CentraSite

API Management Solutions

Version 9.6

April 2014

This document applies to CentraSite Version 9.6.

Specifications contained herein are subject to change and these changes will be reported in subsequent release notes or new editions.

Document ID: IINM-BU-APIMGNT-96-20140318

Table of Contents

Preface

This document describes how to use CentraSite Business UI for API management.

The content is organized under the following sections:

CentraSite and API Management	Gives an introduction of the CentraSite's real-time API management solutions.
Getting Started with CentraSite API Management	Briefly describes how to get started with the CentraSite's API Management.
Creating an API	Describes how to create an API (asset) in the catalog.
Viewing Details for an API	Describes how to view the information stored for APIs.
Editing Properties of an API	Describes how to view an API's attributes and how to change them.
Setting Permissions on an API	Describes how to assign instance-level permissions on an API.
Configuring the API Consumption Settings	Describes how to configure the type of authentication (API key or OAuth2 token) required for consuming an API.
Managing API Keys and OAuth Tokens	Describes how to manage your API keys and OAuth 2.0 access tokens.
Approving a Request	Describes how to proceed with the approval process of API requests.
Deleting an API	Describes how to remove an API from the catalog.
Working with Email Notifications	Describes how to use the predefined email templates and also create email templates specific to the API Management.
Working with Predefined Policies	Describes how to use the predefined design/change-time policies specific to the API Management.

1 CentraSite and API Management

A new wave of innovation is revolutionizing enterprises as mobile internet users exceed internet desktop users. Today's enterprises are looking at leveraging their existing and new IT assets across multiple channels that include not only the existing internet based browser-centric model, but more importantly, cater to mobile device users. In addition, new opportunities to leverage these assets with third party sources, allows for innovative solutions and new operating models.

CentraSite's Application Programming Interface (API) Management Solutions enable enterprises to selectively externalize their new and existing assets as APIs across various channels, monitor the interface's lifecycle with an integrated infrastructure, and make sure the needs of developers and application using the API are met.

With an integrated infrastructure, you can securely expose your APIs to external developers and partners (By partners we mean any external entities with which your enterprise interacts, such as suppliers and other vendors, dealers and distributors, customers, government agencies, trade organizations and so forth.), and provide design time and run time governance capabilities to the APIs.

CentraSite's support for API Management enables developers, architects and business developers to:

- Publish the right APIs into their organization's central registry.
- Discover APIs and use them to assemble new applications.
- Manage the entire process of creating, publishing, and retiring APIs.
- Obtain detailed information about an API, including the list of its consumers, technical support contacts, disposition in the development lifecycle, usage tips and performance data.
- Control access to CentraSite and to the metadata for individual APIs listed in the registry.
- Impose mandatory approval processes to ensure that APIs accepted into the SOA adhere to organizational standards and policies.
- Get notifications on the APIs they use.

- Model the lifecycle process associated with each API and specify the events that are to be triggered when an API transitions from one lifecycle state to another.

The asset types that are supported for API management are: Service, XML Service, REST Service, Virtual Service, Virtual XML Service, and Virtual REST Service.

Instructions throughout the remainder of this document use the term "API" when referring to the three base types (Service, XML Service, REST Service), and "API Proxy" when referring to the three virtual types (Virtual Service, Virtual XML Service, and Virtual REST Service) in general.

Related sections of the CentraSite documentation provide the information you need for creating and configuring your API.

Note:

2 Getting Started with CentraSite API Management

CentraSite provides a complete API Management solution that ensures success with exposing APIs both within and outside your organization. It provides role focused user interfaces, complies with standards, and delivers on business value.

The types of tasks you can perform in CentraSite API Management depend on the following characteristics of your user account:

- The roles that are associated with your account
- The actions on APIs on which you have access to

The user account to which you belong is either an API provider or an API consumer.

- API Providers (Owners of the API) who belong to a role "Runtime API Provider" are allowed to create and manage (view, edit, delete) their organization's APIs. Additionally, they can virtualize and publish APIs to the run-time layer.
- API Consumers (Consumers of the API) who belong to a role "Asset Consumer" can only "see" the set of APIs that providers have given them permission to view. Additionally, they can invoke (call) the APIs exposed to them.

The following steps outline how to get started with CentraSite for API Management, as soon as a specific API is identified that needs to be exposed in your applications.

1. Create an API (asset) in the CentraSite Business UI. For procedures, see ***Creating an API***.
2. Browse or Search for the API. For procedures, see *Browsing and Searching for APIs*.
3. View information stored for the API. For procedures, see ***Viewing Details for an API***.
4. Specify the endpoints for the API. For procedures, see ***Editing Properties of an API***.
5. Create a virtual copy of the API. For procedures, see *Creating an API Proxy*.
6. Configure the consumption settings for the API. For procedures, see ***Configuring an API for Consumption***.

7. Publish the API to Mediator for consumption. For procedures, see *Publishing an API Proxy*.
8. Request an API by registering as consumer for the API. For procedures, see *Register as Consumers for an API*.
9. Review and approve the consumer registration requests for the API. For procedures, see ***Approving Onboarding Registration Requests***.
10. Review and approve the API key requests for consumption of the API. For procedures, see ***Approving API Key Requests***.
11. Fetch and use your API key or OAuth token for consumption of the API. For procedures, see *Obtaining Your API Keys and Access Tokens for Consumptio*.

Currently, CentraSite supports the API Management concept for the three basic types of services (Service, REST Service, and XML Service) that can be virtualized and published in general. Instructions throughout the remainder of this guide use the term “API” when referring to all three types in general.

3 Creating an API

To create APIs in an organization, you must belong to a role that has the "Create Assets" or "Manage Assets" permission for that organization. To see a list of the predefined roles that include the "Create Assets" or "Manage Assets" permission, see the section *About Roles and Permissions* in the document *Users, Groups, Roles and Permissions*.

To create an API

1 In CentraSite Business user interface, click the **Create Asset** activity. This opens the **Create a New Asset** wizard.

2 In **Basic Information** panel, specify the following fields:

In this field...	Do the following...
Name	*Mandatory.* Enter a name for the API. An API name can contain any character (including spaces). An API name does not need to be unique within the catalog. However, to reduce ambiguity, you should avoid giving multiple APIs of the same type the same name. As a best practice, we recommend that you adopt appropriate naming conventions to ensure that APIs are distinctly named within an organization.
Type	Choose the type of API that you want to create in the catalog. The APIs that are supported out-of-the-box are: Service, REST service, XML Service, Virtual Service, Virtual XML Service, and Virtual REST Service.
Organization	Choose the organization in which the API will be created. (The drop-down list will contain the list of organizations in which you are permitted to create APIs.) If you select an organization other than your own organization, you will nevertheless be the owner of the API.
Version	*Optional.* Enter an identifier for the initial version of the API. This is the user-defined version, as opposed to the automatically assigned system version. You can enter any string in this field, i.e. the version identifier does not need to be numeric. You can also leave the field blank. You can later create new versions of the API.

In this field...	Do the following...
Description	*Optional.* Enter a comment or descriptive information about the API.
Import File	*For a SOAP API.* Specify whether the input file will be read from a URL-addressable location on the network (the **URL** option) or from your local file system (the **File** option). ■ If the file you are importing resides on the network, specify its **URL**. ■ If the file resides in your local file system, specify the file name. You can use the **Choose** button to navigate to the required folder.
Advanced Settings	*For a SOAP API.* 1. If you have specified a URL, and the site you want to access via the URL requires user authentication, under the **Credentials**, enter your username and password for authentication at the URL site. 2. Choose a **Resolution** strategy, which will allow you to specify how the imported files will be handled. For each of the imported files you have one of these options: ■ **Always overwrite**: Overwrite the importing file (WSDL or schema) with new content. ■ **Always create versions**: Create a new version of the file with the new content (if, for example, you want to modify a schema but want to retain its previous version).

3 Click **Next**.

You will not be allowed to move to the next panel unless all of its required parameters have been set.

4 In the **Preview** panel, review the basic information for API before you actually add to CentraSite.

If necessary, you can click **Previous** to return to the **Basic Information** panel and change your specifications.

5 Click **Save** to create the new API.

If at any time you wish to abandon your unsaved API and return to your previous screen, just click the **Cancel** button.

6 Configure the API's extended attributes as described in the section ***Editing the Properties of an API***.

4 Viewing Details for an API

CentraSite provides a summary of details of the API. The details rendered as attributes are grouped together as profiles.

When you view the details of an API, keep the following points in mind:

- The set of APIs that are available to you are the APIs on which you have View permission. You can obtain View permission on an API in the following ways:
  - By belonging to a role that includes any of the following permissions.

This permission...	Allows you to...
View Assets	View all APIs within a specified organization.
Modify Assets	View and edit all APIs within a specified organization.
Manage Assets	View, edit and delete all APIs within a specified organization, and set instance-level permissions on those APIs. This permission also allows you to create APIs.
Create Assets	Add new APIs to a specified organization. You automatically receive Full permission (which implies Modify and View permission) on all APIs that you create.

  - By having View, Modify or Full instance-level permissions on a particular API.
- By default, all CentraSite users belong to the Asset Consumer role. This role includes the "View Assets" permission for the organization to which a user belongs.

  Having the Asset Consumer role gives you implicit view permission on all the APIs in your organization. You can view APIs from other organizations only if you are given permission to do so through the assignment of additional role-based or instance-level permissions.
- In rare instances, an administrator might not grant view permissions to all of the users in an organization. If the administrator of your organization has done this, you will need instance-level permissions on an API in order to view it.

  For more information about permissions, see the CentraSite online documentation section *About Roles and Permissions* in the document *Users, Groups, Roles and Permissions*.

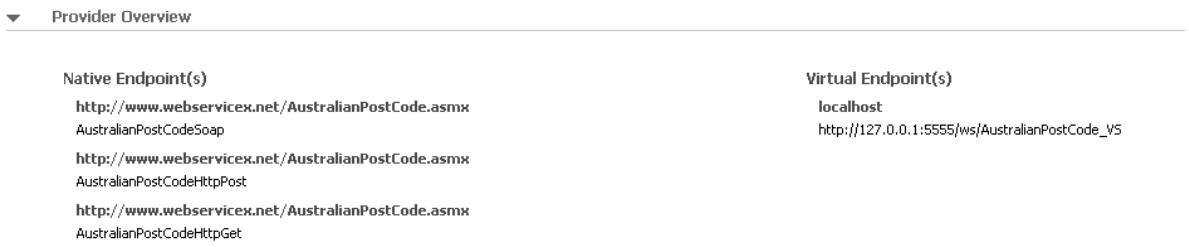
To view details for an API

1. In CentraSite Business UI, use either the *Browse* or *Search* feature to locate an API that you want to view. If you need information on how to browse or search the CentraSite catalog, refer to the section *Browsing the CentraSite Catalog* or *Searching the CentraSite Catalog* in the document *Managing the CentraSite Catalog*.
2. Click the API's hyperlinked name.
3. On the APIs' details page, examine the attributes as necessary. CentraSite will display the attributes for this API.

Remember that you will only see the profiles for which you have View permission. If you have Modify permission on the API, you can edit the API's attributes. For procedures, see *Editing the Properties of an API*.

Viewing a Native/Virtual Endpoint

The **Provider Overview** profile shows a list of the native and virtual endpoints for this API. In this profile, a native endpoint is represented by the *Binding*, and a virtual endpoint is represented as an *Alias* that identifies a specific Access URI (i.e., address where the virtual API is published).



Summary of Profiles in the API

Profiles represent a logical grouping of the information for an API.

The following profiles are available in the API details page:

Profile	Description
Basic Information	Provides basic information about the API. This profile shows individual characteristic such as the API version, type, owner, organization and description. If you are having users watching or consuming this API, CentraSite displays that information on this profile. This profile also contains controls for approving requests placed on this API.
Advanced Information	Provides additional information about the API. This profile shows the technical specifications, and the list of providers and consumers for the API.
Technical Details	Provides technical information about the API. For a SOAP API, this profile includes the WSDL URL and a list of the operations and bindings. For an XML/REST API, the profile includes the schema URL and a list of the resources.
Provider Overview	Displays the list of native and virtual endpoints defined for the API. In this profile, a native endpoint is represented by the *Binding*, and a virtual endpoint is represented as an *Alias* that identifies a specific Access URI (i.e., address where the virtual API is published). This profile also contains control for viewing the enforcement definition of a virtual endpoint.

Profile	Description
Consumer Overview	Displays a list of all virtual endpoints defined for the API. For a SOAP API, this profile displays the Consumer Service WSDL / WSDL URL, and a list of Access URIs and API keys. For a REST based API, this profile displays a list of Access URIs and API keys.
Runtime Metrics	*For SOAP, XML & REST APIs.* Displays the run-time performance metrics associated with the API. If you are using webMethods Mediator, webMethods Insight or another run-time monitoring component to log performance metrics for an API, CentraSite displays those metrics on this profile.
Runtime Events	*For SOAP, XML & REST APIs.* Displays the run-time events associated with the API. If you are using webMethods Mediator, webMethods Insight or another run-time monitoring component to log run-time events for an API, CentraSite displays those events on this profile.

Summary of Actions in the API

An action bar on the details page of an API contains the list of operations that can be performed on the API.

The following actions are available in the API details page:

Action Name	Icon	Usage
Save		You use this action to save the change made to an API's information.
Edit		You use this action to view an API's information and modify them.
Version		You use this action to generate a new version of an API.
Delete		You use this action to remove an API.
Virtualize		You use this action to create a virtual copy of an API.
Attach		You use this action to attach a supporting document to an API.
Watch		You use this action to subscribe notifications when changes are made to an API's information.
Add to List		You use this action to add an API to the My Favorites list.
Remove from List		You use this action to remove an API from the My Favorites list.

Action Name	Icon	Usage
Export		You use this action to export an API from one instance of CentraSite to another.
Consume		You use this action to register as a consumer for an API.
Revert		You use this action to revert an API request than has been submitted for approval.
View Report		You use this action to generate and view reports for an API.
Permission		You use this action to assign instance-level and profile-level permissions on an API.
API Consumption Settings		You use this action to configure the client consumption settings for an API.
Publish		You use this action to publish an API to the Mediator for consumption.
Unpublish		You use this action to unpublish an API from the Mediator.

5 Editing the Properties of an API

This section describes how to view an API's attributes and how to change them.

When editing the properties of an API, keep the following general points in mind:

- If you are not the owner of the API, you cannot edit the API unless you have Modify permission on the API (granted though either a role-based permission or an instance-level permission).
- When you view the details for the API, you will only see profiles for which you have View permission. You will only be able to edit the profiles on which you have Modify permission.
- Some attributes accept only specific types of information. For example, if the asset type includes a URL type attribute, you must supply a URL when you edit that attribute. Other attribute types that require a specific type of value include Date attributes and Email attributes. For a list of the attributes types that an API can include, see *Attribute Data Types* in the document *Managing the CentraSite Catalog*.
- Some attributes are designed to be read-only and cannot be edited even if they appear in an API on which you have Modify permission.

To edit the attributes of an API

1 In CentraSite Business UI, display the detail page of the API whose attributes you want to edit. If you need procedures for this step, see **Viewing Details for an API**.

2 On the API's actions menu, click **Edit**  .

3 To edit an API's basic attributes (Name, Version, Organization, Description etc.) , place the cursor in the appropriate field and modify the text as required.

4 To modify the extended attributes associated with the API, do the following:

1. Select the profile that contains the attribute(s) that you want to modify.
2. Edit the attributes on the profile as necessary.

3. Repeat the above steps for each profile that you want to edit.

5 When you have finished making your edits, click **Save**  .

Note: If at any time you want to abandon your unsaved edits, click **Close**  . CentraSite will ask you if you want to save your edits. Click **No** to abandon your edits and return the API's attributes to their previous settings.

Specifying an Input File

Certain APIs contain one or more associated files. For example, the SOAP API includes a WSDL file and the XML / REST API includes a schema file. You can upload a new file or update an existing file for the API accordingly.

- *For an instance of SOAP-based APIs*. Attach the WSDL file to the catalog entry using **Attach**  in the API's actions menu.
- *For an instance of XML or REST-based APIs*. Attach the schema file to the catalog entry using **Attach** in the API's actions menu.

Specifying a Native Endpoint

APIs (Service, XML service and REST service) can contain one or more operations or resources.

- *For an instance of SOAP-based APIs* If you are using WSDLs along with your SOAP API, attach the WSDL file to the catalog entry using **Attach**  in the API's actions menu.

  CentraSite automatically populates the WSDL URL and the associated operations in the **Technical Details** profile.
- *For an instance of XML or REST-based APIs* If you are using XML schemas along with your XML / REST API, attach the schema file to the catalog entry using **Attach** in the API's actions menu.

  CentraSite automatically populates the schema URL and the associated resources in the **Technical Details** profile.

  After you have specified a schema, specify the following:

Attribute	Description
Endpoint	An endpoint for the API that allows consumers of the API to find and communicate with the API.
Namespace	A binding namespace for the endpoint.
Resource	A name for the resource. You can specify multiple resources for an endpoint.
HTTP Method	HTTP request method(s) for bridging protocols (GET, POST, PUT, DELETE).

6 Setting Permissions on an API

By default, everyone in your organization is permitted to view the APIs that you create. However, only you (as the owner of the API) and users who belong to a role with the "Manage Assets" permission for your organization are allowed to view, edit and delete these API. To enable other users to view, edit and/or delete an API that you have created, you must modify the API's permission settings.

The following sections describe how to set permissions on an API.

Who Can Set Permissions on an API?

When setting permissions on APIs, keep the following points in mind:

- To set permissions on an API, you must belong to a role that has the "Manage Assets" permission or have the Full instance-level permission on the API itself.
- You can assign permissions to any individual user or group defined in CentraSite.
- The groups to which you can assign permissions include the following system-defined groups:

Group Name	Description
Users	All users within a specified organization.
Members	All users within a specified organization and its child organizations.
Everyone	All users of CentraSite *including guest users* (if your CentraSite permits access by guests).

- If a user is affected by multiple permission assignments, the user receives the union of all the assignments. For example, if group ABC has Modify permission on an API and group XYZ has Full permission on the same API, users that belong to both groups will, in effect, receive Full permission on the API.

  The same principle applies to users who have both role-based permissions and instance-level permissions on the same API. In this case, users receive the union of the role-based permission and the instance-level permission on the API.
- If you intend to give users in other organizations access to the API, and the API includes supporting documents that you want those users to be able to view, make sure you give those users permission to view the supporting documents as well as the API itself.

Setting Instance Level Permissions on an API

To assign permissions to an API

1 In CentraSite Business UI, display the details page for the API whose permissions you want to edit. If you need procedures for this step, see the section **Viewing Details for an API**.

2 On the API's actions menu, click the **Permissions**  icon.

3 In the **Assign Permissions** dialog box, select the users or groups to which you want to assign permissions.

4 Use the View, Modify and Full check boxes to assign specific permissions to each user and/or group in the **User/Group Permissions** list as follows:

Permission	Allows the selected user or group to...
View 	View the API.
Modify 	View and edit the API.
Full 	View, edit and delete the API. This permission also allows the selected user or group to assign instance-level permissions to the API.

5 When you assign instance-level permissions on an API, the related objects (for example, bindings, operations, interfaces etc.,) receive the same permissions that are assigned on the API.

6 Expand the **Advanced Settings** section, and do the following:

1. To ensure that the dependent APIs (for example, a WSDL or schema) receive the same permissions, select the checkbox **Propagate asset permissions**. If you unselect this checkbox, the permissions of the dependent APIs will not be modified.
2. To ensure that the dependent APIs of the same object type receive the same profile permissions, select the checkbox **Propagate profile permissions**.

7 If at any time, you wish to remove one or more users' or groups' permissions, click the **Delete**  icon next to the user or group name.

8 Click the **Ok** button to save the permission settings.

9 When you have finished making your changes, click the **Save**  icon.

Setting Instance Level Profile Permissions on an API

To assign instance-level permissions on an API's profiles

1 Choose the API's **Permissions**  action.

2 Locate the user or group for which you wish to set profile permissions. Then click the arrow icon beside the user or group name to open the profile permission list.

3 Use the checkboxes to indicate which profiles the user or group is permitted to view or modify.

4 Click **Ok** to save the new permission settings.

5 When you have finished making your changes, click the **Save**  icon.

7 Configuring the API Consumption Settings

The APIs represented in the CentraSite Business UI require that requests for consumption include a unique identifier for consumption. A unique identifier can do the following:

- **Identify** who is making a request.
- **Authenticate and validate** the client who is making a request.
- **Authorize** whether the client making a request is allowed to make that request.

CentraSite supports two separate mechanisms to create a unique identifier for clients to use for consuming APIs: API keys and OAuth 2.0 tokens.

The API provider (owner of the API) enforces the type of authentication (API key or OAuth2 token) required for consuming an API. Based on the authentication enforced for the API, an API consumer will request the API key or the OAuth2 token in order to consume (call) that API.

This section describes:

Who Can Configure the API Consumption Settings?

To configure the API consumption settings, you must belong to a role that has the "Modify Assets" permission for the organization in which the API resides. Else, at least have the Full instance-level permission on the API itself. However, if you belong to a role that has the "Manage Assets" permission, you can configure the consumption settings for APIs in all organizations. To see a list of the predefined roles that include the "Manage Assets" or "Modify Assets" permission, see the section *About Roles and Permissions* in the document *Users, Groups, Roles and Permissions*.

Note: Until you have the instance-level "Modify" permission on an API (at a minimum), you will not be able to see the **API Consumption Settings** action in the API details page.

Configuring the API Consumption Settings for API Key Authentication

The API Provider (and users who belong to a role with the permissions stated above) can enforce API key authentication by configuring the API's detail page. Such users can configure the following characteristics about client requests for API keys:

- Specify the approval requirements for clients requesting API keys.

  You can specify that requests must be approved by approver groups of your choosing, or you can specify that requests will be automatically approved.
- Configure email messages to be sent to:
  - The approver groups when requests are submitted for approval.
  - The clients to inform them of their approval status.

- Specify the expiration of the API key.

Clients that want to use the API key to call (consume) an API in CentraSite must:

1. Register as a consumer for the API, as specified in *Registering as Consumers for an API*.

   When the client registration request is approved, the client receives an API key (a base64-encoded string of the `consumer-key:consumer-secret` combination). It works for both SOAP and REST calls.
2. To call the API, the client must pass the API key in an HTTP request header or as a query string parameter. The use of this key establishes the client's identity and authentication.

   For information about how consumers will use generated API keys, see *Using Your API Keys for Consumption*.

To configure the API Consumption Settings for API key authentication

1 In CentraSite Business UI, display the details page for the API whose key settings you want to configure. For procedures, see the section *Viewing Details for an API*.

2 On the API details page, click **API Consumption Settings**  .

3 In the API Consumption Settings dialog, select **API Keys**.

4 In the **Usage Contract Expires After** field, type a time interval that represents how long you wish the API key to be active before it expires. Type the time interval in the following format: years (y) months (m) days (d) hours (h) minutes (min). For example, 1y 4w 3d 5h 30m expires the API key after 1 year, 4 weeks, 3 days, 5 hours, and 30 minutes of activity.

   When an API key expires, there are two ways a key can be renewed: a) The user can re-submit a request for consumption, or b) You (the provider) can renew the API key by selecting the **Renew** option. For procedures, see ***Renewing an API Key***.

   This field is optional. The default value "Unlimited" denotes that the API key never expires.

5 Select the **Require Approval** checkbox if you want to initiate an approval workflow for generating and renewing the API key.

   When a client requests for generating or renewing an API key that triggers an approval, CentraSite initiates an approval workflow and submits the client's request to the designated group of approvers.

   Approvers receive the approval request in the **Pending Approval Requests**  in the API details page. Approvers whose user account includes a valid email address also receive an email message informing them that a request is awaiting their approval.

CentraSite does not execute the client's requested operation until it obtains the necessary approvals. If an approver rejects the request, CentraSite notifies the requestor.

Or:

If you choose not to select the **Require Approval** checkbox, the request is automatically approved, and CentraSite executes the client's registration request.

6 If you select the **Require Approval** checkbox, complete the following fields:

Field	Description	
Approval is needed from	`All`	Requests must be approved by all users specified in **Approver Group**. (It does not matter in which order the approvals are issued.) A single rejection will cause the request to be rejected.
	`Any`	*Default.* Requests can be approved or rejected by any single user in **Approver Group**. Only one user from the set of authorized approvers is required to approve or reject the request.
Approver Group	Specify the approver group. You can specify multiple approver groups.	

For more information on approval management, see the section *Working with Approval Workflows* in the document *Administering the CentraSite Business UI*.

7 In the **Key Generation Settings** section, complete the following fields so that CentraSite will send emails consumers initially request API keys.

CentraSite automatically populates the default email settings (Subject, Template, Action) with the `<API Key Settings>` information from the *centrasite.xml* properties file.

Field	Description	
Subject	The text that will appear on the subject line of the email.	
Template	The template that will be used to generate the body of the email message. For information about using email templates, see the section ***Working with Email Notifications***. To specify an additional template, use the plus button to add additional rows. **Important:** CentraSite sends notifications about a request status to the consumer requesting for an API key; only if the client has enabled the **Email** notifications option in his User Preferences page.	
Action	Specify the approval action.	
	Value	**Description**

Field	Description	
	`Approved`	Default. CentraSite sends an email message to the client when requests are approved. If you choose this option, you can use the predefined template *APIKeyGenerationSuccess.html* for approval notifications if you do not want to create an email template of your own.
	`Approval Request`	CentraSite sends an email message to the approver(s) when requests are submitted for approval. If you choose this option, you can use the predefined template *PendingApprovalNotification.html* for pending-approval notifications if you do not want to create an email template of your own.
	`Rejected`	CentraSite sends an email message to the client when requests are rejected. If you choose this option, you can use the predefined template *RejectionNotification.html* for rejection notifications if you do not want to create an email template of your own.

8 In the **Key Renewal Settings** section, complete the following fields so that CentraSite will send emails when consumers request API key renewals.

CentraSite automatically populates the default email settings (Subject, Template, Action) with the `<API Key Settings>` information fetched from the *centrasite.xml* properties file.

Field	Description	
Subject	The text that will appear on the subject line of the email.	
Template	The template that will be used to generate the body of the email message. For information about using email templates, see the section ***Working with Email Notifications***. To specify an additional template, use the plus button to add additional rows. **Important:** CentraSite sends notifications to the client only if the client has enabled the **Email** notifications option in his User Preferences page.	
Action	Specify the approval action.	
	Value	**Description**

Field	Description	
	`Approved`	Default. CentraSite sends an email message to the client when requests are approved. If you choose this option, you can use the predefined template *APIKeyRenewalSuccess.html* for approval notifications if you do not want to create an email template of your own.
	`Approval Request`	CentraSite sends an email message to the approver group(s) when requests are submitted for approval. If you choose this option, you can use the predefined template *APIKeyRenewalPendingNotification.html* for pending-approval notifications if you do not want to create an email template of your own.
	`Rejected`	CentraSite sends an email message to the client when requests are rejected. If you choose this option, you can use the predefined template *RejectionNotification.html* for rejection notifications if you do not want to create an email template of your own.

9 In the **Key Revocation Settings** section, complete the following fields so that CentraSite will send emails when consumers request to have API keys revoked.

CentraSite automatically populates the default email settings (Subject, Template, Action) with the `<API Key Settings>` information fetched from the *centrasite.xml* properties file.

Field	Description
Subject	The text that will appear on the subject line of the email.
Template	The template that will be used to generate the body of the email message to the client. For information about using email templates, see the section ***Working with Email Notifications***. If you choose this option, you can use the predefined template *APIKeyRevocationSuccess.html* for success notifications if you do not want to create an email template of your own. **Important:** CentraSite sends notifications to the client only if the consumer has enabled the **Email** notifications option in his User Preferences page.

10 Click the **Configure** button.

CentraSite internally creates and activates an ***API Key Generation Policy*** specific to the API. When a client registers as a consumer, this policy will start the process of approving and generating the API key.

Configuring the API Consumption Settings for OAuth2 Authentication

The type of OAuth2 authorization grant that Mediator supports is “Client Credentials”. Client credentials are used as an authorization grant when the client is requesting API to protected resources based on an authorization previously arranged with the authorization server. That is, the client application gains authorization when it successfully registers with CentraSite as a consumer.

The API provider (and users who belong to a role with the permissions stated above) can enforce OAuth 2.0 authentication by configuring the API’s detail page. Such users can configure the following characteristics about the approval process of granting OAuth2 client credentials:

- Specify the approval requirements for client requests for client credentials.

  You can specify that requests must be approved by approver groups of your choosing, or you can specify that requests will be automatically approved.
- Configure email messages to be sent to:
  - The approver groups when requests are submitted for approval.
  - The clients to inform them of their approval status.

Clients that want to use the OAuth2 protocol to call APIs in CentraSite must:

1. Register as a consumer for the API, as specified in *Registering as Consumers for an API*.

   When the client registration request is approved, the client receives client credentials (a client_id and client_secret).
2. Request an OAuth2 access token by passing the client credentials to the Mediator-hosted REST service mediator.oauth2.getOAuth2AccessToken. This service will provide an OAuth2 access token to the client. For more information about this service, see *Fetching and Using Your OAuth2 Access Tokens for Consumption* .
3. To call the API, the client must pass their OAuth access token in an HTTP request header.

   An OAuth2 token is a unique token that a client uses to invoke APIs using the OAuth 2.0 protocol. The token contains an identifier that uniquely identifies the client. The use of a token establishes the client's identity, and is used for both the authentication and authorization.

To configure the API Consumption Settings for OAuth 2.0 authentication

1 In CentraSite Business UI, display the details page for the API whose OAuth 2.0 token settings you want to configure. For procedures, see the section *Viewing Details for an API*.

2 On the API details page, click **API Consumption Settings**  .

3 In the API Consumption Settings dialog, select **OAuth2**.

4 In the **Refresh Token After** field, type the period of time after which Mediator should refresh the token after it expires.

This field is optional. The default value "Unlimited" denotes that the token never expires.

5 Select the **Require Approval** checkbox if you want to initiate an approval workflow for generating the client credentials.

When a client request triggers an approval, CentraSite initiates an approval workflow and submits the client's request to the designated group of approvers. Approvers receive the approval request in the **Pending Approval Requests**  in the API details page. Approvers whose user account includes a valid email address also receive an email message informing them that a request is awaiting their approval.

CentraSite does not execute the client's requested operation until it obtains the necessary approvals. If an approver rejects the request, CentraSite notifies the requestor.

Or:

If you choose not to select the **Require Approval** checkbox, the request is automatically approved, and CentraSite executes the client's registration request.

6 If you select the **Require Approval** checkbox, complete the following fields:

Field	Description	
Approval is needed from	`All`	Requests must be approved by all users specified in **Approver Group**. (It does not matter in which order the approvals are issued.) A single rejection will cause the request to be rejected.
	`Any`	*Default.* Requests can be approved or rejected by any single user in **Approver Group**. Only one user from the set of authorized approvers is required to approve or reject the request.
Approver Group	Specify the approver group. You can specify multiple approver groups.	

For more information on approval management, see the section *Working with Approval Workflows*.

7 In the **Key Generation Settings** section, complete the following fields so that CentraSite will send emails when a client requests a token.

CentraSite automatically populates the default email settings (Subject, Template, Action) with the `<API Key Settings>` information from the *centrasite.xml* properties file.

Field	Description	
Subject	The text that will appear on the subject line of the email.	
Template	The template that will be used to generate the body of the email message. For information about using email templates, see the section ***Working with Email Notifications***. To specify another template, use the plus button to add additional rows. **Important:** CentraSite sends notifications about a request status to the client only if the client has enabled the **Email** notifications option in his User Preferences page.	
Action	Specify the approval action.	
	Value	**Description**
	`Approved`	Default. CentraSite sends an email message to clients when requests are approved. If you choose this option, you can use the predefined template *APIKeyGenerationSuccess.html* for approval notifications if you do not want to create an email template of your own.
	`Approval Request`	CentraSite sends an email message to the approver group(s) when requests are submitted for approval. If you choose this option, you can use the predefined template *PendingApprovalNotification.html* for pending-approval notifications if you do not want to create an email template of your own.
	`Rejected`	CentraSite sends an email message to clients when requests are rejected. If you choose this option, you can use the predefined template *RejectionNotification.html* for rejection notifications if you do not want to create an email template of your own.

8 Click the **Configure** button.

When a client registers as a consumer, an approval request is sent to the approvers you specified above.

8 Managing API Keys and OAuth 2.0 Tokens

This section describes to how an API Provider (owner) can manage API keys and OAuth2 tokens.

To manage the various operations (Generate, Renew, Revoke or Delete) on an API key or OAuth token, you must belong to a role that has the "Modify Assets" permission for the organization in which the API resides. Else, at least have the Full instance-level permission on the API itself. However, if you belong to a role that has the "Manage Assets" permission, you can configure the consumption settings for APIs in all organizations. To see a list of the predefined roles that include the "Manage Assets" or "Modify Assets" permission, see the section *About Roles and Permissions* in the document *Users, Groups, Roles and Permissions*.

The following sections describe how to manage your API keys and OAuth tokens.

Satisfying Key and OAuth Token Generation Requirements

For a user to consume an API with the API key or an OAuth token, the following prerequisites must be met:

- Ensure that you have configured the API Consumption Settings so that the API is configured for either API key authentication or OAuth2 authentication, as described in ***Configuring the API Consumption Settings.***
- Ensure that a run-time target instance (for example, Mediator) is up and running. For information on targets, see the section *Run-Time Targets*.

The API provider (and users who belong to a role with the permissions stated above) can satisfy the prerequisites.

Sometimes you might have to require an approval to generate an API key or OAuth token. If you selected the **Require Approval** option when you configure the API's consumption settings, CentraSite will not generate the API key or OAuth token until the required approvals are obtained. However, if an approval workflow is not configured for the API, the key or OAuth token is generated.

Once the API key or OAuth 2.0 request is approved by the designated approvers, an email notification is sent to both the API provider and API consumer.

CentraSite provides predefined email templates intended to be used for the API key or OAuth token generation. By default, these templates are configured in the *centrasite.xml* file. But, if you do not want to use the predefined email templates, you can create your own templates and configure the *centrasite.xml* file as necessary. For more information on how to configure the email templates for API key or OAuth token generation, see the following section ***Configuring the email templates for API key or OAuth token generation***.

For more information on how to configure the email notifications for API key or OAuth token generation in the CentraSite Business UI, see ***Configuring the API Consumption Settings*** .

Configuring the Email Templates for API Key or OAuth Token Generation

Notifications informing details and usage of the new API key or OAuth token are generated and sent to both the API provider and API consumer.

There are three kinds of key generation notifications:

- An API key or OAuth token request is pending for approval - an information type message to the API provider.
- Your API key or OAuth token request is approved - an information type message to the API consumer.
- Your API key or OAuth token request is rejected - an information type message to the API consumer.

You can configure delivery of such notifications in the *centrasite.xml* configuration file.

To configure notifications for API key or OAuth token generation

1 Use a text editor to open the *centrasite.xml* file for the API key or OAuth token generation notifications, which is typically located in the `<CentraSiteInstallDir>\cast\cswebapps\BusinessUI\` directory.

2 Locate the `KeyGenerationSettings` element in the file.

The key generation notification settings would look like the following:

```
<KeyGenerationSettings>
   <Approve ↩
subject="CS_MSG_INMBU_DEFAUL_EMAIL_SUBJECT_ACCESS_KEY_GENERATION_SUCCESS_OR_APPROVE" ↩
template="APIKeyGenerationSuccess.html" />
   <ApprovalRequest ↩
subject="CS_MSG_INMBU_DEFAUL_EMAIL_SUBJECT_ACCESS_KEY_GENERATION_PENDING" ↩
template="PendingApprovalNotification.html" />
   <Reject ↩
subject="CS_MSG_INMBU_DEFAUL_EMAIL_SUBJECT_ACCESS_KEY_GENERATION_REJECT" ↩
template="RejectionNotification.html" />
</KeyGenerationSettings>
```

3 Uncomment the section `API Key Settings` to enable key generation notifications.

4 Use the `Approve` property to set the subject and body of the notification message for the consumers whose API key or OAuth token request is approved.

5 Use the `ArppovalRequest` property to set the subject and body of the notification message for the provider who has an API key or OAuth token request pending for approval.

6 Use the `Reject` property to set the subject and body of the notification message for the consumers whose API key or OAuth token request is rejected.

7 Save and close the file.

8 Restart Software AG Runtime.

Renewing an API Key

After an API key is generated, sometimes you might have to renew the old key due to expiration or security concerns. You can also change expiration period for the API key or set it so that the key never expires.

The API provider (and users who belong to a role with the permissions stated above), can renew an API key.

Note: The **Renew** option is not available for the OAuth 2.0 tokens.

To renew an API key, the following prerequisites must be met:

- Ensure that you have configured the API Consumption Settings so that the API is configured for either API key authentication or OAuth2 authentication, as described in ***Configuring the API Consumption Settings.***
- Ensure that a target instance (for example, Mediator) is up and running. For information on targets, see the section *Run-Time Targets*.

The API provider (and users who belong to a role with the permissions stated above), can renew an API key.

To renew an API key

1 In CentraSite Business UI, display the details page for the API whose key you want to renew. For procedures, see the section *Viewing Details of an API*.

2 Locate the hyperlinked text “N” Consumers in the description area of the **Basic Information** profile, for example, “N” Consumers.

3 Click on the hyperlinked number “N” to see the list of keys available for the API.

4 Click on the hyperlinked API key name to see more information about who consume the API.

5 Review expiration date of the API key. A value of “Unlimited” indicates that the key never expires.

6 Locate the API key you want to renew.

7 Mouse over the API key name, and click on the **Renew**  icon displayed to the right hand side.

Important: If the API key has an unlimited expiration period, the **Renew** icon is *NOT* visible in the user interface.

Changing the Default Key Expiration Interval

API keys have a default expiration period, which you specify when you ***configure the API key consumption settings***.

You can also change expiration period for the API key or set it so that the key never expires.

Sometimes you might have to require an approval to renew (refresh) the API key. If you selected the **Require Approval** option when you ***configured the API key consumption settings***, CentraSite will not renew the API key until the required approvals are obtained. However, if an approval workflow is not configured for the API, the key is renewed instantly. For more information about approval actions, see the section *Working with Approval Workflows* in the document *Administering the CentraSite Business UI*.

Once the API key renewal request is approved by the designated approvers, an email notification informing the new validity of API key is sent to both the API provider and API consumer.

CentraSite provides predefined email templates only intended for the API key renewal. By default, these templates are configured in the *centrasite.xml* file. But, if you do not want to use the predefined email templates, you can create your own templates and configure the *centrasite.xml* file as necessary. For more information on how to configure the email templates for API key renewal, see the following section ***Configuring the email templates for key renewal***.

The API key with the new validity is republished to the Mediator, triggered by a *Deploy API Key* action that is included in the ***API Key Renewal* policy**.

For more information on how to configure the email notifications for API key renewal in the CentraSite Business UI, see ***Configuring the API Consumption Settings***.

Configuring the Email Templates for Key Expiration

Notifications informing about upcoming API key expiration and generated API key expired are generated and sent to the API consumer.

A consumer can have two kinds of key expiration notifications:

- API key has expired - a critical event type message.
- API key expires soon - a warning type message. It will be generated "n" days before the key expiration date and displayed every day before the key actually expires.

You can configure delivery of such notifications in the *centrasite.xml* configuration file.

To configure templates for API key expiration

1 Use a text editor to open the *centrasite.xml* file for the key expiration notifications, which is typically located in the `<CentraSiteInstallDir>\cast\cswebapps\BusinessUI\` directory.

2 Locate the `ExpiryNotificationSettings` element in the file.

The expiration notification settings would look like the following:

```
<ExpiryNotificationSettings>
  <ExpiredNotification subject="Access key has expired!" ↩
template="APIKeyExpiredNotification.html" />
  <AdvanceNotification subject="Access key about to expire!" ↩
template="APIKeyExpirationNotification.html" />
  <SchedulerExecutionFrequency>12h</SchedulerExecutionFrequency>
  <AdvanceNotificationInterval>5d</AdvanceNotificationInterval>
</ExpiryNotificationSettings>
```

3 Uncomment the section `API KEY EXPIRATION CONFIGURATION` to enable key expiration notifications.

4 Use the `ExpiredNotification` property to set the subject and body of the notification message for the consumers whose API key has expired.

5 Use the `AdvanceNotification` property to set the subject and body of the notification message for the consumers whose API keys are due to expire.

6 Use the `SchedulerExecutionFrequency` attribute to specify how frequently to check for the expiration status of API keys. Enter the time interval in the following format: years (y), months (m), days (d), hours (h), minutes (min).

7 Use the `AdvanceNotificationInterval` attribute to specify how many days should be consumers notified before the key expiration (in days). Then the consumers are entitled receive a notification message as configured in the `AdvanceNotification` property. Enter the time interval in the following format: years (y) months (m) days (d) hours (h) minutes (min).

8 Save and close the file.

Important: If you have set up a Software AG Runtime cluster with load balancing, locate the `CENTRASITE ACCESS URL CONFIGURATION` element, and ensure that the `lb_or_reverse_proxy_url` attribute in the following property points to the load balancer's IP/Port.

```
<CentraSite url="http://localhost:53305/CentraSite/CentraSite" ↩
lb_or_reverse_proxy_url="http://localhost:53307"/>
```

9 Restart Software AG Runtime.

Configuring the Email Templates for Key Renewal

Notifications informing the new validity of the API key are generated and sent to both the API provider and API consumer.

There are three kinds of key renewal notifications:

- An API key renewal request is pending for approval - an information type message to the API provider.
- Your API key renewal request is approved - an information type message to the API consumer.
- Your API key renewal request is rejected - an information type message to the API consumer.

You can configure delivery of such notifications in the *centrasite.xml* configuration file.

To configure email templates for API key renewal

1 Use a text editor to open the *centrasite.xml* file for the key renewal notifications, which is typically located in the `<CentraSiteInstallDir>\cast\cswebapps\BusinessUI\` directory.

2 Locate the `KeyRenewalSettings` element in the file.

The key renewal notification settings would look like the following:

```
<KeyRenewalSettings>        <Approve ↩
subject="CS_MSG_INMBU_DEFAUL_EMAIL_SUBJECT_ACCESS_KEY_RENEWAL_SUCCESS_OR_APPROVE" ↩
template="APIKeyRenewalSuccess.html" />        <ApprovalRequest ↩
subject="CS_MSG_INMBU_DEFAUL_EMAIL_SUBJECT_ACCESS_KEY_RENEWAL_PENDING" ↩
template="APIKeyRenewalPendingNotification.html" />        <Reject ↩
subject="CS_MSG_INMBU_DEFAUL_EMAIL_SUBJECT_ACCESS_KEY_RENEWAL_REJECT" ↩
template="RejectionNotification.html" />      </KeyRenewalSettings>
```

3 Uncomment the section `API Key Settings` to enable key renewal notifications.

4 Use the `Approve` property to set the subject and body of the notification message for the consumers whose API key renewal request is approved.

5 Use the `ArppovalRequest` property to set the subject and body of the notification message for the provider who has an API key renewal request pending for approval.

6 Use the `Reject` property to set the subject and body of the notification message for the consumers whose API key renewal request is rejected.

7 Save and close the file.

8 Restart Software AG Runtime.

Revoking an API Key

After issuing an API key, you might want to revoke the key if you find serious error in the API. When you revoke an API key, client access to the associated API is blocked, and the client that is assigned that key can no longer access the resources exposed by that API.

The API provider (and users who belong to a role with the permissions stated above), can revoke an API key.

Note: The **Revoke** option is not available for the OAuth 2.0 tokens.

To revoke an API key, the following prerequisites must be met:

- Ensure that you have configured the API Consumption Settings so that the API is configured for either API key authentication or OAuth2 authentication, as described in ***Configuring the API Consumption Settings.***
- Ensure that a target instance (for example, Mediator) is up and running. For information on targets, see the section *Run-Time Targets*.

To revoke an API key

1 In CentraSite Business UI, display the details page for the API whose key you want to revoke. For procedures, see the section *Viewing Details for an API*.

2 Locate the hyperlinked text "N" Consumers in the description area of the **Basic Information** profile, for example, "N" Consumers.

3 Click on the hyperlinked number "N" to see the list of keys available for the API.

4 Click on the hyperlinked API key name to see more information about who consume the API.

5 Locate the API key you want to revoke.

6 Mouse over the API key name, and click on the **Revoke** icon displayed to the right hand side.

A confirmation message appears that the API key will be revoked.

Once the API key revocation is processed, CentraSite sends an email message to the API consumer informing that the request has been processed successfully.

CentraSite provides predefined email template only intended for the API key revocation. By default, this template is configured in the *centrasite.xml* file. But, if you do not want to use the predefined email template, you can create your own template and configure the *centrasite.xml* file as necessary.

For more information on how to configure an email template for API key revocation, see the following section ***Configuring the email notification for key revocation***.

For more information on how to configure an email notification for API key revocation in the CentraSite Business UI, see ***Configuring the API Consumption Settings***.

Configuring the Email Notification for Key Revocation

Notification informing the successful processing of an API key revocation is sent to the API consumer.

You can configure delivery of such notification in the *centrasite.xml* configuration file.

To configure email templates for API key revocation

1 Use a text editor to open the *centrasite.xml* file for the key revocation notification, which is typically located in the `<CentraSiteInstallDir>\cast\cswebapps\BusinessUI\` directory.

2 Locate the `KeyRevocationSettings` element in the file.

The key revocation notification settings would look like the following:

```
<KeyRevocationSettings>
  <Approve ↩
subject="CS_MSG_INMBU_DEFAUL_EMAIL_SUBJECT_ACCESS_KEY_REVOCATION_NOTIFICATION" ↩
template="APIKeyRevocationSuccess.html"/>
</KeyRevocationSettings>
```

3 Uncomment the section `API Key Settings` to enable key revocation notifications.

4 Use the `Approve` property to set the subject and body of the notification message for the consumers whose API key revocation request is processed successfully.

5 Save and close the file.

6 Restart Software AG Runtime.

Deleting an API Key

Deleting an API key permanently removes the entry for the API key (that is, it removes the instance of the API key from the CentraSite registry/repository). Deleting an API key will not remove the API that is associated with it.

The API provider (and users who belong to a role with the permissions stated above), can delete an API key.

When you delete an API key, keep the following points in mind:

- You cannot delete an API key that is in the "pending" mode (example, awaiting a renew approval).
- Deletion of an API key will succeed only if the key is already revoked.

To delete an API key

1 In CentraSite Business UI, display the details page for the API key that you want to delete. If you need procedures for this step, see the section ***Viewing Details for an API***.

2 On the API key's actions menu, click **Delete**  .

3 When you are prompted to confirm the delete operation, click **Yes**.

The API key is permanently removed from the CentraSite registry.

You can delete multiple API keys in a single step. The rules described above for deleting a single API key apply also when deleting multiple API keys.

Important: A key must be revoked before it can be deleted.

To delete multiple API keys in a single operation

1 In CentraSite Business UI, use either the Browse or Search feature to select a set of API keys you want to delete. If you need information on how to browse or search the Business UI, refer to the section *Browsing the CentraSite Catalog* or *Searching the CentraSite Catalog* in the document *Managing the CentraSite Catalog*.

2 Mark the checkbox next to the name of each API key you want to delete.

3 In the actions menu, click **Delete**  .

Note: If one or more or the selected API keys are in pending mode (example, awaiting approval), an error message will appear and no API key will be deleted.

9 Approving a Request

If you are the CentraSite Administrator, an API provider or a designated approver, CentraSite places requests for your review and approval.

This section details on how to review and approve the API related requests.

Requests for Consumer Onboarding Registration

The onboarding requests for *a user* or *an organization with user* is tracked in the following ways:

- If the user has specified an existing organization in the CentraSite registry, the Consumer Onboarding request is visible in the details page of the organization that is configured in the specified organization's "Consumer Onboarding" policy.
- If the user has specified an organization that does not exist in the CentraSite registry, the organization with Consumer Onboarding request is visible in the Default Organization's details page.
- If the user has not specified any organization, the Consumer Onboarding request is visible in the details page of the organization that is configured in the "Global Onboarding" policy.

Users with the “Manage Organizations” system-level permission (such as the users with the role "CentraSite Administrator") can view and approve onboarding requests for any organization. Users with the “Organization Administrator” organization-level role for a given organization can perform view and approve onboarding requests on that organization.

To view and approve consumer registration requests

1 In CentraSite Business UI, display the details page for the organization whose user registration request you want to review and approve.

2 You will see the pending user registration requests () in the description area of the **Basic Information** profile, for example, "`N user registration requests are pending`”.

If there are no pending approval requests for the organization, this is displayed as “`0`".

3 Click the hyperlinked number (“`N`”) to open the **Pending User Registration Requests** dialog. This dialog contains a list of all requests that have been submitted for the particular organization, including requests that were auto-approved.

4 Choose the user registration request that you want to review and approve by clicking its hyperlinked name.

The details for the request will appear in the **User Registration Requests** dialog.

5 In the **Comment** text box, type a comment. (e.g., *”Request rejected. Add required specifications to this user and resubmit”*.)

6 Click the **Accept** or **Reject** button as appropriate to approve or reject the request.

Requests for API Key Management

When a user submits an API request that requires an approval, CentraSite initiates an approval workflow and submits the user's request to both the API provider and designated group of approvers.

Approvers receive the approval requests in the API details page in CentraSite Business UI. Approvers whose user account includes a valid email address also receive an email message informing them that a request is awaiting their approval.

CentraSite does not process an API request until it obtains the necessary approvals. If an approver rejects the request, CentraSite notifies the requestor and ignores further processing.

The following requests for API key management can trigger an approval workflow:

- Generating an API Key / OAuth Token
- Renewing an API Key
- Revoking an API Key

Note: For CentraSite to issue email messages, an administrator must first configure CentraSite's email server settings. For procedures, see the section *Configuring the Email Server* in the document *Basic Operations*.

Important:

Points to consider when approving or rejecting an API key request for consumption:

- If the user who makes an API request is also an authorized approver for the action, the request is auto-approved. (In other words, the requestor's approval is granted implicitly.)
- If an API provider has configured the **Require Approval** option in the **API Consumption Settings** for "Anyone" approval mode, only one user in the group is required to approve or reject the request. This is the default mode.
- If an API provider has configured for the "All" approval mode, the request must be approved by all users in the approver group (it does not matter in which order the approvals are obtained). A rejection by any approver in the group will cause the request to be rejected.

To view and approve consumer registration requests

1 In CentraSite Business UI, display the details page for the API whose request you want to review and approve.

2 You will see the pending approval requests () for an API in the description area of the **Basic Information** profile, for example, "`N number of pending approvals`".

If there are no pending approval requests for the API, this is displayed as "0".

3 Click the hyperlinked number ("N") to open the **Pending Approval Requests** dialog. This dialog contains a list of requests that have been submitted for the particular API, including requests that were auto-approved.

4 Choose the API request that you want to review and approve by clicking its hyperlinked name.

The details for the request will appear in the **API Request** dialog.

5 In the **Comment** text box, type a comment. (e.g., *"Request rejected. Add required specifications to this asset and resubmit"*.)

6 Click the **Accept** or **Reject** button as appropriate to approve or reject the request.

10 Deleting an API

Deleting an API permanently removes the API from the CentraSite registry.

When you delete an API, CentraSite removes the registry entry for the API (that is, it removes the instance of the API from CentraSite's object database). Also note that:

- You cannot delete the predefined APIs (not even if you have the default permissions associated with the "CentraSite Administrator" role).
- If you are not the owner of the API, you cannot delete the API unless you have “Manage Assets” permission (granted though a role-based permission) or at least Full permission on the API (granted through an instance-level permission).
- You cannot delete an API that is in pending state (e.g., awaiting approval).
- You cannot delete an API if any user in your CentraSite registry is currently modifying the API.
- Deleting an API will not remove the supporting documents that are attached to it.

You can delete a single proxy API or a selected set of proxy APIs. The descriptions in this section give you details on how to do this.

Deleting a Single API

To delete a single API

1 In CentraSite Business UI, display the details page for the API that you want to delete. If you need procedures for this step, see the section *Viewing Details for an API*.

2 On the API’s actions menu, click **Delete** ( ).

3 When you are prompted to confirm the delete operation, click **Yes**.

The API is permanently removed from the CentraSite registry.

Deleting a Set of APIs

You can delete multiple APIs in a single step. The rules described above for deleting a single API apply also when deleting multiple APIs.

Important: If you have selected several APIs where one or more of them are predefined APIs, only those APIs you have permission for will be deleted. The same applies to any other APIs for which you do not have the required permission.

To delete multiple APIs in a single operation

1 In CentraSite Business UI, use either the *Browse* or *Search* feature to select a set of APIs you want to delete. If you need information on how to browse or search the CentraSite catalog, refer to the section *Browsing the CentraSite Catalog* or *Searching the CentraSite Catalog* in the document *Managing the CentraSite Catalog*.

2 Mark the checkbox next to the name of each API you want to delete.

3 In the actions menu, click **Delete** ().

Note: If one or more or the selected APIs is in pending state (e.g., awaiting approval), an error message will appear and no APIs will be deleted.

11 Working with Email Notifications

You can configure the approval workflow system so that users receive email notifications when workflow-related events occur. Notifications can be sent to users who have requests to approve. You can use predefined email templates for workflow notifications, or you can use a custom email template for each workflow that you create. For example, if you have an approval request workflow, you can use an email template that was written specifically for approval request.

Note: For CentraSite to issue email messages, an administrator must first configure CentraSite's email server settings. For procedures, see the section *Configuring the Email Server* in the document *Basic Operations*.

The content is organized under the following topics:

Predefined Email Templates Installed with CentraSite

The following predefined email templates are installed with CentraSite. These templates are provided for you to use with the API Management workflow listed below if you do not want to create your own email templates.

Template Name	Description	To use with...
APIKeyGenerationSuccess.html	Default email template used when an approval request for API key generation is approved.	The `Approved` action in the Key Generation Settings panel.
PendingApprovalNotification.html	Default email template used when an approval request for API key generation is submitted to approvers.	The `Approval Request` action in the Key Generation Settings panel.
APIKeyRenewalSuccess.html	Default email template used when an approval request for	The `Approved` action in the Key Renewal Settings panel.

Template Name	Description	To use with...
	API key renewal is approved.	
APIKeyRenewalPendingNotification.html	Default email template used when an approval request for API key renewal is submitted to approvers.	The `Approval Request` action in the Key Renewal Settings panel.
RejectionNotification.html	Default email template used when an approval request is rejected.	The `Rejected` action in the Key Generation Settings and Key Renewal Settings.
APIKeyRevocationSuccess.html	Default email template used when an approval request for API key revocation is approved.	The `Approved` action in the Key Revocation Settings panel.
APIKeyExpiredNotification.html	Default email template used when an API key has expired.	In the *centrasite.xml* file located in the *<CentraSiteInstallDir>\cast\cswebapps\BusinessUI* directory
APIKeyExpirationNotification.html	Default email template used when an API key is about to expire.	In the *centrasite.xml* file located in the *<CentraSiteInstallDir>\cast\cswebapps\BusinessUI* directory
OnboardingSuccessMessage.html	Default notification template used for	The `Onboarding Organization` action in the Global Onboarding Policy. - OR -

Template Name	Description	To use with...
	notifying a consumer that a request for consumer onboarding has been processed successfully.	The `Onboarding User` action in the Consumer Onboarding Policy.
APIKeyDeployFailed.html	Default notification template used for notifying a provider that an API key generation has failed.	For internal use.

Custom Email Template

You can use a custom email template for each workflow that you create. To write an email template for a workflow, see the instructions in *Create Email Templates for Workflow Notifications* below.

Create Email Templates for Workflow Notifications

You can use a specific email template for each workflow that you create. For example, if you have an API Consumption Approval workflow, you can use an email template that was written specifically for the API consumption approval.

Complete the following procedures to create a custom email template.

1. Create your own custom HTML email template.

   Your HTML document should include the <html> and <label> tags as shown in the example below.

Example of a Notify API Key Generation Email Template

```
<html>
    Congratulations! ${policycontext.consumer.name},<br/><br/>
    Your Consumption Request for the API ${entity.name} on ${request.date} has ↩
been processed successfully. <br/>
    You can now access the API using the API Key - <b> ${policycontext.apikey} ↩
</b>. The key expires on <b> ${apikey.expirationdate} </b><br/><br/>
    <b>Information about API usage:</b>
 <br>${api.usage}</br>
</html>
```

2. Specify the key parameters.

Set this parameter...	To specify...
{policycontext.consumer.name}	Name of the consumer.
{entity.name}	Name of the API.
{request.date}	Date of the request for API consumption.
{policycontext.apikey}	The API key.
{apikey.expirationdate}	Expiration date of the API key.
{api.usage}	Usage tips for the API key.

12 Working with Predefined Policies

CentraSite's approval-management framework enables you to review a request and approve or reject the request when certain time events occur in the registry. For example, you might require a system architect to review and approve all APIs before they are switched to a productive state.

To impose an approval process on a change time event, you create an *approval policy* for the event. An approval policy is a policy that contains one of CentraSite's built-in *approval actions*.

The content is organized under the following topics:

Summary of the Predefined Policies

CentraSite provides predefined policies specific to the Business UI.

By default, predefined policies are not displayed by CentraSite Control. To view predefined policies, you must enable the **Show Predefined Policies** option on the Design/Change-Time Policy page.

Policy Name	Description
Global New User Account	See ***Using the User Registration Policy***.
Global Onboarding	See ***Using the Consumer Onboarding Policy***.
API Key Generation	See ***Using the API Key Generation Policy***.
API Key Renewal	See ***Using the API Key Renewal Policy***.
API Key Revocation	See ***Using the API Key Revocation Policy***.

User Registration Policies

The New Account policies trigger an approval workflow when users request for an account in the CentraSite registry.

When users request a CentraSite account (as described in *Creating Your New Account*), the policy is triggered and the “User Registration” or an “Organization with User Registration” request is submitted to all members of the approval list specified in the “Initiate Approval” action. Then, the approvers can either approve or decline the request. If the approvers approve the request, the users will be registered in the CentraSite registry, and appropriate permissions will be assigned to users.

To use the CentraSite's new account feature, you *must configure* the “Global New User Account Policy” and every organization's “New User Account Policy”.

Note: You do not need to explicitly activate the new account policies.

Global New User Account Policy

The *Global New User Account Policy* enables an automated user registration to address the following scenarios:

- If the user does not explicitly specify an organization, the policy registers the user in the organization defined in the "Onboarding Organization" action of the policy. By default, it is set to "Default Organization".
- If the user specifies an organization which does not currently exist in the CentraSite registry, the policy creates the new organization, and registers the user in the new organization.

Note: To use the email options provided by this policy, CentraSite must have a connection to an SMTP email server. For instructions on how to configure CentraSite's connection to an email server, see the section *Configuring the Email Server* in the document *Basic Operations*.

The *Global New User Account Policy* has input parameters that you must set to enforce the user registration.

To configure the input parameters for Global New User Account Policy

1 Display the Global New User Account Policy Details page whose actions you want to configure. If you need procedures for this step, see *Viewing or Changing a Policy*.

2 On the **Actions** tab do the following:

1. *Mandatory.* To configure the **Initiate Approval** action, set the following parameters:
   - *Mandatory.* **Approver Group**: Specify the designated group of approvers.
   - *Mandatory.* **Approval is needed from**: Specify an approval mode "All" or "Anyone".

   Click **Save** to update the parameter settings.
2. For more information about configuring the Initiate Approval action, see the section *Initiate Approval* in the document Built-In Design/Change-Time Actions Reference.
3. To configure the **Onboarding Organization** action, set the following parameters:
   - *Mandatory.* **Onboarding Organization**: Specify the organization in which you want to register the user, when the requestor has not specified any organization. By default, "Default Organization".
   - **Onboarding Success Message**: Specify a notification template for the new user account success message. By default, "NewAccountSuccessMessage.html".
4. Click **Save** to update the parameter settings.

New User Account Policy

The “New User Account Policy” of an organization enables an automated registration of user for the particular organization.

Note: To use the email options provided by this policy, CentraSite must have a connection to an SMTP email server. For instructions on how to configure CentraSite's connection to an email server, see the section *Configuring the Email Server* in the document *Basic Operations*.

The *New User Account Policy* has input parameters that you must set to enforce the user registration.

To configure the input parameters for New User Account Policy

1 Display the New User Account Policy Details page whose actions you want to configure. If you need procedures for this step, see *Viewing or Changing a Policy*.

2 On the **Actions** tab do the following:

1. On the **Initiate Approval** action, set the parameters:
   - *Mandatory.* **Approver Group**: Specify the designated group of approvers.
   - *Mandatory.* **Approval is needed from**: Specify an approval mode "All" or "Anyone".
   - Click **Save** to update the parameter settings.
2. On the **Onboarding User** action, set the parameters:
   - **Onboarding Organization**: Specify the organization in which you want to register the user. By default, "Default Organization".
   - **Onboarding Success Message**: Specify a notification template for the new user account success message. By default, "NewAccountSuccessMessage.html".
   - Click **Save** to update the parameter settings.

Consumer Onboarding Policies

CentraSite's approval-management framework enables you to configure policies that trigger approval processes when guest users (i.e. users without a valid CentraSite user account) try to access and register as consumers of APIs.

When users register as consumers for APIs (as described in *Virtualizing APIs Using the CentraSite Business UI > Registering as Consumers for an API*), the policy is triggered and the “User Registration” or an "Organization with User Registration" request is submitted to all members of the approval list specified in the “Initiate Approval” action. Then, the approvers can either approve or decline the request. If the approvers approve the request, the users will be registered as consumers, and appropriate permissions will be assigned to users.

To use the CentraSite's consumer-onboarding feature, you *must configure* the “Global Onboarding Policy” and every organization's “Consumer Onboarding Policy”.

Note: You do not need to explicitly activate the onboarding policies.

Global Onboarding Policy

The *Global Onboarding Policy* enables an automated onboarding to address the following scenarios:

- If the user does not explicitly specify an organization, the policy onboards the user in the organization defined in the "Onboarding Organization" action of the policy. By default, it is set to "Default Organization".
- If the user specifies an organization which does not currently exist in the CentraSite registry, the policy creates the new organization, and onboards the user in the new organization with an "Organization Administrator" role.

On successful onboarding of an user within the specified organization, CentraSite performs the API consumption process that has already been initiated.

Note: To use the email options provided by this policy, CentraSite must have a connection to an SMTP email server. For instructions on how to configure CentraSite's connection to an email server, see the section *Configuring the Email Server* in the document *Basic Operations*.

The *Global Onboarding Policy* has input parameters that you must set to enforce the consumer onboarding.

To configure the input parameters for Global Onboarding Policy

1 Display the Global Onboarding Policy Details page whose actions you want to configure. If you need procedures for this step, see *Viewing or Changing a Policy*.

2 On the **Actions** tab do the following:

1. *Mandatory.* To configure the **Initiate Approval** action, set the following parameters:
   - *Mandatory.* **Approver Group**: Specify the designated group of approvers.
   - *Mandatory.* **Approval is needed from**: Specify an approval mode "All" or "Anyone".

   Click **Save** to update the parameter settings.
2. For more information about configuring the Initiate Approval action, see the section *Initiate Approval* in the document Built-In Design/Change-Time Actions Reference.
3. To configure the **Onboarding Organization** action, set the following parameters:
   - *Mandatory.* **Onboarding Organization**: Specify the organization to which you want to onboard the user as a consumer, when user requesting for an account has not specified any organization. By default, "Default Organization".

- **Onboarding Success Message**: Specify a notification template for the consumer onboarding success message. By default, "OnboardingSuccessMessage.html".

4. Click **Save** to update the parameter settings.

Consumer Onboarding Policy

The "Consumer Onboarding Policy" of an organization enables an automated onboarding of user for that organization. On successful onboarding, performs the API consumption process that has already been initiated. If the API consumption includes an approval workflow, on approval, CentraSite generates the API key. On the other hand, if the API consumption does not include an approval workflow, CentraSite generates the API key immediately.

Note: To use the email options provided by this policy, CentraSite must have a connection to an SMTP email server. For instructions on how to configure CentraSite's connection to an email server, see the section *Configuring the Email Server* in the document *Basic Operations*.

The *Consumer Onboarding Policy* has input parameters that you must set to enforce the consumer onboarding.

To configure the input parameters for Consumer Onboarding Policy

1 Display the Consumer Onboarding Policy Details page whose actions you want to configure. If you need procedures for this step, see *Viewing or Changing a Policy*.

2 On the **Actions** tab do the following:

1. On the **Initiate Approval** action, set the parameters:
   - *Mandatory.* **Approver Group**: Specify the designated group of approvers.
   - *Mandatory.* **Approval is needed from**: Specify an approval mode "All" or "Anyone".
   - Click **Save** to update the parameter settings.
2. On the **Onboarding User** action, set the parameters:
   - **Onboarding Organization**: Specify the organization to which you want to onboard the user as consumer. By default, "Default Organization".
   - **Onboarding Success Message**: Specify a notification template for the consumer onboarding success message. By default, "OnboardingSuccessMessage.html".
   - Click **Save** to update the parameter settings.

API Key Generation Policy

To prevent unauthorized access of an API, API Providers generate the API key which serve as an user access token for identify the final consumer of the particular API.

When a consumer registers as a consumer for an API (as described in *Virtualizing APIs Using the CentraSite Business UI > Registering as Consumers for an API*), CentraSite internally creates and triggers an API Key Generation policy for the API. A request for the API consumption is subsequently submitted to all members of the approval list specified in the Initiate Approval action. The approvers can either approve or decline the request. If the approvers approve the request, CentraSite generates the API key, deploys the generated key in the Mediator, and notifies the consumer that the API is now ready for consumption using the generated key.

Note: To use the email options provided by this policy, CentraSite must have a connection to an SMTP email server. For instructions on how to configure CentraSite's connection to an email server, see the section *Configuring the Email Server* in the document *Basic Operations*.

The following actions are typically used with the API Key Generation policy.

- The *Initiate Approval* action is generally used to obtain necessary approvals for a consumer prior to executing the *API Key Generator* action.
- The *API Key Generator* action is used to generate the API key for an API, and thereby create a relationship between the API and the specified consumer.
- The *Deploy API Key* is typically executed after the *API Key Generator* action to deploy the generated key in the Mediator.
- The *Send Email Notification* action is used to send an email message with details of the new API key to the consumer.

Object Scope

Virtual Service, XML Service, REST Service, Virtual XML Service, Virtual REST Service

Event Scope

OnTrigger

Initiate Approval

Initiates an approval workflow.

When this action is executed, CentraSite initiates the approval process. CentraSite will not process any subsequent actions in the policy or execute the requested operation until the approvals specified by the Initiate Approval action are received.

For more information about creating approval policies, see the section *Working with Approval Workflows* in the document *Administering the CentraSite Business UI*.

Input Parameters

<table>
<tr><td>User</td><td>String The user name that will be used together with the Password parameter as authentication credentials for performing a request on an API. The credentials are stored in the approval request and passed to the API for completing the approval.

This parameter is only visible to users with the CentraSite Administrator role.</td></tr>
<tr><td>Password</td><td>String The password that will be used together with the User parameter as authentication credentials.

This parameter is only visible to users with the CentraSite Administrator role.</td></tr>
<tr><td>Approval Flow Name</td><td>String The name to be given to the approval workflow that this action initiates. This name serves to identify the workflow in the approver's Pending Approvals.

An approval flow name can contain any combination of characters, including a space.

You can also include substitution tokens in the name to incorporate data from the target object on which the policy is acting. For a list of the allowed tokens, see the list of Substitution Tokens shown in the Send Email Notification action.</td></tr>
<tr><td>Approver Group</td><td>String Array The user group (or groups) that identifies the set of users who are authorized to approve the requested operation.

Note: If the user groups specified in Approver Group are empty at enforcement time, the user's request is auto-approved.</td></tr>
<tr><td>Approval is Needed From</td><td>String The manner in which the approval is to be processed:
<table>
<tr><th>Value</th><th>Description</th></tr>
<tr><td>AnyOne</td><td>Default The request can be approved or rejected by any single user in Approver Group. In this mode, only one user from the set of authorized approvers is required to approve or reject the request.</td></tr>
</table></td></tr>
</table>

	EveryOne	The request must be approved by all users specified in Approver Group. (It does not matter in which order the approvals are issued.) A single rejection will cause the request to be rejected.
Reject State	The lifecycle state that is to be assigned to the API if the approval request is rejected. If this parameter is not specified, the API's lifecycle state does not change when a rejection occurs. The lifecycle model must define a valid transition from the state that the target object is in at the time it is submitted for approval to the state specified in Reject State. Otherwise, the target object's state will not be switched when a rejection occurs. For more information about using this parameter, see the topic *Switching the State of an Object when an Approval Request is Rejected* in the section *Working with Approval Workflows* in the document *Administering the CentraSite Business UI*.	
Send Pending Approval Email	*Boolean* Specifies whether CentraSite is to send an email message to specified users and/or groups when the request is initially submitted for approval. If you enable this option, you must set the following parameters to specify the text of the message and to whom it is to be sent. **Note:** If the request is auto-approved, this message is not sent. **Note:** CentraSite automatically sends the email message to the approvers in addition to the users and/or groups that you specify below.	
	Users	*Array of Users* Users who are to receive the email. **Note:** You can specify the recipients of the email using the Users parameter, the Groups parameter, or both.
	Groups	*Array of Groups* Groups whose users are to receive the email. **Note:** CentraSite will only send the email to those users in the group whose CentraSite user account includes an email address.
	Subject	*String* The text that you want to appear in the subject line of the email. This text can include substitution tokens to insert run-time data into the subject line. For available tokens, see the list of Substitution Tokens shown in the *Send Email Notification* action.
	Use Email Template	*Email Template* Specifies the template that is to be used to generate the body of the email message. For more information about using email templates, see the topic *Predefined Email Templates Installed with CentraSite* in the section *Working with Email Notifications* . **Note:** You can use the predefined template, PendingNotification.html, for pending-approval notifications if you do not want to create an email template of your own.

		Note: If you use an email template to generate the body of the message, you cannot specify the body of the message using the `Custom Message` parameter. (In other words, you specify the body of the message using either the `Use Email Template` *or* the `Custom Message` parameter.)
	`Custom Message`	*TextArea* The text of the email message. This text can include substitution tokens to insert run-time data into the message. For available tokens, see the list of Substitution Tokens shown in the *Send Email Notification* action. **Note:** If you use the `Custom Message` parameter to specify the body of the email message, you cannot generate the body of the message using an email template. (In other words, you specify the body of the message using either the `Custom Message` *or* the `Use Email Template` parameter.)
	`Format`	*String* Specifies whether the message in the `Custom Message` parameter is formatted as HTML or plain text.
	`Include owner in notification`	*Boolean* When the parameter is enabled, CentraSite sends the email to the provider of the API (on which the policy is acting) in addition to the other recipients.
`Send Approval Email`	*Boolean* Specifies whether CentraSite is to send an email message to specified users and/or groups when the request is approved. If you enable this option, you must set the following parameters to specify the text of the message and to whom it is to be sent. **Note:** CentraSite automatically sends the email message to the user who submitted the approval request in addition to the users and/or groups that you specify below. **Note:** When the EveryOne option is specified in the `Approval is Needed From` parameter, CentraSite sends this email only after all approvers have approved the request.	
	`Users`	See description of `Users` parameter above.
	`Groups`	See description of `Groups` parameter above.
	`Subject`	See description of `Subject` parameter above.
	`Use Email Template`	See description of `Use Email Template` parameter above. **Note:** You can use the predefined template, ApprovalNotification.html, for approval notifications if you do not want to create an email template of your own.
	`Custom Message`	See description of `Custom Message` parameter above.
	`Format`	See description of `Format` parameter above.
	`Include owner in notification`	See description of `Include owner in notification` parameter above.

`Send Rejection Email`	*Boolean* Specifies whether CentraSite is to send an email message to specified users and/or groups when the request is rejected. If you enable this option, you must set the following parameters to specify the text of the message and to whom it is to be sent. **Note:** CentraSite automatically sends the email message to the approvers (except for the approver who rejected the request) and to the user who submitted the approval request in addition to the users and/or groups that you specify below.	
	`Users`	See description of `Users` parameter above.
	`Groups`	See description of `Groups` parameter above.
	`Subject`	See description of `Subject` parameter above.
	`Use Email Template`	See description of `Use Email Template` parameter above. **Note:** You can use the predefined template, RejectApprovalNotification.html, for rejection notifications if you do not want to create an email template of your own.
	`Custom Message`	See description of `Custom Message` parameter above.
	`Format`	See description of `Format` parameter above.
	`Include owner in notification`	See description of `Include owner in notification` parameter above.

API Key Generator

Generates an API key for the API.

Input Parameters

`Key Expiration Interval`	*String. Mandatory.* Specifies the time interval an API key can remain active. When the interval expires, the current key is marked expired.

Deploy API Key

Initiates an API key deployment in the target (for example, Mediator).

Note: If the target is down/unreachable, this action will fail. In this case, the API Provider is notified through the configured email.

Input Parameters

None.

Send Email Notification

Sends an email message to specified users and/or groups.

Note: During an iteration of the policy, if the connection to a SMTP email server fails, this policy action returns a failure code. CentraSite writes the failure message to the policy log; however performs the next action in the policy (if one exists).

Input Parameters

`Users`	*Array of Users* Users who are to receive the email. **Note:** You can specify the recipients of the email using the `Users` parameter, the `Groups` parameter, or both.
`Groups`	*Array of Groups* Groups whose users are to receive the email. **Note:** CentraSite will only send the email to those users in the group whose CentraSite user account includes an email address.
`Subject`	*String* The text that you want to appear in the email's subject line. This text can include substitution tokens to insert run-time data into the subject line. For information about using substitution tokens, see *Substitution Tokens*, below.
`Use Email Template`	*Email Template* Specifies the template that is to be used to generate the body of the email message. For more information about using email templates, see the topic *Predefined Email Templates Installed with CentraSite* in the section *Working with EMail Notifications* . **Note:** You can use the predefined template, NotifyAPIKeyGenerationToConsumer.html, as your email template if you do not want to create an email template of your own. **Note:** If you use an email template to generate the body of the message, you cannot specify the body of the message using the `Custom Message` parameter. (In other words, you specify the body of the message using either the `Use Email Template` *or* the `Custom Message` parameter.)
`Custom Message`	*TextArea* The text of the email message. This text can include substitution tokens to insert run-time data into the message. For information about using substitution tokens, see Substitution Tokens, below. **Note:** If you use the `Custom Message` parameter to specify the body of the email message, you cannot generate the body of the message using an email template. (In other words, you specify the body of the message using either the `Custom Message` *or* the `Use Email Template` parameter.)
`Format`	*String* Specifies whether the custom mail message is formatted as HTML or plain text.
`Include owner in notification`	*Boolean* When enabled, this parameter sends the email notification to the provider of the API on which the policy is acting in addition to the users specified by the `Users` and `Groups` parameters.

API Key Renewal Policy

After an API key is generated, users sometimes want to renew the old key due to expiration or security concerns. API Consumers can re-generate/renew API keys to change the default expiration time of an API key, consumer of an API generates the API key which serves as an authentication token when the consumer requests for consumption of the API.

When a consumer requests for renewing an API key (as described in *Renewing API Keys*), CentraSite internally creates and triggers an API Key Renewal policy for the API. A request for the API key renewal is subsequently submitted to all members of the approval list specified in the Initiate Approval action. The approvers can either approve or decline the request. If the approvers approve the request, CentraSite re-generates the API key, deploys the generated key in the Mediator, and notifies the consumer that the API is now ready for consumption using the newly generated key.

Note: To use the email options provided by this policy, CentraSite must have a connection to an SMTP email server. For instructions on how to configure CentraSite's connection to an email server, see the section *Configuring the Email Server* in the document *Basic Operations*.

The following actions are typically used with the API Key Renewal policy.

- The *Initiate Approval* action is generally used to obtain necessary approvals for a consumer prior to executing the *Renew API Key* action.
- The *Renew API Key* action is used to re-define the default expiration interval of an API key, and re-generate the API key for the API.
- The *Deploy API Key* is typically executed after the *Renew API Key* action to redeploy the newly generated key in the Mediator.
- The *Create Auditable Events* action is used to capture the audit logs in changing the validity of the API key.
- The *Send Email Notification* action is used to send an email message to the API consumer with details of the new validity of API key.

Object Scope

API Key

Event Scope

On-Trigger

Initiate Approval

Initiates an approval workflow.

When this action is executed, CentraSite initiates the approval process. CentraSite will not process any subsequent actions in the policy or execute the requested operation until the approvals specified by the Initiate Approval action are received.

For more information about creating approval policies, see the section *Working with Approval Workflows* in the document *Administering the CentraSite Business UI*.

Input Parameters

<table>
<tr><td>User</td><td>String The user name that will be used together with the Password parameter as authentication credentials for performing a request on an API. The credentials are stored in the approval request and passed to the API for completing the approval.

This parameter is only visible to users with the CentraSite Administrator role.</td></tr>
<tr><td>Password</td><td>String The password that will be used together with the User parameter as authentication credentials.

This parameter is only visible to users with the CentraSite Administrator role.</td></tr>
<tr><td>Approval Flow Name</td><td>String The name to be given to the approval workflow that this action initiates. This name serves to identify the workflow in the approver's Pending Approvals.

An approval flow name can contain any combination of characters, including a space.

You can also include substitution tokens in the name to incorporate data from the target object on which the policy is acting. For a list of the allowed tokens, see the list of Substitution Tokens shown in the Send Email Notification action.</td></tr>
<tr><td>Approver Group</td><td>String Array The user group (or groups) that identifies the set of users who are authorized to approve the requested operation.

Note: If the user groups specified in Approver Group are empty at enforcement time, the user's request is auto-approved.</td></tr>
<tr><td>Approval is Needed From</td><td>String The manner in which the approval is to be processed:

<table><tr><th>Value</th><th>Description</th></tr><tr><td>AnyOne</td><td>Default The request can be approved or rejected by any single user in Approver Group. In this mode, only one user from the set of authorized approvers is required to approve or reject the request.</td></tr></table></td></tr>
</table>

	EveryOne	The request must be approved by all users specified in Approver Group. (It does not matter in which order the approvals are issued.) A single rejection will cause the request to be rejected.
Reject State	The lifecycle state that is to be assigned to the API if the approval request is rejected. If this parameter is not specified, the API's lifecycle state does not change when a rejection occurs. The lifecycle model must define a valid transition from the state that the target object is in at the time it is submitted for approval to the state specified in Reject State. Otherwise, the target object's state will not be switched when a rejection occurs. For more information about using this parameter, see the topic *Switching the State of an Object when an Approval Request is Rejected* in the section *Working with Approval Workflows* in the document *Administering the CentraSite Business UI*.	
Send Pending Approval Email	*Boolean* Specifies whether CentraSite is to send an email message to specified users and/or groups when the request is initially submitted for approval. If you enable this option, you must set the following parameters to specify the text of the message and to whom it is to be sent. **Note:** If the request is auto-approved, this message is not sent. **Note:** CentraSite automatically sends the email message to the approvers in addition to the users and/or groups that you specify below.	
	Users	*Array of Users* Users who are to receive the email. **Note:** You can specify the recipients of the email using the Users parameter, the Groups parameter, or both.
	Groups	*Array of Groups* Groups whose users are to receive the email. **Note:** CentraSite will only send the email to those users in the group whose CentraSite user account includes an email address.
	Subject	*String* The text that you want to appear in the subject line of the email. This text can include substitution tokens to insert run-time data into the subject line. For available tokens, see the list of Substitution Tokens shown in the *Send Email Notification* action.
	Use Email Template	*Email Template* Specifies the template that is to be used to generate the body of the email message. For more information about using email templates, see the topic *Predefined Email Templates Installed with CentraSite* in the section *Working with Email Notifications* . **Note:** You can use the predefined template, PendingNotification.html, for pending-approval notifications if you do not want to create an email template of your own.

		Note: If you use an email template to generate the body of the message, you cannot specify the body of the message using the `Custom Message` parameter. (In other words, you specify the body of the message using either the `Use Email Template` *or* the `Custom Message` parameter.)
	`Custom Message`	*TextArea* The text of the email message. This text can include substitution tokens to insert run-time data into the message. For available tokens, see the list of Substitution Tokens shown in the *Send Email Notification* action. **Note:** If you use the `Custom Message` parameter to specify the body of the email message, you cannot generate the body of the message using an email template. (In other words, you specify the body of the message using either the `Custom Message` *or* the `Use Email Template` parameter.)
	`Format`	*String* Specifies whether the message in the `Custom Message` parameter is formatted as HTML or plain text.
	`Include owner in notification`	*Boolean* When the parameter is enabled, CentraSite sends the email to the provider of the API (on which the policy is acting) in addition to the other recipients.
`Send Approval Email`	*Boolean* Specifies whether CentraSite is to send an email message to specified users and/or groups when the request is approved. If you enable this option, you must set the following parameters to specify the text of the message and to whom it is to be sent. **Note:** CentraSite automatically sends the email message to the user who submitted the approval request in addition to the users and/or groups that you specify below. **Note:** When the EveryOne option is specified in the `Approval is Needed From` parameter, CentraSite sends this email only after all approvers have approved the request.	
	`Users`	See description of `Users` parameter above.
	`Groups`	See description of `Groups` parameter above.
	`Subject`	See description of `Subject` parameter above.
	`Use Email Template`	See description of `Use Email Template` parameter above. **Note:** You can use the predefined template, ApprovalNotification.html, for approval notifications if you do not want to create an email template of your own.
	`Custom Message`	See description of `Custom Message` parameter above.
	`Format`	See description of `Format` parameter above.
	`Include owner in notification`	See description of `Include owner in notification` parameter above.

Send Rejection Email	*Boolean* Specifies whether CentraSite is to send an email message to specified users and/or groups when the request is rejected. If you enable this option, you must set the following parameters to specify the text of the message and to whom it is to be sent. **Note:** CentraSite automatically sends the email message to the approvers (except for the approver who rejected the request) and to the user who submitted the approval request in addition to the users and/or groups that you specify below.	
	Users	See description of Users parameter above.
	Groups	See description of Groups parameter above.
	Subject	See description of Subject parameter above.
	Use Email Template	See description of Use Email Template parameter above. **Note:** You can use the predefined template, RejectApprovalNotification.html, for rejection notifications if you do not want to create an email template of your own.
	Custom Message	See description of Custom Message parameter above.
	Format	See description of Format parameter above.
	Include owner in notification	See description of Include owner in notification parameter above.

Renew API Key

Re-generates an API key with new validity for the API.

Input Parameters

Key Expiration Interval	*String. Mandatory.* Specifies the new time interval a re-generated API key can remain active. When the interval expires, the current key is marked expired.

Deploy API Key

Re-deploys the API key with new validity in the target (for example, Mediator).

Note: The action is prone to failure due to the fact that the target may be down/unreachable. In case of failure, the API Provider is intimated through the configured email. For example, if an API key is already deployed in multiple targets and upon API key renewal, re-deployment fails in a couple of targets, a mail would be sent to API Provider informing that the API key deployment failed in the listed targets. Currently, API Provider is not allowed to deploy an API key alone. Instead, the Provider has to redeploy the API to deploy the updated key (after taking corrective actions in mediator).

Input Parameters

Create Auditable Events

Creates an audit log for changing the default expiration interval of the API key.

Input Parameters

`Context Key`	*String. Mandatory.*
`Context Value`	*String. Mandatory.*

Send Email Notification

Sends an email message to specified users and/or groups.

Note: To use this action, CentraSite must have a connection to an SMTP email server. For instructions on how to configure CentraSite's connection to an email server, see the section *Configuring the Email Server* in the document *Administrator-Level Configuration Tasks*.

Note: During an iteration of the policy, if the connection to a SMTP email server fails, this policy action returns a failure code. CentraSite writes the failure message to the policy log; however performs the next action in the policy (if one exists).

Input Parameters

`Users`	*Array of Users* Users who are to receive the email. **Note:** You can specify the recipients of the email using the `Users` parameter, the `Groups` parameter, or both.
`Groups`	*Array of Groups* Groups whose users are to receive the email. **Note:** CentraSite will only send the email to those users in the group whose CentraSite user account includes an email address.
`Subject`	*String* The text that you want to appear in the email's subject line. This text can include substitution tokens to insert run-time data into the subject line. For information about using substitution tokens, see *Substitution Tokens*, below.
`Use Email Template`	*Email Template* Specifies the template that is to be used to generate the body of the email message. For more information about using email templates, see the topic *Predefined Email Templates Installed with CentraSite* in the section *Working with EMail Notifications* . **Note:** You can use the predefined template, NotifyAPIKeyGenerationToConsumer.html, as your email template if you do not want to create an email template of your own. **Note:** If you use an email template to generate the body of the message, you cannot specify the body of the message using the `Custom Message` parameter. (In other words, you

	specify the body of the message using either the `Use Email Template` *or* the `Custom Message` parameter.)
`Custom Message`	*TextArea* The text of the email message. This text can include substitution tokens to insert run-time data into the message. For information about using substitution tokens, see Substitution Tokens, below. **Note:** If you use the `Custom Message` parameter to specify the body of the email message, you cannot generate the body of the message using an email template. (In other words, you specify the body of the message using either the `Custom Message` *or* the `Use Email Template` parameter.)
`Format`	*String* Specifies whether the custom mail message is formatted as HTML or plain text.
`Include owner in notification`	*Boolean* When enabled, this parameter sends the email notification to the provider of the API on which the policy is acting in addition to the users specified by the `Users` and `Groups` parameters.

API Key Revocation Policy

After an API key is generated, users sometimes want to revoke the key in case of malfunction. API Provider can revoke API keys to disable access to an API subscribed by a consumer.

When a provider requests for revocation of an API key (as described in *Revoking API Keys*), CentraSite internally creates and triggers an API Key Revoke policy for the API. A request for the key revocation is subsequently submitted to all members of the approval list specified in the Initiate Approval action. The approvers can either approve or decline the request. If the approvers approve the request, CentraSite revokes the API key, and notifies the consumer that the API is now unavailable for consumption.

Note: To use the email options provided by this policy, CentraSite must have a connection to an SMTP email server. For instructions on how to configure CentraSite's connection to an email server, see the section *Configuring the Email Server* in the document *Basic Operations*.

The following actions are typically used with the API Key Revocation policy.

- The *Revoke API Key* action is used to revoke an API key for the API.
- The *Create Auditable Events* action is used to capture the audit logs in revoking the API key.
- The *Send Email Notification* action is used to send an email message to the API consumer about revocation of the API key.

Object Scope

API Key

Event Scope

On-Trigger

Revoke API Key

Revokes an existing key for the API.

Input Parameters

None.

Create Auditable Events

Creates an audit log for revoking the API key.

Input Parameters

`Context Key`	*String. Mandatory.*
`Context Value`	*String. Mandatory.*

Send Email Notification

Sends an email message to specified users and/or groups.

Note: To use this action, CentraSite must have a connection to an SMTP email server. For instructions on how to configure CentraSite's connection to an email server, see the section *Configuring the Email Server* in the document *Administrator-Level Configuration Tasks*.

Note: During an iteration of the policy, if the connection to a SMTP email server fails, this policy action returns a failure code. CentraSite writes the failure message to the policy log; however performs the next action in the policy (if one exists).

Input Parameters

`Users`	*Array of Users* Users who are to receive the email. **Note:** You can specify the recipients of the email using the `Users` parameter, the `Groups` parameter, or both.
`Groups`	*Array of Groups* Groups whose users are to receive the email. **Note:** CentraSite will only send the email to those users in the group whose CentraSite user account includes an email address.

`Subject`	*String* The text that you want to appear in the email's subject line. This text can include substitution tokens to insert run-time data into the subject line. For information about using substitution tokens, see *Substitution Tokens*, below.
`Use Email Template`	*Email Template* Specifies the template that is to be used to generate the body of the email message. For more information about using email templates, see the topic *Predefined Email Templates Installed with CentraSite* in the section *Working with EMail Notifications* . **Note:** You can use the predefined template, NotifyAPIKeyGenerationToConsumer.html, as your email template if you do not want to create an email template of your own. **Note:** If you use an email template to generate the body of the message, you cannot specify the body of the message using the `Custom Message` parameter. (In other words, you specify the body of the message using either the `Use Email Template` *or* the `Custom Message` parameter.)
`Custom Message`	*TextArea* The text of the email message. This text can include substitution tokens to insert run-time data into the message. For information about using substitution tokens, see Substitution Tokens, below. **Note:** If you use the `Custom Message` parameter to specify the body of the email message, you cannot generate the body of the message using an email template. (In other words, you specify the body of the message using either the `Custom Message` *or* the `Use Email Template` parameter.)
`Format`	*String* Specifies whether the custom mail message is formatted as HTML or plain text.
`Include owner in notification`	*Boolean* When enabled, this parameter sends the email notification to the provider of the API on which the policy is acting in addition to the users specified by the `Users` and `Groups` parameters.