Prerequisites

Prerequisites

About Tenants

A tenant is a container for policies that enable an administrator to exercise domain-based access control so that qualified users can access privileges, such as tenant administration and networking administration. You must configure a tenant before you can deploy any Layer 4 to Layer 7 services.

About Security Domains

A security domain is a concept that allows you to scope which tenant is accessible by which user. For example, if you create `Tenant1`, `Tenant2`, and `Tenant3`, you can create three security domains—`securitydomain1`, `securitydomain2`, and `securitydomain3`—and the administrators of each tenant would be associated with the respective security domain.

About Layer 3 Networks

Layer 3 is the network layer of the Open Systems Interconnection (OSI) communication model. An Layer 3 network configuration refers to the configuration of how traffic forwarding works to the outside of the fabric. Layer 3 is used to discover the address of other nodes, select routes, select quality of service, and forward incoming messages for local host domains to the transport layer. The Layer 3 network is used by all of the application endpoint groups (EPGs) that are used by the tenant.

About Bridge Domains

A bridge domain represents a Layer 2 forwarding construct within the fabric. One or more endpoint groups (EPGs) can be associated with one bridge domain or subnet. A bridge domain can have one or more subnets that are associated with it. One or more bridge domains together form a tenant network.

About Application Profiles

An application profile defines the policies, services and relationships between endpoint groups (EPGs). Each application profile contains one or more EPGs that can communicate with the other EPGs in the same application profile and with EPGs in other application profiles according to the contract rules.

About Contracts

A contract contains all of the filters that will be applied between endpoint groups (EPGs) that produce and consume the contract. A contract involves EPGs that are called providers and consumers. A contract defines the protocols and ports on which a provider and consumer are allowed to communicate.

Configuring a VLAN Pool

A VLAN pool is also known as a VLAN namespace. You can configure a VLAN pool.

Step 1 In the **CREATE VCENTER DOMAIN** dialog box, choose **Create VLAN Pool** from the **VLAN Pool** drop-down list. The **CREATE VLAN POOL** dialog box appears.

Step 2 Complete the following fields:

Name	Description
Name field	The name of the VLAN pool.
Description field	The description of the VLAN pool.
Allocation Mode radio buttons	The allocation mode of the VLAN pool. You can choose **Dynamic Allocation** or **Static Allocation**. **Note** Choose**Dynamic Allocation** if VMM needs to be integrated when devices are virtual.
Encap Blocks section	The encapsulation block ranges, which specify which VLANs to use while using a virtual appliance for performance graphs. To create an encapsulation block range, see .

Step 3 Click **SUBMIT**. The **CREATE VLAN POOL** dialog box closes and the VLAN pool is created.

Configuring an Encapsulation Block Range

An encapsulation block range specifies which VLANs to use while using a virtual appliance for performance graphs. You can configure an encapsulation block range.

Step 1 In the **CREATE VLAN POOL** dialog box, click + in the **Encap Blocks** section. The **CREATE RANGES** dialog box appears.

Step 2 Complete the following fields:

Name	Description
From field	The minimum value for the encapsulation block range.
To field	The maximum value for the encapsulation block range.

Step 3 Click **OK**. The **CREATE RANGES** dialog box closes and the encapsulation block range is created.

Configuring a Physical Domain

Physical domains control the scope of where a given VLAN namespace is used. The VLAN namespace that is associated with the physical domain is for non-virtualized servers, although it can also be used for static mapping of port-groups from virtualized servers. You can configure a physical domain for physical device types.

Before You Begin

- Configure a tenant. See .

Step 1 From the **Physical Domain** drop-down list, choose **Create Physical Domain**. The **CREATE PHYSICAL DOMAIN** dialog box appears.

Step 2 Complete the following fields:

Name	Description
Name field	The name of the physical domain profile.
VLAN Pool field	The VLAN pool of the physical domain. The VLAN pool specifies the range or pool for VLANs that is allocated by the APIC for the service graphs that are using this physical domain. To create a VLAN pool, see Configuring a VLAN Pool, on page 2.

Step 3 Click **Submit**. The **CREATE PHYSICAL DOMAIN** dialog box closes and the physical domain is created.

Configuring a VMM Domain

A Virtual Machine Manager (VMM) domain defines the scope of use of a given VLAN namespace for virtualized servers. A Virtual Machine Manager (VMM) domain is also called a vCenter domain. You can configure a VMM domain.

Before You Begin

- Configure a tenant. See .
- Configure a device cluster on the tenant. See Configuring a Device Cluster.

Step 1 From the **VMM Domain** drop-down list, choose **Create vCenter Domain**. The **CREATE VCENTER DOMAIN** dialog box appears.

Step 2 Complete the following fields:

Name	Description
Name field	The name of the VMM domain profile.
Virtual Switch radio buttons	The mode of the virtual switch.
Associated Attachable Entity Profile field	The attachable entity profile that is to be associated with the VMM domain. The attachable entity profile is required to attach a VMM domain to the fabric.
VLAN Pool field	The VLAN pool of the VMM domain. The VLAN pool specifies the range or pool for VLANs that is allocated by the Application Policy Infrastructure Controller (APIC) for the service graphs that are using this VMM domain. To configure a VLAN pool, see Configuring a VLAN Pool, on page 2.
vCenter Credentials section	The credentials to use for connecting to the VMM domain. To configure vCenter credentials, which are also known as VMM credentials, see .
vCenter/vShield section	The vCenter/vShield controller profile to use with the VMM domain. To configure a vCenter/vShield controller profile, see .

Step 3 Click **OK**. The **CREATE VMM DOMAIN** dialog box closes and the VMM domain is created.

Configuring VMM Credentials

VMM credentials are required for connecting to the VMM domain. You can configure VMM credentials.

Step 1 In the **CREATE VCENTER DOMAIN** dialog box, click + in the **vCenter Credentials** section. The **CREATE VCENTER CREDENTIAL** dialog box appears.

Step 2 Complete the following fields:

Name	Description
Profile Name field	The name of the profile to use for logging into the VMM domain.
Description field	The description of the user account profile.
Username field	The name of the user to use for the credentials.
Password field	The password of the specified user.
Confirm Password field	The confirmation of the password of the specified user.

Step 3 Click **OK**. The **CREATE VCENTER CREDENTIAL** dialog box closes and the VMM credentials are created.

Configuring a vCenter/vShield Controller Profile

You can configure a vCenter/vShield controller profile.

Step 1 In the **CREATE VCENTER DOMAIN** dialog box, click + in the **vCenter/vShield** section. The **CREATE VCENTER/VSHIELD CONTROLLER** dialog box appears.

Step 2 Complete the following fields:

Name	Description
Type radio buttons	The profile type of the controller.
Name field	The name of the vCenter/vShield controller profile.
Address field	The hostname or IP address of the vCenter/vShield controller profile.
Stats Collection radio buttons	Enables or disables statistics collection.
Management EPG field and drop-down list	Choose the management endpoint group (EPG) in the Virtual Machine Manager (VMM) controller profile.
Associated Credential field and drop-down list	Choose the VMM credentials to use with the vCenter/vShield controller profile.

Step 3 Click **OK**. The **CREATE VCENTER/VSHIELD CONTROLLER** dialog box closes and the vCenter/vShield controller profile is created.

Configuring a Tenant

You can configure a tenant.

Step 1 On the menu bar, click the **TENANTS** tab. The **Tenant** window appears.

Step 2 On the submenu bar, click **ADD TENANT**. The **CREATE TENANT** dialog box appears, showing the **TENANT** page.

Step 3 Complete the following fields:

Name	Description
Name field	The name of the tenant.
Alias field	The alias for the tenant. The alias can be a simpler and more descriptive name than the tenant's name when referring to a single tenant. You can assign a particular alias name to only one tenant; the system will prevent you from assigning the same alias name to a second tenant.
Description field	The description of the tenant.
Tags field	A search keyword or term that is assigned to the tenant. A tag allows you to group multiple objects by a descriptive name. You can assign the same tag name to multiple objects and you can assign one or more tag names to an object.
Monitoring Policy field	The endpoint group (EPG) monitoring policy name.
Security Domains section	The security domains of the tenant. You do not need to choose a security domain to deploy Layer 4 to Layer 7 services. For information about creating a security domain, see the *Cisco APIC Getting Started Guide*.

Step 4 Click **Next**. The **NETWORK** page appears, and the tenant is created. To configure the Layer 3 network, see .

Configuring a Bridge Domain

You can configure a bridge domain.

Before You Begin

- Configure a Layer 3 (L3) network. See .

Step 1 On the **BRIDGE DOMAIN** page of the **CREATE TENANT** dialog box, complete the following fields:

Name	Description
Name field	The name of the bridge domain.
Description field	The description of the bridge domain.

Name	Description
Forwarding drop-down list	Choose the forwarding method of the bridge domain.
L2 Unknown Unicast radio buttons	The forwarding method for unknown Layer 2 destinations. These radio buttons appear only if you chose **Custom** in the **Forwarding** drop-down list.
Unknown Multicast Flooding radio buttons	Click **Flood** or **Optimized Flood**. These radio buttons appear only if you chose **Custom** in the **Forwarding** drop-down list.
Multi Destination Flooding radio buttons	Click **Flood in EPG**, **Drop**, or **Flood in BD**. These radio buttons appear only if you chose **Custom** in the **Forwarding** drop-down list.
ARP Flooding check box	Put a check in this box to enable ARP flooding. If flooding is disabled, unicast routing will be performed on the target IP address. This check box is unchecked by default. This check box appears only if you choose **Custom** in the **Forwarding** drop-down list.
GARP-Based Detection check box	Put a check in this box to enable gratuitous ARP (GARP)-based detection. Enabling ARP flooding enables GARP-based detection by default. This feature allows endpoints to be updated within this bridge domain when a GARP is received. A GARP is an ARP broadcast-type of packet that is used to verify that no other device on the network has the same IP address as the sending device. This check box appears only if you put a check in the **ARP Flooding** check box.
Unicast Routing check box	Put a check in this check box to enable unicast routing. Unicast routing is the forwarding method based on predefined forwarding criteria (IP or MAC address). This check box is unchecked by default. This check box appears only if you chose **Custom** in the **Forwarding** drop-down list.
IGMP Snoop Policy drop-down list	The Internet Group Management Protocol (IGMP) snooping policy. You do not need to choose an IGMP snooping policy to deploy Layer 4 to Layer 7 services.
Config BD MAC Address check box	Put a check in this check box to configure the bridge domain MAC address.

Name	Description
MAC Address field	The MAC address of the bridge domain. This field appears only if you put a check in the **Config BD MAC Address** check box.
Subnets section	The subnets of the bridge domain. Click +, complete the fields, and click **UPDATE** to add a subnet. You can add multiple subnets.
DHCP Labels section	The DHCP labels of the bridge domain. You do not need to configure a DHCP label to deploy Layer 4 to Layer 7 services. For information about configuring a DHCP label, see the *Cisco APIC Getting Started Guide*.

Step 2 Click **OK**. The next **NETWORK** page appears, and the bridge domain is created. On this page, you can add the Layer 2 (L2) external cache, the L3 external cache, additional networks, and additional bridge domains.

Step 3 Click **Next**. The **APPLICATION** page appears, which is used to configure application profiles. To configure an application profile, see .

Configuring a Layer 3 Network

You can configure a Layer 3 (L3) network.

Before You Begin

- Configure a tenant. See .

Step 1 On the **NETWORK** page of the **CREATE TENANT** dialog box, click + to add a network. The **CREATE NEW NETWORK** dialog box appears.

Step 2 Complete the following fields:

Name	Description
Name field	The name of the network.
Description field	The description of the network.
BGP Timers drop-down list	Choose the Border Gateway Protocol (BGP) timers of the network. To configure a new BGP timers policy, see Configuring a BGP Timers Policy.

Name	Description
OSPF Timers drop-down list	The Open Shortest Path First (OSPF) timers policy. The OSPF timer policy provides the Hello timer and Dead timer intervals configuration. You can choose the default policy or create a new policy. You do not need to choose a OSPF timer policy to deploy Layer 4 to Layer 7 services.
Monitoring Policy drop-down list	Choose the monitoring policy of the network.

Step 3 Click **Next**. The **BRIDGE DOMAIN** page appears, and the L3 network is created. To configure the bridge domain, see .

Configuring an Application Profile

You can configure an application profile.

Before You Begin

- Configure a bridge domain. See .

Step 1 On the menu bar, click the **TENANTS** tab. The **Tenant** window appears.

Step 2 On the submenu bar, click the tab of the tenant for which you want to configure an application profile. The **Tenant** window for the selected tenant appears in the **Work** pane.

Step 3 In the **Navigation** pane, expand the tenant's branch.

Step 4 Click **Application Profiles**. The **Application Profiles** window appears in the **Work** pane.

Step 5 Choose **ACTIONS** > **Create Application Profile**. The **CREATE APPLICATION PROFILE** dialog box appears.

Step 6 Complete the following fields:

Name	Description
Name field	The name of the application profile.
Alias field	The alias for the application profile. The alias can be a simpler and more descriptive name than the application profile's name when referring to a single application profile. You can assign a particular alias name to only one application profile; the system will prevent you from assigning the same alias name to a second application profile.
Description field	The priority of the application profile.
Tags field	A search keyword or term that is assigned to the application profile. A tag allows you to group multiple objects by a descriptive name. You can assign the same tag name to multiple objects and you can assign one or more tag names to an object.

Name	Description
Monitoring Policy drop-down list	Choose the endpoint group (EPG) monitoring policy name.

Step 7 In the **EPGs** section, click +. The **CREATE APPLICATION EPG** dialog box appears.

Step 8 Complete the following fields:

Name	Description
Name field	The name of the application EPG.
Alias field	The alias for the application EPG. The alias can be a simpler and more descriptive name than the application EPG's name when referring to a single application EPG. You can assign a particular alias name to only one application EPG; the system will prevent you from assigning the same alias name to a second application EPG.
Description field	The description of the application EPG.
Tags field	A search keyword or term that is assigned to the application EPG. A tag allows you to group multiple objects by a descriptive name. You can assign the same tag name to multiple objects and you can assign one or more tag names to an object.
QoS class drop-down list	Choose the quality of service priority class ID.
Custom QoS drop-down list	The quality of service traffic priority class ID. The custom class is a user-configurable differentiated services code point (DSCP) value. You do not need to choose a quality of service traffic priority class ID to deploy Layer 4 to Layer 7 services.
Bridge Domain drop-down list	Choose the name of the bridge domain that is associated with the application EPG.
Monitoring Policy drop-down list	Choose the endpoint group (EPG) monitoring policy name.
Associated Domain Profiles (VMs or bare metals) section	The domain profiles that are associated with the application EPG. Click + to add a domain profile. You can add more than one domain profile.
Statically Link with Leaves/Paths check box	Check this check box to link the application EPG statically with leafs and paths.

Step 9 If you checked the **Statically Link with Leaves/Paths** check box, click **NEXT**. The **LEAVES/PATHS** page appears.

a) In the **Leaves** section, click + to add a leaf.

b) Complete the following fields:

Name	Description
Node drop-down list	Choose the node to use as a leaf.
Encap field	The VLAN to use for encapsulation. The range is from 1 to 4094.

Name	Description
Deployment Immediacy drop-down list	Choose whether the deployment of this leaf association will occur immediately or when needed.
Mode drop-down list	Choose the mode of the static association with the leaf.

c) Click **UPDATE**. The leaf is added.
d) In the **Paths** section, click + to add a path.
e) Complete the following fields:

Name	Description
Path drop-down list	Choose the node to use as a path.
Encap field	The VLAN to use for encapsulation. The range is from 1 to 4094.
Deployment Immediacy drop-down list	Choose whether the deployment of this path association will occur immediately or when needed.
Mode drop-down list	Choose the mode of the static association with the path.

f) Click **UPDATE**. The path is added.

Step 10 Click **OK**. The **CREATE APPLICATION EPG** dialog box closes.

Step 11 In the **Provided Contracts** section, click + to add a provided contract. The **ADD PROVIDED CONTRACT** dialog box appears.

Step 12 Complete the following fields:

Name	Description
Contract Type drop-down list	Choose the type of the contract.
Name drop-down list	Choose the name of the contract. You can select **default**, a preexisting contract, or **Create New Contract**.

Step 13 Click **OK**. The **ADD PROVIDED CONTRACT** dialog box closes.

Step 14 n the **Consumed Contracts** section, click + to add a provided contract. The **ADD CONSUMED CONTRACT** dialog box appears.

Step 15 Complete the following fields:

Name	Description
Contract Type drop-down list	Choose the type of the contract.

Name	Description
Name drop-down list	Choose the name of the contract. You can select **default**, a preexisting contract, or **Create New Contract**.

Step 16 Click **OK**. The **ADD CONSUMED CONTRACT** dialog box closes.

Step 17 If any neighbors exist, in the **Neighbors** section, click + to add a neighbor. The **ADD NEIGHBOR** dialog box appears.

Step 18 Click **SUBMIT**. The **CREATE APPLICATION PROFILE** dialog box closes, and the application profile is configured.

Configuring a Contract

You can configure a contract.

Before You Begin

- Configure a tenant. See .
- Configure a device cluster on the tenant. See Configuring a Device Cluster.

Step 1 On the menu bar, click the **TENANTS** tab. The **Tenant** window appears.

Step 2 In the **Navigation** pane, expand the tenant's tree and an application profile's tree under that tenant for which you want to configure a contract.

Step 3 Choose **Contracts**.

Step 4 Choose **Actions** > **Create Contract**. The **CREATE CONTRACT** dialog box appears.

Step 5 Complete the following fields:

Name	Description
Name field	The name of the contract.
Scope field	The scope of the contract.
Priority field	The priority of the contract.
Description field	The description of the contract.

Step 6 In the **Subjects** section, click + to add a contract subject. The **CREATE CONTRACT SUBJECT** dialog box appears.

Step 7 Complete the following fields:

Name	Description
Name field	The name of the contract subject.

Name	Description
Description field	The description of the contract subject.

Step 8 In the **Filter Chain** section, click + to add a filter.

Step 9 Choose the tenant for which the filter applies, and choose a service graph to use with the filter. Any traffic that is matched by the contract is redirected to the service graph.

Step 10 Click **UPDATE**. The filter is created.

Step 11 Click **OK**. The **CREATE CONTRACT SUBJECT** dialog box closes, and the contract subject is created.

Step 12 Click **SUBMIT**. The **CREATE CONTRACT** dialog box closes, and the contract is created.

Configuring a Management Endpoint Group

You can configure a new management endpoint group (EPG) to use with a device cluster.

Before You Begin

- Configure a tenant. See .
- Configure a device cluster on the tenant. See Configuring a Device Cluster.

Step 1 From the **Create Device Cluster** dialog box, choose **Create Management EPG** from the **EPG** drop-down list. The **Create Management EPG** dialog box appears.

Step 2 Complete the following fields:

Name	Description
Application Profile field	The application profile to use with the management EPG. If a profile does not already exist, you can create one by choosing **Create Application Profile**.
Name field	The name for the application profile.
Alias field	The alias for the management EPG. The alias can be a simpler and more descriptive name than the management EPG's name when referring to a single management EPG. You can assign a particular alias name to only one management EPG; the system will prevent you from assigning the same alias name to a second management EPG.
Description field	The description of the management EPG.
QoS class drop-down list	Choose the quality of service class of the management EPG. If your device cluster uses physical appliances, choose **Unspecified**.

Name	Description
Bridge Domain drop-down list	Choose the bridge domain node to use with the management EPG.

Step 3 In the **Domains (VMM, Physical, or External) Associated to Interfaces** section, click + to add a domain.

Step 4 Complete the following fields:

Name	Description
Domain Profile drop-down list	Choose the domain profile to use with this management EPG.
Deployment Immediacy drop-down list	Choose whether to deploy the domain immediately or when needed.
Resolution Immediacy drop-down list	Choose how policies are pushed to leaf nodes: • **Immediate—**All policies, including VLAN bindings, NVGRE bindings, VXLAN bindings, contracts, and filters, are pushed to leaf nodes upon attaching a Hypervisor physical NIC. The Link Layer Discovery Protocol (LLDP) or OpFlex used to resolve Hypervisor-to-leaf node attachment. • **On-Demand—**Policies are pushed to leaf nodes only upon attaching a physical NIC and associating a virtual NIC with a port group (an EPG).

Step 5 In the **Reserved IP addresses for APICs** section, click + to create an IP address pool. The **CREATE IP ADDRESS POOL** dialog box appears.

Step 6 Complete the following fields:

Name	Description
Name field	The name for the IP address pool.
Gateway Address fields	The gateway's IP address and subnet mask.

Step 7 In the **Address Ranges** section, click +.

Step 8 Complete the following fields:

Name	Description
From field	The starting point of the IP address range.
To field	The ending point of the IP address range.

Step 9 Click **UPDATE**. The address range gets added to the **Address Ranges** section.

Step 10 Click **OK**. The **CREATE IP ADDRESS POOL** dialog box closes.

Step 11 Click **Submit**. The **Create Management EPG** dialog box closes and the management EPG is created.