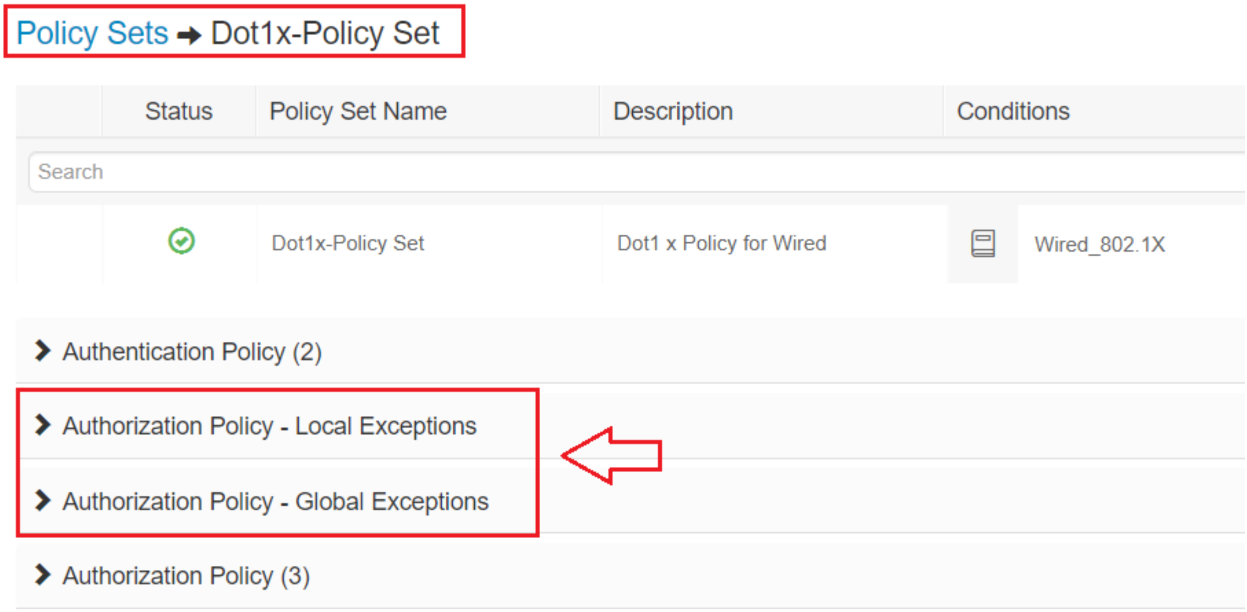
Authorization Policies:

Authorization policies are a component of the Cisco ISE network authorization service. This service allows you to define authorization policies and configure authorization profiles for specific users and groups that access your network resources. Authorization policies can contain conditional requirements that combine one or more identity groups using a compound condition that includes authorization checks that can return one or more authorization profiles. Authorization profiles are used when creating authorization policies in ISE. An authorization policy is composed of authorization rules. Authorization rules have three elements: name, attributes, and permissions. The permission element maps to an authorization profile.

Field Name	Description
Status	Enabled: This policy condition is active. Disabled: This policy condition is inactive and will not be evaluated. Monitor Only: This policy condition will be evaluated, but the result will not be enforced.
Rule Name	Enter a unique name for this policy.
Conditions	From a new policy row, click the plus (+) icon or from an existing policy row, click the Edit icon to open the Conditions Studio.
Results or Profiles	Select the relevant authorization profile, which determines the different levels of permissions offered to the configured security group. If you have not yet configured the relevant authorization profile, you can do so inline.
Results or Security Groups	Select the relevant security group, which determines the groups of users relevant to the specific rule. If you have not yet configured the relevant security group, you can do so inline.
Results or Command Sets	Command sets enforce the specified list of commands that can be executed by a device administrator. When a device administrator issues operational commands on a network device, ISE is queried to determine whether the administrator is authorized to issue these commands.
Results or Shell Profiles	TACACS+ shell profiles control the initial login session of the device administrator.
Hits	Hits are indicating the number of times the conditions have matched.
Actions	Click cog icon from the Actions column to view and select different actions: Insert new row above: Insert a new authorization rule above the rule from which you opened the Actions menu. Insert new row below: Insert a new authorization rule below the rule from which you opened the Actions menu. Duplicate above: Insert a duplicate authorization rule above the rule from which you opened the Actions menu, above the original set. Duplicate below: Insert a duplicate authorization rule below the rule from which you opened the Actions menu, below the original set. Delete: Delete the rule.

Authorization Policy Exceptions:

Within each policy set, you can define regular authorization policies, as well as local exception rules and global exception rules. Global authorization exception policies enable you to define rules that override all authorization rules in all of your policy sets. The local authorization exception rule overwrites the global exception rule. The authorization rules are processed in the following order: first the local exception rule, then the global exception rule, and finally, the regular rule of the authorization policy.



Policy Sets → Dot1x-Policy Set

	Status	Policy Set Name	Description	Conditions
	✓	Dot1x-Policy Set	Dot1 x Policy for Wired	Wired_802.1X

Search

› Authentication Policy (2)

› Authorization Policy - Local Exceptions

› Authorization Policy - Global Exceptions

› Authorization Policy (3)

Authorization Policy—Local Exceptions:

Use Authorization Policy-Local Exception section to configure local authorization exception rules that are specific to a policy set.

Authorization Policy—Global Exceptions:

You can use Authorization Policy-Global Exceptions section to configure global authorization exception rules that are shared across all policy sets.