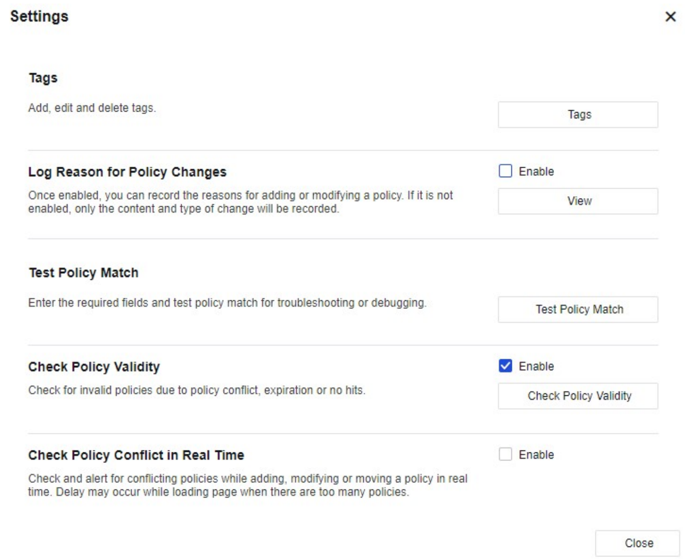


Settings ×

Tags

Add, edit and delete tags.

Log Reason for Policy Changes

□ Enable

Once enabled, you can record the reasons for adding or modifying a policy. If it is not enabled, only the content and type of change will be recorded.

Test Policy Match

Enter the required fields and test policy match for troubleshooting or debugging.

Check Policy Validity

☑ Enable

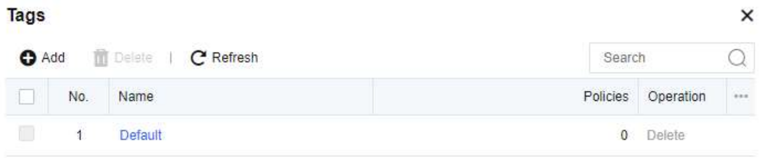
Check for invalid policies due to policy conflict, expiration or no hits.

Check Policy Conflict in Real Time

□ Enable

Check and alert for conflicting policies while adding, modifying or moving a policy in real time. Delay may occur while loading page when there are too many policies.

Tags: Set related tag operations, including adding, editing, and deleting tags. See the figure below.

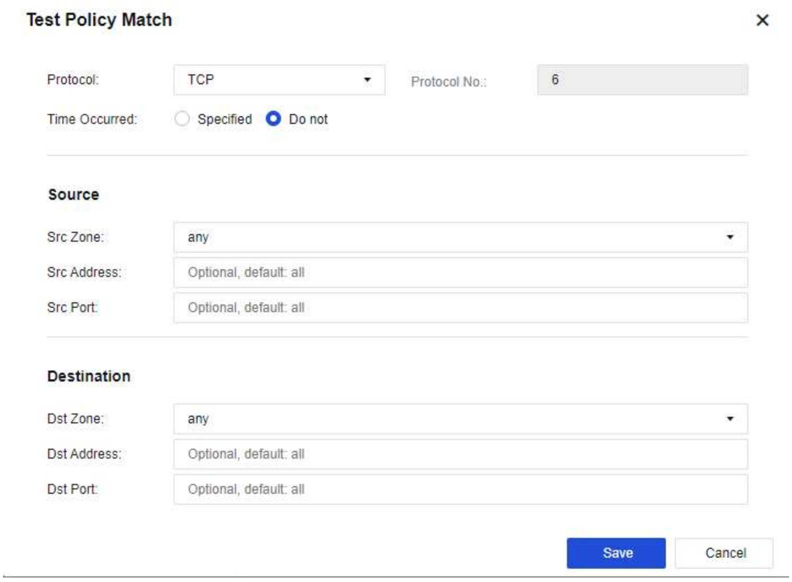


Tags ×

□	No.	Name	Policies	Operation
□	1	Default	0	Delete

Log Reason for Policy Changes: After this parameter is enabled, you can record the reasons for adding or modifying a policy. If it is not enabled, only the content and type of change will be recorded. Click **View** to go to the **Policy Lifecycle Management** page.

Test Policy Match: Tests whether the policy matches based on the quintuple. See the figure below.



Test Policy Match

Protocol: TCP
Protocol No.: 6
Time Occurred: ○ Specified ● Do not

Source

Src Zone: any
Src Address: Optional, default: all
Src Port: Optional, default: all

Destination

Dst Zone: any
Dst Address: Optional, default: all
Dst Port: Optional, default: all

Check Policy Validity: Checks invalid policies.

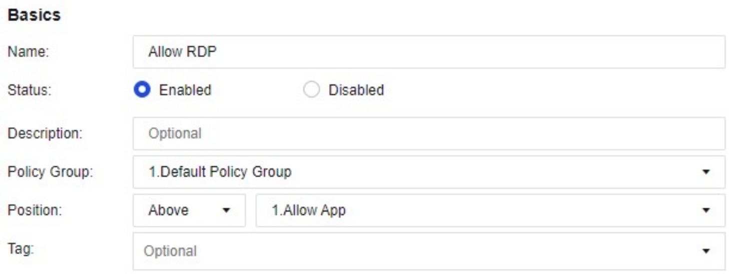
Check Policy Conflict in Real-Time: Checks and alerts for conflicting policies in real-time while adding, modifying, or moving a policy in real-time. After this function is enabled, a delay may occur while loading a page when there are too many policies.

7.2.1.1.1 Application Control Configuration case

An enterprise does not allow R&D department personnel to use IM chat tools during working hours. When R&D personnel uses IM tools, the device will refuse the request. To implement this function, you need to add an application control policy on Network Secure.

Operation Steps

Step 1. Navigate to Policy > Application Control Policy, and click Add. Then, the Add Application Control Policy dialog box appears.



Basics

Name: Allow RDP

Status: ● Enabled ○ Disabled

Description: Optional

Policy Group: 1.Default Policy Group

Position: Above 1.Allow App

Tag: Optional

The relevant parameters in the **Basics** section can be set as follows:

Name: Enter Allow RDP.

Status: Select Enabled.

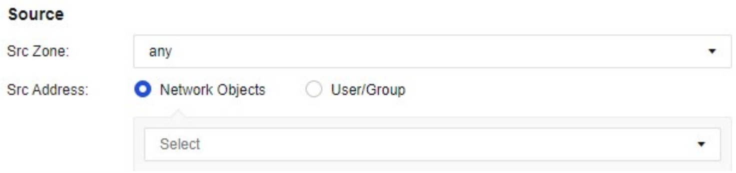
Description: Enter custom descriptions, such as Personnel in R&D Department is not allowed to use IM.

Policy Group: Select a default policy group.

Position: Set the priority before the P2P download is limited.

Tag: Enter a customizable tag or select a default one.

Step 2. Select a custom LAN zone for the Src Zone parameter. For more information about how to define a zone, see Section 5.2 Zone. Select a custom R&amp;D department for the Src Address parameter. For more information about how to define a user group, see Section 7.6.2 User Management.



Source

Src Zone: any

Src Address: ● Network Objects ○ User/Group

Select

⚠NOTICE

If the user group is selected in the current policy, you need to enable the authentication function and configured relevant authentication policies. If the authentication policy is not enabled, this application control policy will not take effect.

Step 3. Set the parameters in the Destination section: Select WAN for the Dst Zone parameter, All for the Dst Address parameter, any for the Services parameter, and Remote Login/RemoteDesktop for the Applications parameter.