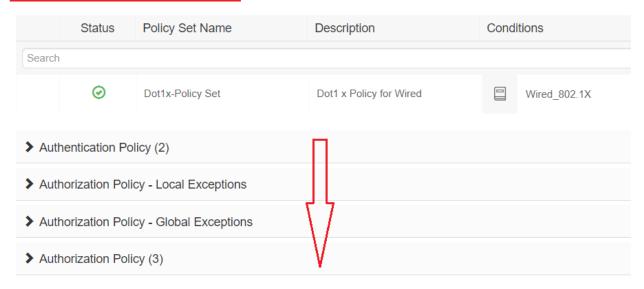
## **Policy Sets:**

Policy sets (both network access and device administration sets) enable you to logically group authentication and authorization policies within the same set. You can have several policy sets based on an area, such as policy sets based on location, access type and similar parameters. When you install ISE, there is always one policy set defined, which is the default policy set, and the default policy set contains within it, predefined and default authentication, authorization and exception policy rules. When creating policy sets, you can configure these rules (configured with conditions and results) in order to choose the network access services on the policy set level, the identity sources on the authentication policy level, and network permissions on the authorization policy levels. You can define one or more conditions using any of the attributes from the Cisco ISE-supported dictionaries for different vendors. Cisco ISE allows you to create conditions as individual policy elements that can be reused.

Policy Set Configuration Settings	
Fields 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 not be evaluated.
Policy Set Name	Enter a 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.
Description	Enter a unique description for the policy.
Allowed	Choose an allowed protocol that you have already created, or click the (+)
Protocols or	sign to Create a New Allowed Protocol , to Create a New Radius
Server Sequence	Sequence, or to Create a TACACS Sequence.
Conditions	From a new exceptions row, click the plus (+) icon or from an existing
	exception row, click the Edit icon to open the Conditions Studio.
Hits	Hits are indicating the number of times the conditions have matched.
	Hover over the icon to view when this was last updated, reset to zero and
	to view the frequency of updates.
Action	Click the cog icon from the Actions column to view and select different
	actions:
	Insert new row above: Insert a new policy above the policy from which
	you opened the Actions menu.
	Insert new row below: Insert a new policy below the policy from which
	you opened the Actions menu.
	Duplicate above: Insert a duplicate policy above the policy from which
	you opened the Actions menu, above the original set.
	Duplicate below: Insert a duplicate policy below the policy from which
	you opened the Actions menu, below the original set.
	Delete: Delete the policy set.
View	Click the arrow icon to open the Set view of the specific policy set and
	view its authentication, exception, and authorization sub-policies.

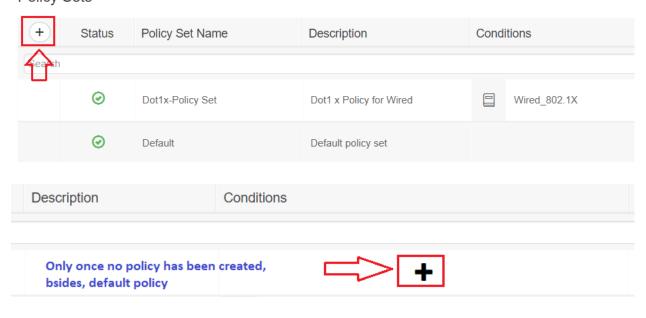
In short, Policy Set is a hierarchical container that is used to logically group authentication and authorization policies. Policy Sets are different collections of Authentication Rules and Authorization Rules that apply to various use-cases in the ISE deployment. The default policy set implemented at initial Cisco ISE installation includes the default ISE authentication and authorization rules. The policy sets reside in an ordered list. The matching criteria are evaluated top-down, with the first matching policy set being selected. The Policy Sets tab under Policy provides an interface to configure authentication and authorization policy for network access control in Cisco ISE.

# Policy Sets → Dot1x-Policy Set



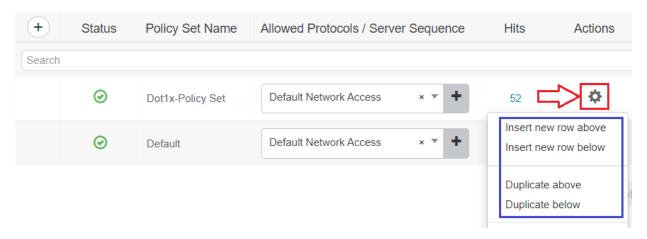
You can still click the check box to add a new Policy Set.

#### Policy Sets



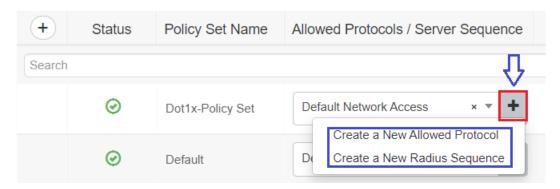
If you want to duplicate a policy set above or below an existing policy set, click on the gear next to the existing policy set.

#### Policy Sets



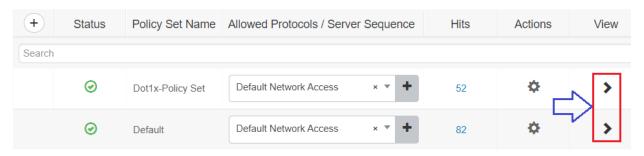
If you would like to create a new Allowed Protocols list, check the + sign next to the box for it and you'll be able to create one on the fly without having to exit Policy Sets.

### Policy Sets



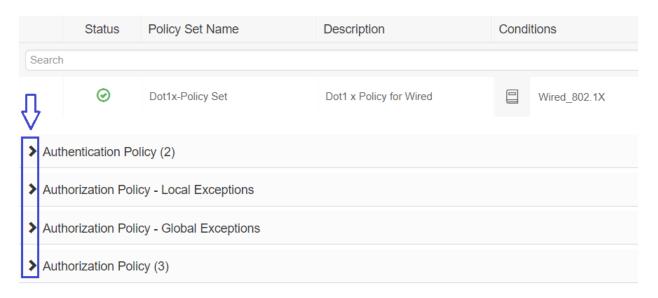
If you want to view the Authentication/Authorization rules, you would click on the Arrow on the right side to go into that specific policy set.

#### **Policy Sets**



You will notice there are a few things different right away. The policies are all collapsed by default but you can easily expand them. You now have a Local Exceptions as well as a Global Exceptions policy if you choose to use it.

Policy Sets → Dot1x-Policy Set



The Authentication Policy Arrow has been click the policy expand.

