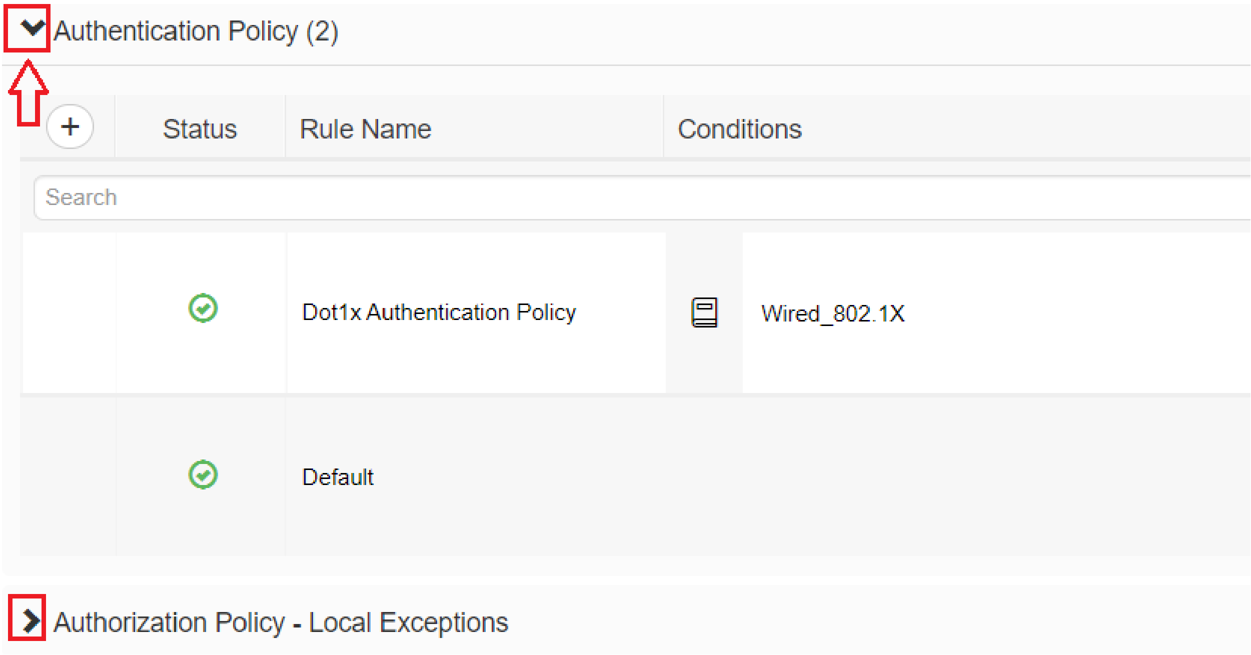
Authentication Policies:

Each policy set can contain multiple authentication rules that together represent authentication policy for that set. Priority of the authentication policies is determined based on the order to those policies as they appear within the policy set itself. You can define one or more conditions using any of the attributes from the Cisco ISE dictionary. Cisco ISE allows you to create conditions as individual policy elements that can be stored in the Library and then can be reused for other rule-based policies. In authentication policies, you can define multiple rules, which consist of conditions and results. ISE evaluates the conditions that you have specified and based on the result of the evaluation, assigns the corresponding results. The identity database is selected based on the first rule that matches the criteria. If you choose the identity method as deny access, a reject message is sent as a response to the request. If you choose an identity database or an identity source sequence and the authentication succeeds, the processing continues to the authorization policy configured for the same policy set.

Reject	Send Access-Reject back to the Network Access Device
Drop	Do not respond to the Network Access Device
Continue	Continue to the authorization policy regardless of authentication pass/fail

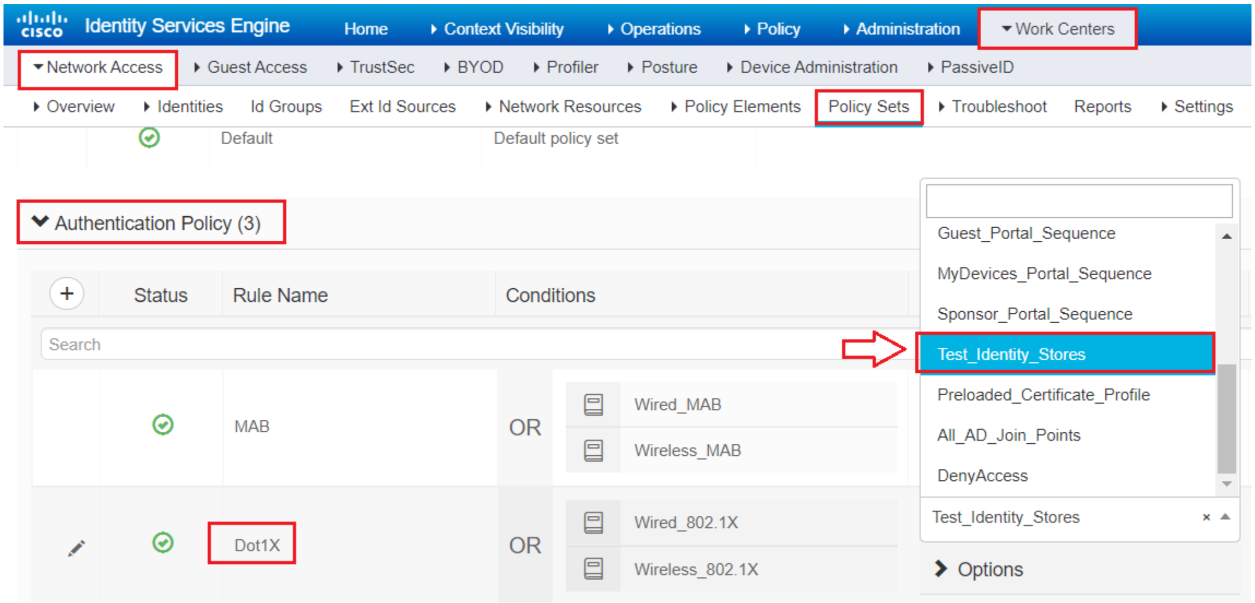
Field Name	Description
Status	Choose the status of this policy. It can be one of the following: Enabled: This policy condition is active. Disabled: This policy condition is inactive and will not be evaluated. Monitor Only: This policy condition will be evaluated, but the result will not be enforced.
Rule Name	Enter a name for this authentication 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.
Use	Choose the identity source that you want to use for authentication.
Options	Define a further course of action for authentication failure, user not found, or process failure events.
Hits	Hits are indicating the number of times the conditions have matched.
Actions	Click the cog icon from the Actions column to view and select different actions: Insert new row above: Insert a new authentication policy above the policy from which you opened the Actions menu. Insert new row below: Insert a new authentication policy below the policy from which you opened the Actions menu. Duplicate above: Insert a duplicate authentication policy above the policy from which you opened the Actions menu, above the original set. Duplicate below: Insert a duplicate authentication policy below the policy from which you opened the Actions menu, below the original set. Delete: Delete the policy set.

The Authentication Policy Arrow has been click the policy expand.



Authentication Policy (2)

Status	Rule Name	Conditions
✓	Dot1x Authentication Policy	Wired_802.1X
✓	Default	



	Default	Default policy set
✓	Default	Default policy set

Authentication Policy (3)

Status	Rule Name	Conditions
✓	MAB	OR Wired_MAB Wireless_MAB
✓	Dot1X	OR Wired_802.1X Wireless_802.1X