SAS® Customer Intelligence 360: Onboarding Guide

Introduction

This documentation covers tasks that account administrators need to perform when they first log on to SAS Customer Intelligence 360. The tasks include setting up DNS CNAME (canonical name) records, configuring content security policies, adding and managing users, and preparing and loading data. Information about additional documentation and training is also provided.

Step 1: Allow Your Websites to Appear in the SAS Customer Intelligence 360 User Interface

To prevent clickjacking and other malicious and inappropriate use of their websites, companies commonly use web servers that deny outside sources the ability to display their content inside an unknown inline frame (iframe). Because SAS Customer Intelligence 360 uses iframes to provide a point-and-click interface that identifies spots and elements on your website, any iframe restrictions must be modified to allow the SAS domain to display your website in an iframe.

If your website does not open in the SAS Customer Intelligence 360 user interface, you must consider one of these methods for resolving the issue depending on the existing settings for your corporate web server:

- Configure the **X-Frame-Option** parameter in the http header to add the SAS Customer Intelligence 360 user interface address as the ALLOW-FROM site. (Maintain any existing settings such as “same origin” when adding the new address.) The header parameter looks like this: `X-Frame-Options: ALLOW-FROM https://design-<xxx>.ci360.sas.com`. In the header, *xxx* is **`use`** (if your tenant is hosted in the United States) or **`euw`** (if your tenant is hosted in Europe).

  Note: The **X-Frame-Option** parameter is deprecated and has been replaced by the frame-ancestors directive for **Content-Security-Policy**. Different browsers handle this setting differently.

  If an ALLOW-FROM site is already specified, **Content-Security-Policy** might be required instead of this setting because multiple ALLOW-FROM settings are not supported by this header.

- Configure the frame-ancestor attribute in the **Content-Security-Policy** parameter in the http header to include the SAS Customer Intelligence 360 user interface address. (Maintain any existing settings such as ‘self’ when adding the new server.) The header parameter looks similar to this:
  `Content-Security-Policy: "frame-ancestors 'self' *.ci360.sas.com;"`

Note: The **frame-ancestors** attribute is equivalent to the **X-Frame-Option** parameter. Because the **frame-ancestors** attribute is not currently supported by all browsers, the **X-Frame-Option** header might be needed instead of (or in addition to) this attribute.

The browser might perform unpredictably if you use the **X-Frame-Option** and **Content-Security-Policy** parameters at the same time. Therefore, both parameters should provide equivalent permissions or only one parameter should be modified.

Step 2: For Hosting on Custom Domains, Set Up CNAMEs to Stop Ad Blockers

Note: This step is strongly recommended for SAS Customer Intelligence 360 websites in order to stop ad blockers from blocking content, script execution, and data collection by SAS Customer Intelligence 360.

By default, SAS Customer Intelligence 360 delivers personalized content from a SAS domain to your website. An ad blocker in your browser can prevent you from receiving personalized content from SAS Customer Intelligence 360 because the blocker might see the content as coming from a third party. To prevent your personalized content from being blocked, it is recommended that you set up CNAMEs so that all SAS Customer Intelligence 360 requests occur in your website's domain and are not seen as suspicious. To set up CNAMEs:

1. Inform SAS Technical Support that you are creating CNAMEs for your domain. This action creates a Technical Support ticket that you need to access in Step 4 on page 3.

2. Determine the short names for your tenants. (As a best practice, set up a tenant for the test environment and a tenant for the production environment.) You need these short names later to determine the endpoints for your CNAMEs. The short names can be found in one of these places:

   - in the welcome email for SAS Cloud. The original email is similar to this example:

     ```
     An account has been created for <tenant short name>, and you have been designated as the primary
     account administrator. In this role, you are responsible for setting
     up the account for your organization.
     ```

   - in the product banner at the top of the page.

3. Create a CNAME record for each listed domain name in your organization's domain name system (DNS). A CNAME record is a resource record in the DNS that specifies that the CNAME record represents an alias to the SAS Customer Intelligence 360 domain names.

   Note: Although the names that you need to point to might not exist yet, you still must set up the CNAME. The target DNS entry is created when SAS is notified that the aliases are in place on the customer side.

   You need at least three CNAME records. Here are the recommended name variations for your servers:

   > **TIP** It is recommended to include **ci360** in the CNAMEs in order to make it easier to debug errors when you use the browser’s developer tools. Also, avoid using **ad** in any of the CNAMEs because the word might trigger ad-blocking software.

   Execution
   : server that loads the SAS tag and sends events. Your CNAME record should be an alias that is similar to **execution-ci360.<*company.com*>** and points to **execution-<*tenant short-name*>.ci360.sas.com**.

   Delivery
   : server that requests content and customizes the delivery of content on the web pages. Your CNAME record should be an alias that is similar to **delivery-ci360.<*customer domain*>** and points to

tng<*tenant short-name*>-ia.aimatch.com. For example, the alias delivery-ci360.acme.com might point to tng1234-ia-aimatch.com.

Content

server that is required for delivering content to your website from within the SAS Customer Intelligence 360 Asset Management System. Otherwise, content for assets must be loaded from your content management system.

Your CNAME record should be an alias that is similar to **content-ci360.<*customer domain*>** and points to **content.aimatch.com**. For example, the alias content-ci360.acme.com might point to content.aimatch.com.

4 After you create the CNAMEs, respond to the original Technical Support ticket that you opened in step 2.1 on page 2.

5 For all new and renewing certificates, SAS uses the AWS Certificate Manager (ACM), which is a certification authority. The ACM initiates a request for the appropriate customer fully qualified domain names (FQDNs). Because AWS is the certification authority, it generates and signs the certificate for a given subject principal without transmission of a certificate signing request (CSR) between the parties. Consequently, X.509 documents are not exchanged during the process.

   SAS Technical Support sends notification that requires the creation of two different CNAME records for domains generated by the ACM in order to verify domain ownership. The CNAME records must remain in place to ensure the automatic renewal of the certificates in the future. The ACM approval process requires that the domain names that are being added to the certificates be visible in a public DNS registry. The site itself does not need to be accessible, but the domain names must resolve.

6 Inform SAS Technical Support that you created the CNAME records. SAS does not receive notification from the ACM.

7 SAS validates that you have created the agreed-upon CNAME records in its domain by performing domain name system (DNS) lookups to determine whether your CNAME records resolve to the correct SAS FQDNs.

8 SAS updates your tenant configuration.

9 SAS uses a third-party tool such as Qualys/SSL Labs to validate the TLS capabilities of all endpoints to determine that the installation is correct and to verify that the browser is trusted.

10 SAS Technical Support informs you when everything is operational and you can load the tag from the CNAME that was created under the Execution server (that is, **execution-<*tenant short-name*>.ci360.sas.com**).

> **TIP** If you want the certificate to be revoked, open a Technical Support ticket to request SAS work with AWS to remove the certificate. Do not remove the DNS alias until the certificate is removed.

Step 3: Configure the Content Security Policies for Your Web Server

Another method companies use to protect their website from cross-site scripting, clickjacking, and other code injection attacks that are caused by the execution of malicious content on a trusted web page is to set a Content Security Policy (CSP) on their web server. CSPs are defined in the web server configuration and transmitted in the http header to specify which items are allowed to be loaded to the website.

If SAS Customer Intelligence 360 is not defined in the content security policy configuration for your company website, these issues might occur:

- Your company website cannot be opened in the SAS Customer Intelligence 360 user interface (iframe). For information about resolving this issue, see “Step 1: Allow Your Websites to Appear in the SAS Customer Intelligence 360 User Interface” on page 1.
- The SAS Customer Intelligence 360 user interface cannot be used to select spots.
- SAS Customer Intelligence 360 cannot collect data or deliver content.
- Explicit error messages about the content security policy appear in the browser console.

If the page loads in the SAS Customer Intelligence 360 user interface but you cannot select items in the user interface, or you see error messages in the browser console when loading your website, your content security policy is too restrictive.

You must add content to your content security to allow the SAS Customer Intelligence 360 script to be loaded and executed so that it can deliver content to your site. For example, if your domain name is “company.com”, the configuration of your Content-Security-Policy might look like this. (The entries relevant to SAS Customer Intelligence 360 are in ***bold***.):

Note: You must have already set up CNAMEs so that the SAS Customer Intelligence 360 scripts come from the site’s domain. For more information, see “Step 2: For Hosting on Custom Domains, Set Up CNAMEs to Stop Ad Blockers” on page 2.

Content-Security-Policy: default-src 'self' data: ; font-src fonts.googleapis.com; script-src 'self' ***'unsafe-inline'*** 'unsafe-eval' ***execution-ci360.company.com;*** connect-src 'self' ***execution-ci360.company.com;*** img-src 'self' ***delivery-ci360.company.com content-ci360.company.com;*** frame-ancestors 'self' *.ci360.sas.com;

Note: If your site is already using Content-Security-Policy settings, add only the relevant changes. If your site is not yet using Content-Security-Policy settings, any changes should be evaluated for their impact on the functionality of your website before you implement the changes.

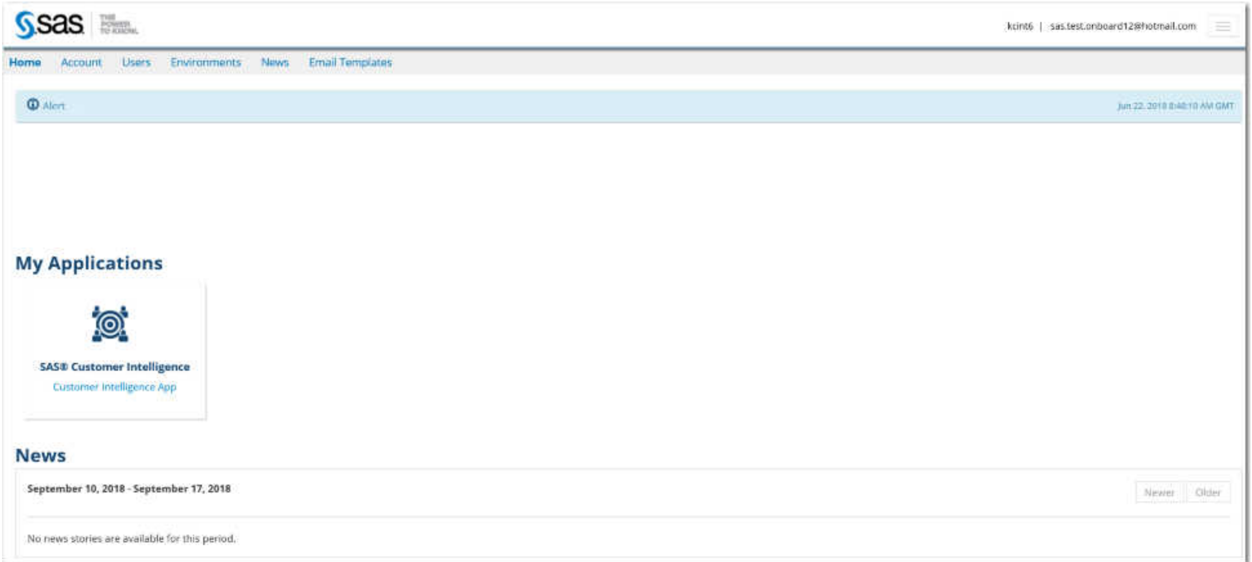
Step 4: Log On to the SAS Cloud and SAS App Central

After your SAS environment has been prepared, you receive an email message from SAS with the title “Welcome to the SAS Cloud! Your account is ready.” The next step is to obtain a SAS Profile and log on to the SAS Cloud.

1. Use your browser to navigate to http://cloud.sas.com/appcentral/home.
2. In the left pane of the SAS Login page, enter your tenant administrator credentials and click **Login**. If you do not have a profile for SAS App Central, click **Create** in the right pane. For more information about creating a profile, see *SAS Cloud: Account Administrator’s Guide*.

   Note: The email address that you use to log on must match the email address where you received the welcome message.

The SAS App Central home page is displayed.



Using SAS App Central, you can perform account administration functions, including adding users, assigning users to roles and environments, and managing email templates.

From the **My Applications** section of the home page, you can access any applications that are associated with your profile. For example, you might have an entry for **SAS Customer Intelligence**, which provides access to the features of SAS Customer Intelligence 360.

Step 5: (Optional) Create an Invitation Email

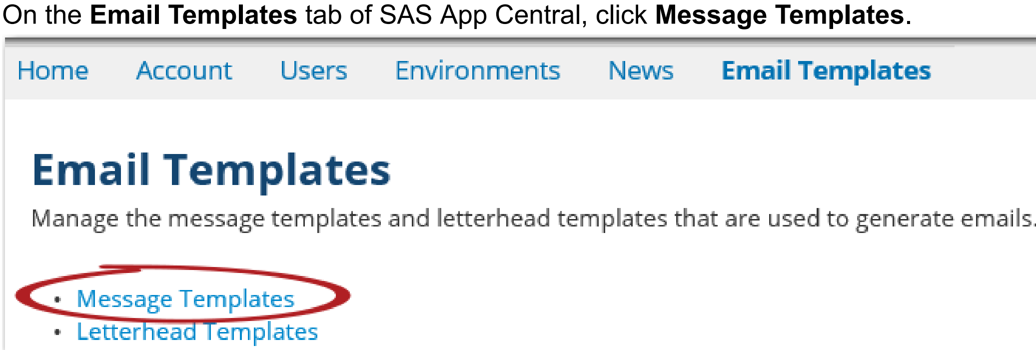
When you add users, you can choose to send them an invitation email. The email welcomes users to the SAS Cloud and provides instructions for logging on. By default, the email is sent using a standard invitation template for your account's preferred locale.

You can customize the invitation email to include the URL that your users need to log on to SAS Customer Intelligence 360. Alternatively, you might create two invitation emails:

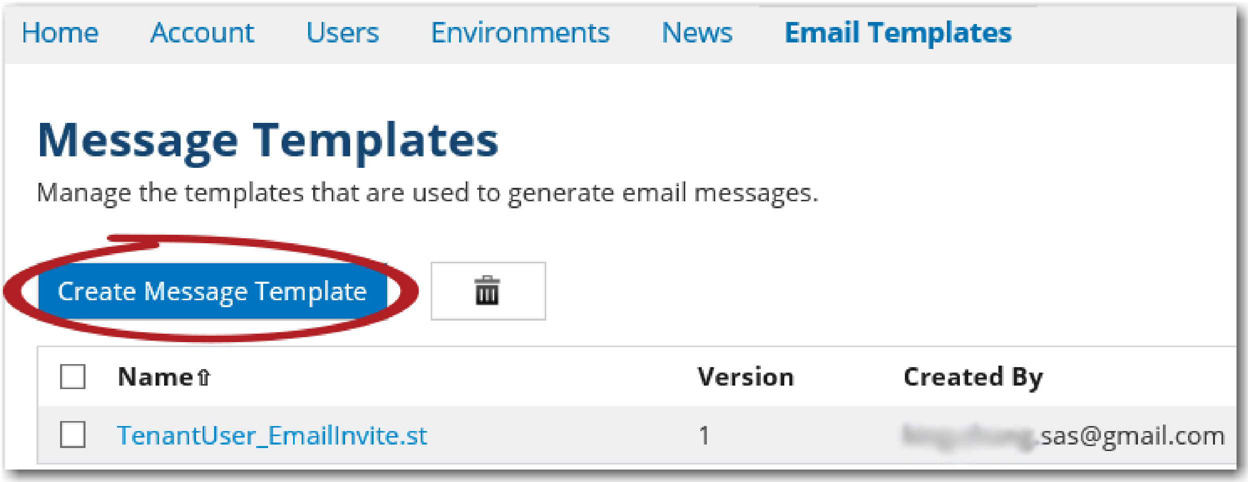
- One email might be sent to users who already have a SAS Profile that they can use to log on to SAS Customer Intelligence 360. That email might contain only the logon URL for SAS Customer Intelligence 360.
- Another email might be sent to users who are new to the SAS Cloud and need both registration instructions for creating their profile and the logon URL for SAS Customer Intelligence 360. In this email, you can remind new users that the email address that they create their profile with must match the email address that the invitation email was sent to.

To create an invitation email:

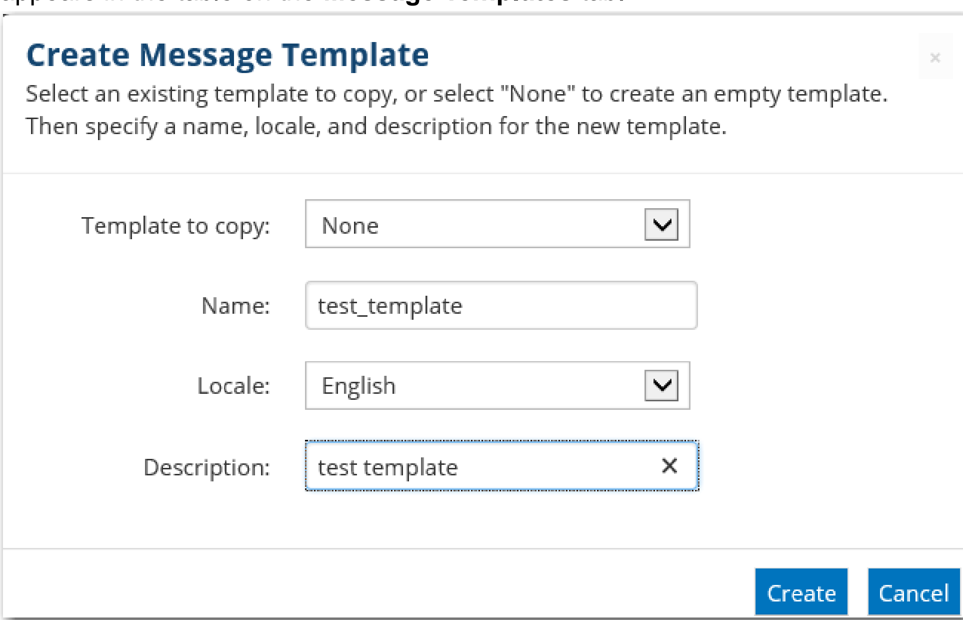
1 On the **Email Templates** tab of SAS App Central, click **Message Templates**.



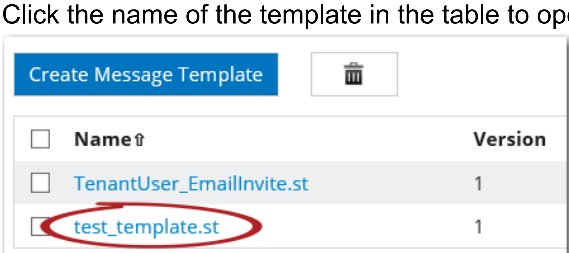
2 Click **Create Message Template**.



3 Complete the fields in the Create Message Template dialog box. If there is an existing template that you want use as a base, select the template from the **Template to copy** list. When you click **Create**, your template appears in the table on the **Message Templates** tab.



4 Click the name of the template in the table to open the editing view.



5 Complete these steps in the editing view:

a Change the template's description and subject line in the corresponding fields.

b Add body content on the **HTML** tab or the **Text** tab.

TIP You might want to include information about role permissions that you set for the user. For more information, see “Step 3: Assign New Users to the Environment” on page 12.

This example text is a recommended HTML template that you can use for new users. You can paste this text into the field on the **HTML** tab:

```
<div>
<a title="SAS - The Power to Know" href="http://www.sas.com">
<img src="https://support.sas.com/images/SAS_TPTK_logo.gif"
alt="SAS Logo" width="181" height="43"></img></a></div>
<p>  </p>
<p>Welcome to SAS Customer Intelligence 360! You have been invited
to use SAS Customer Intelligence 360 as part of the <em><strong>$ACCOUNT_NAME$</strong></em> account.</p>
<p>  </p>
<p>Use your SAS Profile to access <a href="https://platform-<region_code>.ci360.sas.com/
SASCustomerIntelligenceHome/">SAS Customer Intelligence 360</a>.</p>
<p>  </p>
<p>If you do not have a SAS Profile, visit <a href="https://cloud.sas.com">https://cloud.sas.com</a> to
create one. You must have a SAS Profile to log in to SAS Customer Intelligence 360.</p>
<p>Information to help you get started is available at
<a href="http://www.sas.com/customer-intelligence360-get-started">SAS Customer Intelligence 360
Learning Center</a>. This site provides access to user documentation, tutorials, SAS Communities,
and many more learning resources.</p>
<p>  </p>
<p><strong>Additional Resources</strong></p>
<ul>
<li>SAS Technical Support: <a href="http://support.sas.com/ctx/supportform/createForm">
http://support.sas.com/ctx/supportform/createForm</a></li>
<li>SAS Privacy Policy: <a href="http://www.sas.com/en_us/legal/on-demand-privacy.html">
http://www.sas.com/en_us/legal/on-demand-privacy.html</a></li>
</ul>
```

Note: Customize the link to the environment for SAS Customer Intelligence 360 based on the region of your tenant.

Step 6: Manage Users

If there are existing users in the environment, see “Synchronize SAS App Central and SAS Customer Intelligence 360 Roles after Migration” on page 11. Otherwise, continue with step 1.

Step 1: Add Users

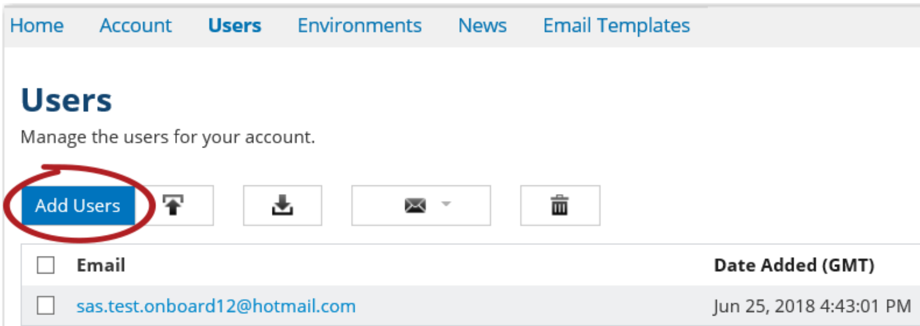
Before users can access software in your SAS Cloud environment, they must be added to SAS App Central. Then, you can assign the users to the environment where the SAS software is hosted.

Add Users Manually

1 Ensure that you have a valid email address for every user that you want to add. The email address that you use for the new user must match the email address in the user’s SAS profile. This is the same email address that the new user uses to log on.

CAUTION! You must have a unique email address for each tenant or environment. For example, if you have two different tenants (a tenant for testing and a tenant for production), you need a separate SAS profile and email address for each tenant. Some email providers enable you to customize your email address with different punctuation or suffixes (for example, myname@email.com might go to the same inbox as my.name@email.com). These variations are valid as unique email addresses.

2 On the **Users** tab, click **Add Users**.



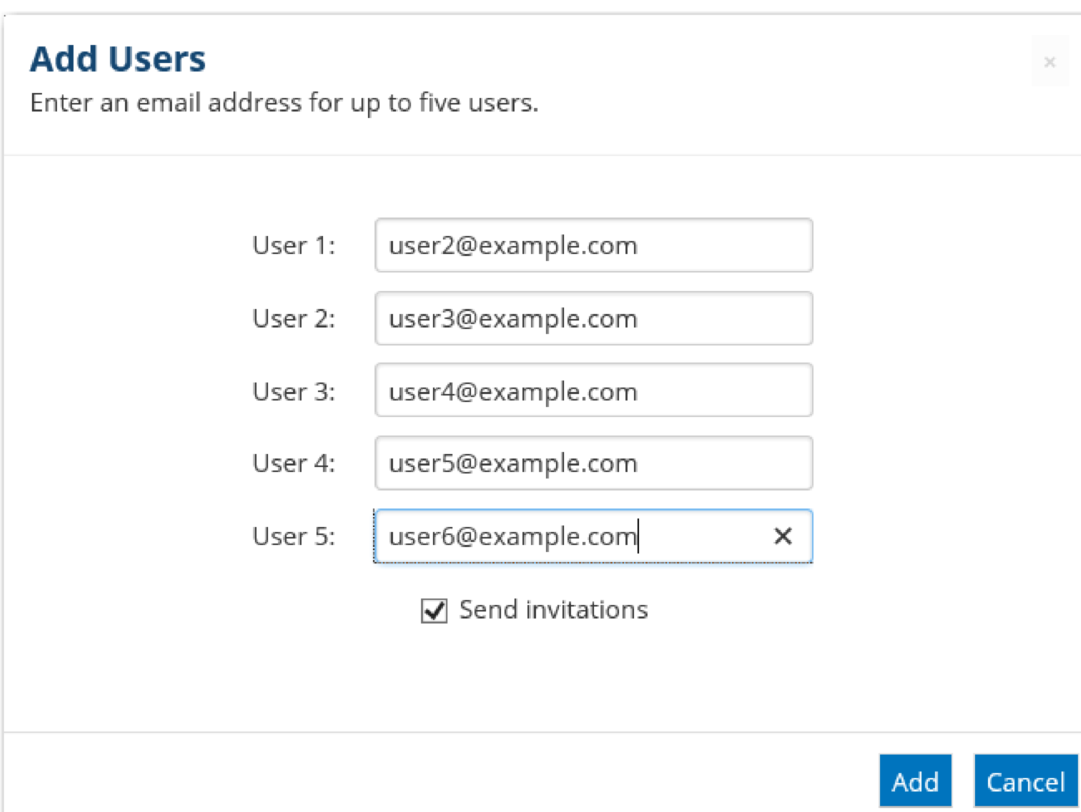
3 Complete these steps in the Add Users dialog box:

a Enter email addresses for up to five users.

b (Optional) Select **Send invitations** if you want invitation emails to be sent immediately. The emails have the subject line “Welcome to the SAS Cloud!” and provide instructions for logging on.

> **TIP** You can preview the invitation emails and customize them on the **Email Templates** tab. You can also send users an email anytime by navigating to the **Users** tab and clicking .

c Click **Add**.



4 Repeat these steps until you have added all of your users. Next, set up user roles in SAS App Central.

Note: Newly added users have View access to the Activities, Assets, Creatives, Data Views, Events, Insights, Messages, Segments, Spots, and Tasks pages in SAS Customer Intelligence 360. The SAS administrator assigns the appropriate roles in SAS Customer Intelligence 360 to limit access or to allow Edit access as required. For more information, see “Managing Users” in *SAS Cloud: Account Administrator’s Guide*.

Upload User Data

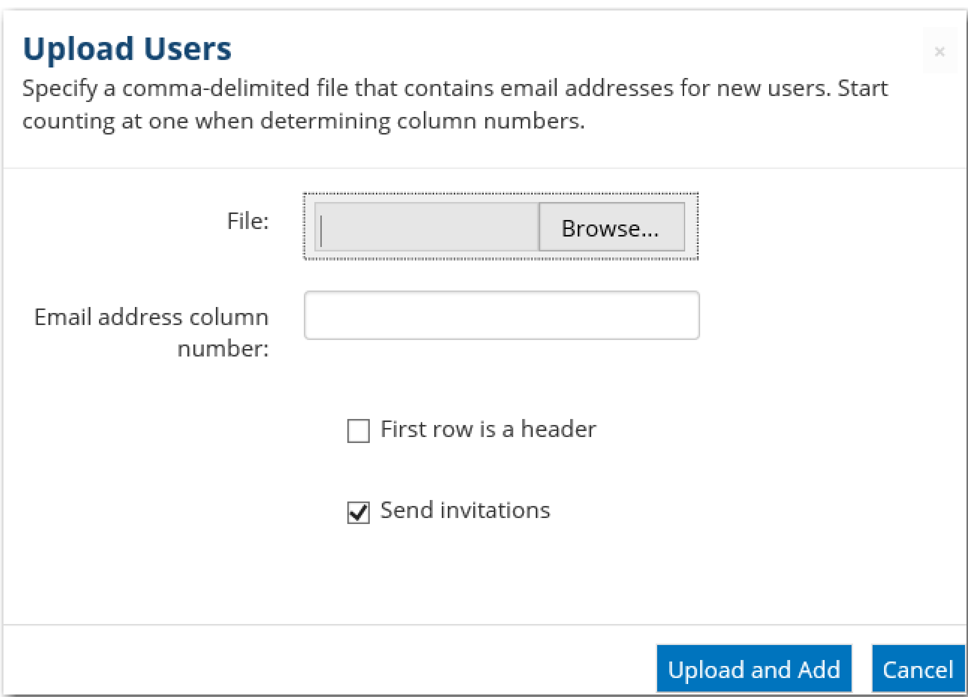
If you have a large number of users, you might want to upload the information in a comma-separated values (CSV) file.

1 Create a CSV file with a list of email addresses. If the file contains data other than email addresses, use commas to separate the data elements. Here is an example of a file where each entry includes a last name, a first name, and an email address:

```
Torres,Juan,Juan.Torres@example.com
Jones,Mary,Mary.Jones@example.com
Patel,Avi,Avi.Patel@example.com
Minami,Yuki,Yuki.Minami@example.com
```

Note: Email addresses must be 32 characters or fewer in length.

2 On the **Users** tab, click .



3 In the Upload Users dialog box, complete these steps:

a In the **File** field, click **Browse** and navigate to the file that you created in step 1.

b Enter the column number that contains the email addresses. In the example file in step 1, the email addresses are in column 3 because they are the third value on each line.

c If the first row of the file contains header information that you want to be ignored, select **First row is a header**.

d Select **Send invitations** if you want invitation emails to be sent immediately to the new users.

TIP You can send the emails later. For more information, see “Send Invitations to New Users” in *SAS Cloud: Account Administrator’s Guide*.

e Click **Upload and Add**.

Note: All of the uploaded user emails are automatically assigned to the `SAS user` role in SAS App Central. Newly added SAS users have View access to the Activities, Assets, Creatives, Data Views, Events, Insights, Messages, Segments, Spots, and Tasks pages in SAS Customer Intelligence 360. The SAS administrator assigns the appropriate roles in SAS Customer Intelligence 360 to limit access or to allow Edit access as required. For information about assigning additional roles such as `SAS administrator` in SAS App Central and assigning users to the tenant’s environment, see “Step 2: Set Up Users’ SAS App Central Roles” on page 10.

Step 2: Set Up Users’ SAS App Central Roles

About SAS App Central Roles

Roles determine what users can do in SAS App Central and in your organization’s SAS environments.

The following table identifies which tasks each role can perform in SAS App Central and which parts of the SAS Customer Intelligence 360 user interface the user has View or Edit permissions to.

Table 1 SAS App Central Roles

SAS App Central Role	Allowed Tasks in SAS App Central	Access to Pages in the SAS Customer Intelligence 360 User Interface
SAS user	View the Home page. From the Home page, access non-administrative SAS applications.	By default, View access to the Activities, Assets, Creatives, Data Views, Events, Insights, Messages, Segments, Spots, and Tasks pages. Administrators must assign Edit permissions for these pages on the User Roles page in SAS Customer Intelligence 360. View and Edit access to all other pages are set by administrators on the User Roles page. For more information, see “List of Roles” in *SAS Customer Intelligence 360: User’s Guide*.
SAS administrator	View the Home page. From the Home page, access applications in the SAS environment that are used for administration.	View and Edit access to all pages. Only SAS administrators have access to all administration areas, including the User Roles area on the General Settings page.
data administrator	View the Home page. From the Home page, access applications in the SAS environment that are used for data management.	Not applicable. This role applies only to SAS App Central.

SAS App Central Role	Allowed Tasks in SAS App Central	Access to Pages in the SAS Customer Intelligence 360 User Interface
account administrator	View the Home page. View account information. Manage users and send emails to users. Assign users to environments and roles. Manage news. Manage email templates.	Not applicable. This role applies only to SAS App Central.

Modify SAS App Central Roles for New or Existing Users

Note: Specify only one role for a user. If you specify both the SAS user role and SAS administrator role, the user does not appear on the **User Roles** page in SAS Customer Intelligence 360.

By default, all users are assigned to the SAS user role in SAS App Central. To assign a user to another SAS App Central role (or to remove a user from a role):

1. On the **Users** tab, click the user's email address.
2. In the **Roles** section of the user's information page, click **Edit**.
3. In the Edit Roles dialog box, select or clear the appropriate check box to specify a role for the user.

   Note: The data administrator and account administrator roles are not applicable to SAS Customer Intelligence 360. Primary tenant administrators might assign the account administrator role to another user in the organization in order to share the responsibility for user management in SAS App Central. For information about modifying an existing data administrator role, see "Synchronize SAS App Central and SAS Customer Intelligence 360 Roles after Migration" on page 11.
4. Click **OK**.

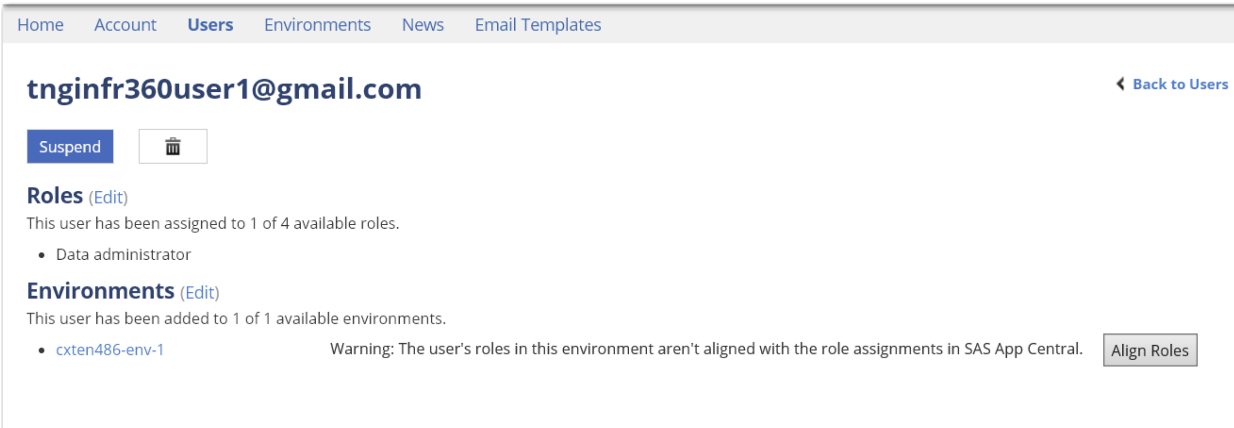
Note: Users must be given access to one or more SAS environments before they can perform all of the tasks associated with their roles. For more information, see "Step 3: Assign New Users to the Environment" on page 12.

Synchronize SAS App Central and SAS Customer Intelligence 360 Roles after Migration

If you migrated from a release of SAS Customer Intelligence 360 where roles are assigned in SAS App Central to a release where the user interface is used to assign roles for SAS Customer Intelligence 360, it is recommended to change the role for existing users who have been assigned only the data administrator role in SAS App Central.

If a user has only the data administrator role, the **Align Roles** button appears in the **Environments** pane after you click the email user ID for a user on the **Users** tab.

Figure 1 Users Tab



To remove the **Align Roles** button:

1 On the **Users** tab, click the user’s email address.

2 In the **Roles** section of the user’s information page, click **Edit**.

3 In the Edit Roles dialog box, clear the check box for **Data administrator** and select the check box for **SAS user**.

4 Click **OK**.

Step 3: Assign New Users to the Environment

Assign each user to the SAS Cloud environment.

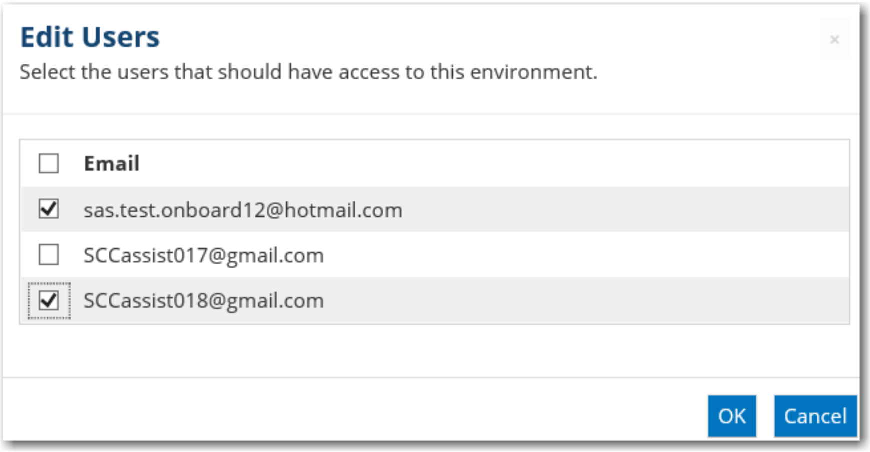
1 On the **Environments** tab, click the link for the environment.

Note: If you administer more than one environment, you must manage other tenant environments with the email address that is associated with that tenant.

2 On the environment page, click **Edit** in the **Users** section.

3 In the Edit Users dialog box, select the email addresses of the users that you want to assign to the environment.

Click **OK** to add the users to the environment’s user list. Initially, the status of a user is Onboarding. After the user successfully logs on to the software, the status changes to Active.



(Optional) Step 4: Remove Users from the Environment

You might need to remove users from the SAS Cloud environment.

1 On the **Environments** tab, click the link for the environment.

   Note: If you administer more than one environment, you must manage other tenant environments with the email address that is associated with that tenant.

2 On the environment page, click **Edit** in the **Users** section.

3 In the Edit Users dialog box, deselect the email addresses of the users that you want to remove from the environment.

   Click **OK** to remove the users from the environment's user list. It might take up to 15 minutes before the user is removed from the environment.

For information about setting up your mobile application, see *SAS Customer Intelligence 360: User's Guide*.