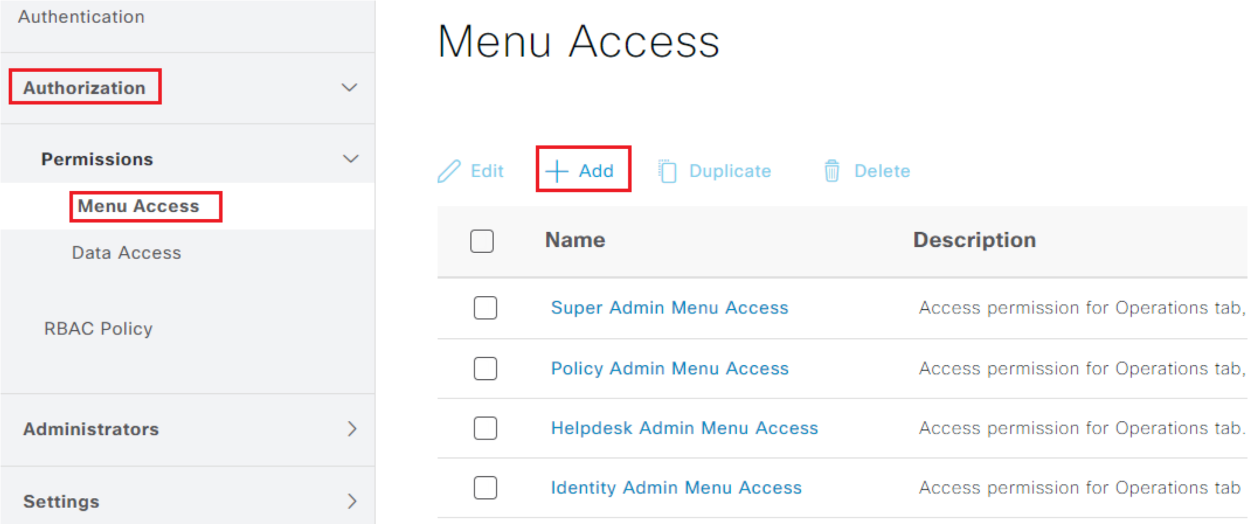
Configure Permissions:

There are two types of permissions in Cisco ISE that can be configured for a user group:

Menu Access:

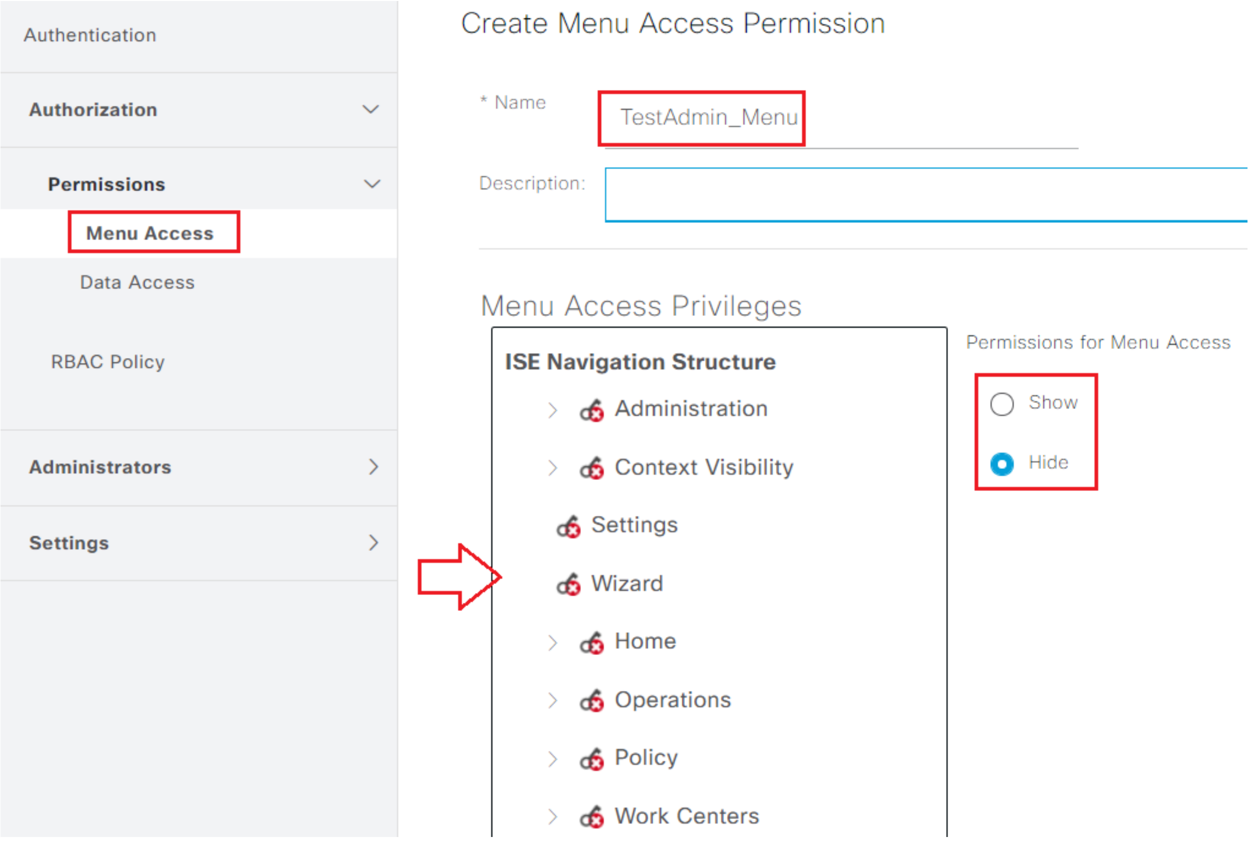
Menu Access controls the navigational visibility on ISE. There are two options for every tab, Show or Hide, that can be configured. A Menu Access rule can be configured to show or hide selected tabs. In order to configure a Menu Access policy, navigate to Administration > System > Admin Access > Authorization > Permissions > Menu Access.



Menu Access

☐	Name	Description
☐	Super Admin Menu Access	Access permission for Operations tab,
☐	Policy Admin Menu Access	Access permission for Operations tab,
☐	Helpdesk Admin Menu Access	Access permission for Operations tab.
☐	Identity Admin Menu Access	Access permission for Operations tab

Click Add. Each navigational option in ISE can be configured to be shown/hidden in a policy.



Create Menu Access Permission

* Name: TestAdmin_Menu

Description:

Menu Access Privileges

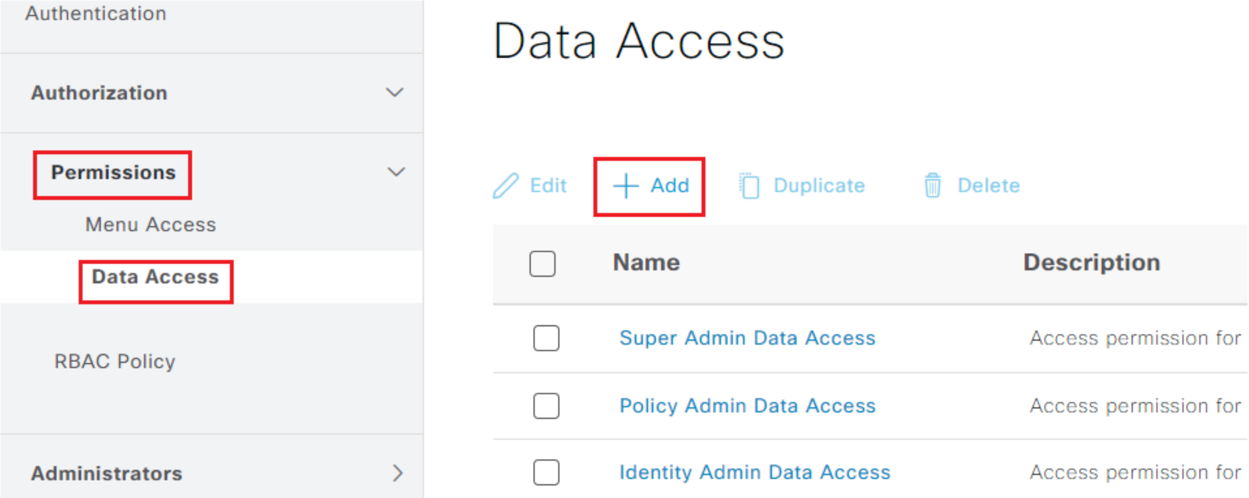
Permissions for Menu Access

○ Show

● Hide

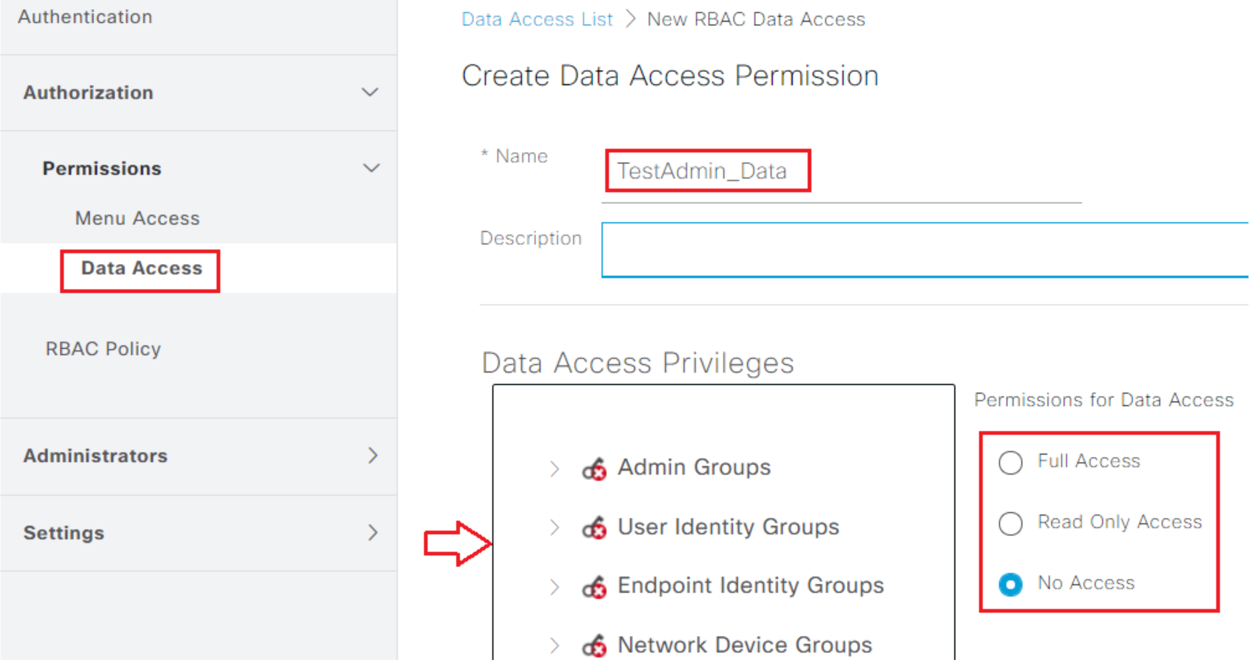
Data Access:

Data Access controls the ability to read/access/modify the Identity Data on ISE. Access permission can be configured only for Admin Groups, User Identity Groups, Endpoint Identity Groups, and Network Device Groups. There are three options for these entities on ISE which can be configured. They are Full Access, Read-Only Access, and No Access. A Data Access rule can be configured to choose one of these three options for each tab on ISE. Menu Access and Data Access policies must be created before they can be applied to any admin group. There are a few policies that are built-in by default but they can always be customized or a new one can be created. In order to configure Data Access policy, navigate to Administration > System > Admin Access > Authorization > Permissions > Data Access.



□	Name	Description
□	Super Admin Data Access	Access permission for
□	Policy Admin Data Access	Access permission for
□	Identity Admin Data Access	Access permission for

Click Add to create new policy and configure permissions to access Admin/User Identity /Endpoint Identity/Network Groups.



Create Data Access Permission

* Name TestAdmin_Data

Description

Data Access Privileges

Permissions for Data Access

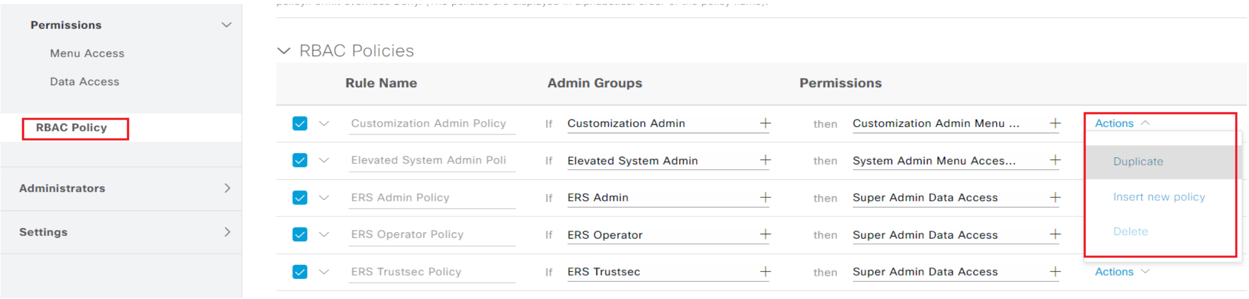
○ Full Access

○ Read Only Access

● No Access

Configure RBAC Policies:

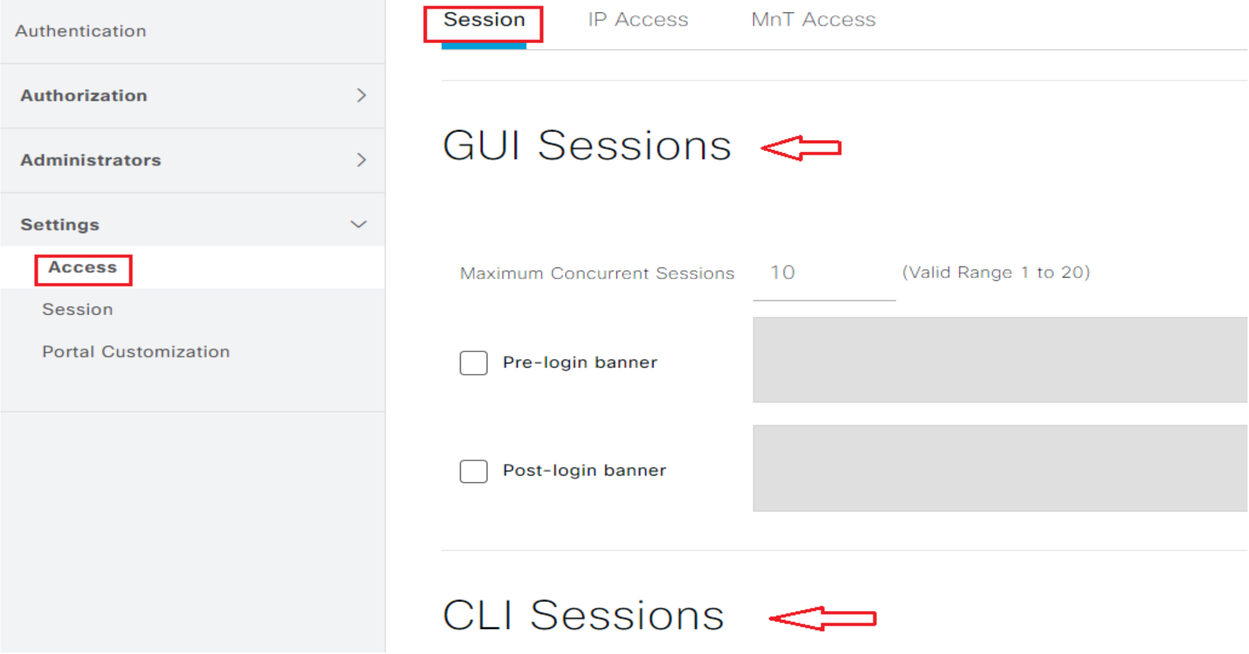
RBAC stands for Role-Based Access Control. Role (Admin Group) to which a user belongs can be configured to use the desired Menu and Data Access policies. There can be multiple RBAC policies configured for a single role OR multiple roles can be configured in a single policy to access Menu and/or Data. All of those applicable policies are evaluated when an admin user tries to perform an action. The final decision is the aggregate of all policies applicable to that role. If there are contradictory rules which permit and deny at the same time, the permit rule overrides the deny rule. System-created and default policies cannot be updated, and default policies cannot be deleted. Multiple Menu/Data Access permissions cannot be configured in a single rule. To configure these policies, navigate to Administration > System > Admin Access > Authorization > RBAC Policy. Click Actions to Duplicate/Insert/Delete a policy.



	Rule Name		Admin Groups		Permissions	
☑	Customization Admin Policy	If	Customization Admin	then	Customization Admin Menu ...	Actions
☑	Elevated System Admin Poli	If	Elevated System Admin	then	System Admin Menu Acces...	
☑	ERS Admin Policy	If	ERS Admin	then	Super Admin Data Access	
☑	ERS Operator Policy	If	ERS Operator	then	Super Admin Data Access	
☑	ERS Trustsec Policy	If	ERS Trustsec	then	Super Admin Data Access	Actions

Configure Settings for Admin Access:

In addition to the RBAC policies, there are a few settings that can be configured which are common to all the admin users. In order to configure the number of Maximum Sessions Allowed, Pre-login, and Post-login Banners for GUI and CLI, navigate to Administration > System > Admin Access > Settings > Access. Configure these under the Session tab.



GUI Sessions

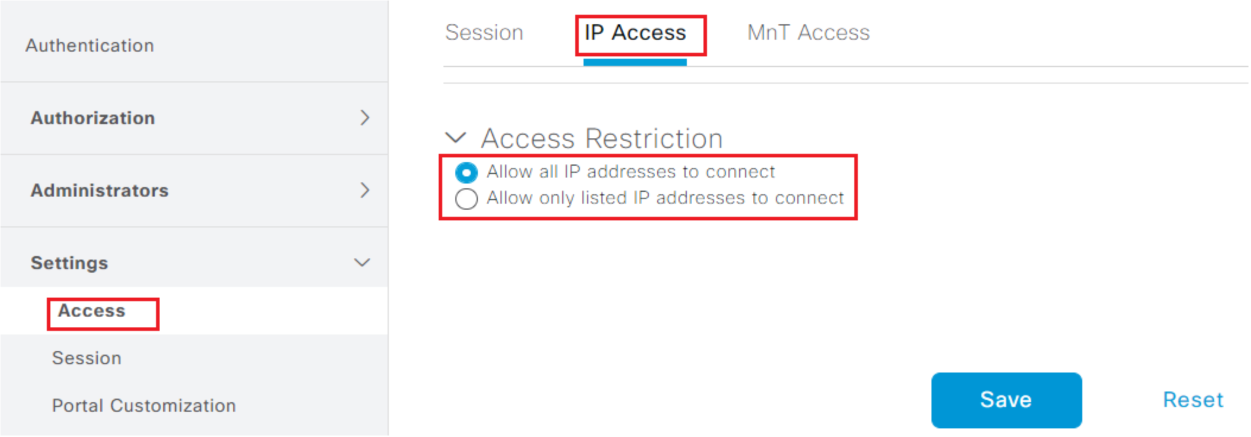
Maximum Concurrent Sessions 10 (Valid Range 1 to 20)

□ Pre-login banner

□ Post-login banner

CLI Sessions

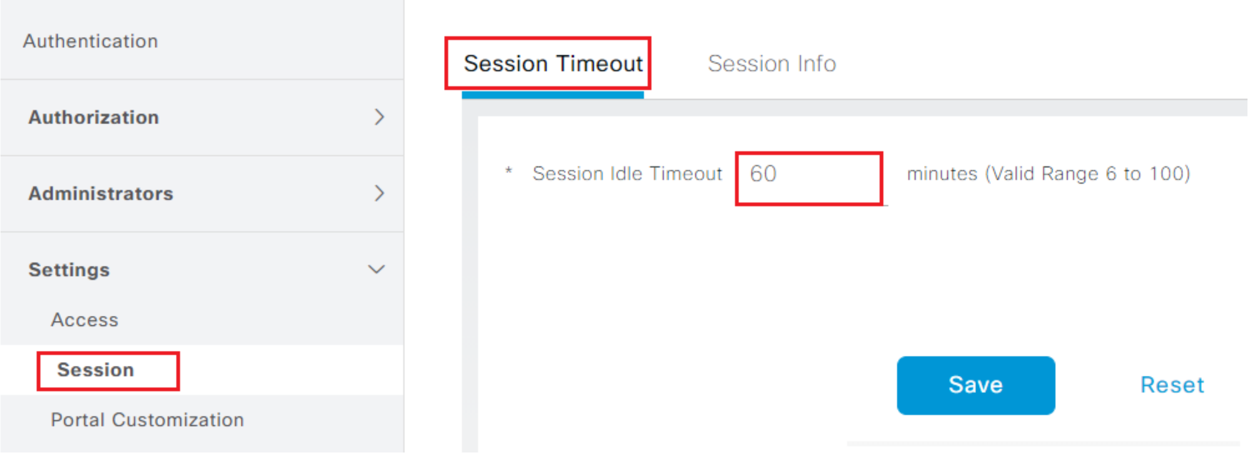
To configure the list of IP addresses from which the GUI and the CLI can be accessed, navigate to Administration > System > Admin Access > Settings > Access & navigate to the IP Access tab.



Access Restriction

● Allow all IP addresses to connect
○ Allow only listed IP addresses to connect

In order to configure a timeout value due to the inactivity of a session, navigate to Administration > System > Admin Access > Settings > Session. Set this value under the Session Timeout tab.



* Session Idle Timeout 60 minutes (Valid Range 6 to 100)