Alibaba Cloud Security Center

Operation

Issue: 20200630

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Document conventions

Style	Description	Example
	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 **Notice:** If the weight is set to 0, the server no longer receives new requests.
	A note indicates supplemental instructions, best practices, tips, and other content.	 **Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings** > **Network** > **Set network type**.
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click **OK**.
Courier font	Courier font is used for commands.	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`

Style	Description	Example
{} or {a|b}	This format is used for a required value, where only one item can be selected.	switch {active|stand}

Contents

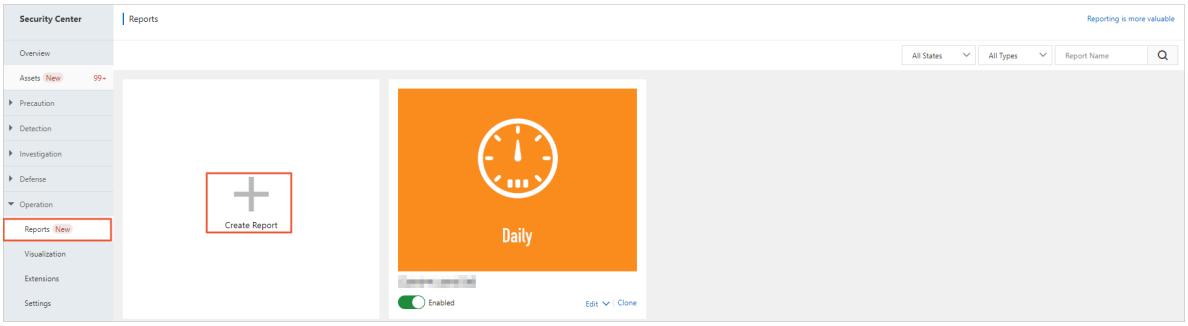
1 Security reports

Security Center Advanced and Enterprise editions support custom security reports. You can customize the data that is included in a report, and specify the email addresses of the recipients. Custom reports help you monitor the security status of your assets.

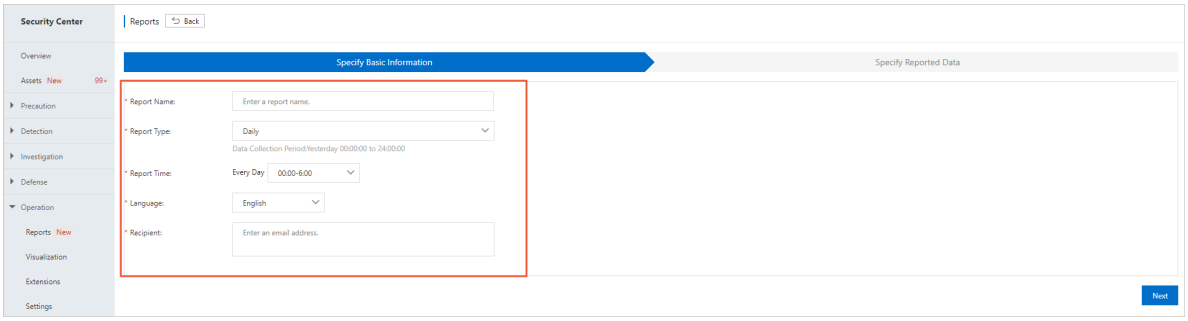
Procedure

The following procedure shows how to manage security reports in the Security Center console.

1. Log on to the Security Center console, and choose **Operation** > **Reports**.
2. On the **Reports** page, click **Create Report**.

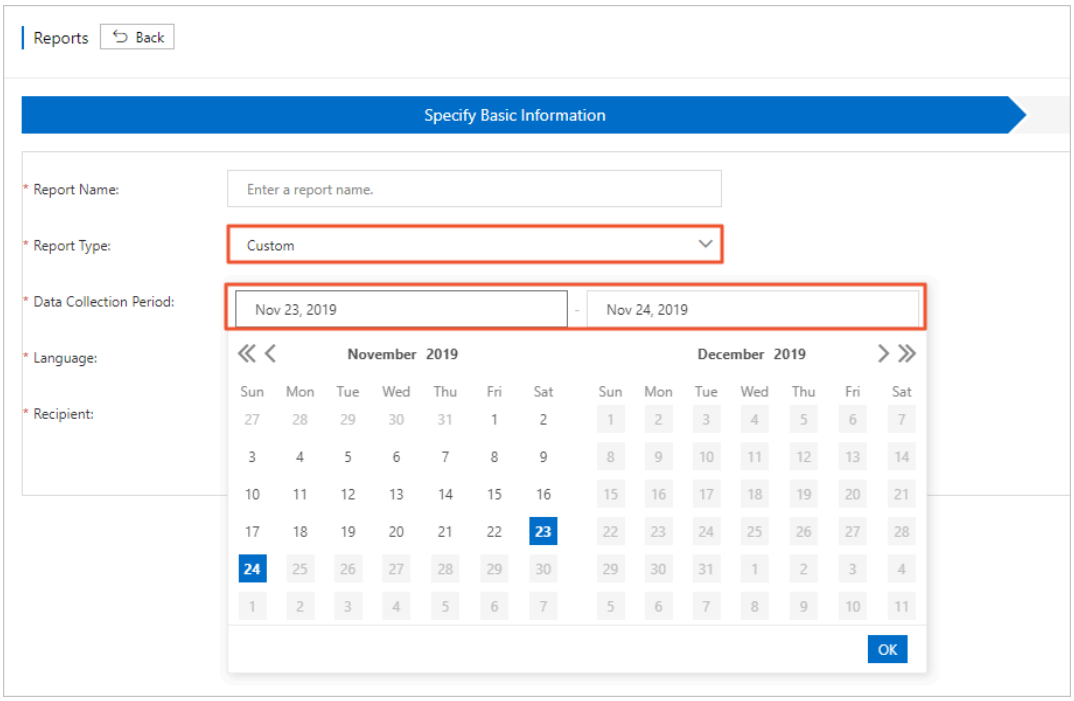


3. On the **Specify Basic Information** tab, enter the required information.



- **Report Name**: specify a name for the report.
- **Report Type**: select a report type from the drop-down list. Supported report types are Daily, Weekly, Monthly, and Custom.

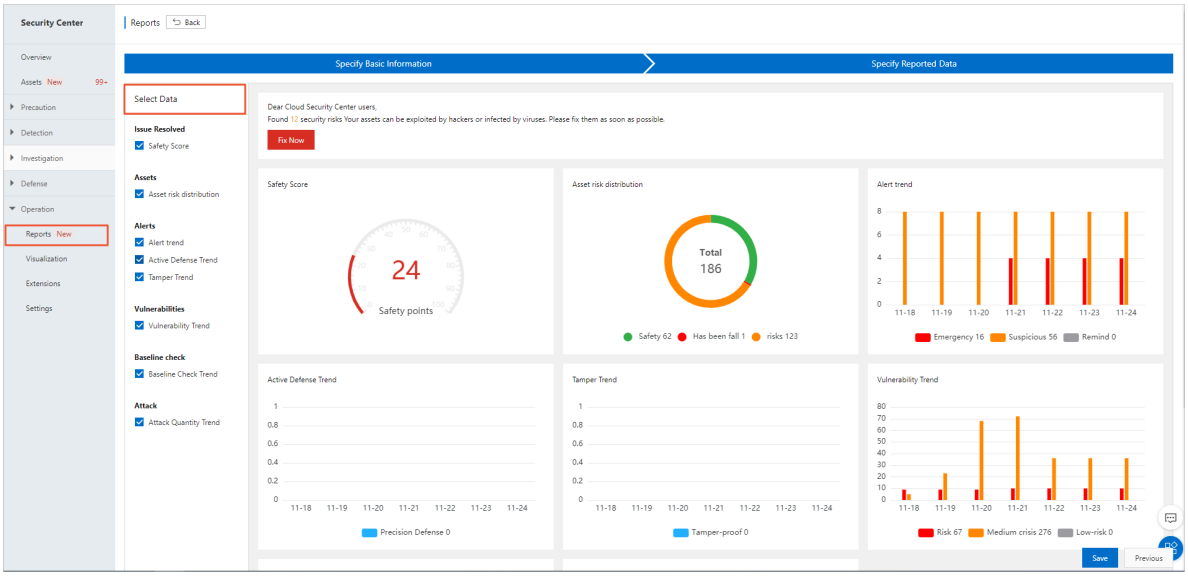
  If you select Custom, you must set the **Data Collection Period** parameter to specify the report generation cycle.



- **Report Time**: select a time period from the drop-down list. Reports are sent to you during the specified time period every day, on every Monday, or on the first day of every month. Supported time periods are 00:00-6:00, 6:00-12:00, 12:00-18:00, and 18:00-24:00.
- **Recipient**: enter the email addresses of the recipients.

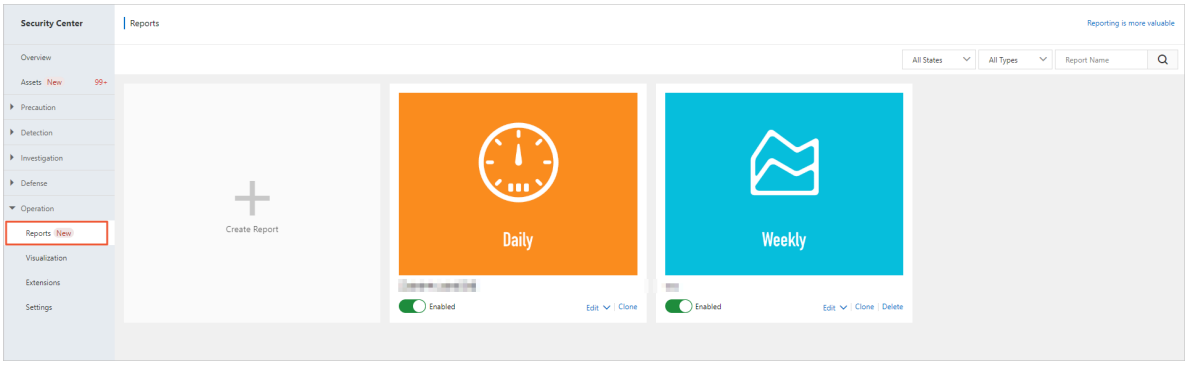
4. Click **Next**.

5. On the **Specify Report Data** tab, select the types of data that you want to display in the report. You can select assets, alerts, vulnerabilities, baseline check, attacks, and other data that relates to operations security.



6. Click **Save** to create the report.

   Reports that you have created are listed on the **Reports** page.



   By default, reports are enabled after they are created. Security Center sends reports to the specified email addresses during the specified **time period**. If you no longer need a

type of security reports, click the **Enabled** toggle under the report to disable this report type.

- By default, Security Center automatically creates a report that can be edited or cloned. However, you cannot change its **report type**.
- You can edit, clone, and delete reports.
- After you create a custom report, you can click **Send Now** to send the report to the specified recipients.
- You can filter reports by status, type, and report name.

Notice:

You can create up to nine reports, excluding the default report created by Security Center.

2 Task management

2.1 Playbook overview

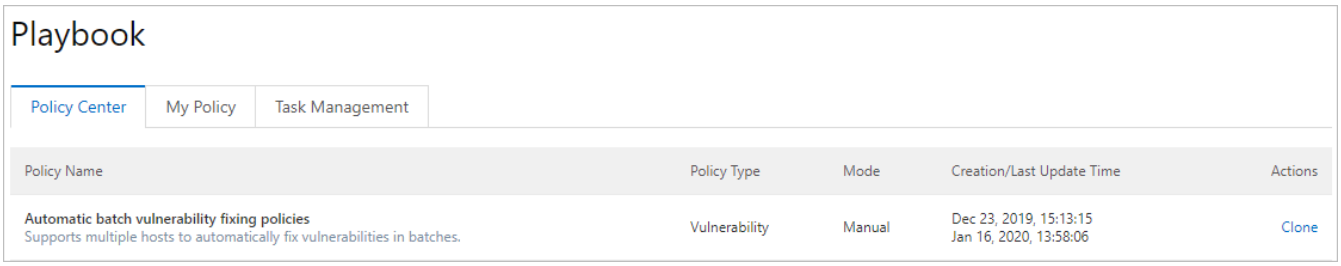
Security Center provides the playbook feature that supports automated orchestration. This feature orchestrates repetitive workload logic in responses of security events and generates automated processing policies accordingly. This helps you reinforce system security. After you create a task, the playbook runs the task on the specified assets. This topic describes the policy center, my policy, and task management functions.

Background

The playbook feature is supported by the Enterprise edition only.

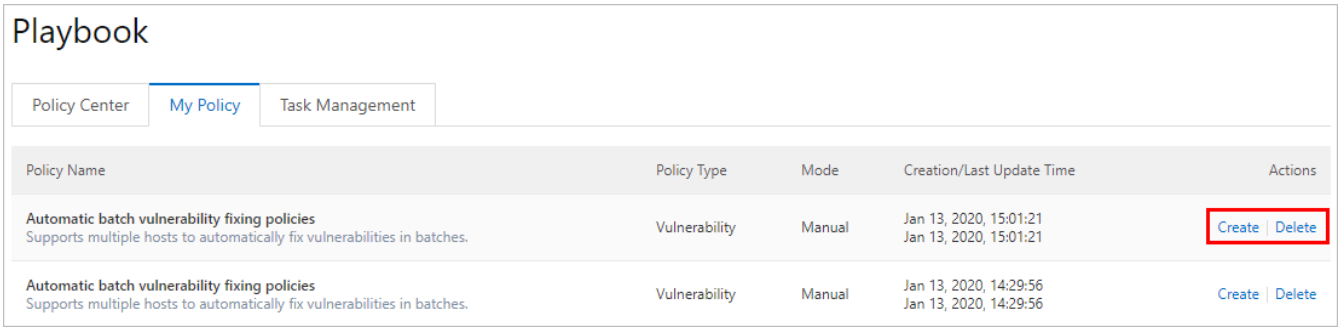
Policy center

The **Policy Center** tab provides the template of **Automatic Batch Vulnerability Fixing Policies**. This type of policy automatically fixes vulnerabilities on multiple hosts. On this page, you can quickly create policies by using this template. In the Actions column, click **Clone** to create a new policy and add it to the **My Policy** tab.



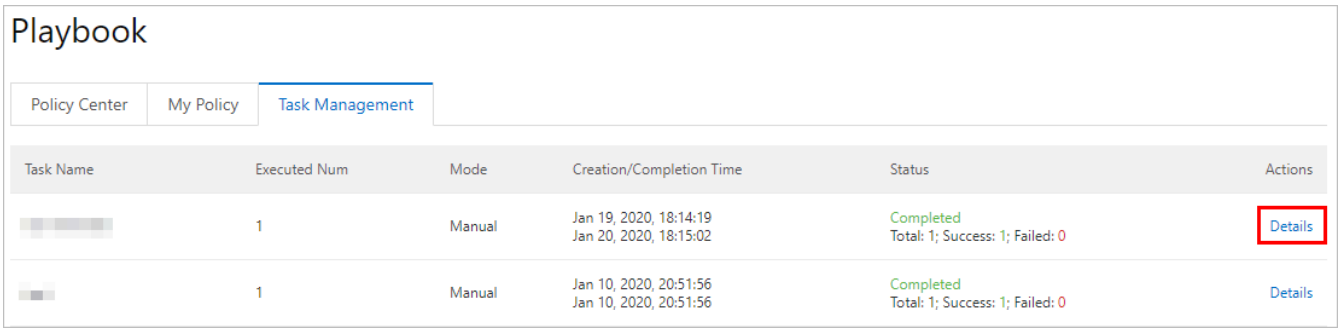
My policy

The **My Policy** tab displays information about all automation policies that you have created. The information includes the policy name, policy type, mode, creation time, and last update time. On this tab, you can create tasks under an existing policy. For more information, see Create a task.



Task management

The **Task Management** tab displays the information about all tasks that you have created. The information includes the task name, the number of times that a task has been executed, mode, creation time, completion time, and task status. You can view details of tasks that you have created on this tab. For more information, see #unique_7.



2.2 Create a task

When you create a task, you can set parameters to have the playbook automatically run the task on the specified assets. This helps you reinforce system security. This topic describes how to create a task.

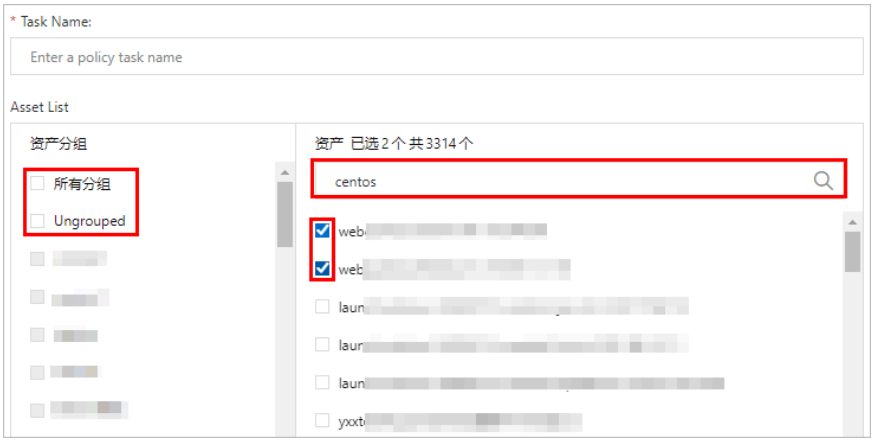
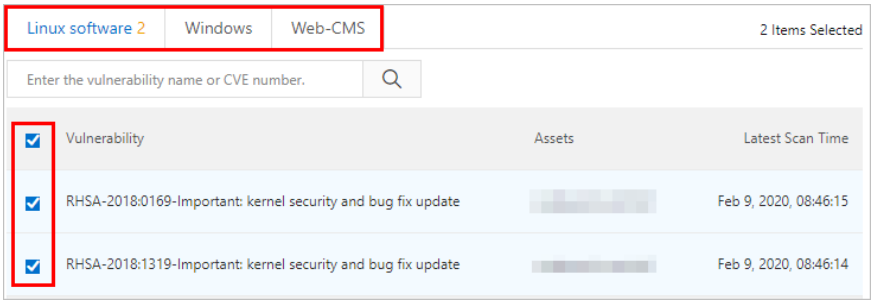
Prerequisites

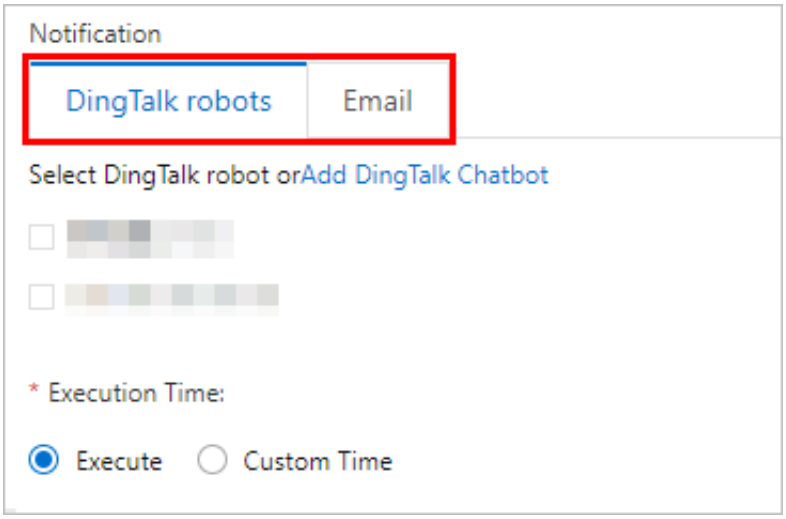
You have created a policy by using the policy template provided by the policy center. To create a policy, navigate to the **Playbook** > **Policy Center** page, find the template, and then click **Clone** in the Actions column.

Procedure

1. Log on to the Security center console.
2. In the left-side navigation pane, choose **Playbook** > **My Policy**.
3. On the **My Policy** tab, find the target policy and click **Create** in the Actions column.

4. On the **Create** page, set the following parameters.

Parameter	Description
Task Name	Specify a name for the task.
Asset List	Follow these steps to select the target assets where you want to run the task. You can select one or more assets from different asset groups, or directly select asset groups. • In the **Asset List**, select the target asset groups from the **Asset Groups** list. All assets in the selected groups are automatically selected. You can select and remove assets from the **Selected Assets** list on the right side. • You can also enter an asset name in the search box in the **Selected Assets** list to search for specific assets. Fuzzy match is supported. Select the target assets from the search results. **Note:** The task runs only on the **Selected Assets**. 
Vulnerability	Select the vulnerabilities that you want to fix. You can view vulnerabilities on the **Linux software**, **Windows**, or **Web-CMS** tab. **Note:** Each tab displays the vulnerabilities in the selected assets. 

Parameter	Description
Notification	**DingTalk Chatbots** and **Emails** are supported. After the system runs the task, the system sends you notifications through the specified notification method. • **DingTalk Chatbot**: Select the DingTalk chatbots that are used to send notifications. You can also click **Add DingTalk Chatbot** to add a new DingTalk chatbot. For more information about how to add a DingTalk chatbot, see Alert settings. • **Email**: Enter email addresses. Separate multiple email addresses with commas (,). 
Execution Time	Supports **Execute** and **Custom Time**. • **Execute**: After the task is created, the system immediately runs the task. • **Custom Time**: After the task is created, the systems runs the task at the specified **Custom Time**.

5. Click **Create**.

Result

After the task is created, the system returns a "**Created**" message and redirects you to the **Task Management** tab.

What's next

After the task is run, you can view the task details on the **Task Management** tab. For more information about how to view task details, see View task details.

3 Container signature

The container signature feature supports signing container images and verifying container image signatures. This feature ensures that only trusted images are deployed and prevents unauthorized images from starting. This helps you improve asset security.

Prerequisites

Complete the following operations before you use container signature.

- Make sure that you have created a Key Management Service (KMS) key based on the asymmetric encryption algorithm.

  For more information about how to create a KMS key, see #unique_10/unique_10_Connect_42_section_yhn_otu_mvs.

  > **Note:**
  > Only the asymmetric encryption algorithm supports the container signature feature. When you create a KMS key, set **Key Spec** to RSA_2048 and set **Purpose** to SIGN/VERIFY. For more information about the asymmetric encryption algorithm, see #unique_11/unique_11_Connect_42_section_ulz_lvl_ugd.

- You have created a Kubernetes cluster in the China (Hong Kong) region and installed the kritis-validation-hook component in the cluster.

  > **Note:**
  > Currently, only Kubernetes clusters that are deployed in the China (Hong Kong) region support the container signature feature.

  For more information about how to create a Kubernetes cluster, see #unique_12.

  For more information about the kritis-validation-hook component, see #unique_13.

- If this is your first time using container signature, you must grant Security Center the required permission to access relevant services.

Limits

Only the Enterprise edition of Security Center supports container signature. If you are using the Basic or Advanced edition, you must upgrade to the Enterprise edition to use container signature.

Procedure

1. Log on to the Security Center console.
2. In the left-side navigation pane, choose **Precaution** > **Container Signature**.
3. Choose **Container Signature** > **Witness** to create a witness.

   If you have already created a witness, skip this step and perform step 4.

   On the **Witness** tab, click **Create a witness** and set the parameters. Click **OK** to complete creating a witness.

   The following table lists the descriptions of the parameters.

Parameter	Description
Witness	When you configure the security policy for container signature, you need to select a witness to authorize your target container. We recommend that you enter a name that is easy to identify.
Select a certificate	Select the KMS key that you have created from the certificate list. **Note:** Only the asymmetric encryption algorithm supports the container signature feature. When you create a KMS key, set **Key Spec** to RSA_2048 and set **Purpose** to SIGN/VERIFY. For more information about the asymmetric encryption algorithm, see #unique_11/unique_11_Connect_42_section_ulz_lvl_ugd.
Description	Enter remarks for the witness.

4. Create a security policy.

   On the **Security Policy** tab, click **Add Policy** and set the parameters. After that, click **OK** to complete creating a policy.

   The following table lists the descriptions of the parameters.

Parameter	Description
Policy Name	When you configure the security policy for container signature, you must select a witness to authorize your target cluster. We recommend that you enter a name that is easy to identify.
Witness	Select a witness that you have created from the witness list. For more information, see Step 3.

Parameter	Description
Application Cluster	After you select the cluster group that needs to use container signature, select the target **Cluster Namespace**.
Policy Enabled	After you create a policy, turn on the status switch to enable the policy. **Note:** By default, the policy is disabled. If the policy is disabled, it does not take effect.
Remarks	Enter remarks for the policy.

What's next

After you create and enable the security policy for container signature, container images with the enabled security policy are labeled as **Trusted Image**.

Note:

Currently, the feature that displays trusted signature labels is not available, but it will be available soon.

4 Multi-account control

Security Center provides the multi-account control feature to allow you to manage Alibaba Cloud accounts and member accounts. Risks detected in these accounts are displayed on the Multi-account Control page.

Prerequisites

In the Resource Management console, you have already created member accounts or invited other Alibaba Cloud accounts. For more information about how to create members accounts, see #unique_15.

Context

If this is your first time using multi-account control, you must grant Security Center access to Resource Management.

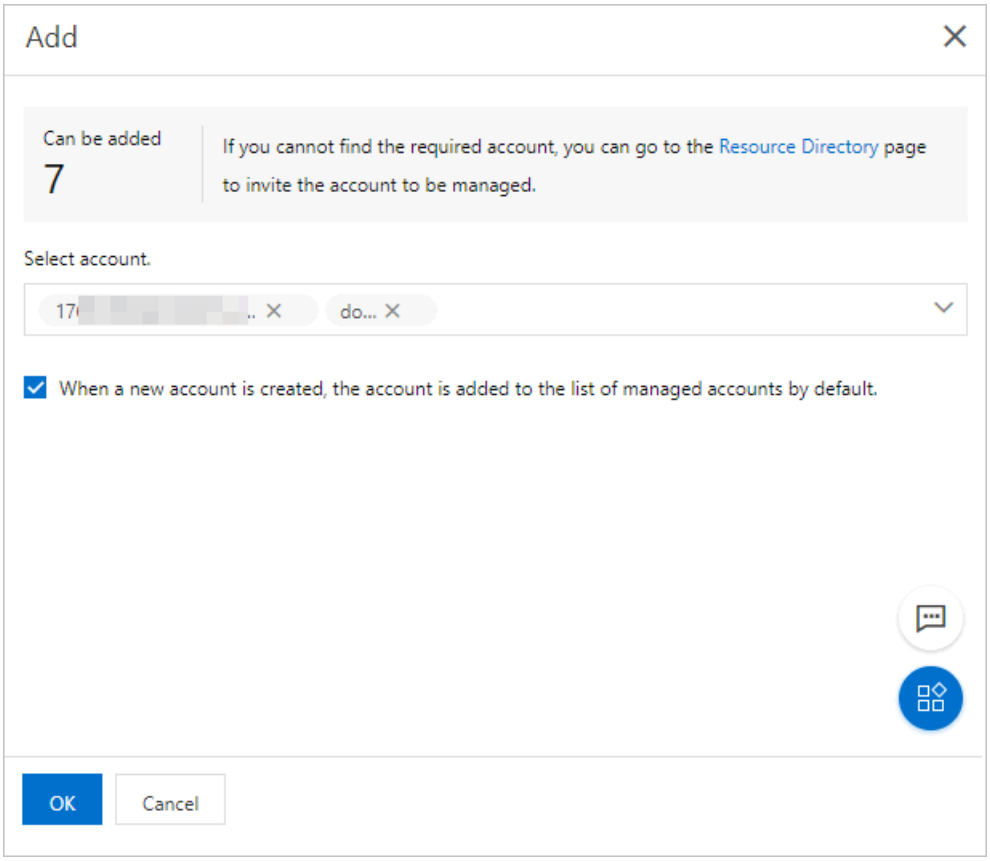
Note:

Currently, only the Enterprise edition of Security Center supports multi-account control.

Procedure

1. Log on to the Security Center console.
2. In the left-side navigation pane, choose **Operation** > **Multi-account Control**.
3. On the **Multi-account Control** page, click **Add**.

4. On the **Add** page, click **Select account.** to select one or more accounts from the drop-down list.



If no account is available on the **Add** page, you must go to the Resource Management console and perform the following operations on the **Resource Directory** page:

- Create member accounts. You can create resource and Alibaba Cloud accounts. For more information, see #unique_15.
- Invite other Alibaba Cloud accounts. You can only invite Alibaba Cloud accounts. For more information, see #unique_16.

5. Optional: If you select the **When a new account is created, the account is added to the list of managed accounts by default.** check box, newly created accounts are automatically added to multi-account control list.

After you add accounts to the list, on the **Multi-account Control** page, you can perform the following operations:

- Search for accounts added to the multi-account control list.
- View the Security Center edition, security score, and security risks of all accounts.
- Click **View** to go to the **Resource Directory** page in the **Resource Management** console. On the **Resource Directory** page, you can view directory information about all assets,

create new members, invite new members, and upgrade a resource account to an Alibaba Cloud account.

- Click **Delete** to remove an account from the multi-account control list.