creating a UUID Pool

UUID Pools represent a collection of UUID items that can be allocated to server profiles.

-
- Step 1** From the left navigation panel, click **Pools > UUID > Create UUID Pool**.
The **UUID Pool** wizard appears.
- Step 2** Add the following information on the **General** page:
- **Organization**—An organization to which the UUID pool belongs.
 - **Name**—Name of the UUID pool.
 - **Set Tags**—An optional tag to identify and search for the UUID pool.
 - **Description**—An optional description of the UUID pool.
- Step 3** Click **Next**. The **Pool Details** page appears.
- Step 4** In the **Configuration** section, add the UUID Prefix number in hexadecimal format. Example, 1728E8C7-7B40-47E8
- Step 5** In the **UUID Blocks** section, add the following configuration details:
- **From**—Indicates the UUID suffix number of the block in hexadecimal format. Example, 9EDE-0E52924AC87A
 - **Size**—Indicates the number of UUID identifiers in the block. The size ranges from 1 to 1000.
- Step 6** To add more blocks, click + and then add the starting UUID suffix and total number of UUID identifiers in the new block.
- Step 7** Click **Create**.
-

The newly created UUID pool appears in the list of UUID pools.

UUID Pool Details

Details

Displays the list of UUID pools.

Property	Essential Information
Details	
Name	Displays the name of the UUID pool
Type	Displays the type of the pool.
Size	Displays the total number of identifiers the UUID pool contains.
Used	Displays the number of UUID already in use from the pool.
Reserved	Displays the total number of UUID that have been reserved to be used later.
Available	Displays the number of UUID available for usage.

Property	Essential Information
Last Update	The date and time when the when the UUID pool was last updated.
Description	Description of the UUID Pool.
Organization	Displays the organization under which the UUID Pool is created.
Configuration	
UUID Prefix	Displays the UUID prefix value of the pool.
From	Displays the UUID suffix value of the pool. Note Cisco Intersight selects the identity in sequential manner, that is, the lowest available identity from the pool.
To	Displays the range of the block size. Note This value is dependent on the UUID pool size property.
Size	Displays the UUID pool size
Usage	
UUID, Status, Server Profile, and Source	Displays the UUID assigned to the server profile, status of usage (Reserved or Used) and the associated server profile. Source can be Self or Other , where Self is ID used or reserved by this pool and Other is ID used or reserved statically or by another pool.

WWN Pools

A World Wide Name (WWN) pool is a collection of WWNs for use by the Fibre Channel vHBAs in a Cisco UCS Domain. You create separate pools for the following:

- WW node names assigned to the server
- WW port names assigned to the server



Note A WWN ID can not be reused across WWPN and WWNN pools. To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, Cisco Intersight uses the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:xx:xx:xx.

If you use WWN pools in server profiles, you do not have to manually configure the WWNs that will be used by the server associated with the server 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 WWNN pool is a WWN pool that contains only WW node names. If you include a pool of WWNNs in a server profile, the associated server is assigned a WWNN from that pool.

WWPN Pools

A WWPN pool is a WWN pool that contains only WW port names. If you include a pool of WWPNs in a server profile, the port on each vHBA of the associated server is assigned a WWPN from that pool.

Creating a WWNN Pool

To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, Cisco Intersight uses the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:xx:xx:xx.

-
- Step 1** From the left navigation panel, click **Pools > WWNN > Create WWNN Pool**.
The **WWNN Pool** wizard appears.
- Step 2** Add the following information on the **General** page:
- **Name**—Name of the WWNN pool
 - **Description**—An optional description of the WWNN pool.
 - **Organization**—An optional entry of the organization to which the WWNN pool belongs.
 - **Add Tag**—An optional tag to identify and search for the WWNN pool.
- Step 3** Click **Next**. The **Pool Details** page appears.
- Step 4** Add the following configuration information in the **Initiator Blocks** area:
- **From**—Indicates the first WWN identifier of the block.
 - **Size**—Indicates the maximum number of identifiers that the block can contain.
- Step 5** To add more blocks, click + and then add the starting WWN identifier and maximum number of identifiers that the block can contain.
- Step 6** Click **Create**.
-

The newly created WWNN pool appears in the list of WWNN pools.

WWNN Pool Details

Details

Displays the list of WWNN pools. To ensure the uniqueness of the Cisco UCS WWNNs in the SAN fabric, Cisco recommends using the following WWN prefix 20:00:00:25:b5:00:00:01

Property	Essential Information
Name	The name of the WWNN pool.
Size	The total number of WWNNs in the pool.
Used	The number of WWNNs in the pool that have been used, and are no longer available.
Reserved	Displays the total number of WWNNs in the pool that have been reserved to be used later.
Available	Displays the total number of WWNNs in the pool that are available to be used.
Description	A description of the WWNN pool.
Last Update	When the WWNN pool was last updated.
Configuration	
From	Displays the WWNN prefix value of the pool. Note Cisco Intersight selects the identity in sequential manner, that is, the lowest available identity from the pool.
To	Displays the WWNN suffix value of the pool.
Size	Displays the WWNN pool size
Usage	
Identifier, Status, Server Profile, and Source	Displays the WWNN, status of usage (Reserved or Used) and associated server profiles. Source can be Self or Other , where Self is ID used or reserved by this pool and Other is ID used or reserved statically or by another pool.
Actions	
Edit	Allows to add or modify the configuration details of the WWNN pool.
Delete	Allows to delete the WWNN pool.

Creating a WWPN Pool

To ensure the uniqueness of the Cisco UCS WWNNs and WWPNs in the SAN fabric, Cisco Intersight uses the following WWN prefix for all blocks in a pool: 20:00:00:25:B5:xx:xx:xx.

Step 1 From the left navigation panel, click **Pools > WWNN > Create WWPN Pool**.

The **WWPN Pool** wizard appears.

Step 2 Add the following information on the **General** page:

- **Name**—Name of the WWPN pool
- **Description**—An optional description of the WWPN pool.
- **Organization**—An optional entry of the organization to which the WWPN pool belongs.
- **Add Tag**—An optional tag to identify and search for the WWPN pool.

Step 3 Click **Next**. The **Pool Details** page appears.

Step 4 Add the following configuration information in the **Initiator Blocks** area:

- **From**—Indicates the first WWN identifier of the block.
- **Size**—Indicates the maximum number of identifiers that the block can contain.

Step 5 To add more blocks, click + and then add the starting WWN identifier and maximum number of identifiers that the block can contain.

Step 6 Click **Create**.

The newly created WWPN pool appears in the list of WWPN pools.

WWPN Pool Details

Details

Displays the list of WWPN pools. To ensure the uniqueness of the Cisco UCS WWPNs in the SAN fabric, Cisco recommends using the following WWN prefix 20:00:00:25:b5:00:00:01

Property	Essential Information
Name	The name of the World Wide Port Name pool.
Size	The total number of WWPNs in the pool.
Used	The number of WWPNs in the pool that have been used, and are no longer available.
Description	A description of the WWPN pool.
Last Update	When the WWPN pool was last updated.

IQN Pools

An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs. 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 sharing the same prefix.

Creating an IQN Pool

An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers. The IQN pool details are used for configuring blocks of IQN identifiers.

Procedure

	Command or Action	Purpose
Step 1	From the left navigation panel, click Create Pools > IQN > Start .	The IQN Pool wizard appears.
Step 2	Add the following information on the General page: <ul style="list-style-type: none"> • Organization—The organization of the IQN pool. • Name—Name of the IQN pool. • Add Tag—The tag to identify and search for the IQN pool. • Description—The description the IQN pool. 	
Step 3	Click Next . The Pool Details page appears.	
Step 4	Add the following configuration information for IQN pools in the Configuration area: <ul style="list-style-type: none"> • Prefix—The prefix for any IQN blocks created for this pool. IQN prefix must have the following format "iqn-yyyy-mm.naming-authority", where the naming authority is usually the reverse syntax of the internet domain of the naming authority. Example, iqn1.2021-01.alpha.com • Suffix—The suffix for this block of IQNs. Enter from 1 to 64 characters. You can use any letter or number, as well as the special characters . (period), : (colon), and - (hyphen). • From—The first iSCSI Qualified Name (IQN) suffix in the block. • Size—The number of identifiers this block can hold. 	

The newly created IQN pool appears in the list of IQN pools.

IQN Pool Details

Details

Displays the list of IQN pools.

Property	Essential Information
Details	

Property	Essential Information
Name	Displays the name of the IQN pool.
Type	Displays the type of the pool.
Size	Displays the total number of identifiers the IQN pool contains.
Used	Displays the number of identifiers already in use from the pool.
Reserved	Displays the total number of identifiers that have been reserved to be used later.
Available	Displays the number of identifiers available for usage.
Description	A description of the IQN pool.
Last Update	The date and time when the IQN pool was last updated.
Organization	Users in a Default Organization automatically has access to all the resources available for the user account.
Tags	Displays the tags for the pools.
Configuration	
Prefix	Displays the prefix for IQN blocks created for this pool.
Suffix	Displays the suffix for this block of IQNs.
From	The first suffix number in the block. Note Cisco Intersight selects the identity in sequential manner, that is, the lowest available identity from the pool.
To	The number of identifiers that the block can hold.
Usage	
IQN Address, Status, Server Profile, and Source	Displays the IQN address, status of usage (Reserved or Used) and associated server profiles. Source can be Self or Other , where Self is ID used or reserved by this pool and Other is ID used or reserved statically or by another pool.
Actions	
Edit	Allows to add or modify the configuration details of the IQN pool.

Property	Essential Information
Delete	Allows to delete the IQN pool.

Resource Pools

Pools enable you to logically group and manage resources (servers and other endpoints) more efficiently. You can assign servers to a resource pool and can continue with the automated server profile assignment. For more information on the server profile association using resource pools, see [Configuring Server Profiles](#).

Persistent Resource Pool Assignment

When a server that is a part of a pool is decommissioned, it appears in the **Decommissioned Resources** section of the **Resource Pool Details View** and **Server Details View**. When the server is recommissioned, it gets assigned to the same pool again. The same behavior occurs when a server is decommissioned, moved to a different chassis or slot, and then recommissioned. Thus, you do not need to manage the pool reassignment for that server when physical changes occur in the deployment environment.



Note To convert an existing resource pool into a persistent Resource Pool, edit the Resource Pool.

Change in Behavior for API or Terraform Users

API or Terraform users can use APIs to create new Resource Pools using either Managed Object IDs (MOIDs) or Serial selectors.

However, if an API user edits a Resource Pool that uses a MOID from the UI to enable persistent Resource Pool assignment, the system will internally convert these MOID selectors to Serial selectors, and the MOIDs will no longer be accessible through APIs. For more information on the payload for creating Resource Pools, see [API documentation](#).



Note Using the edit resource pool option, a resource with an active lease cannot be removed from the resource pool.

Creating a Resource Pool

A resource pool represents a collection of resources that can be associated to the configuration entities such as server profiles.

Step 1 From the left navigation panel, click **Create Pools > Resource > Start**.

The **Resource Pool** wizard is displayed.

Step 2 Add the following information on the **General** page:

- **Organization**—The organization of the Resource pool.
- **Name**—Name of the Resource pool.
- **Target Platform**—The target platform type as UCS Standalone server or UCS FI-Attached server.

- **Set Tags**—The tag to identify and search for the Resource pool.
- **Description**—The description of the Resource pool.

Step 3 Click **Next**. The **Resource Pool Details** page is displayed with the list of discovered servers based on the target platform type.

Step 4 Select the servers from the **Resource Selection** table.

Step 5 Click **Create**.

The newly created Resource pool appears in the list of Resource pools.

Resource Pool Details

Details - Displays the details of the resource pools.

Property	Essential Information
Details	
Name	Displays the name of the resource pool.
Type	Displays the type of the pool.
Size	Displays the total number of resources that the Resource pool contains.
Used	Displays the number of resources that are already used, and are unavailable for use.
Available	Displays the number resource pool available for usage.
Last Update	The date and time of the resource pool that was last updated.
Resource	
Type	Displays the resource pool type. Note Currently, Intersight supports only server type as a resource for the resource pool.
Selection	Displays the resource pool selection type. Currently, only manual (Static) selection is supported.
Target Platform	Displays the target platform. This could any of the following: <ul style="list-style-type: none"> • Standalone • FI-Attached
Description	Description of the resource pool.

Property	Essential Information
Organization	Displays the organization under which the Resource Pool is created
Configuration	
Note	The configuration properties of the resource pool differs with the resource type associated.
Status	<p>Displays the status of the resource. This can be any of the following:</p> <ul style="list-style-type: none"> • Available—Indicates the resource is available for use. • Used—Indicates the resource is already used in a resource pool.
Decommissioned Resources: This section displays the details of decommissioned servers.	
Note	The section is displayed only when a server has been decommissioned and is already a part of the resource pool.
Name	Displays the name of the decommissioned server.
Type	Displays whether the server is a Cisco UCS C-Series server or a Cisco UCS B-Series server.
ID	Displays the unique ID assigned to the decommissioned server. This field applies only to Cisco UCS C-Series servers.
Model	Displays the model of the server.
Serial Number	Displays the serial number of the server.
Decommissioned Date	Displays the time stamp at which the server was decommissioned.
Usage	
Resource Name	Displays the resource name.
Leasing Entity	<p>Displays the configuration entity.</p> <p>Note A resource can be part of different pools but are allowed to be associated to only one leasing entity.</p>
Use Case	Displays the consumer of the resource. Example, Server Profile.

Property	Essential Information
Resource Usage	<p>Displays the resource consumption types. The types can be:</p> <ul style="list-style-type: none"> • Current—The resource is associated and used in the current resource pool. • Other Pool—The resource is associated and used in an other pool. • Direct—The resource is directly associated with the server profile without using resource pool.



Note Using an edit resource pool option, a resource with an active lease cannot be removed from the resource pool.

Virtual Routing and Forwarding

Virtual Routing and Forwarding (VRF) is an IP technology that allows multiple instances of a routing table to coexist on the same router at the same time. Because the routing instances are independent, the same or overlapping IP addresses can be used without conflict. A VRF creates a namespace for IP address management. IP pools are VRF-aware in Cisco Intersight.

VRF Guidelines

The following guidelines and limitations apply for VRF instances:

- Intersight creates a default VRF for an account, and manages IP address allocation within the context of this default VRF.
- Within a single VRF instance, IP addresses must be unique. Between different VRF instances, you can have overlapping IP addresses.
- If IP Pools are shared between VRF instances, ensure that there are no overlapping IP addresses.

Creating a VRF Instance

Virtual Routing and Forwarding (VRF) is a networking technology that creates multiple virtual networks within a single network entity.

Step 1 From the left navigation panel, click **Virtual Routing And Forwarding > VRFs > Create VRF**.

The **VRF** wizard appears.

Step 2 Add the following information on the **General** page:

- **Name**—Name of the VRF instance
- **Description**—An optional description of the VRF instance.

- **Organization**—An optional entry of the organization to which the VRF instance belongs.
- **Add Tag**—An optional tag to identify and search for the VRF instance.

Step 3 Click **Create**.

The newly created VRF instance appears in the list of VRFs.

