

AnyNet IRIS QSG

About AnyNet IRIS

AnyNet IRIS enables you to easily and securely deploy required IAM roles and policies to selected AWS regions for integration with AWS Marketplace.

AnyNet IRIS is supported on the following operating systems:



- Windows 10 version 1903 and above
- macOS 10.14 and above



For information about the IAM managed policies you need to use the *AnyNet Cellular Connectivity for AWS IoT SaaS* product, see [Required IAM Managed Policies](#).



For information about the IAM permissions you need to use the *AnyNet Cellular Connectivity for AWS IoT SaaS* product, see [Required IAM permissions](#).

After deploying resources, you can use AnyNet IRIS to review the status of your things in each region in a specified time period, view the deployed Cloud Formation template contents, as well as manage configuration and updates.



For more information, see [Reviewing thing connectivity using AnyNet IRIS](#).

Getting Started: preparing the cloud

Before you begin

Ensure your system supports the AnyNet IRIS installation. For more information, see *Installing AnyNet IRIS* on page 3.

Preparing the cloud overview

In order to integrate your things with AWS, this document will take you through the following steps:

1. Sign up for an Amazon Web Services (AWS) account, or log into an existing account: <https://aws.amazon.com>
For instructions, see: [How do I create and activate a new AWS account?](#)
2. Subscribe to *AnyNet Cellular Connectivity for AWS IoT*.
3. Within your AWS root account, create a mandatory dedicated AWS IAM user account for AnyNet IRIS.
4. Install and configure AnyNet IRIS.

Subscribing to AnyNet Cellular Connectivity for AWS IoT

Use AWS Marketplace to subscribe to *AnyNet Cellular Connectivity for AWS IoT*, which will enable you to connect your thing to AWS IoT Core.

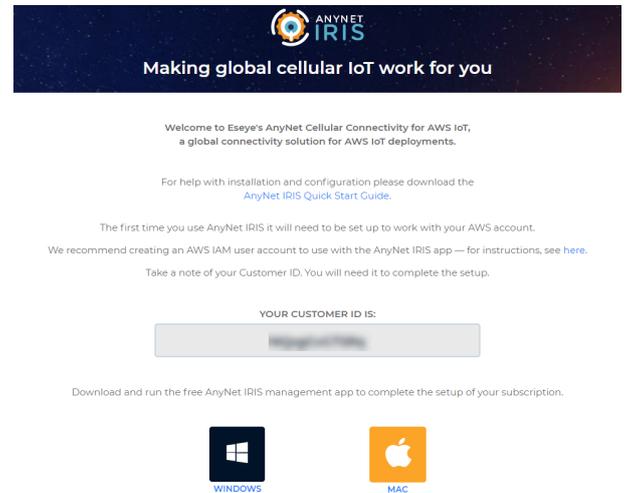
1. Log into your AWS account.
2. Go to [AnyNet Cellular Connectivity for AWS IoT](#).
AnyNet Cellular Connectivity for AWS IoT opens in the AWS Marketplace.
3. Select **Continue to Subscribe**.
The service pricing options are displayed.

4. Select **Subscribe**.

A Congratulations! You are now subscribed! message appears.

5. Select **Set Up Your Account**.

The AnyNet Cellular Connectivity for AWS IoT Welcome page appears.



Make a note of your Customer ID. Leave this window open to refer back to it when you set up the IAM user account, and also when you install and configure AnyNet IRIS.

Next, set up an AWS IAM user account with specific IAM permissions..

Creating a dedicated IAM user account

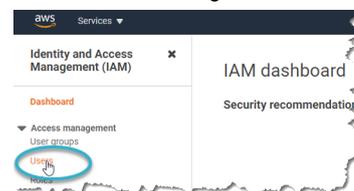


Do not use the AWS account root to set up the required IAM permissions. For more information, see [AWS account root user](#).

For detailed information about why you need a dedicated IAM user account, see [About the required AWS IAM user for AnyNet IRIS](#).

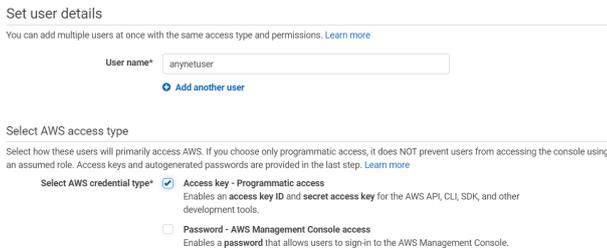
To create an IAM user account:

1. Ensure you have signed in to AWS Management Console.
2. Navigate to *IAM Services* using the following URL: <https://console.aws.amazon.com/iam/>
3. In the left-hand navigation menu, select **Users**.

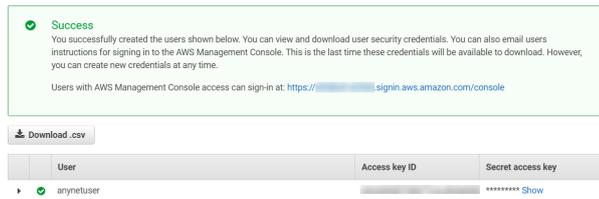


Any previously created IAM users are listed in the right-hand pane.

4. Select **Add User**.
5. Type the user name for the new user.
This is the sign-in name for AWS, for example: *anynetuser*.
6. In the Select AWS access type section, select the **Access key – Programmatic access** check box only.



7. Select **Next: Permissions**.
We will add permissions later.
8. Select **Next: Tags**.
Add any required tags according to your operational policies.
9. Select **Next: Review** to review your choices.
10. Select **Create user** to create the IAM user.



The Access key ID and Secret access key are displayed. AnyNet IRIS will use these security credentials to perform necessary requests against your AWS account.

You can view and download the Secret access key once only. If you forget the Secret access key, you will need to regenerate it on your AWS user account. For more information, see: [AWS security credentials - programmatic access](#).

11. Click **Download.csv** to store the keys locally on your computer.
12. Select **Close**.

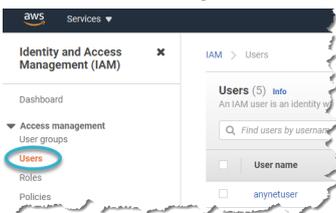
Next, you must attach the required policies to this IAM user account.

Attaching IAM policies to an existing user

You must attach policies to the dedicated IAM user in order to grant specific permissions, which will allow AnyNet IRIS to function.

For detailed information about each policy, see [Required IAM Managed Policies](#).

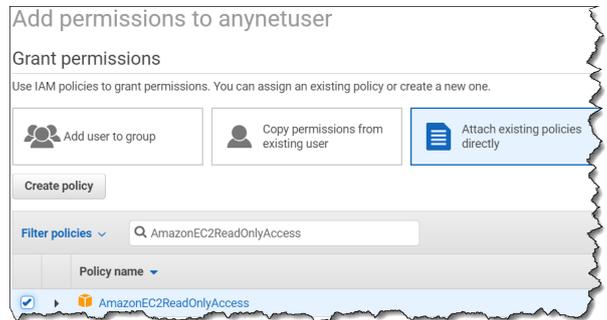
1. Ensure you remain signed into AWS as the root user.
2. Navigate to *IAM Services* using the following URL:
<https://console.aws.amazon.com/iam/>
3. In the left-hand navigation menu, select **Users**.



The AnyNet IRIS user you created is listed.

4. Select the AnyNet IRIS IAM user name.
For example, select **anynetuser**. The IAM user Summary appears.

5. On the *Permissions* tab, select **Add permissions**.
6. Under *Grant permissions*, select **Attach existing policies directly**.
7. Using the **Search** box, search for:
AmazonEC2ReadOnlyAccess.
8. Select the check box alongside the returned result.



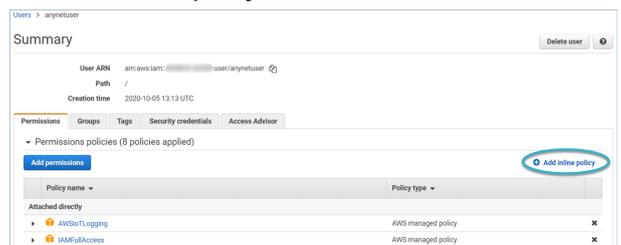
9. Search for each of the following policies in turn, ensuring you select the check box alongside each returned listing:
 - **AmazonEventBridgeFullAccess**
 - **AmazonS3FullAccess**
 - **AWSCloudFormationFullAccess**
 - **AWSCloudTrail_FullAccess**
 - **AWSIoTFullAccess**
 - **AWSIoTLogging**
 - **IAMFullAccess**

If you select the wrong policy, clear the check mark alongside it.

10. Select **Next: Review**.
The selected policies are displayed.

| Type | Name |
|----------------|-----------------------------|
| Managed policy | AmazonEC2ReadOnlyAccess |
| Managed policy | AmazonEventBridgeFullAccess |
| Managed policy | AmazonS3FullAccess |
| Managed policy | AWSCloudFormationFullAccess |
| Managed policy | AWSCloudTrail_FullAccess |
| Managed policy | AWSIoTFullAccess |
| Managed policy | AWSIoTLogging |
| Managed policy | IAMFullAccess |

11. Select **Add permissions**.
The updated Summary page appears.
12. Select **Add inline policy**.



13. On the *JSON* tab, replace the existing text with the following JSON script:



To preserve JSON formatting, copy the script from the following link: [JSON inline policy](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowCrossAccountAccess",
      "Action": [
        "sts:AssumeRole"
      ],
      "Effect": "Allow",
      "Resource":
"arn:aws:iam::001813207414:role/AnyNetSecure@
<customer_id>"
    },
    {
      "Sid":
"DenyAllUserAndOrganizationRelatedActions",
      "Action": [
        "iam:AddUserToGroup",
        "iam:AttachUserPolicy",
        "iam:CreateUser",
        "iam>DeleteUser",

"iam>DeleteUserPermissionsBoundary",
        "iam>DeleteUserPolicy",
        "iam:DetachUserPolicy",

"iam:PutUserPermissionsBoundary",
        "iam:PutUserPolicy",
        "iam:RemoveUserFromGroup",
        "iam:TagUser",
        "iam:UntagUser",
        "iam:UpdateUser",
        "organizations:*"
      ],
      "Effect": "Deny",
      "Resource": "*"
    }
  ]
}
```

14. In the JSON text, replace `<customer_id>` with your AnyNet Cellular Connectivity for AWS IoT Customer ID. If you cannot remember your Customer ID, see [Viewing the AnyNet IRIS Welcome page](#).
15. Select **Review policy**. The Review policy page appears.

16. In the **Name** field, type a name for the policy, for example: *AnyNetSecurePolicy*.
17. Select **Create policy**. The IAM user account Permissions policies updates to include the inline policy.

After you have completed creating the IAM user and have attached the essential policies, next you must install and configure AnyNet IRIS.

Installing AnyNet IRIS

Before you begin

To configure AnyNet IRIS you need:

- AWS Marketplace Customer ID
- AWS IAM user credentials

Installing AnyNet IRIS for Windows 10

1. On the AnyNet IRIS Welcome page, select:



The AnyNet IRIS Setup.exe downloads.

2. Run **AnyNet IRIS Setup <version>.exe**, where `<version>` is the latest version.



Depending on your Windows security, a warning may appear. Ensure that you run the *AnyNet IRIS Setup <version>.exe* app anyway.

AnyNet IRIS installs and opens.

3. Next, configure AnyNet IRIS.

For more information, see *Configuring AnyNet IRIS* on the next page.

Installing AnyNet IRIS for macOS

1. On the AnyNet IRIS Welcome page, select:



The AnyNet IRIS-*<version>*.dmg file downloads.

2. Double-click **AnyNet IRIS-*<version>*.dmg**, where *<version>* is the latest version.
3. Drag the AnyNet IRIS icon into the **Applications** folder.
4. In the **Applications** folder, double-click the AnyNet IRIS application to open it.
5. Next, configure AnyNet IRIS.
For more information, see *Configuring AnyNet IRIS* below.

Configuring AnyNet IRIS

Credentials are not communicated outside of the AnyNet IRIS application, and are used to create the Foundation CloudFormation stack. This is the base stack required to deploy resources to the AWS regions you select.



Only the Access Key ID is stored locally within the application. The Secret access key is not stored in the application.



Only deploy the AWS Foundation CloudFormation stack once per IAM user account. It can only exist in a single Service Region.

To configure AnyNet IRIS:

1. Using the AnyNet IRIS application, on the *AWS credentials* page, type the IAM user credentials, then select **Next**.
You can find the user credentials in the Download.csv file. For more information, see [Download.csv file](#) on page 2.



Do not use your AWS root user account to configure AnyNet IRIS. For more information, see [Creating a dedicated IAM user account on page 1](#).

If required, follow the onscreen instructions to create an access key.



You may prefer to copy and paste the credentials using keyboard shortcuts.

2. On the *Customer ID* page, type the AWS Marketplace **Customer ID** for AnyNet IRIS.
If required, follow the onscreen instructions to discover your Customer ID.
3. Select **Next**.
4. On the *Foundation Stack* page, select the region where you want to deploy the initial Foundation CloudFormation stack.

The options displayed in the drop-down list depend on the IAM permissions and regions you set up when you created the custom IAM user account.

5. If required, select **Stack Preview** to expand the preview and ensure the stack is compliant with your organisation's stack requirements.
6. Select **Next** to deploy the stack to the selected region.
The initial stack enables Eseye cross-account access to your customer account.



indicates the deployment has completed successfully.



indicates the deployment has failed, which may occur because AWS is not ready. Try again. If required, select the supplied link on the *Foundation Stack* page to view the full log files. If you cannot progress, contact Support:

cloudconnect@eseye.com.

7. Select **Continue**.
8. On the *Email Notifications* page, type the email addresses where you want to send AnyNet IRIS advisory and alert notifications, then select **Next**.
AnyNet IRIS emails each supplied email address with a verification link.
9. Open each email, then select the **Confirm subscription** link to verify that email address.

The AWS Subscription confirmed page appears for each subscription. The AnyNet IRIS Email Notifications page updates.



indicates successful subscription.



indicates the subscription has failed. If you cannot progress, contact Support: cloudconnect@eseye.com.

10. Using AnyNet IRIS, select **Continue**.
11. On the *Service Region* page, select the AWS IoT regions where you want to deploy AnyNet IRIS resources.
12. Select **Complete** to deploy the resource stack to the selected regions.
This may take a few minutes to complete.
13. Select **Review** to view Configuration, Status and Updates information.
For information about using AnyNet IRIS, including viewing and setting parameters, see [Reviewing thing connectivity](#).

Continue configuring your system to send and receive data.

| Technical Support: | Sales: |
|--|---|
| UK: +44 1483 802503 France: +33 9 87 67 53 37 Australia: +61 8 9551 5200 USA: +1 484-935-3130 Brazil: +55 11 4950-7015 Email: support@eseye.com | UK: +44 1483 802501 France: +33 9 87 67 53 36 Norway: +47 454 62 017 USA: +1 512-813-0599 Brazil: +55 11 5059-1574 Africa: +27 87 551 8200 Email: sales@eseye.com |