

Restricting Access Using Security Domains and Node Rules

- Restricting Access by Domains, on page 1
- Assigning a Node to a Domain, on page 2
- Guidelines and Limitations for Security Domains and Node Rules, on page 2
- Creating a Security Domain, on page 3
- Creating a Node Rule to Assign Access to a Node, on page 3
- Configuring a User with a Security Domain, on page 4
- Custom Roles and Privileges, on page 5
- Use Case Example of Configuring an RBAC Node Rule, on page 7

Restricting Access by Domains

Security domains allow fabric administrators to expose resources selectively to a set of users and provide those users with the required level of permissions to read and modify those resources. By using security domains, multiple set of users can share the underlying infrastructure while having separated management access to their resources.

Starting with Cisco Application Policy Infrastructure Controller (APIC) release 5.0(1), you can configure security domains as "Restricted." A restricted security domain allows a fabric administrator to prevent a group of users from viewing or modifying any objects created by a group of users associated with a different security domain when users in both groups have the same assigned privileges.

For example, a user associated with restricted security domain domainA cannot see policies, profiles, or users configured by users associated with security domain domainB. Users associated with domainB can see policies, profiles, or users configured by users associated with domainA, unless domainB is also configured as restricted. A user will always have read-only visibility to system-created configurations for which the user has proper privileges. You can give a user associated with a restricted security domain a broad level of privileges within that domain without the concern that the user could inadvertently affect another tenant's physical environment.

The following figure illustrates the concept of restricted security domains:

Figure 1: Restricted Security Domains



Restricted security domains play an important role in providing multi-tenancy capabilities in policies and profiles outside the tenant level, such as in access policies. Even if access policies do not belong to any tenant, by using separated restricted security domains per tenant, users from each tenant can create access policies that are hidden to users in other tenants.

Assigning a Node to a Domain

Using an RBAC node rule, the fabric administrator can assign a physical node, such as a leaf switch, to a security domain. This node assignment allows a user in that security domain to access and perform operations on a node assigned as part of the node rule. Only a user with node management privileges within the security domain can configure nodes assigned to that domain. The user has no access to nodes outside of the security domain, and users in other security domains have no access to the node assigned to the security domain. To create or modify configurations on a node assigned to the security domain, a user in that domain must also be assigned to domain all with the port-mgmt role that contains the custom-port-privilege privilege by default or a custom role that contains the custom-port-privilege.



Note

When configuring a local user who will manage ports on an assigned node, you must grant the user a role in domain all, and the admin role in the security domain to which the node is assigned. Both roles must have the **Role Privilege Type** configured as Write.

Guidelines and Limitations for Security Domains and Node Rules

When configuring security domains and node rules, follow these guidelines and limitations. In this section, a "restricted node user" is a user in a restricted security domain to which a node has been assigned.

- When upgrading from an earlier Cisco Application Policy Infrastructure Controller (APIC) release to a 5.0 release, you must reconfigure any rules, policies, or roles that use the more granular earlier privileges.
- When downgrading from a Cisco APIC 5.0 release to an earlier release, you must manually edit and retain default roles. Roles modified under a Cisco APIC 5.0 release are retained.
- A spine switch cannot be assigned using RBAC node rules.

- When creating RBAC node rules, you should not assign a node to more than one security domain.
- A restricted node user can configure only policies. An admin user should perform node configuration and troubleshooting.
- A restricted node user can access default system-created managed objects.
- A restricted node user can view fabric-level fault counts in the Fault Dashboard.
- A restricted node user can view node-level faults, such as those from AAA servers, NTP servers, and DNS servers.
- If an admin or nonrestricted domain user associates a relationship policy to an access policy created by a restricted node user, that policy will be visible to the restricted node user.
- You cannot configure a restricted node user using the CLI.
- By default, the port-mgmt role has the custom-port-privilege privilege that contains predefined access policy managed objects. You can add more managed objects using the procedure in Configuring a Custom Privilege, on page 5.

Creating a Security Domain

Use this procedure to create a security domain.

- **Step 1** On the menu bar, choose $\mathbf{Admin} > \mathbf{AAA}$.
- **Step 2** In the **Navigation** pane, click **Security**.
- **Step 3** In the Work pane, select the Security Domains tab.
- Step 4 In the Work pane, click on the Actions icon drop-down list and select Create Security Domain.
- **Step 5** In the **Create Security Domain** dialog box, perform the following actions:
 - a) In the Name field, type a name for the security domain.
 - b) (Optional) Set the Restricted Domain control to No (the default) or Yes.

If you configured the security domain as a restricted domain, users who are assigned to this domain cannot see policies, profiles, or users configured by users associated with other security domains.

c) Click Submit.

Creating a Node Rule to Assign Access to a Node

Use this procedure to configure an RBAC node rule that assigns a physical node, such as a leaf switch, to a security domain.

Before you begin

Create a security domain to which the node will be assigned.

Step 1	On the menu bar, choose $\mathbf{Admin} > \mathbf{AAA}$.								
Step 2	In the Navigation pane, click Security.								
Step 3	In the Work pane, select the RBAC Rules tab and the Node Rules subtab.								
Step 4	In the Work pane, click the Actions icon drop-down list and select Create RBAC Node Rule.								
Step 5	From the Node ID drop-down list, select the node to be assigned.								
	Tip The Node ID drop-down list contains additional drop-down lists for sorting the nodes by ID, name, or type.								
Step 6	In the Port Rules taskbar, click the + icon and perform the following actions:								
	a) Type a Name for the RBAC node rule.								
	b) From the Domain drop-down list, select the security domain to which the node will be assigned.								
	c) Click Update.								
	d) Click Submit.								

What to do next

Assign users who will manage the node assigned to the security domain.

Configuring a User with a Security Domain

Use this procedure to add a local user as an admin in a security domain.

 \mathcal{P}

Tip This procedure shows the minimum steps for this task, omitting detailed information and optional steps. For a more detailed general procedure for adding a new local user, see Configuring a Local User Using the GUI.

Before you begin

The security domain(s) that the user will access are defined.

- **Step 1** On the menu bar, choose **Admin** > **AAA**.
- **Step 2** In the **Navigation** pane, click **Users**.

In the Work pane, verify that you are in the Local Users tab.

- **Step 3** In the **Work** pane, click the Actions icon drop-down list and select **Create Local User**.
- **Step 4** In the **STEP 1 > User Identity** dialog box, perform the following actions:
 - a) In the Login ID field, add a user ID.
 - b) In the **Password** fields, enter and confirm a password for the user.
 - c) Click Next.
- **Step 5** In the **STEP 2** > **Security** dialog box, under **Security Domain**, check the boxes for the domain 'all' and for the security domain that has the associated RBAC node rule, then click **Next**.
- **Step 6** In the **STEP 3 > Roles** dialog box, perform the following actions:

- a) In the taskbar for the domain 'all,' click the + icon to assign a role for the user in that domain.
- b) From the Role Name drop-down list, choose 'port-mgmt' and configure the Role Privilege Type as 'Write.'
- c) Click Update.
- d) In the taskbar for the security domain, click the + icon to assign a role for the user in that domain.
- e) From the Role Name drop-down list, choose 'admin' and configure the Role Privilege Type as 'Write.'
- f) Click Update.

Step 7 Click Finish.

Custom Roles and Privileges

Creating a Custom Role with Custom Privileges

Use this procedure to create a role and choose a set of privileges.

Before you begin

Refer to the set of predefined roles and privileges listed in AAA RBAC Roles and Privileges to determine which privileges should be available in the custom role. If you need read or write access to a managed object (MO) that is not exposed in a predefined privilege, you can configure a custom privilege, as described in in Configuring a Custom Privilege, on page 5.

Step 1 On the menu bar, choose **Admin** > **AAA**.

Step 2 In the **Navigation** pane, click **Security**.

- **Step 3** In the Work pane, select the Roles tab.
- **Step 4** In the **Work** pane, click on the Actions icon drop-down list and select **Create Role**.
- **Step 5** In the **Create Role** dialog box, perform the following actions:
 - a) In the Name field, type a name for the role.
 - b) From the **Privileges** table, check the box or boxes of the desired privileges for this role.
 - c) Click Submit.

What to do next

If you selected a custom privilege, such as custom-privilege-1, follow the steps in Configuring a Custom Privilege, on page 5 to choose the managed objects (MOs) that will be exposed with this custom privilege.

Configuring a Custom Privilege

Use this procedure to configure a custom privilege, providing read or read/write access to one or more managed objects (MOs) that are not exposed in a predefined privilege.

Managed object classes are described in the Cisco APIC Management Information Model Reference. For each MO class, the reference lists the predefined roles that have read or read/write privileges for that class.

For each predefined privilege, you can see a list of MO classes and the read/write permission by using the Cisco APIC Roles and Privileges Matrix.

To configure a custom privilege with read or write access permission to an MO class, you must use the APIC REST API. For instructions on using the API, see the *Cisco APIC REST API Configuration Guide*.

Compose and send an APIC REST API POST in the format below to create an object of class ada: RbacClassPriv.

Example:

```
POST https://<APIC-IP>/api/node/mo/uni/rbacdb/rbacclpriv-<moClassName>.json
```

```
{
    "aaaRbacClassPriv":
    {
        "attributes":
        {
            "name": "<moClasssName>",
            "wPriv": "<privilege>",
            "rPriv": "<privilege>"
        }
    }
}
```

In the *moClassName* value of the URI, include the name of the object class for which you are configuring access. In the payload, provide the following attributes:

- name: Name of the object class for which you are configuring access.
- wPriv: Name of the custom privilege that will include write access to objects of the class.
- rPriv: Name of the custom privilege that will include read access to objects of the class.

To assign read and write access to a custom privilege, enter the name of the custom privilege in both wPriv and rPriv.

Example

This example shows how to configure the custom privilege custom-privilege-1 with both read and write access to objects of the class fabric:Pod.

POST https://apic-aci.cisco.com/api/node/mo/uni/rbacdb/rbacclpriv-fabricPod.json

```
{
    "aaaRbacClassPriv":
    {
        "attributes":
        {
            "name": "fabricPod",
            "wPriv": "custom-privilege-1",
            "rPriv": "custom-privilege-1"
        }
    }
}
```

What to do next

Add the custom privilege to a custom role, using the procedure described in Creating a Custom Role with Custom Privileges, on page 5.

Use Case Example of Configuring an RBAC Node Rule

This section explains a use case that has a mix of configuration options described in this document. See the other parts of this document for information about each option. The use case is based on the following scenario:

Imagine that you have multiple tenants and multiple leaf nodes in your Cisco Application Centric Infrastructure (ACI) fabric. For multi-tenancy, you want to allow a user to manage a specific tenant and a specific set of leaf nodes only. For example:

- User1 can manage only Tenant1, leaf node 101 and 102.
- User2 can manage only Tenant2, leaf node 201 and 202.

The following figure illustrates the requirements:



This can be achieved by using security domains and RBAC node rules. At a high level, the configuration steps are as follows:

- **1.** Create security domains
- 2. Create RBAC node rules

3. Create users



The following figure illustrates the relationship between the configurations for User1 in this example:

User1 has three security domains:

- Domain all with port-mgmt role: Enables User1 to manage ports related configuration on the assigned leaf nodes.
- Domain Tenant1 with admin role: Enables User1 to manage Tenant1.
- Domain Leaf100 with admin role: Enables User1 to manage Leaf101 and 102.

The following figure illustrates the relationship between the configurations for User2 in this example:



User2 has three security domains as well:

- Domain all with port-mgmt role: Enables User2 to manage ports related configuration on the assigned leaf nodes.
- Domain Tenant2 with admin role: Enables User2 to manage Tenant2.
- Domain Leaf200 with admin role: Enables User2 to manage Leaf201 and 202.

The following subsections explain the configuration steps in greater detail. The sections describe only the configurations for User1 and Tenant1. The configurations for User2 and Tenant2 follow the same process.

Step 1: Create Security Domains

The first step is to create the security domains: Tenant1 and Leaf100. Although you can combine these security domains, this example uses separate security domains.

To create the domains, in the GUI, go to Admin > AAA > Security > Security Domains > Create Security Domain.

cisco	APIC					admi	. Q 🖸 🖏	00
System	Tenants	Fabric	Virtual Networking	Admin Operations	Apps Integrations			
	AAA	I Schedulers	I Firmware I E	xternal Data Collectors Config	Rollbacks Import/Export			
ала		090	User Mana	agement - Security				
O Quick S	Start			Management Sett	inge Security Domaine	Poles PRAC Pula	o Dublic Kou M	
Authen	tication			management Sett	Security Domains	Noies Rond Role:	s Public Key M	
Users	v J		Name		Des	cription	Create	Security Domain
			ACI-SCVM	M			Delete	
			ACI-VDS					
			al					
			common					
			mgmt					
				Name: Description: Restricted Domain:	Tenantil : optional : No Yes]	
					Create Security D	omain		08
					Name: Le	af100		
					Description: Op	tional		
					Restricted Domain:	No Yes		
					\square			
					_			

Cancel Submit

In this example, **Restricted Domain** is set to **Yes** for security domain Leaf100, which prevents that User1 from seeing the interface policy group, VLAN pool, and other access policies created by other users in different security domains. Exceptions are the default interface policies. Regardless of the **Restricted Domain** configuration, default interface policies are visible to the leaf RBAC user. That said, if **Restricted Domain** is enabled, the user cannot make a change to the configuration of the default policies.

The **Restricted Domain** is not enabled for security domain Tenant1. For tenant policies, the tenant itself provides enough management isolation, hence it is not required. If you use the same security domain for both tenant RBAC and node RBAC, then enabling the **Restricted Domain** may be required.

For the tenant RBAC, a tenant must be associated to a security domain. This example associates Tenant1 to security domain "Tenant1." To associate the domains, in the GUI, go to **Tenant > Policy > Security Domains**.

cisco	APIC								ad	imin Q	0 💱 🤇	•
System	Tenants	Fabric	Virtual Netwo	orking	Admin	Operations	Apps	Integra	ations			
	ААА	Schedulers	I Firmware	Extern	nal Data Collect	tors Config F	Rollbacks	I Import/Exp	port			
		User Mar	lagement - Se	ecurity							G	
Authent	ication		N	lanagem	ent Settings	Security D	omains	Roles	RBAC R	ules Pr	ublic Key Mana	gement
Security	1										0.	· **-
🚞 Users		 Name 					Descr	ription				
		ACI-SCVN	IM									
		ACI-vDS										
		all										
		common										
		mgmt										
		Tenant1										
		User1	•									
		До	DIC						adn	nin 🗿 (• • ••	
	CI	sco /										
	Sy	stem Te	nants Fabri	ic V	irtual Netwo	orking Adm	nin Op	erations	Apps	Integrat	ions	
	ALL	TENANTS I	Add Te I	Tenant S	earch: name c	or descr	l comm	non I Ten	ant1 I tena	int1 PB	R I mgmt	
	Tena	ant1	na	To To	nont Too							~ ~
		Outer Store		v ⊺e	nant - Tena	anti						00
	, ∎	Tenant1		< s	ummary	Dashboard	Policy	Operatio	nal Sta	its Hea	Ith Faults	н>
	~	Application	n Profiles	8	🗊 🛆 🕐		_				0 <u>+</u>	**-
	>	Networkin	9	Prope	erties							
	2	Contracts			,	Name: Tenant1						
	Ś	Services			Descri	iption: optional						
		Security		1								
					Annota	ations: 🖶 Click t	to add a new	annotation			_	
					Global	Alias:						
						GUID:						÷ +
						 Provide 	r	GUID		Ac	count Name	
						Associ	ate to	Tena	nt1 wi	th		
						Securit		main "	Tenan	+1"		
			1			Securi	UY DOI	nain	Terial			
					Monitoring F	Policy: select a va	alue					
				(Security Dor	mains:					ſ	計 十
						 Name 			Des	cription		
						Tenant1						
				``								

Step 2: Create RBAC Node Rules

The next step is to create RBAC node rules to add Leaf101 and Leaf102 to security domain Leaf100. To create the RBAC node rules, in the GUI, go to Admin > AAA > > Security > RBAC Rules > Node Rules > Create RBAC Node Rule.

The following figure shows the RBAC rule for node 101:

cisco	APIC					admin 🔍	0 6 0
System	Tenants	Fabric	Virtual Networking	Admin Operatio	ns Apps	Integrations	
	ААА	Scheduler	rs Firmware External	Data Collectors Co	onfig Rollbacks	Import/Export	
^{AAA} ((090	User Ma	nagement - Security		_		800
C Quick S	Start		Management Settings	Security Domains	Roles	RBAC Rules Publi	c Key Management
Security	y			Explicit Rules	Implicit Rules	Implicit Partial Rule	s Node Rules
Users	_					ſ	0 ± %-
		Node ID					Create RBAC Node Rule
				No items h Select Actions t	ave been found. o create a new item.		Delete
	rooto DR		lo Pulo			0	
		Node ID: 101				U	
	Po	rt Rules:				Û	+
		Na 10	me Domain 1 Leaf10	n 00			
		Creat	e RBAC Node Rul	e			? ×
			Node ID: 102 Port Rules:				☆ +
			Name	Domain			
			102	Leaf100			
						Canc	el Submit

Repeat the same configuration for node 102.

Step 3: Create Users

The last step is to create a user: User1. To create the user, in the GUI, go to Admin > AAA > Users > Create Local User.

At the Security and Roles configuration steps, choose the following security domains and roles:

.

- all: Role port-mgmt with the Write privilege
- Leaf100: Role admin with the Write privilege
- Tenant1: Role admin with the Write privilege

You can use the same configuration for remote users, using either Cisco AVPairs or LDAP group maps, using the procedure described in the "RADIUS, TACACS+, LDAP, RSA, SAML, OAuth 2, and DUO" chapter.

cisco	APIC					admin Q		
System	Tenants	Fabric	Virtual Networking	Admin Opera	tions Apps	Integrations		
	AAA	Schedulers	s Firmware Extern	al Data Collectors	Config Rollbacks	I Import/Export		
AA () O Quick SI	tart ication	Users				Local Us	Remote Users	9
Users		 Login I 	D First Nam	e Last N	ame	Email	Pic Create Local User	
		admin						
	Creat	e Local	User					?×
	STEP 3	> Roles			1. User Identity	/ 2. Set	3. Roles	
	(Domair	n all:				ī	+
			Role Name		R	ole Privilege Type	_	
	1		port-mgmt		V	Vrite		
	(Domain Leaf	100:				1	+
			Role Name		R	ole Privilege Type		
	1		admin		V	Vrite		
	(Domain Tena	int1:				1	+
			Role Name		R	ole Privilege Type		
	1		admin		V	Vrite		

Verifying the RBAC Node Rule

User1 can manage only Tenant1, Leaf 101 and 102. For example:

• User1 cannot see other tenants other than Tenant1 with write privilege and the common tenant with read privilege.

- User1 cannot see other leaf nodes other than Leaf101 and 102 in Leaf Selectors.
- User1 cannot see access policies other than those created by users associated with the same security domain, or system-created policies (read-only).

cisco APIC					
System Tenants Fabric	Virtual Networking	Operations	Apps Integration	s	
ALL TENANTS Add Tenant Tenant	Search: name or descr	I common I Tenar	x1		
All Tenants					
▲ Name	Alias	Descriptio	n	Bridge Domains	
common		Tenant Crea	ated Using Ansible	1	
Tenant1				0	
cisco APIC					
System Tenants Fabric	Virtual Letworking	Operations 4	nns Integrations		
Invento y I Access Po	licies	operations	integrations		
Policies					
C Oulek Start		Leaf Switches - Pro	ofiles		
Switches					
🗸 🖿 Leaf Switches	Create Leaf Prof	file			? ×
> Profiles	STEP 1 > Profile			1. Profile 2. Assoc	ciations
> Policy Groups	1				
> 💼 Spine Switches	Description:	optional	•		
> 🛅 Modules					
> Therfaces	Leaf Selectors:			-	
> Poscies		Name	Blocks	Policy Group	
> Pools	l		select switches	 select an option 	\∨
			🔄 ID 🛛 Name	Profiles	
			🔲 101 Pod1-Le	eaf1	
			102 Pod1-L	eaf2	
	-				