Identity and Access Management

Getting Started

Issue 08

Date 2021-03-27

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Contents

1 Before You Start

Reading this document will help you to:

- Create Identity and Access Management (IAM) users.
- Create user groups based on your organization's business functions.
- Assign permissions to user groups.
- Create IAM users for employees in your organization.
- Enable IAM users to log in to HUAWEI CLOUD.

Prerequisites

You already have an account. If you do not have an account, create one.

Example Scenario

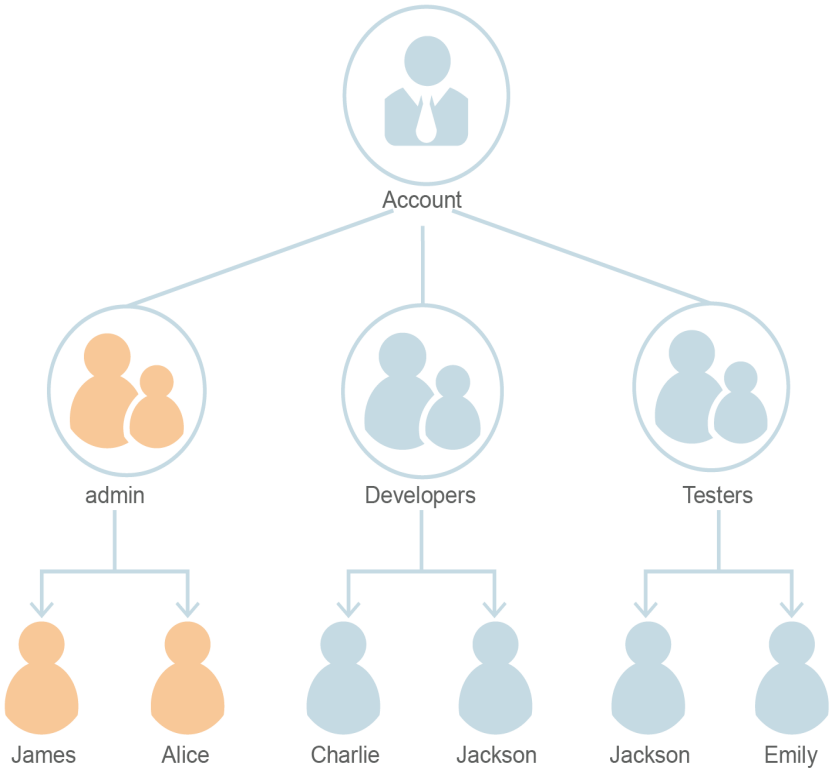
A is a website development company that has three functional teams in Hong Kong. Instead of creating an account for each employee in company A, the company's administrator can register an account to purchase resources and control access permissions. The administrator can create IAM users for employees and assign permissions to the users. For the definitions of an account and IAM user, see **Basic Concepts**.

Company A is used as an example to demonstrate how an enterprise can use IAM to configure cloud service permissions.

Organizational Structure

- Management team (**admin** group in **Figure 1-1**): manages employees and resources, assigns permissions, and allocates resources. The team members include James and Alice.
- Development team (**Developers** group in **Figure 1-1**): develops websites. The team members include Charlie and Jackson.
- Test team (**Testers** group in **Figure 1-1**): tests websites. The team members include Jackson and Emily. Jackson develops and tests websites, so he needs to join both the **Developers** and **Testers** groups to obtain the required permissions.

Figure 1-1 User management model



User Groups and Required Resources

- **admin** group: manages user permissions using IAM.
- **Developers** group: develops websites using Elastic Cloud Server (ECS), Elastic Load Balance (ELB), Virtual Private Cloud (VPC), Relational Database Service (RDS), Elastic Volume Service (EVS), and Object Storage Service (OBS).
- **Testers** group: performs functional and performance testing on websites by using the Application Performance Management (APM) service.

User Management Process

1. The administrator of company A logs in to HUAWEI CLOUD, creates user groups **Developers** and **Testers**, and grants them permissions. For details, see **Step 1: Create User Groups and Assign Permissions**.
2. The administrator creates IAM users for members of the three functional teams. The members then log in to HUAWEI CLOUD as IAM users. For details, see **Step 2: Create IAM Users and Log In**.

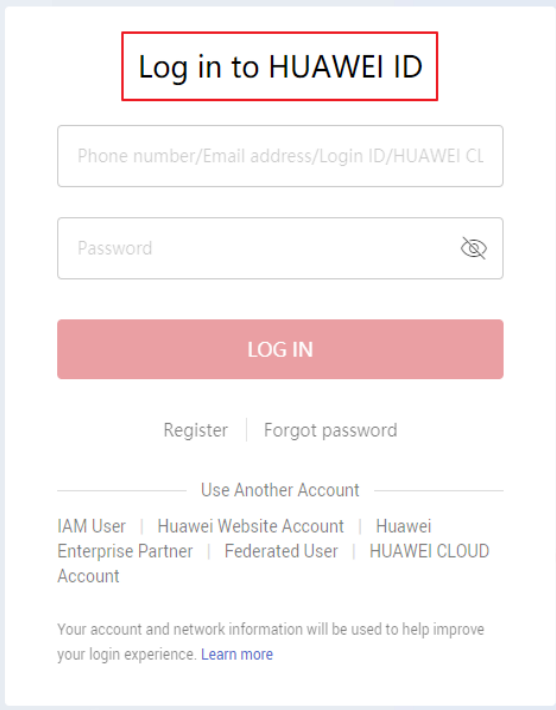
2 Step 1: Create User Groups and Assign Permissions

Company A has three functional teams, including the management (**admin** group), development, and test teams. The default group **admin** is generated after company A's administrator registers an account. The administrator needs to create another two groups in IAM for the development and test teams.

Creating User Groups

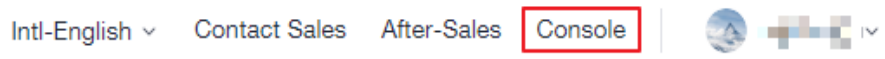
Step 1 Use your HUAWEI ID to enable HUAWEI CLOUD services, and then log in to HUAWEI CLOUD.

Figure 2-1 Logging in to HUAWEI CLOUD



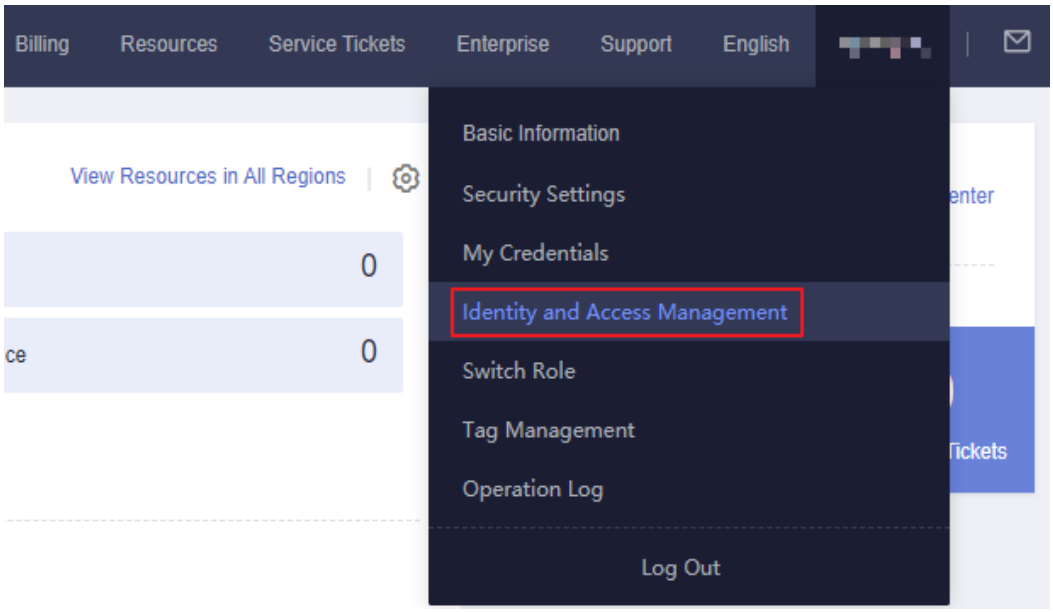
Step 2 Click **Console** in the upper right corner.

Figure 2-2 Accessing the management console



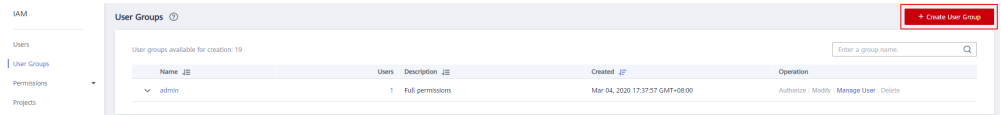
Step 3 On the management console, hover the mouse pointer over the username in the upper right corner, and choose **Identity and Access Management** from the drop-down list.

Figure 2-3 Accessing the IAM console



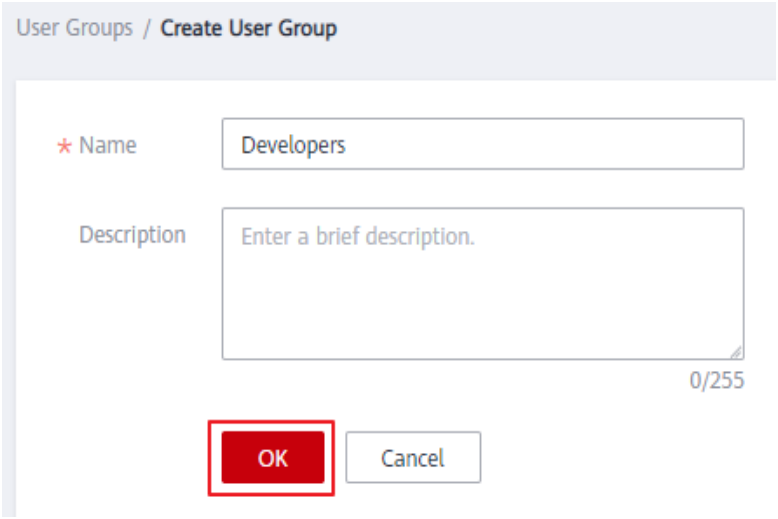
Step 4 On the IAM console, choose **User Groups** and click **Create User Group**.

Figure 2-4 Creating a user group



Step 5 Enter **Developers** for **User Group**, and click **OK**.

Figure 2-5 Setting the user group information



Step 6 Repeat steps **Step 4** and **Step 5** to create the **Testers** group.

----End

Assigning Permissions to User Groups

Developers in company A need to use ECS, RDS, ELB, VPC, EVS, and OBS, so the administrator needs to assign the required permissions to the **Developers** group to enable access to these services. Testers in this company need to use APM, so the administrator needs to assign the required permissions to the **Testers** group to enable access to the service. After permissions are assigned, users in the two groups can access the corresponding services. **For details about the permissions of all cloud services, see System Permissions.**

Step 1 Determine the permissions policies to be attached to each user group.

Determine the policies (see **Table 2-1**) by referring to **System Permissions**. Regions are geographic areas where services are deployed. If a project-level service policy is attached to a user group for a project in a specific region, the policy takes effect only for that project.

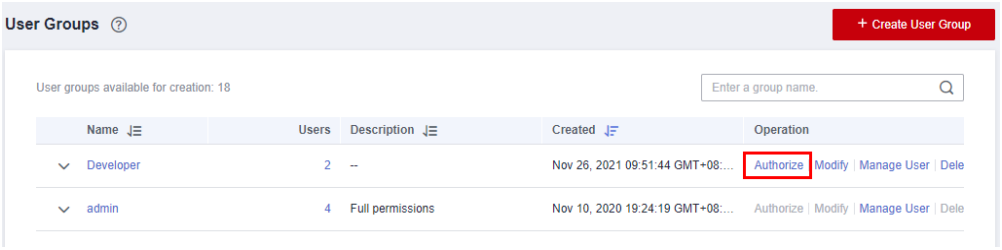
Table 2-1 Required permissions policies

User Group	Cloud Service	Region	Policy or Role
Developers	ECS	Specific regions	ECS FullAccess
	RDS	Specific regions	RDS FullAccess
	ELB	Specific regions	ELB FullAccess
	VPC	Specific regions	VPC FullAccess
	EVS	Specific regions	EVS FullAccess
	OBS	Global	OBS OperateAccess

User Group	Cloud Service	Region	Policy or Role
Testers	APM	Specific regions	APM FullAccess

Step 2 In the user group list, click **Authorize** in the row containing the user group **Developers**.

Figure 2-6 Authorizing a user group



Step 3 Assign permissions to the user group for region-specific projects.

1. All the services in **Table 2-1** except OBS are deployed in specific projects. Select desired permissions for project-level services and click **OK**.
2. Specify the scope as **Region-specific projects**, select **CN-Hong Kong**, and click **OK**.

   Because company A is located in Hong Kong, select **CN-Hong Kong** to reduce network latency and allow quick service access. Then users in the **Developers** group can access the specified project-level services in **CN-Hong Kong** but do not have permissions to access the services in other regions.

Step 4 Assign permissions to the user group for the global service project.

1. Select **OBS OperateAccess** and click **Next**.
2. Specify the scope as **Global service project** and click **OK**.

Step 5 Repeat steps 2 to 5 to attach the **APM FullAccess** policy to the **Testers** group in the **CN-Hong Kong** region.

----End

3 Step 2: Create IAM Users and Log In

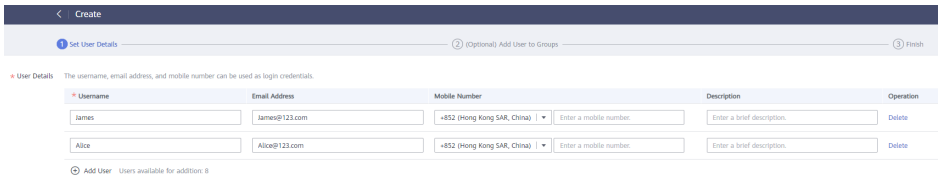
Use the account of company A to create IAM users for employees and add the users to the user groups created in the previous section. The IAM users have their own passwords to log in to HUAWEI CLOUD, and can use resources based on assigned permissions.

Creating IAM Users

Step 1 Choose **Users** from the navigation pane, and click **Create User**.

Step 2 Specify the user information and access type. To create more users, click **Add User**. A maximum of 10 users can be created at a time.

Figure 3-1 Configuring user information



NOTE

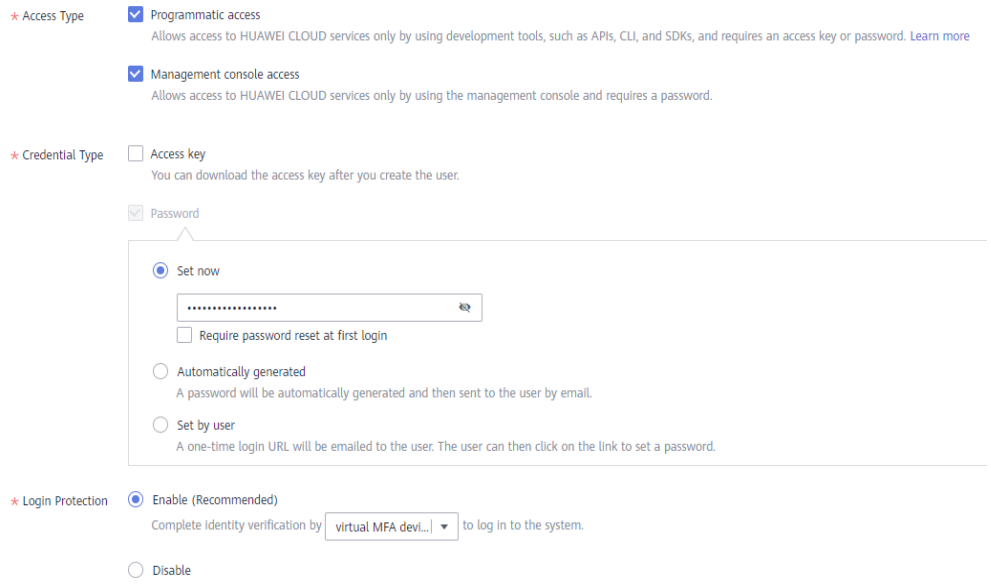
- Users can log in to HUAWEI CLOUD using the username, email address, or mobile number.
- If users forget their password, they can reset it through email address or mobile number verification. If no email address or mobile number has been bound to users, users need to request the administrator to reset their password.

Table 3-1 User information

Parameter	Description
Username	Username that will be used to log in to HUAWEI CLOUD, for example, **James** and **Alice**. This field is required.

Parameter	Description
Email Address	Email address of the IAM user that can be used as a login credential. IAM users can bind an email address after they are created. This field is required if you have specified the access type as **Set by user**.
Mobile Number	Mobile phone number of the IAM user that can be used as a login credential. IAM users can bind a mobile number after their accounts are created. This field is optional.
Description	Additional information about the IAM user. This field is optional.

Figure 3-2 Setting the access type



- **Programmatic access**: Select this option to allow the user to access cloud services using development tools, such as APIs, CLI, and SDKs. You can generate an **access key** or set a **password** for the user.
- **Management console access**: Select this option to allow the user to access cloud services using the management console. You can set or generate a password for the user or request the user to set a password at first login.

NOTE

- If the user **accesses cloud services only by using the management console**, specify the access type as **Management console access** and the credential type as **Password**.
- If the user **accesses cloud services only through programmatic calls**, specify the access type as **Programmatic access** and the credential type as **Access key**.
- If the user **needs to use a password as the credential for programmatic access** to certain APIs, specify the access type as **Programmatic access** and the credential type as **Password**.
- If the user needs to **perform access key verification** when using certain services in the console, specify the access type as "**Programmatic access** + **Management console access**" and the credential type as "**Access Key** + **Password**". For example, the user needs to perform access key verification when creating a data migration job in the Cloud Data Migration (CDM) console.

Table 3-2 Setting the credential type and login protection

Credential Type and Login Protection		Description
Access key		After you create the user, you can download the **access key (AK/SK)** generated for the user. **Each user can have a maximum of two access keys.**
Password	Set now	Set a password for the user and determine whether to require the user to reset the password at first login. If you are the user, select this option and set a password for login. You do not need to select **Require password reset at first login**.
	Automatically generated	The system automatically generates a login password for the user. After the user is created, you can download the EXCEL password file and provide the password to the user. The user can then use this password for login. **This option is available only when you create a single user.**
	Set by user	A one-time login URL will be emailed to the user. The user can click on the link to log in to the console and set a password. If you are an administrator setting the password for the user, select this option and enter an email address and a mobile number. The user can then set a password by clicking on the one-time login URL sent over email. The login URL is valid for **seven days**.

Credential Type and Login Protection		Description
Login Protection	Enable (Recommended)	If login protection is enabled, the user will need to enter a verification code in addition to the username and password during login. Enable this function for account security. You can choose from SMS-, email-, and virtual MFA–based login verification.
	Disable	To enable login protection for an IAM user after creation, see **Modifying IAM User Information**.

Step 3 (Optional) Click **Next** to add the users to specific user groups.

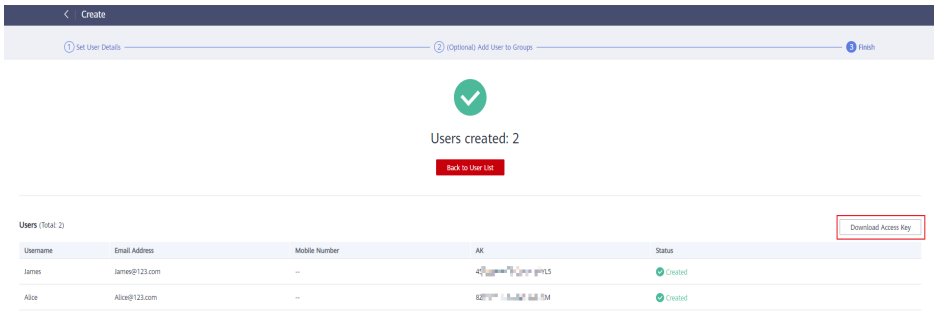
- The users will inherit the permissions assigned to the user groups.
- You can also create new groups as required.

NOTE

The default user group **admin** has the administrator permissions and the permissions required to use all cloud resources. For the mapping relationships between company A's employees and the user groups, see **Figure 1-1**.

Step 4 Click **Create**. If you have specified the access type as **Programmatic access** (see **Table 3-2**), you can download the access keys on the **Finish** page.

Figure 3-3 Users created successfully



Step 5 Repeat steps **Step 1** through **Step 4** to create users Charlie, Jackson, and Emily, and add them to the corresponding groups.

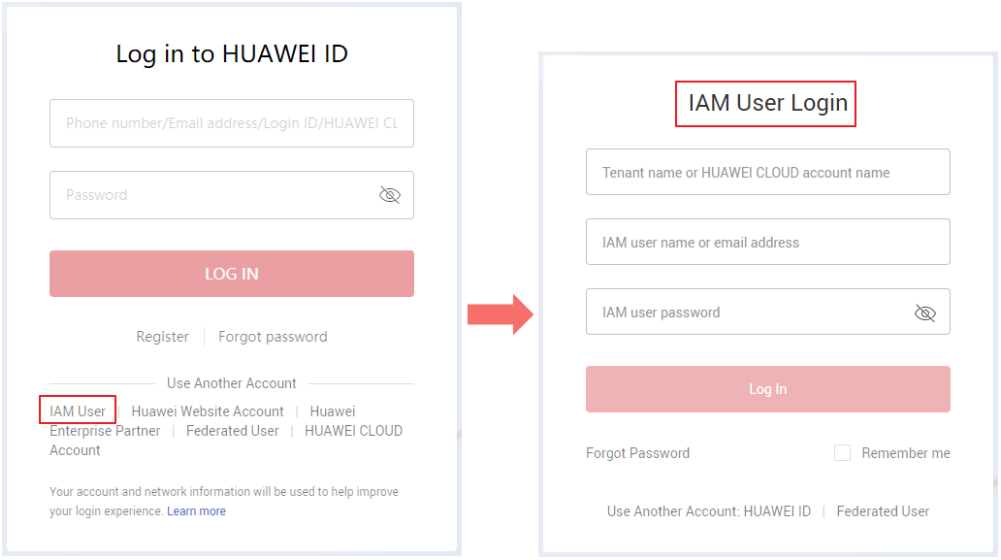
----End

IAM User Login

After using the account of company A to create users **James**, **Alice**, **Charlie**, **Jackson**, and **Emily**, provide the account name, IAM user names, and IAM users' initial passwords to corresponding employees. Employees can use their own usernames and passwords to access HUAWEI CLOUD. If IAM user login fails, employees can contact the administrator to **reset their password**.

Step 1 Click **IAM User** on the login page, and then enter your **Tenant name or HUAWEI CLOUD account name**, **IAM user name or email address**, and **IAM user password**.

Figure 3-4 Logging in as an IAM user



- **Tenant name or HUAWEI CLOUD account name**: the name of the account that was used to create the IAM user
- **IAM user name or email address**: the username (for example, **James**) or email address of the IAM user You can obtain the username and password from the administrator.
- **IAM user password**: the password of the IAM user (not the password of the account)

Step 2 Click **Log In**.

----End

4 Change History

Table 4-1 Change history

Released On	Description
2021-11-30	This issue is the tenth official release, which incorporates the following change: Modified section **Step 1: Create User Groups and Assign Permissions** according to optimization of the authorization function.
2021-09-02	This issue is the ninth official release, which incorporates the following change: Optimized section **Step 1: Create User Groups and Assign Permissions** according to changes to the permissions management function.
2021-03-27	This issue is the eighth official release, which incorporates the following change: Updated the document based on the new feature of HUAWEI ID login.
2020-12-30	This issue is the seventh official release, which incorporates the following change: Updated the document based on changes in the login page, security settings function, and UI strings.
2020-10-27	This issue is the sixth official release, which incorporates the following change: Updated the screenshots of the login page based on the login method change.

Released On	Description
2020-06-08	This issue is the fifth official release, which incorporates the following change: Updated the following sections to include descriptions about HUAWEI ID login: **Step 1: Create User Groups and Assign Permissions** **Step 2: Create IAM Users and Log In**
2020-02-10	This issue is the fourth official release, which incorporates the following change: Modified section **Step 1: Create User Groups and Assign Permissions** based on policy name changes.
2020-01-19	This issue is the third official release, which incorporates the following change: Modified section **Step 1: Create User Groups and Assign Permissions** based on console changes.
2019-06-06	This issue is the second official release, which incorporates the following change: Optimized the steps for assigning permissions in **Step 1: Create User Groups and Assign Permissions**.
2019-02-26	This issue is the first official release.