Cisco API Console User Guide 2.0

October 3, 2013

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: 78-xxxxx-xx

CONTENTS

Preface--Cisco API Console User Guide

Revised: October 3, 2013

Preface

This chapter covers the following topics:

- About this Document
- Overview

About this Document

This document provides information about the API Services, and contains information on how to get started using the different services. This document describes the process of registering users, obtaining authorized credentials, and how to use the credentials with the various API service calls. The last section of this document explains how to use the different metric tools that are available on the API console.

Overview

This guide will explain the steps needed to be taken to on-board to Web APIs provided by Cisco. This guide will cover obtaining a user account, assigning party and role assignments to that user account for a specific company, and using Cisco's API Console for the registration of a client application that will call Cisco's Web APIs.

These instructions are intended from Cisco's Customers or Partners that intend to create client applications from Cisco Provided APIs.

CHAPTER 1

On-Boarding-CCO-Registration

Revised: October 3, 2013

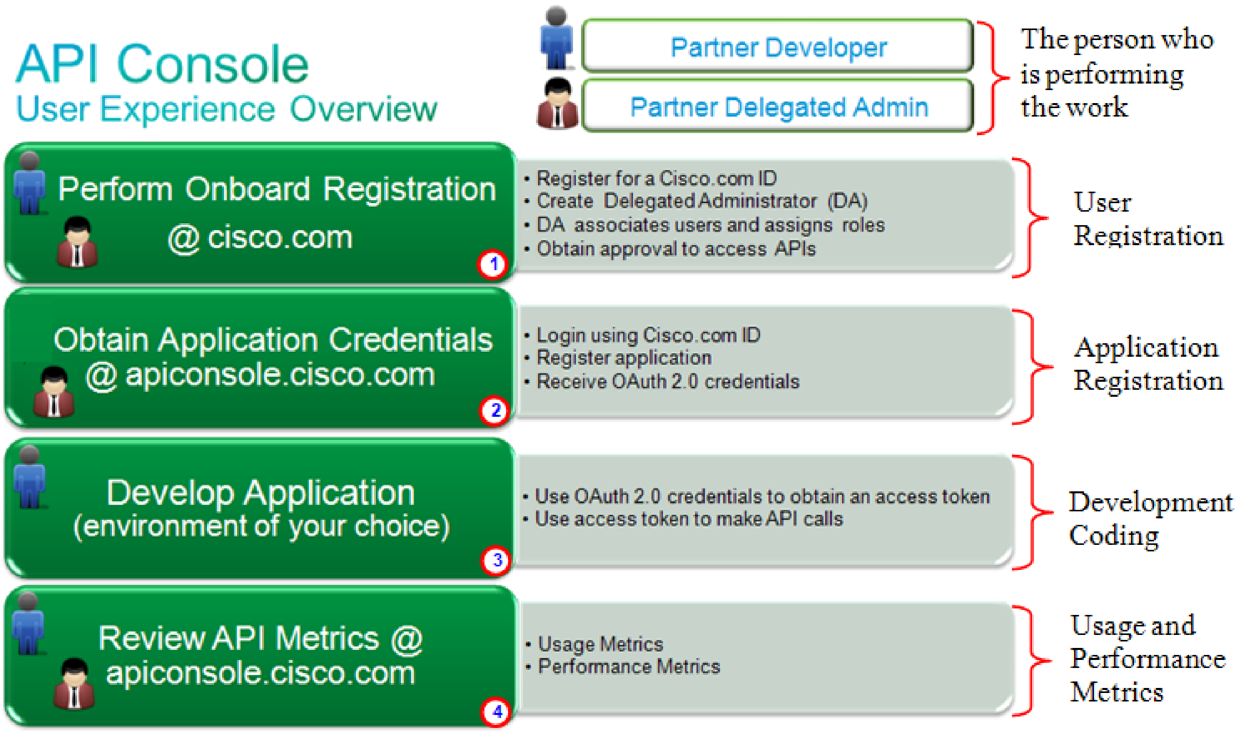
Introduction

This chapter introduces the user to CCO Registration and CSAM, gives an overview of the Delegated Administrator process, and describes following areas:

- Overview of the API Process
- Register for a CCO ID
- On Boarding Overview
- The API Console

Overview of the API Process

There are four main steps that allow users to initiate the API service calls and obtain access to the product information noted in the graphic below. The first two steps consist of user and application registration; while the last two steps are related to development and metrics use. These four procedures are outlined in the following graphic:



The procedures are described below in more detail:

1. **Perform Onboard Registration**: This is for user registration. This process, also referred to as on-boarding, is where the following actions occur:
   - User registers for a CCO ID (or they may use their existing one if already registered) and is nominated by a Cisco Administrator to become a Delegated Administrator (DA).
   - The DA associates other CCO ID users to a company and assigns them roles, which gives them access to the API console.

Note Only one DA is assigned by Cisco, however, that DA may assign other users to the role of DA. The DA is responsible for associating users and assigning them service roles.

2. **Register a client application with the API Console**:
   - Creates client credentials (assigns name, description, and chooses OAuth v2.0 grant types requested from their client application).
   - Subscribes that client application to 1 or more of the APIs provided by Cisco.
   - Registration of a client application creates a “unique client identifier” that will identify your client application to Cisco Token services.
3. **Develop Application (Client code developed by the customer or partner)**:
   - Utilizes Cisco's Token services to acquire an OAuth v2.0 access-tokens
   - Place API calls to chosen APIs (leveraging the access-token from the previous step).
4. **Review API Metrics**: This lets the user(s) review various usage and performance metrics that are associated with the API service calls.

Perform Onboard Registration

The following section provides information about the following areas:

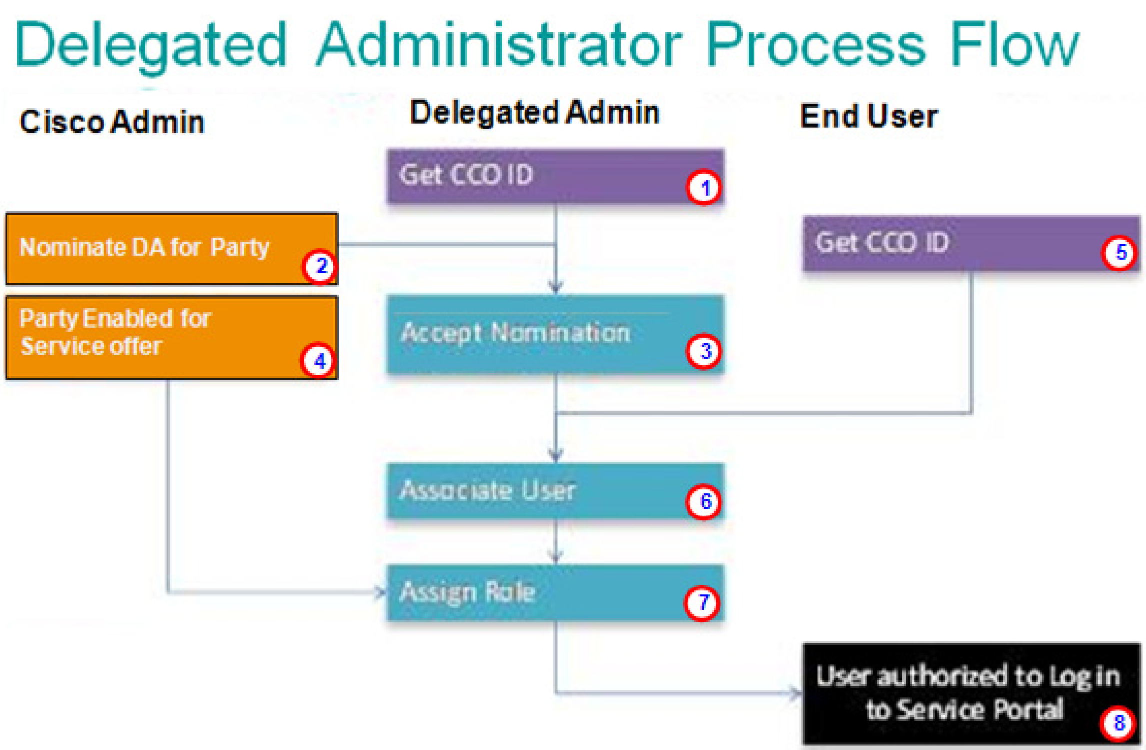
- Register for a CCO ID
- On Boarding Overview

On Boarding Overview

This section relates to the "Cisco Services Access Management (CSAM)" section on page 2-1. Cisco Service Access Management (CSAM), which enables partners to self-administer role-based user access to various Cisco Service programs. Self-administration is based upon the concept of Delegated Administration. Access is first granted, by Cisco, to one trusted person at the customer or Partner Company, who then assumes responsibility for assigning access privileges to the rest of the users at their company.

You may already be using some other tool or process to manage CCO IDs for your users; however, CSAM is needed to perform these additional tasks:

- Associating users to a party.
- Assigning that user a role on the API Console.



Note Party is also known as an entitled company.

To assign a Delegated Administrator and have the DA assign other users, the following steps must be completed:

Step 1 Each user must have a Cisco ID (CCO ID). If a partner or customer (end user) does not have a Cisco ID, one can be requested via the "Account" link at the top of the www.cisco.com home page, and then by going to "New User" and clicking on Register Now. See the "Register for a CCO ID" section on page 1-4.

Step 2 Once the proper individual has been identified, a Cisco Administrator nominates that person to take on the role of Delegated Administrator for their company. A nomination e-mail message is automatically sent to that individual; the e-mail contains a link to the CSAM system. See the "Delegated Administrator Nomination" section on page 2-1.

Step 3 The partner accepts the administrator's DA nomination. See "Delegated Administrator Nomination" section on page 2-1.

Step 4 The Cisco Administrator enables the party for the API service offer.

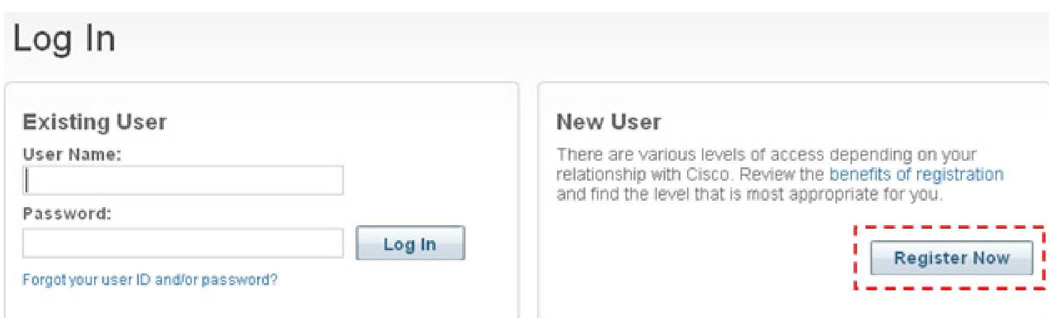
Step 5 The Delegated Administrator can now associate and assign roles to different end users. See Chapter 2, "Associating a User to Your Company," and Chapter 2, "Assigning a Role to a User."

Step 6 Once these above tasks are completed the users are authorized to login into the API console service portal. See the API Console User Guide for more information how to register applications for development.

Register for a CCO ID

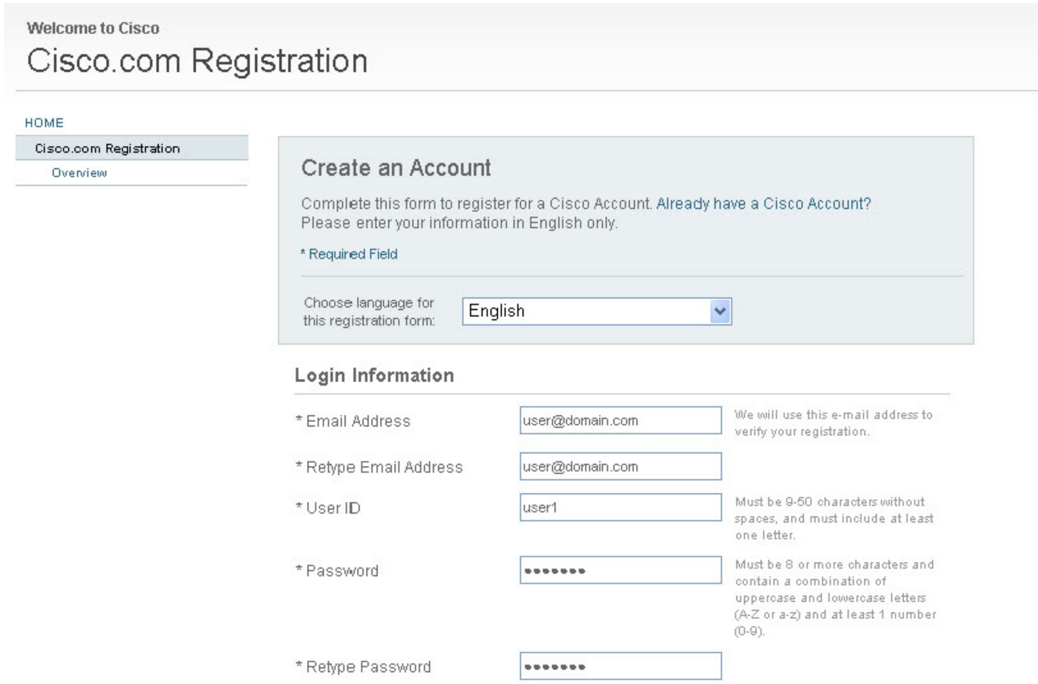
The first requirement is to have a valid CCO ID; if the user does not have one they will need to register for a CCO ID by performing the following steps:

Step 1 Navigate to the CSAM home page at URL http://tools.cisco.com/CDCEB; a CCO login window appears.



Step 2 Click **Register Now**. The Cisco.com Registration window will be displayed.

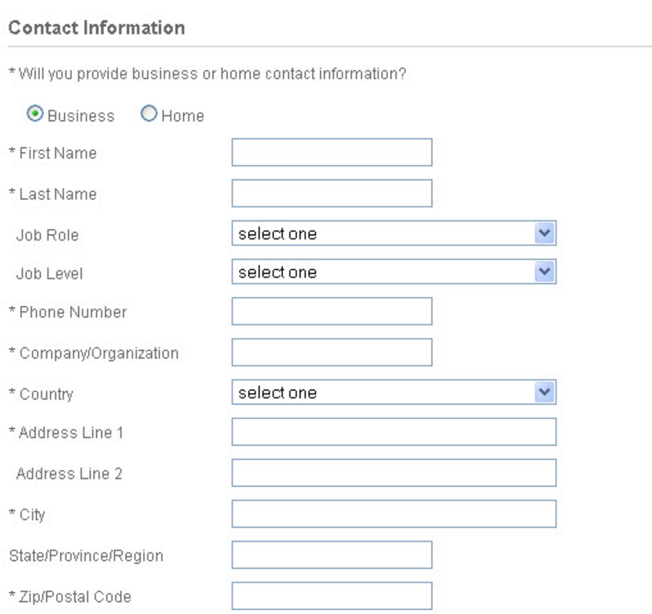
Figure 1-1 CCO Login Information



Note Ensure that all of the fields marked with an asterisk are completed. These are mandatory fields.

Step 3 In the **Contact Information** section, the user is given the option of choosing either "Business," or "Home." contact information. If the "Home" choice is made, the fields will change to reflect a non-business entry.

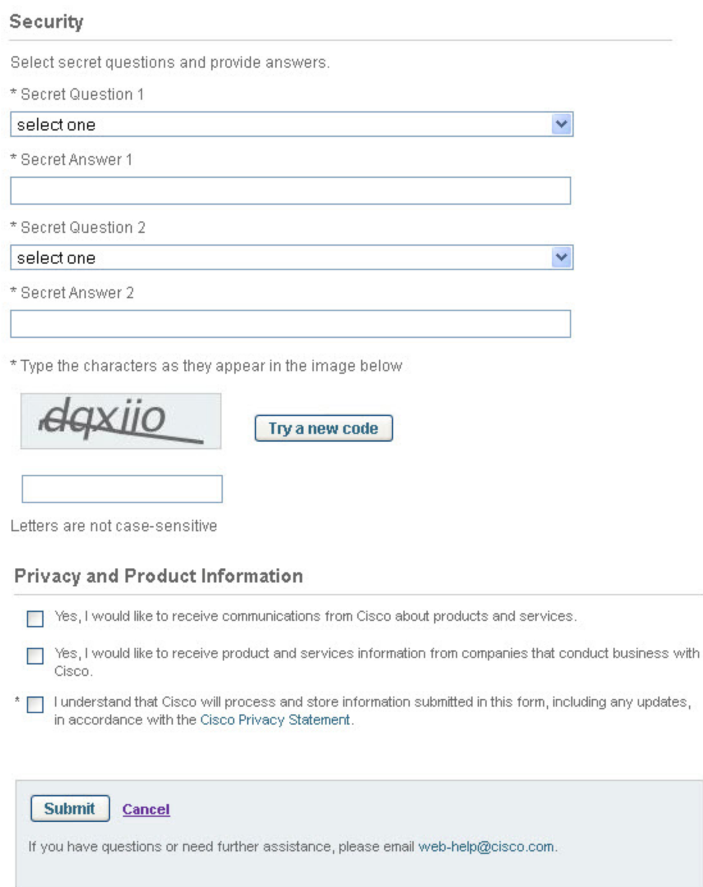
Figure 1-2 CCO Contact Information



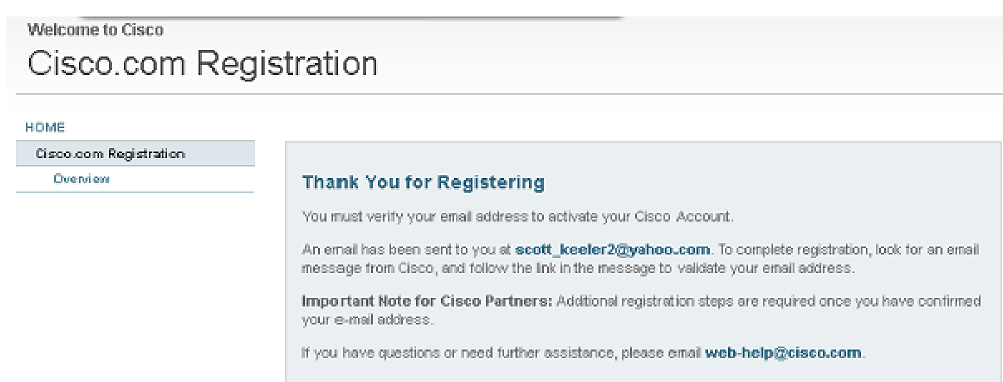
Step 4 The **Security** section requires the user select several secret questions with answers, as well as filling in the captcha field. The user can opt into receiving communications and product information by selecting the appropriate checkboxes.

Note The user ***must*** select the checkbox advising them that Cisco will store the information provided.

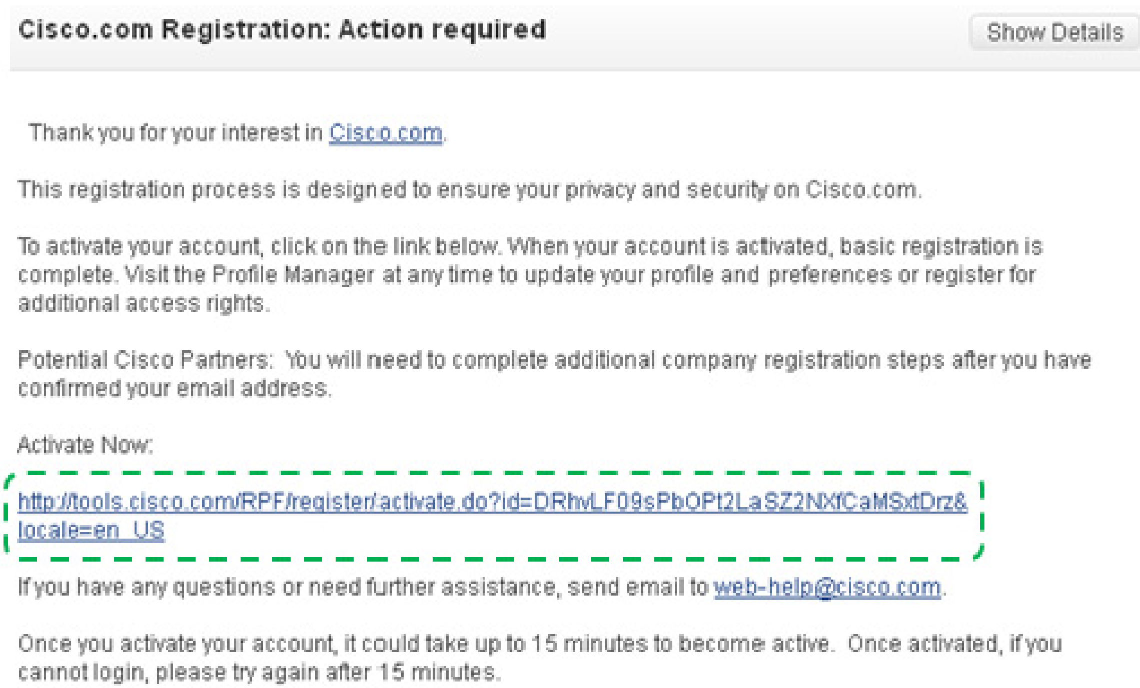
Figure 1-3 CCO Security Section



Step 5 After filling out all the required information, click **Submit** at the bottom of the window. A registration confirmation window will be displayed.



Step 6 The system will then send an e-mail to the user's registered e-mail ID which will contain actionable content.



Cisco.com Registration: Action required

Show Details

Thank you for your interest in Cisco.com.

This registration process is designed to ensure your privacy and security on Cisco.com.

To activate your account, click on the link below. When your account is activated, basic registration is complete. Visit the Profile Manager at any time to update your profile and preferences or register for additional access rights.

Potential Cisco Partners: You will need to complete additional company registration steps after you have confirmed your email address.

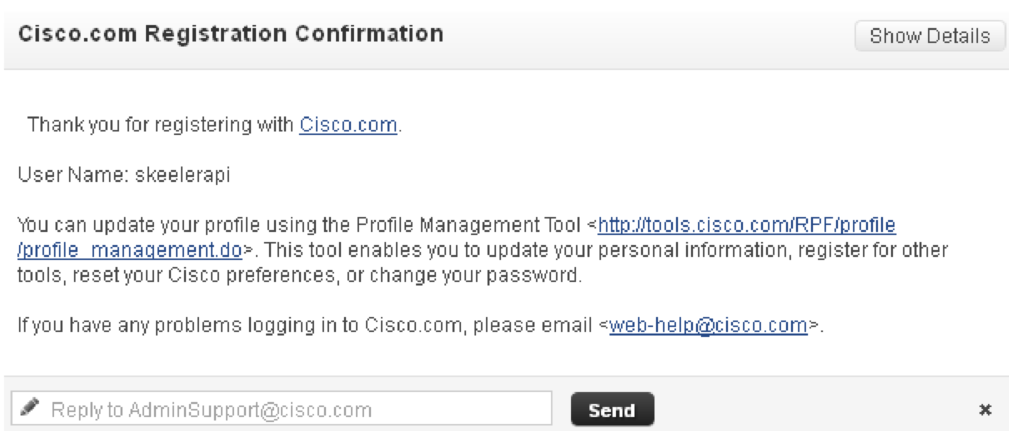
Activate Now:

http://tools.cisco.com/RPF/register/activate.do?id=DRhvLF09sPbOPt2LaSZ2NXfCaMSxtDrz&locale=en_US

If you have any questions or need further assistance, send email to web-help@cisco.com.

Once you activate your account, it could take up to 15 minutes to become active. Once activated, if you cannot login, please try again after 15 minutes.

Step 7 The user must open the e-mail and click the **Activate Now** link to complete the registration process. The Cisco.com confirmation page will open.



Cisco.com Registration Confirmation

Show Details

Thank you for registering with Cisco.com.

User Name: skeelerapi

You can update your profile using the Profile Management Tool <http://tools.cisco.com/RPF/profile/profile_management.do>. This tool enables you to update your personal information, register for other tools, reset your Cisco preferences, or change your password.

If you have any problems logging in to Cisco.com, please email <web-help@cisco.com>.

Reply to AdminSupport@cisco.com

Send

- A "Thank You" message window appears which indicates that an e-mail has been sent to the personal e-mail address used to register the new CCO ID.
- The system will RE-EMAIL a final confirmation e-mail that provides a link to activate your CCO ID.

CHAPTER 2

Cisco Services Access Management

Revised: October 3, 2013

Cisco Services Access Management (CSAM)

Cisco Services Access Management (CSAM) provides for "party-centric" role-based access to new Cisco Smart Services. Rather than requiring a contract administrator to explicitly add a user to each and every contract to which they should be able to get support, party-centric access allows for all users that are associated to the customer or partner "party" to get access to the support services to which their company is authorized. The level of access can be further filtered or controlled through the assignment of specific access roles, allowing for a tailored user experience.

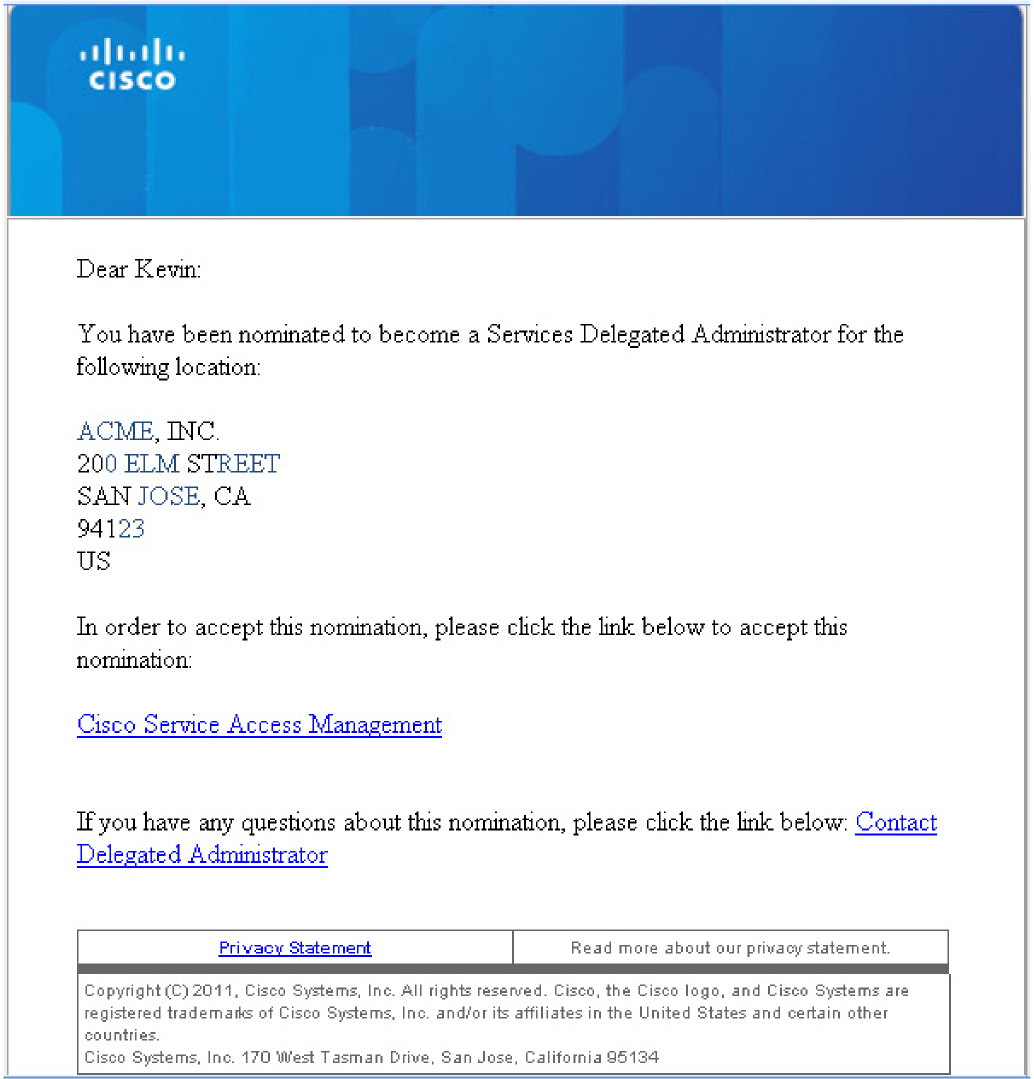
This chapter covers the following areas:

- Delegated Administrator Nomination
- Associating a User to Your Company
- Assigning a Role to a User
- Role Assignment-Show Existing Users
- Role Assignment-Search for Users by Full Name
- Role Assignment-Search by Cisco ID or E-mail

Delegated Administrator Nomination

Only one partner is assigned as a Delegated Administrator (DA); that DA will then associate other users and assign them service roles. To become a DA, a Cisco Administrator must nominate the user for that customer/partner company. An e-mail notification is sent to the nominated user's CCO ID indicating their Cisco Account is now associated with their designated company, and that they have been nominated to become the DA.

A sample nomination e-mail is shown below.



Dear Kevin:

You have been nominated to become a Services Delegated Administrator for the following location:

ACME, INC.
200 ELM STREET
SAN JOSE, CA
94123
US

In order to accept this nomination, please click the link below to accept this nomination:

Cisco Service Access Management

If you have any questions about this nomination, please click the link below: Contact Delegated Administrator

Privacy Statement	Read more about our privacy statement.

Step 1 Click the “Cisco Service Access Management” link, which indicates acceptance of the DA nomination.

Step 2 The nominated administrator will then be linked to the CSAM home page at https://tools.cisco.com/CDCEB. After logging in, the DA will be presented with an “End User License Agreement (EULA)” for CSAM.

Cisco Service Access Management Agreement

YOU MUST READ CAREFULLY AND ACCEPT ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS CISCO SERVICE ACCESS MANAGEMENT ("SAM") DELEGATED ADMINISTRATOR AGREEMENT ("AGREEMENT") BEFORE YOU MAY ACCESS OR USE SAM.

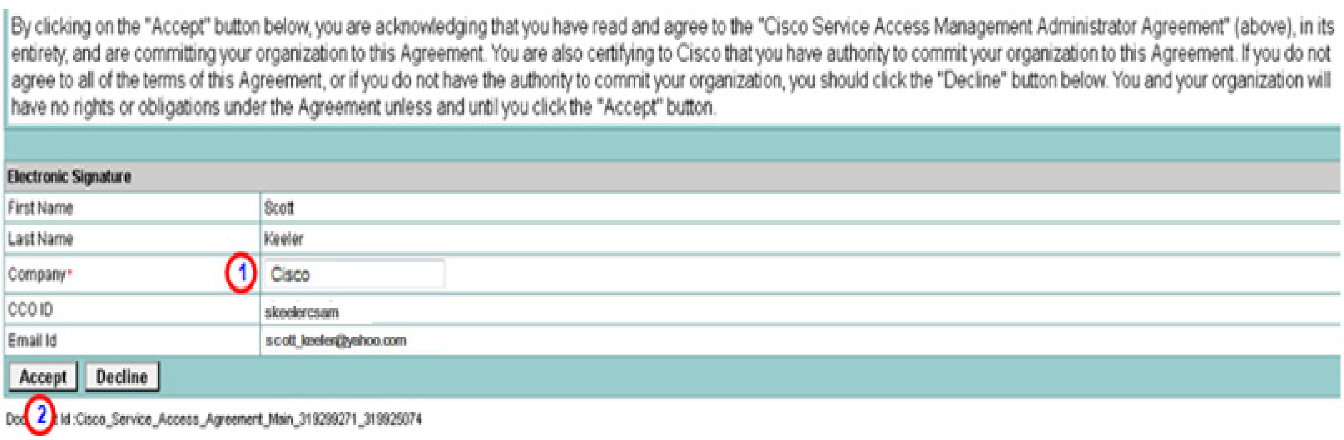
IF YOU DO AGREE TO ALL OF THE TERMS AND CONDITIONS, YOU SHOULD CLICK THE "ACCEPT" BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS AND CONDITIONS, YOU SHOULD CLICK THE "DECLINE" BUTTON AT THE END OF THIS AGREEMENT.

BY CLICKING THE "ACCEPT" BUTTON, YOU ARE BINDING YOURSELF AND THE BUSINESS ENTITY THAT YOU REPRESENT (COLLECTIVELY, "CUSTOMER") TO THIS AGREEMENT WITH CISCO SYSTEMS, INC. (OR ITS SUBSIDIARY OR AFFILIATE THAT PROVIDES YOU ACCESS TO SAM) ("CISCO"). YOU FURTHER CERTIFY TO CISCO THAT YOU ARE AUTHORIZED TO ENTER INTO THIS AGREEMENT ON BEHALF OF CUSTOMER. IF YOU DO NOT AGREE TO ALL OF THE TERMS OF THE AGREEMENT, THEN CISCO IS UNWILLING TO GRANT YOU ACCESS TO OR USE OF SAM; AND YOU MAY CONTACT YOUR CISCO REPRESENTATIVE TO DISCUSS ALTERNATIVE METHODS TO RESTRICT ACCESS TO CISCO SERVICES ON BEHALF OF CUSTOMER.

All capitalized terms have the meanings assigned to them in the Glossary (Exhibit A), incorporated into this Agreement. This Agreement becomes effective when you manually click "Accept."

The general purposes of this Agreement are to:

Step 3 After reading the terms and conditions, go to the bottom of the EULA for CSAM.



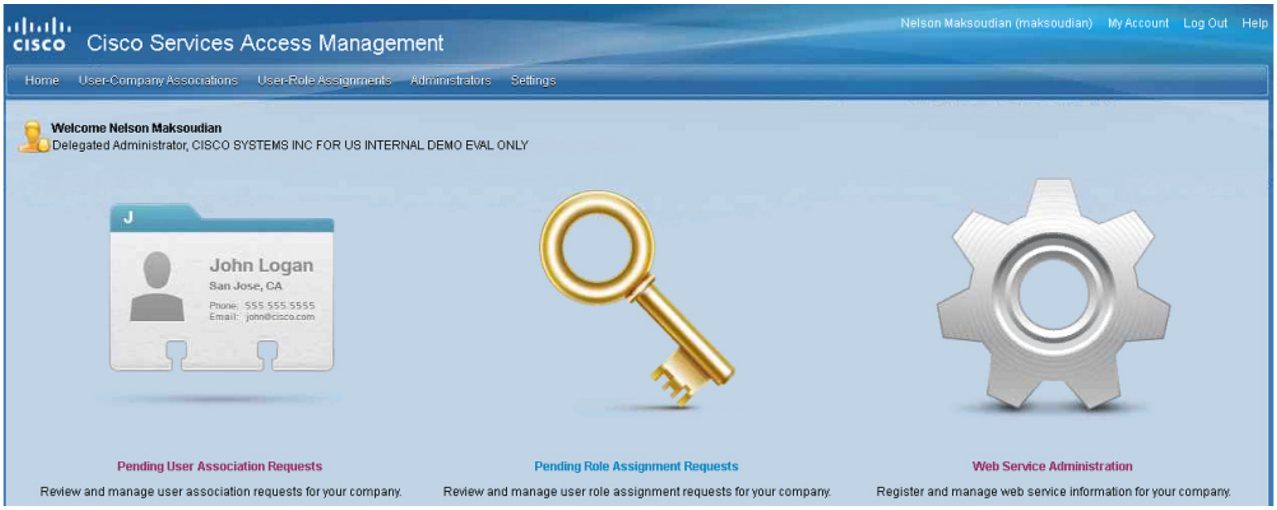
By clicking on the "Accept" button below, you are acknowledging that you have read and agree to the "Cisco Service Access Management Administrator Agreement" (above), in its entirety, and are committing your organization to this Agreement. You are also certifying to Cisco that you have authority to commit your organization to this Agreement. If you do not agree to all of the terms of this Agreement, or if you do not have the authority to commit your organization, you should click the "Decline" button below. You and your organization will have no rights or obligations under the Agreement unless and until you click the "Accept" button.

Electronic Signature	
First Name	Scott
Last Name	Keeler
Company* (1)	Cisco
CCO ID	skeelercsam
Email Id	scott_keeler@yahoo.com

Accept (2) Decline

Doc Id :Cisco_Service_Access_Agreement_Main_319299271_319925074

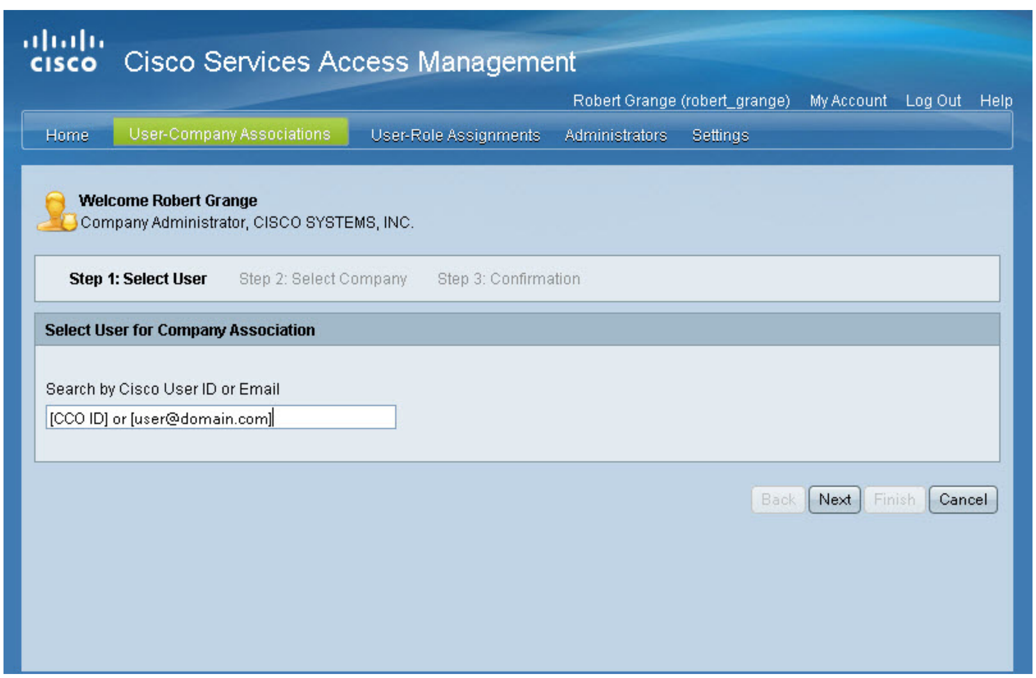
1. The first and last name, CCO ID and personal e-mail address fields will already be completed. The DA must enter their company name (i.e., Cisco) and then click **Accept**.
2. A confirmation pop-up appears, and the Cisco Services Access Management (CSAM) home page is displayed.



Associating a User to Your Company

After the Cisco Administrator's nomination has been accepted to become a party DA, the DA can associate and assign roles to users for their company. To associate users do the following:

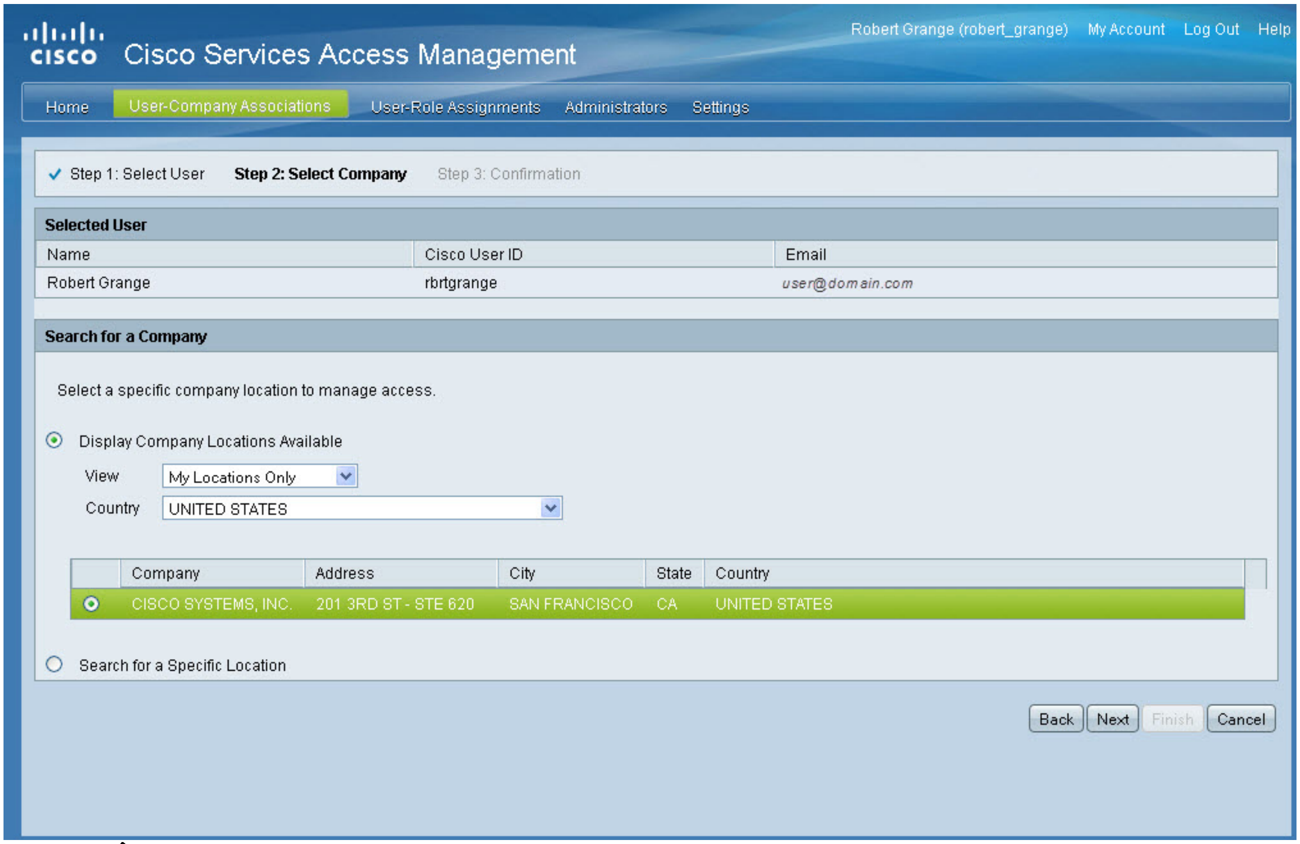
Step 1 On the CSAM menu choose **User-Company Associations > Associate User to My Company**. The "Select User for Company Association" page will open:



Step 2 Complete the field with *either* the user's Cisco User ID, or E-mail.

Warning **Do not use both the Cisco ID and E-mail together in this field. If both are entered CSAM will return an error and invalidate the entry.**

Step 3 Click **Next**.The “Select Company” page will open.



Note If the DA is associated with only one location, then that location will already be selected when the “Select Company” page is displayed. However, if the DA is associated with other locations, and that location is not the DA’s default location, then the DA will need to search for that location using the “View” and “Country” drop down menus

Step 4 Click **Next**. The confirmation page will open. Check that the details are correct.

Step 5 Click **Finish**. A pop up window will open showing the association process has been completed. From this window, the DA has the option of assigning service access roles to the just added user by clicking **Yes**, or they can close the window by clicking **No**.

Step 6 If the DA has chosen to assign roles to a user, continue onto the “Assigning a Role to a User” section on page 2-5.

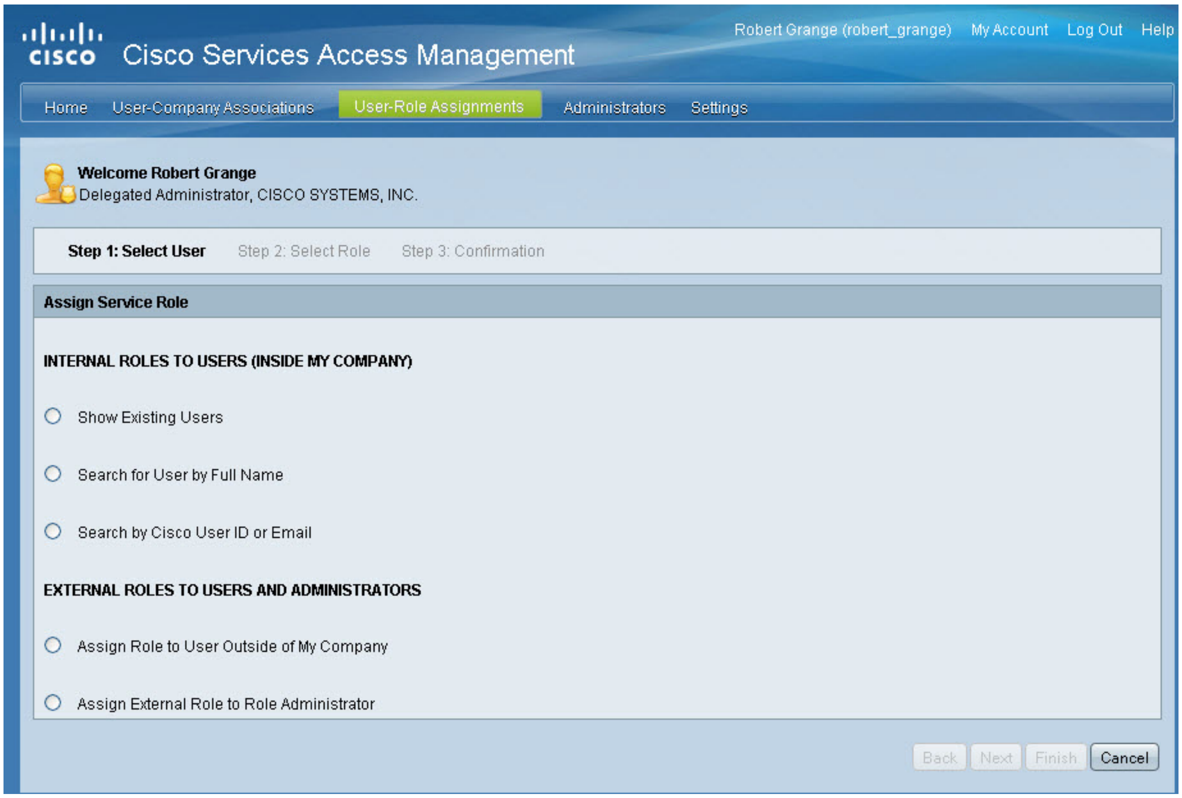
Assigning a Role to a User

A service role must be assigned to a user who is going to develop the API service calls so they can access the API console.

Note The Delegated Administrator will need to assign themselves to a user role in order to access The API Console. Delegated administrators are not assigned a user role by default.

To assign a role to a user, proceed to Step 1.

Step 1 On the CSAM menu choose **User-Company Associations > Assign Roles to Users**. The "Select User" page will open.



Step 2 In the Assign Service Role area, click a radio-button for one of the following options:

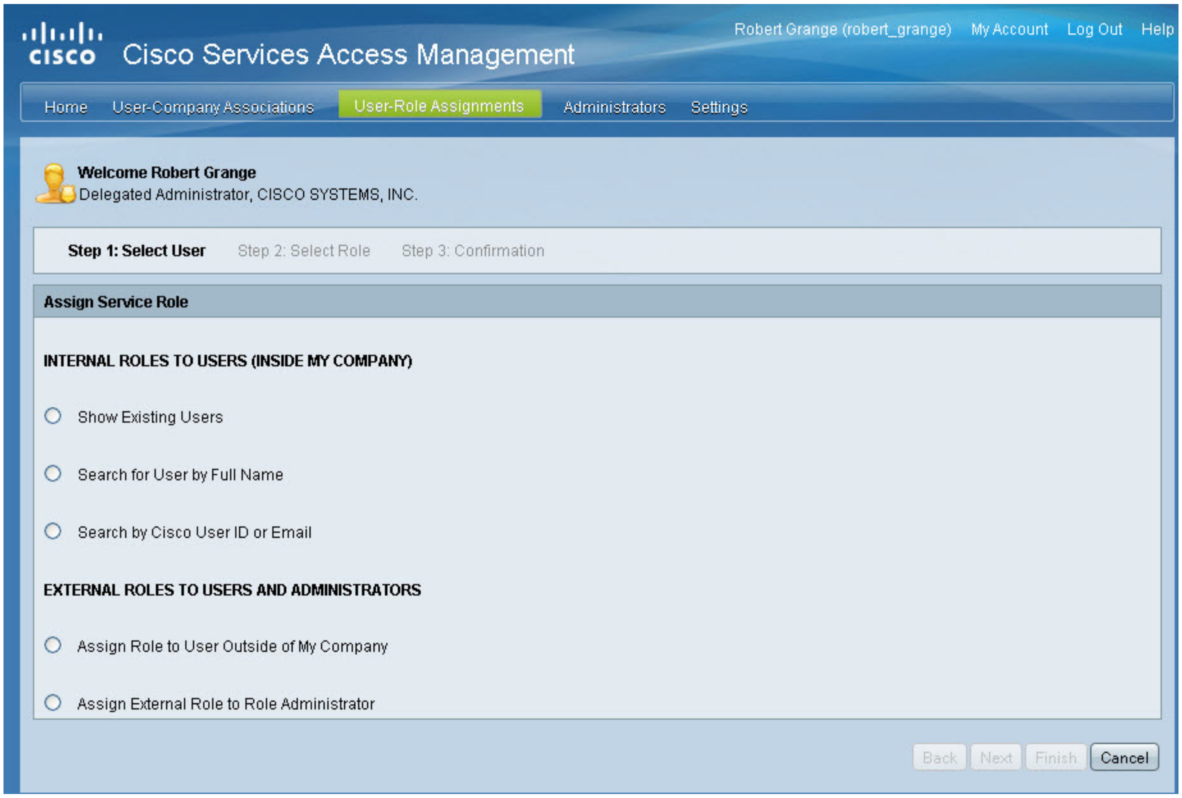
- **Show Existing Users**
- **Search for User by Full Name**
- **Search by Cisco User ID or E-mail**

Note If the DA has clicked **Yes** in **Step 5 on page 5 "Associating a User to Your Company,"** the application will automatically search for the user, and the "Search by Cisco User ID or E-mail" section will be expanded and automatically completed. Simply **click** "Next."

Role Assignment-Show Existing Users

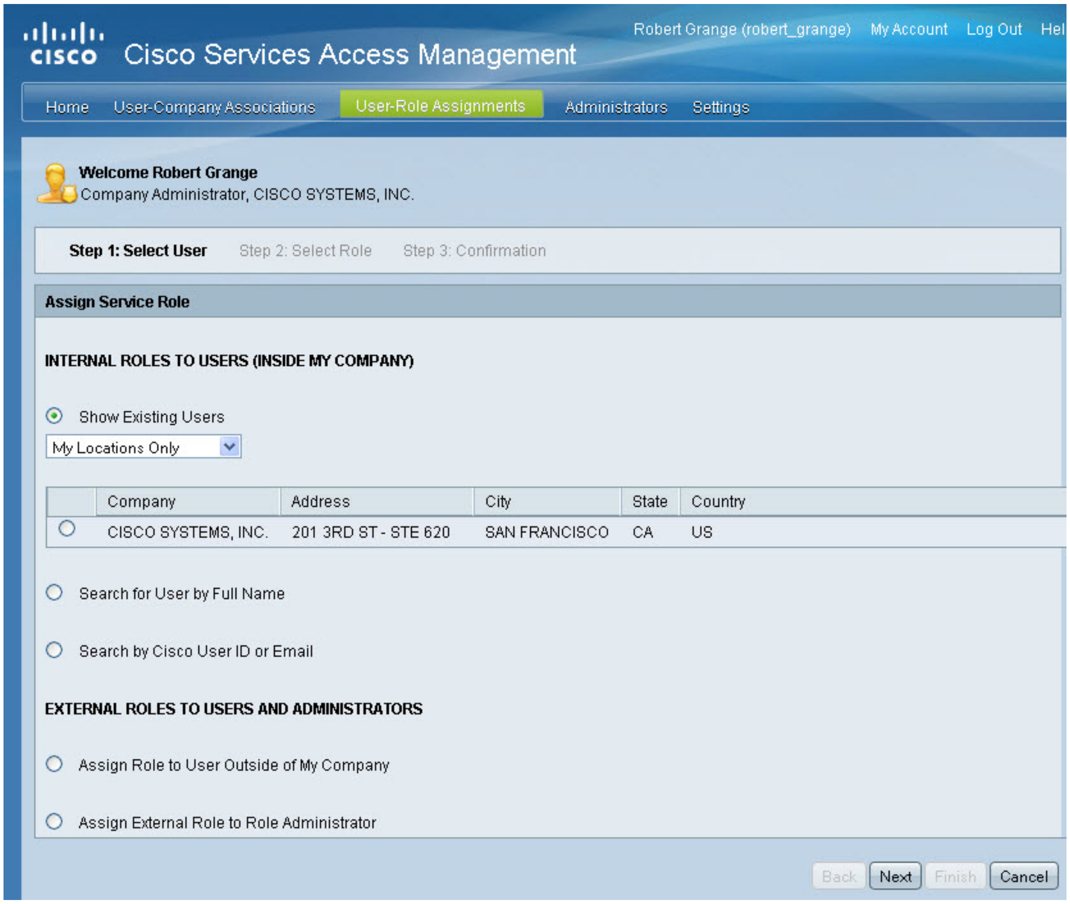
The "Show Existing Users" function allows the DA to search for all users currently active in the system in order to assign roles to those users. To assign roles using this function, use the following steps:

Step 1 Navigate to the user selection page by clicking on **User-Role Assignments > Assign Roles to Users**. The “Assign Service Role” page will open.

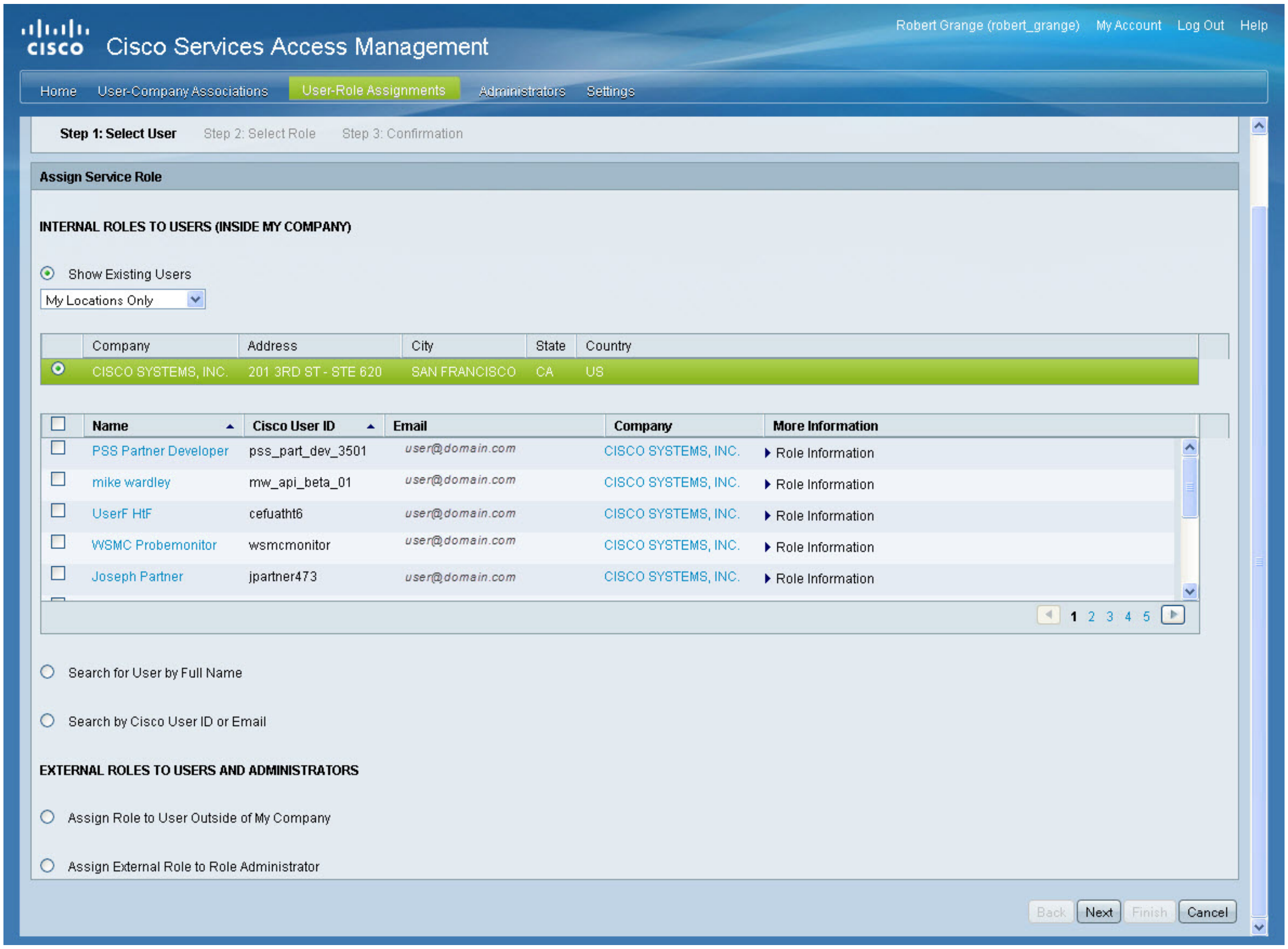


Step 2 Click on **Show Existing Users**. The system will display a page allowing the DA to choose a company for the assignment of roles.

Note Once the **Show Existing Users** has been selected, please wait for the response, it may take several minutes to process the request.



Step 3 Click on the radio button next to the company of choice. Once a selection has been made, the application will automatically populate with a list of all current existing users associated with the DA's company.



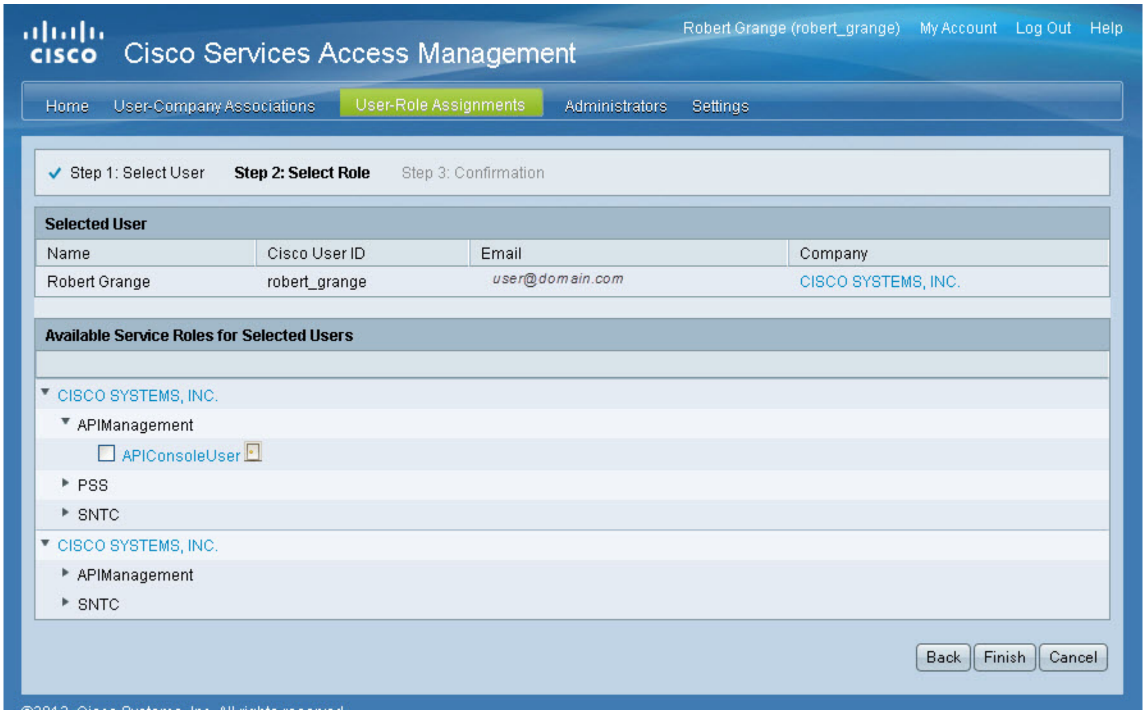
Step 4 Click the checkbox next to the name(s) roles are to be assigned to.

Note If all of the users on the page are to be selected, click on the checkbox next to **Name** in the header row. This will select all of the names on the current page for role assignment.

Step 5 Click **Next**. The "Select Role" page will be displayed.

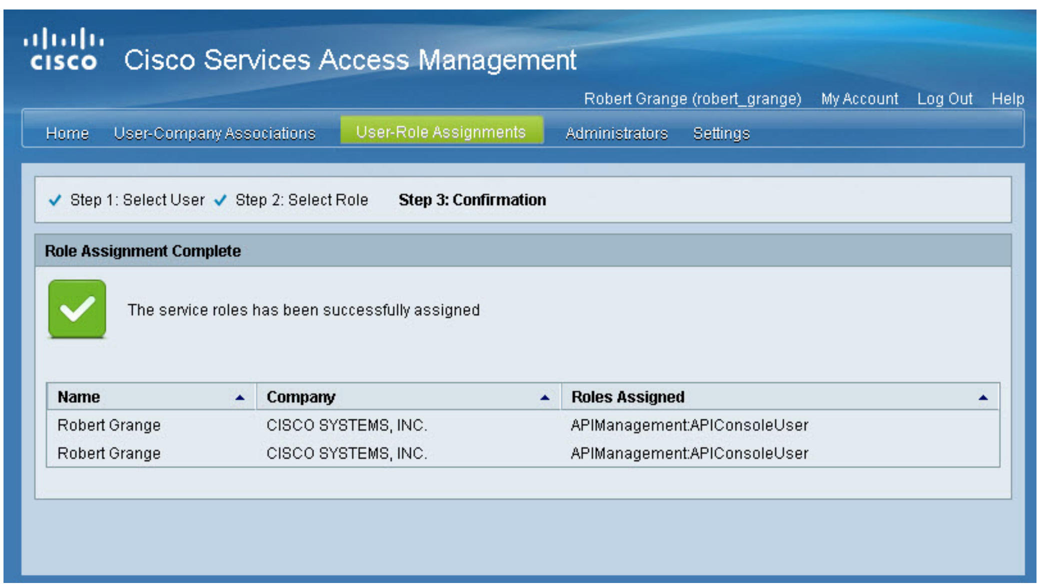
Step 6 Expand the Services Roles list by clicking on the triangle next to the desired service role.

Figure 2-1 ***Select Role***



Step 7 Click the checkbox next to the role to be assigned.

Step 8 Click **Finish**. A confirmation page will be displayed showing the roles assigned to the user(s).



The associated user will receive a confirmation e-mail informing them that their Cisco ID has been associated to the DA's company, and will indicate the role(s) assigned to them.

Role Assignment-Search for Users by Full Name

When adding user(s) for role assignment, the DA may search by the user's full name.

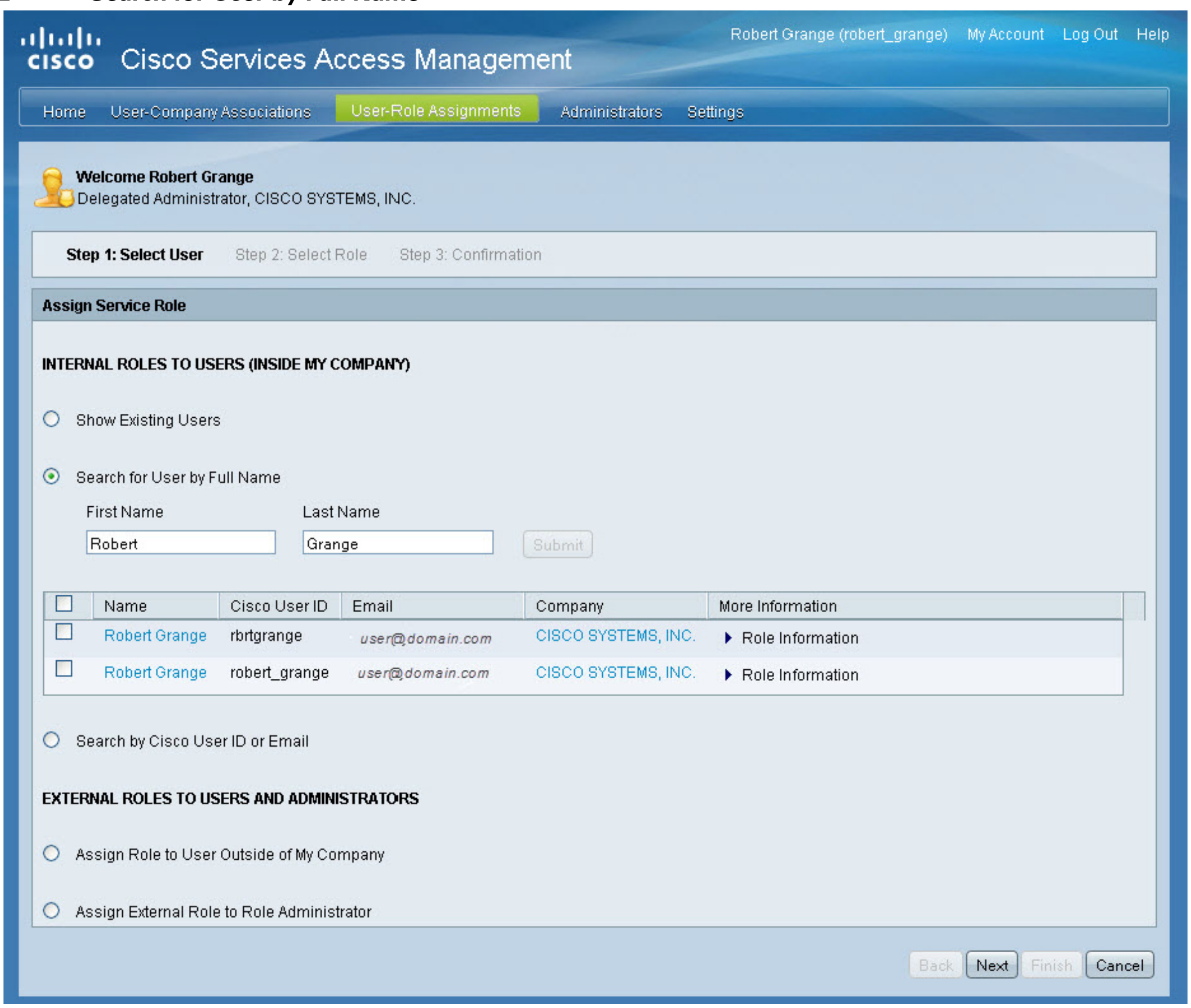
Step 1 Navigate to the user selection page by clicking on **User-Role Assignments > Assign Roles to Users**. The "Assign Service Role" page will open.

Step 2 Click on **Search for User by Full Name**, CSAM will display the first/last name fields. Complete the first/last name fields.

Step 3 Click **Submit**. The application will return any known users by their full name. See Figure 2-2 below.

Note It is important to remember that if the DA searches by the user's full name, that both the first and last name fields must be completed. If not, CSAM will return an error.

Figure 2-2 Search for User by Full Name



Step 4 Check the box next to the user to be assigned a role.

Step 5 Click **Next**. The user's name, the CCO ID, and personal e-mail address are added as an entry in the "Selected User" table. Check to ensure this information/user is correct. See Figure 2-1 on page 2-10

Step 6 Follow Steps 7-8 on page 2-10 to complete the role assignment.

Role Assignment-Search by Cisco ID or E-mail

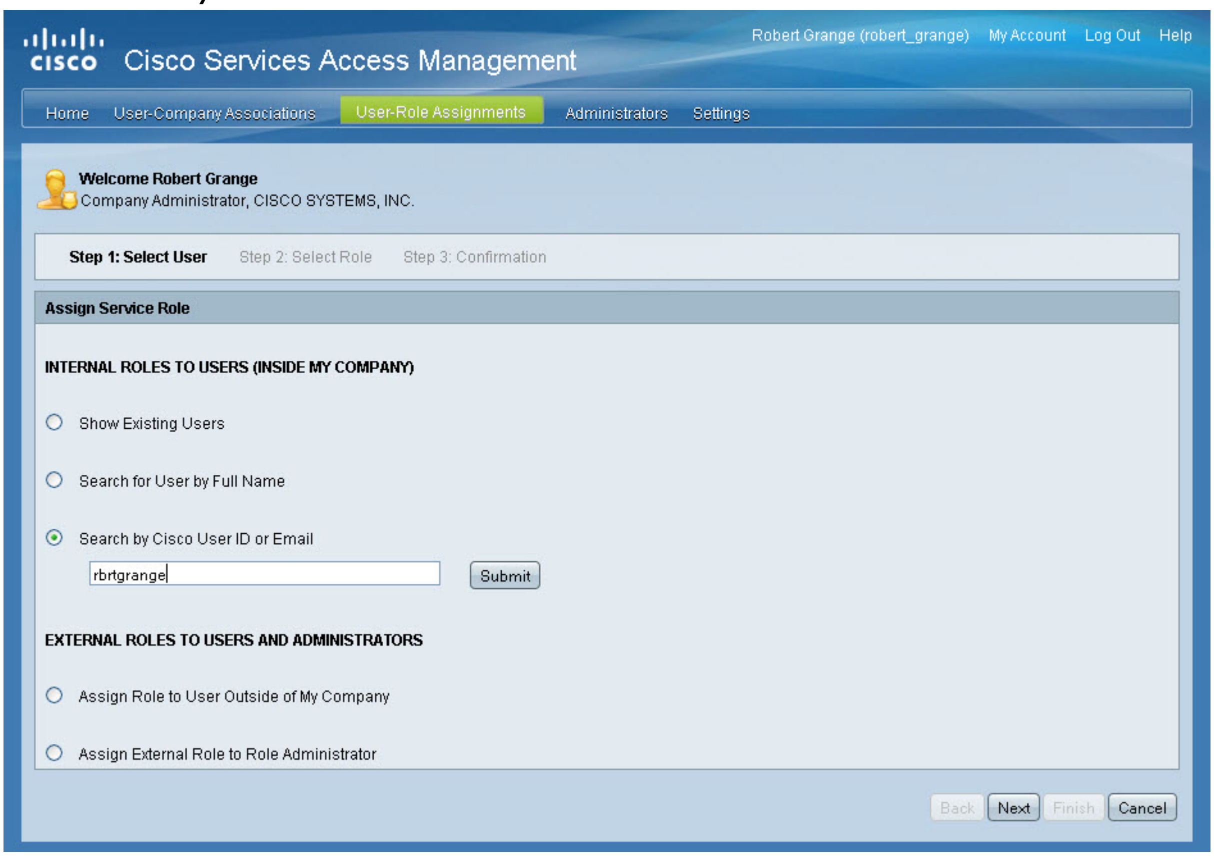
A DA may also search for a user by their Cisco ID, or E-mail. To utilize this function, do the following:

Step 1 Navigate to the user selection page by clicking on **User-Role Assignments > Assign Roles to Users**. The “Assign Service Role” page will open.

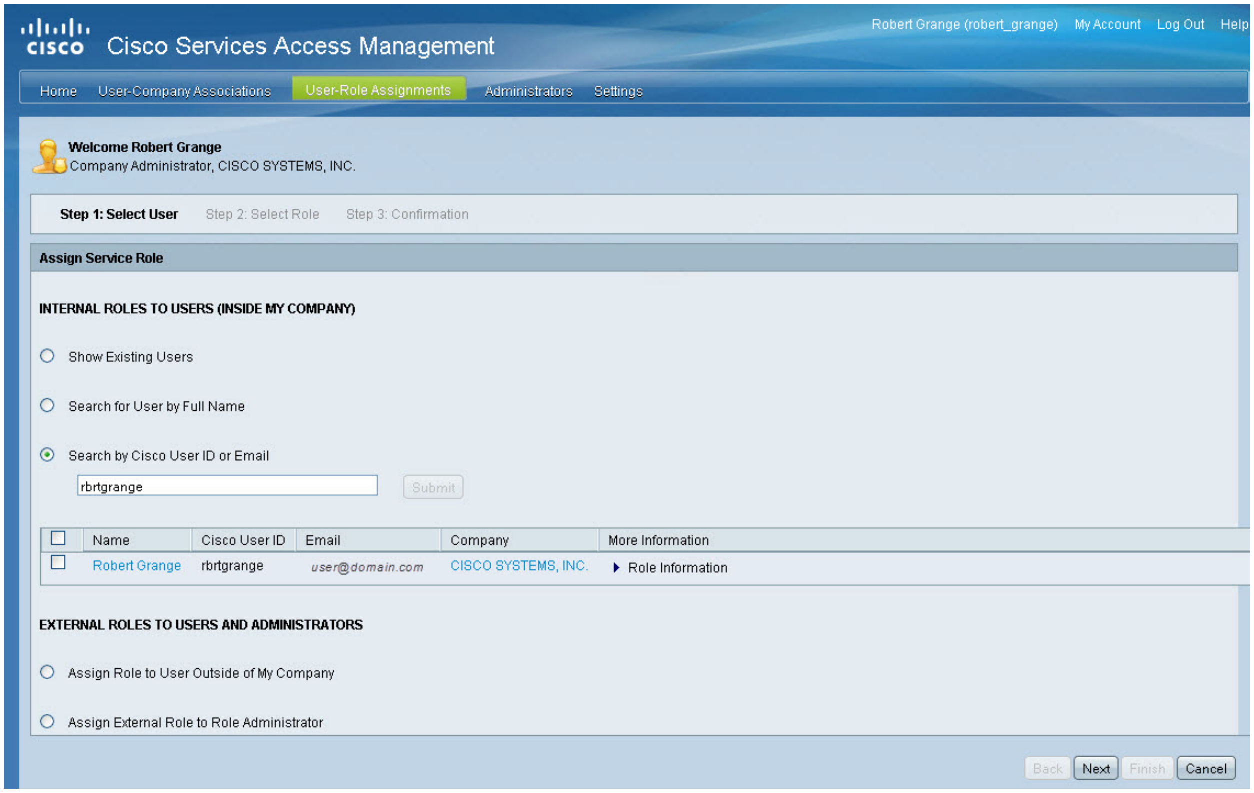
Step 2 Click on **Search by User ID or E-mail**, CSAM will display a single field. Complete the field by using *either* the Cisco ID, or E-mail associated with the user. Figure 2-3 on page 2-12 shows the field with the user ID.

Warning **Do not use both the Cisco ID and E-mail together in this field. If both are entered CSAM will return an error and invalidate the search.**

Figure 2-3 Search by Cisco User ID or E-mail

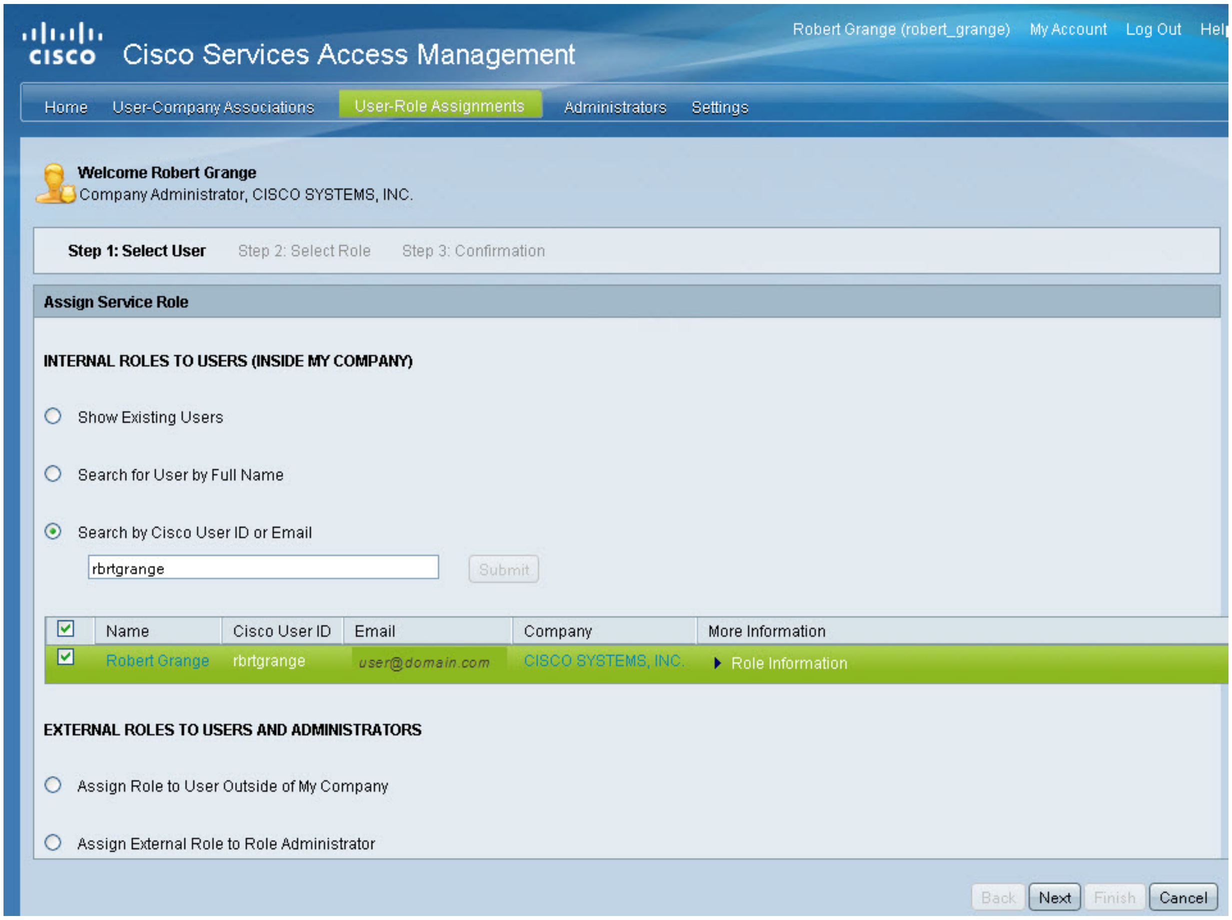


Step 3 Click **Submit**. If the user is in the database and has been associated with the DA’s company, CSAM will return the user’s information.



The DA may view the currently assigned roles by clicking on the triangle next to **Role Information**.

Step 4 Click the check box next to the user's name.



Step 5 Click **Next**.

Step 6 Follow Steps 6-8 on page 2-10 to complete the role assignment.

CHAPTER 3

API Console Usage

Revised: October 3, 2013

The API Console

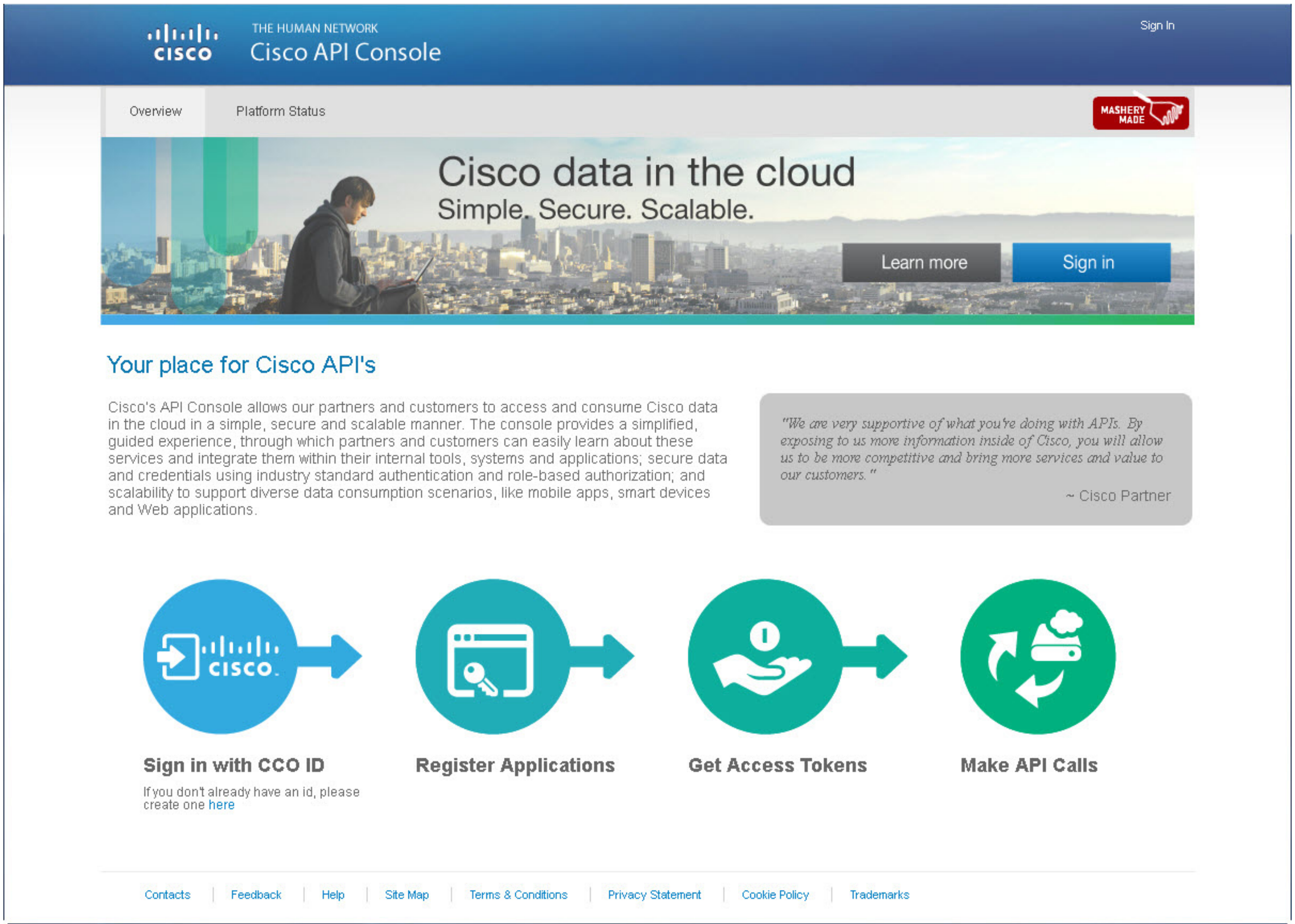
This chapter relates to usage of the API Console, and assumes the user has completed the steps in the Chapter 1, "On-Boarding-CCO-Registration", and Chapter 2, "Cisco Services Access Management (CSAM)".

This chapter covers the following areas:

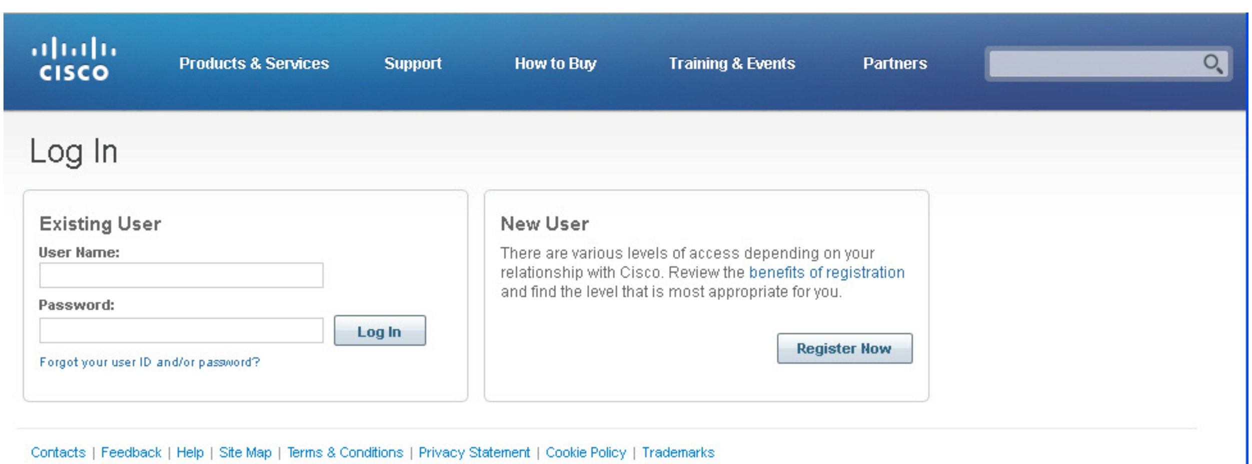
- Accessing the API Console
- Home Page
- Register an Application
- My Applications
- My APIs
- Support

Accessing the API Console

In a web browser navigate to https://apiconsole.cisco.com. The API Console home page appears:



Step 1 Click on "Sign In" link in the upper right portion of the pane to login to the API console. The Cisco log in page will be displayed:

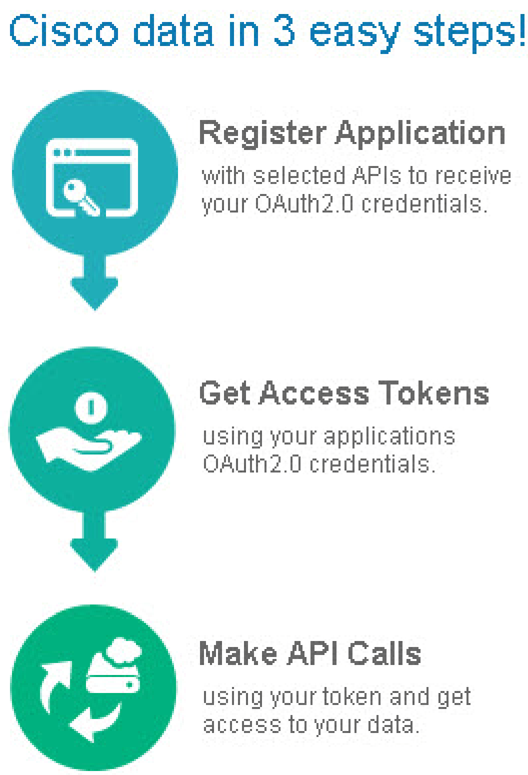


Step 2 Complete the User Name and Password fields and **click** Log In.

Step 3 The "Home" page will open.

Home Page

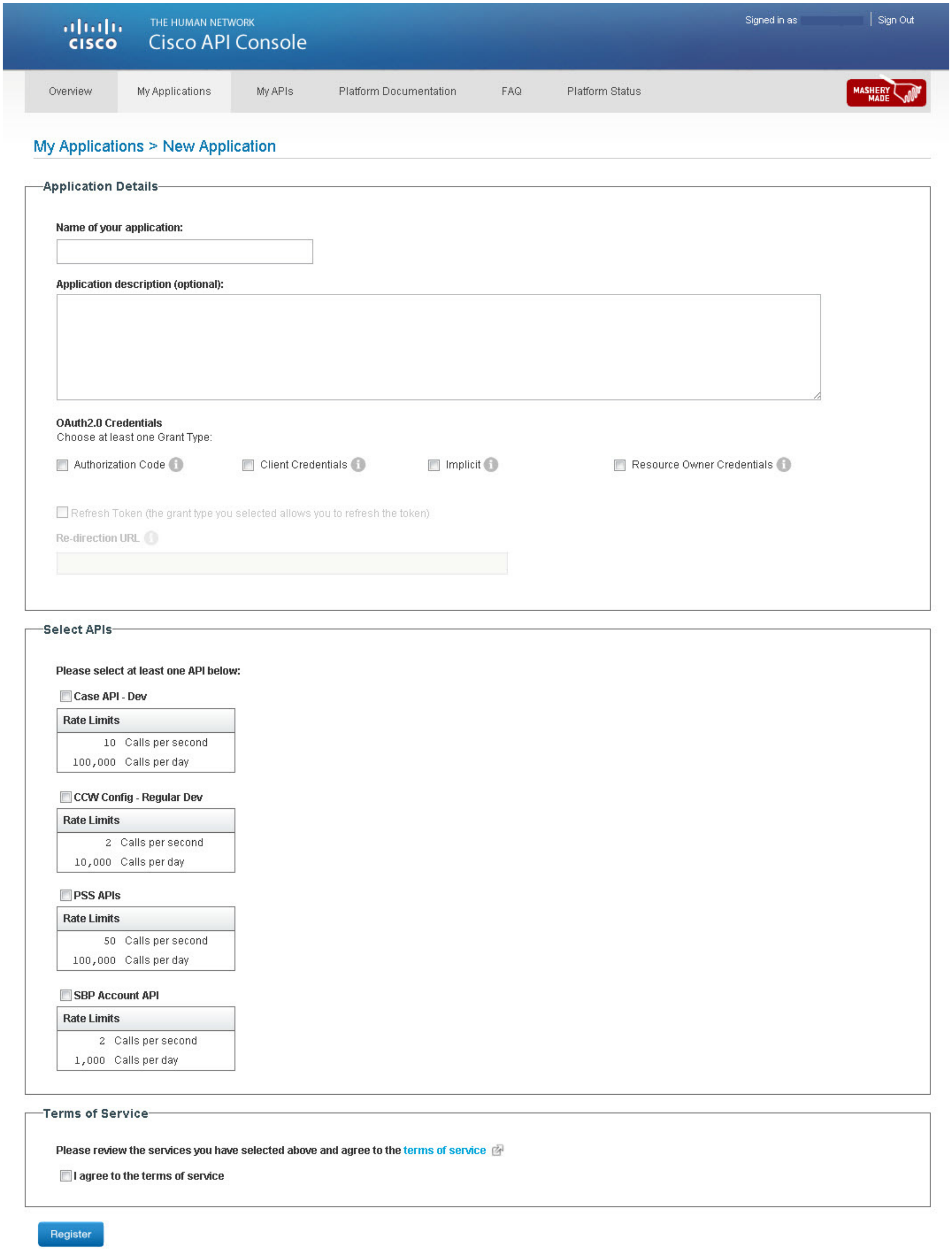
The Home page identifies the steps necessary to be completed before the user can run any of the API calls.



Register an Application

This section describes the information needed, and the steps that need to be performed to register an API application. Use the following steps to register an application:

Step 1 From the "Home" page, click on "Register a new application" link. The "Cisco API Console New Application" page will open:


THE HUMAN NETWORK
Cisco API Console
Signed in as [redacted] | Sign Out
Overview
My Applications
My APIs
Platform Documentation
FAQ
Platform Status
MASHERY MADE
My Applications > New Application
Application Details
Name of your application:
Application description (optional):
OAuth2.0 Credentials
Choose at least one Grant Type:
Authorization Code
Client Credentials
Implicit
Resource Owner Credentials
Refresh Token (the grant type you selected allows you to refresh the token)
Re-direction URL
Select APIs
Please select at least one API below:
Case API - Dev
Rate Limits
10 Calls per second
100,000 Calls per day
CCW Config - Regular Dev
Rate Limits
2 Calls per second
10,000 Calls per day
PSS APIs
Rate Limits
50 Calls per second
100,000 Calls per day
SBP Account API
Rate Limits
2 Calls per second
1,000 Calls per day
Terms of Service
Please review the services you have selected above and agree to the terms of service
I agree to the terms of service
Register

- Required Fields
  - **Name of your application**
- Optional Fields
  - **Application Description**

Step 2 In the “**Name of your application**” field, fill in the name of the application that is being registered.

Step 3 Select the OAuth2.0 Grant Type (see the Glossary for expanded explanations of the OAuth2.0 Grant Types) to be used with the application. The available choices are:

- **Authorization Code**
- **Client Credentials**
- **Implicit**
- **Resource Owner Credentials**
- **Refresh Token (Token Validation)–Only valid for Authorization Code or Resource Owner Credential grant types.**
- **Register Callback URL**

Note At least one or more OAuth v2.0 Grant type requested from this Client ***must be selected*** (checked). If either the Authorization Code or Implicit grant types are chosen, then entering a Redirection URL (where your client is known to execute) ***is required***. The URL must be chosen at the time of registration. If the URL is not chosen, the platform will not allow the API to be registered.

The current recommendation for grant type usage:

- Client Credentials Grant are for a hosted client applications (Machine to Machine) from a trusted environment.
- AuthCode Grant for Web Server application (from a trusted environment).
- Implicit Grant for JavaScript or Native Mobile/Desktop applications.
- Resource Owner Grant is not recommended.

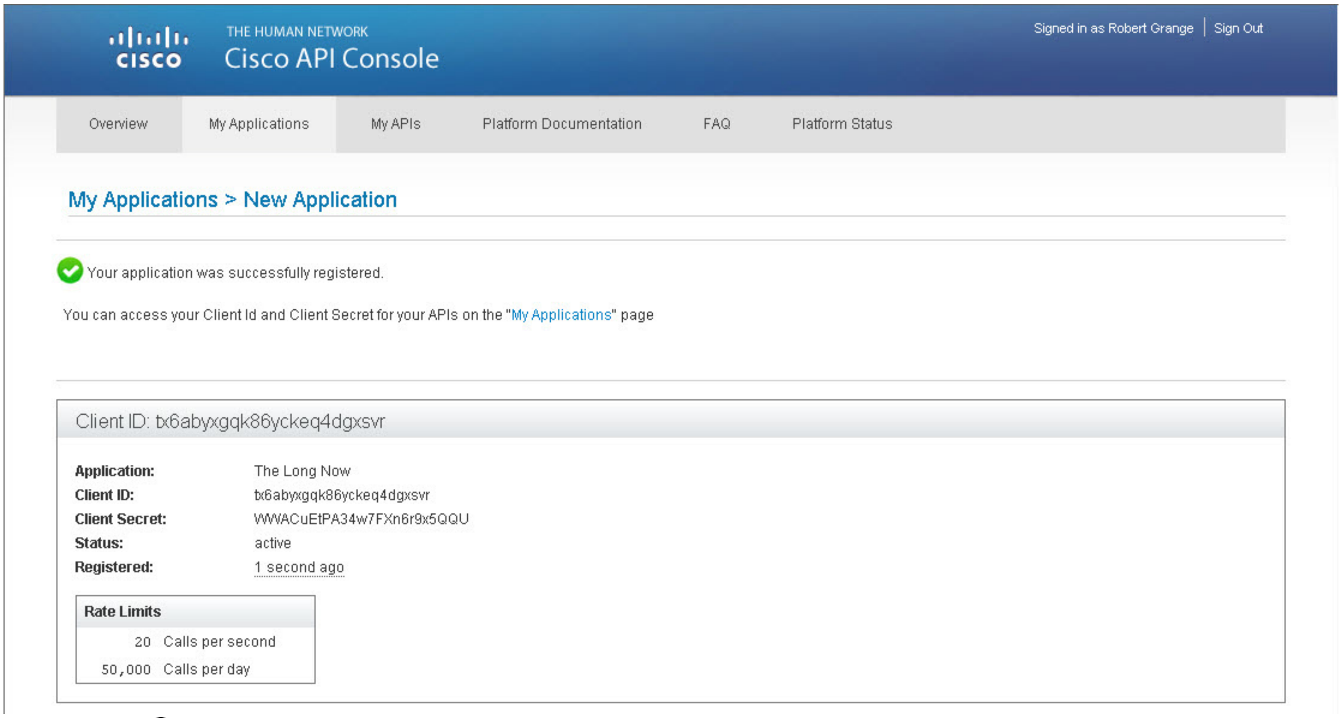
Note One client application rarely utilizes more than one of the above grant types.

Step 4 Select an API to be used with the application.

Step 5 Read the **Terms of Service**, then check the **I agree to the terms of service** agreement check box.

Step 6 Click the **Register** button.

After the application registration is completed the console window displays an “Application Registered” message.



Tip This is simply the confirmation page detailing the application has been successfully registered, and that the Client ID and the Client Secret have been issued. The user will be able to refer to their "My Applications" page at any time to retrieve their Client ID and Client Secret.

Along with the registration confirmation, the window displays the following information:

- The API(s) registered with the application.
- **Application:** The name of the registered application.
- **Client ID / Client Secret:** The Client ID and Client Secret are used together as input for the Cisco Token services (as they identity the client application) to acquire an access-token or grant/code. Only access-tokens accompany an API call.

Tip The **Client ID** and **Client Secret** are the *OAuth 2.0* credentials used by the API service call to obtain the access token. It is recommended that users return to the "My Applications" page to retrieve these credentials. It is also recommended to keep the Client ID/Client Secret private and not to share that information (for example, using the same restrictions as sharing a password).

- **Status:** Indicates the status of the application.
- **Registered:** Indicates the length of time since the application was registered.

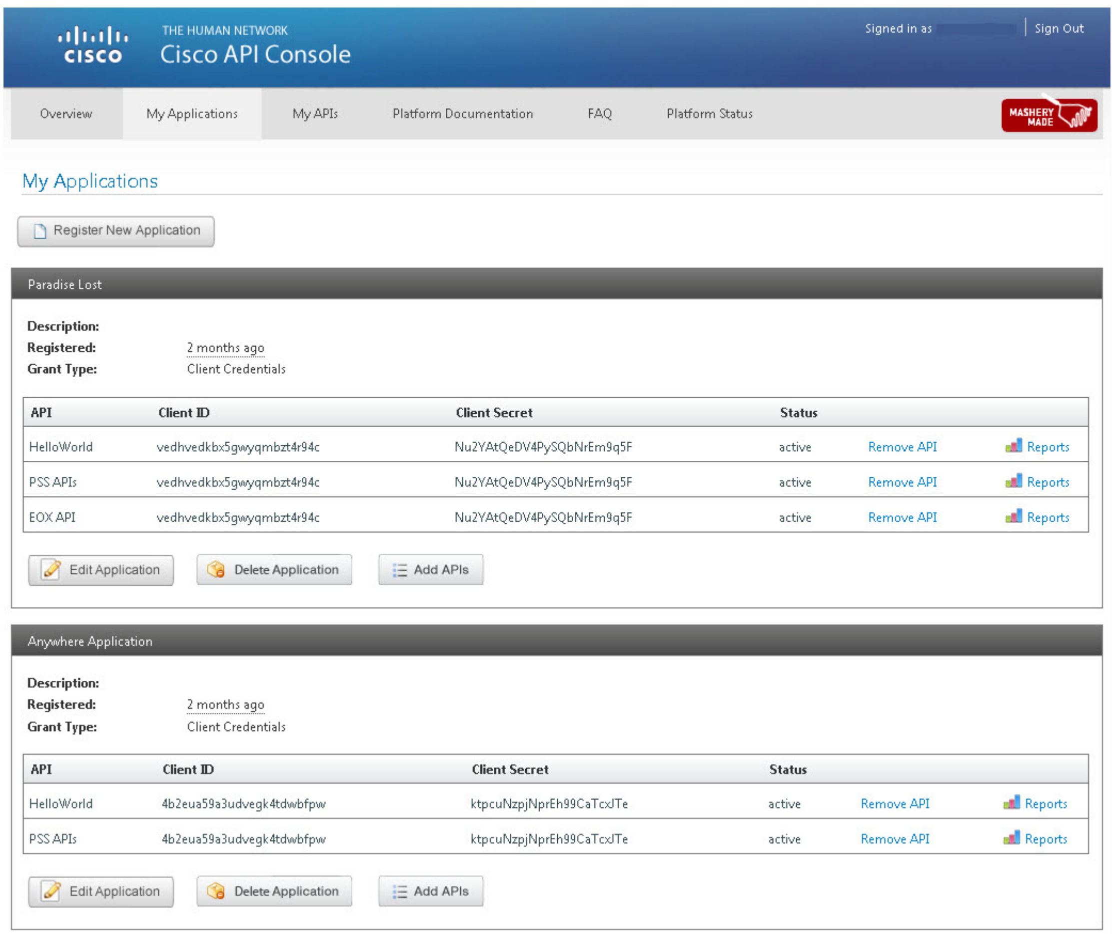
Step 7 Click on "**My Applications**" either below the header graphic, or the link directly below the "Your application was successfully registered" statement. This will open the user's account page.

My Applications

The "**My Applications**" link will open a page displaying information for any currently registered applications (see below). When utilizing the API console, this page contains the Client ID and Client Secret obtained after the completion of the "Register an Application" section on page 3-3.

The console window lists the data by client application (name); each set of APIs associated with the application; the Client ID and Client Secret; and status for each of the client applications integration to a Cisco API. Also provided are Reports, Edit Application, and Manage APIs links. The page allows the user to perform the following tasks:

- Review API Metrics
- View Reports
- Edit an Application
- Add APIs



Review API Metrics

The API Console provides usage reporting of all of the API service calls that are made, and lets the user view reports that display different user and performance metrics. The Reports option also lets the user set various time frames to view user and performance metrics.

View Reports

The Reports console window gives the user the option to specify a time frame to view information about monitored method calls and error codes. The current time frame options are:

- Today
- Last 7 Days
- This Month
- Last Month

To access the metrics information, do the following:

Step 1 Click on "**Reports**" in the Client ID Pane. The Client ID Activity console window appears and displays the following information:

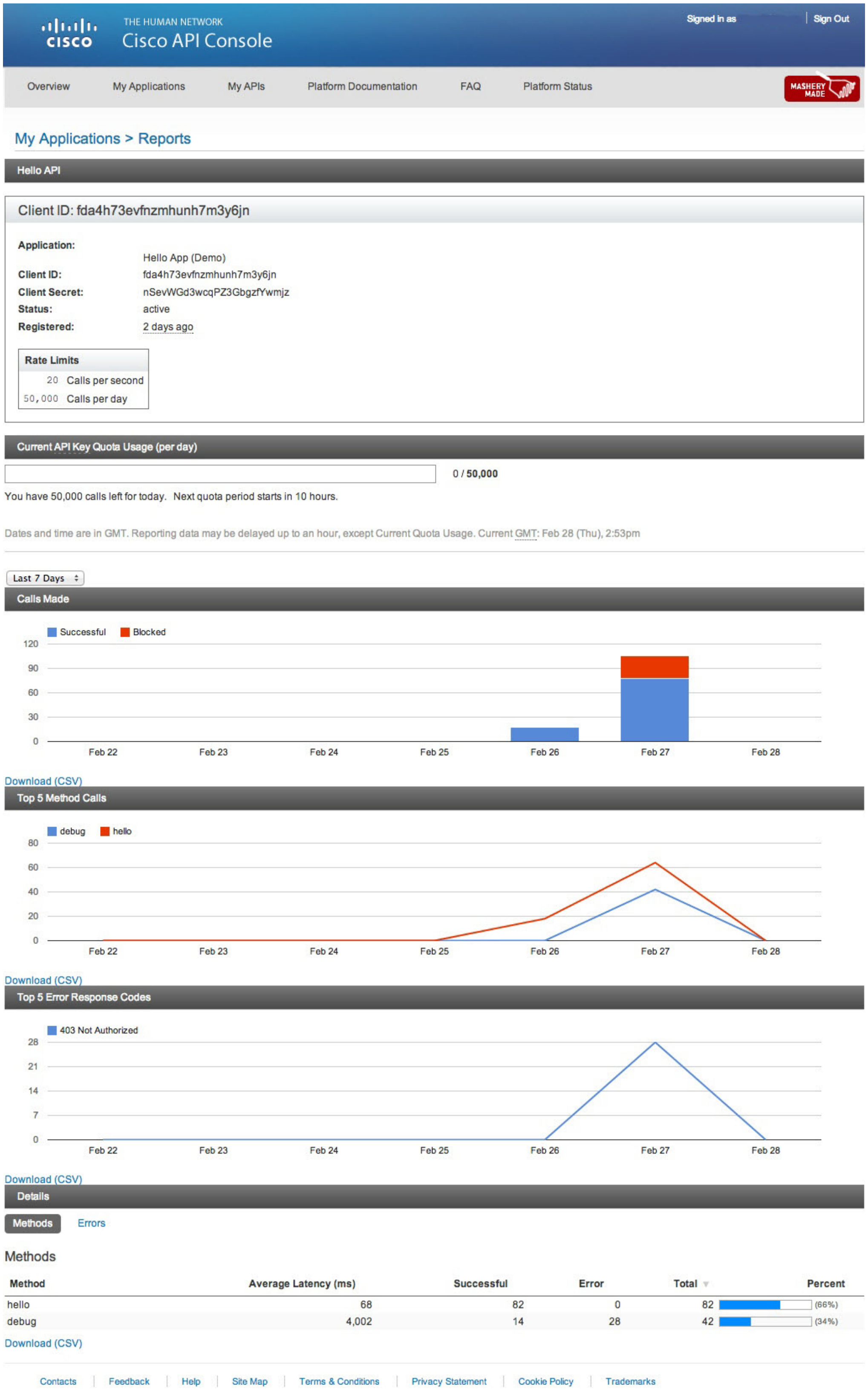
- Identifies what portion of the allotted daily quota has already been used. Quota usage counters can be delayed up to 20 minutes.
- Lets the user specify a time frame.
- **All API Calls** – lists all the API service calls that were made.
- **Top 5 Method Calls** – identifies the five API service calls that were made most often.
- **Top 5 Error Response Codes** – identifies the five API error response codes that occurred most often.

Note All charts / tables of usage counts can be delayed up to 45 minutes.

- **Details** has two different categories of information:
- **Methods** – lists what method calls were used, and identifies when they were used.
- **Errors** – alerts the user to any errors that occurred when specific API calls were made. This gives the user the ability to investigate and fix any errors they may have encountered.

Step 2 Once the page has been displayed. The user can change the time period using the drop down menu to view the metrics for those time periods. Once a new selection has been made from the drop down window, the page will refresh with the metrics for the chosen time frame.

Note If the user is not on the "My Applications" page, they can access the page by clicking on the "My Applications" link below the header graphic.


THE HUMAN NETWORK
Cisco API Console
Signed in as
Sign Out
Overview
My Applications
My APIs
Platform Documentation
FAQ
Platform Status
My Applications > Reports
Hello API
Client ID: fda4h73evfnzmhunh7m3y6jn
Application: Hello App (Demo)
Client ID: fda4h73evfnzmhunh7m3y6jn
Client Secret: nSevWGd3wcqPZ3GbgzfYwmjz
Status: active
Registered: 2 days ago
Rate Limits
20 Calls per second
50,000 Calls per day
Current API Key Quota Usage (per day)
0 / 50,000
You have 50,000 calls left for today. Next quota period starts in 10 hours.
Dates and time are in GMT. Reporting data may be delayed up to an hour, except Current Quota Usage. Current GMT: Feb 28 (Thu), 2:53pm
Last 7 Days
Calls Made
Successful
Blocked
Feb 22
Feb 23
Feb 24
Feb 25
Feb 26
Feb 27
Feb 28
Download (CSV)
Top 5 Method Calls
debug
hello
Download (CSV)
Top 5 Error Response Codes
403 Not Authorized
Download (CSV)
Details
Methods
Errors
Methods
Method | Average Latency (ms) | Successful | Error | Total | Percent
hello | 68 | 82 | 0 | 82 | (66%)
debug | 4,002 | 14 | 28 | 42 | (34%)
Download (CSV)
Contacts | Feedback | Help | Site Map | Terms & Conditions | Privacy Statement | Cookie Policy | Trademarks

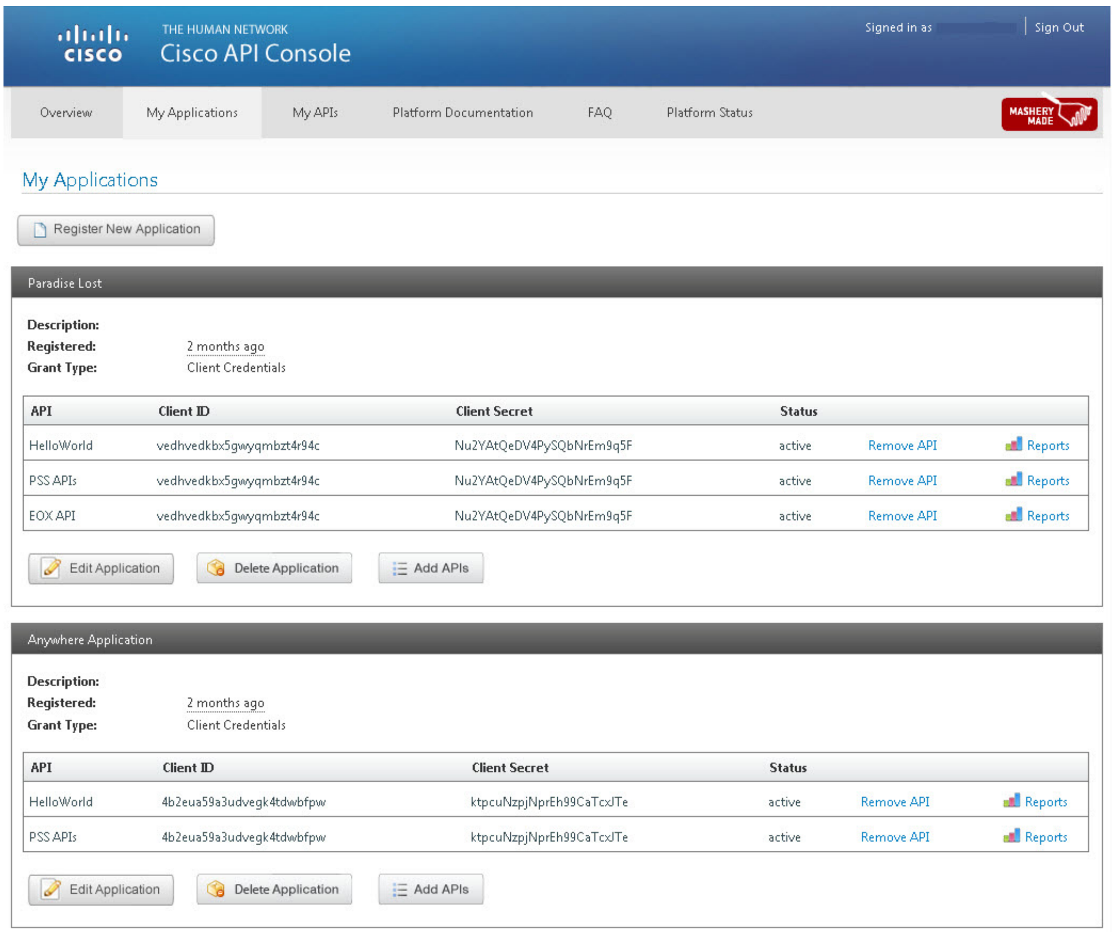
Edit an Application

The “Edit” function allows the user to update information for the chosen application. The user can change the name, description. or add a new grant type to a registered application.

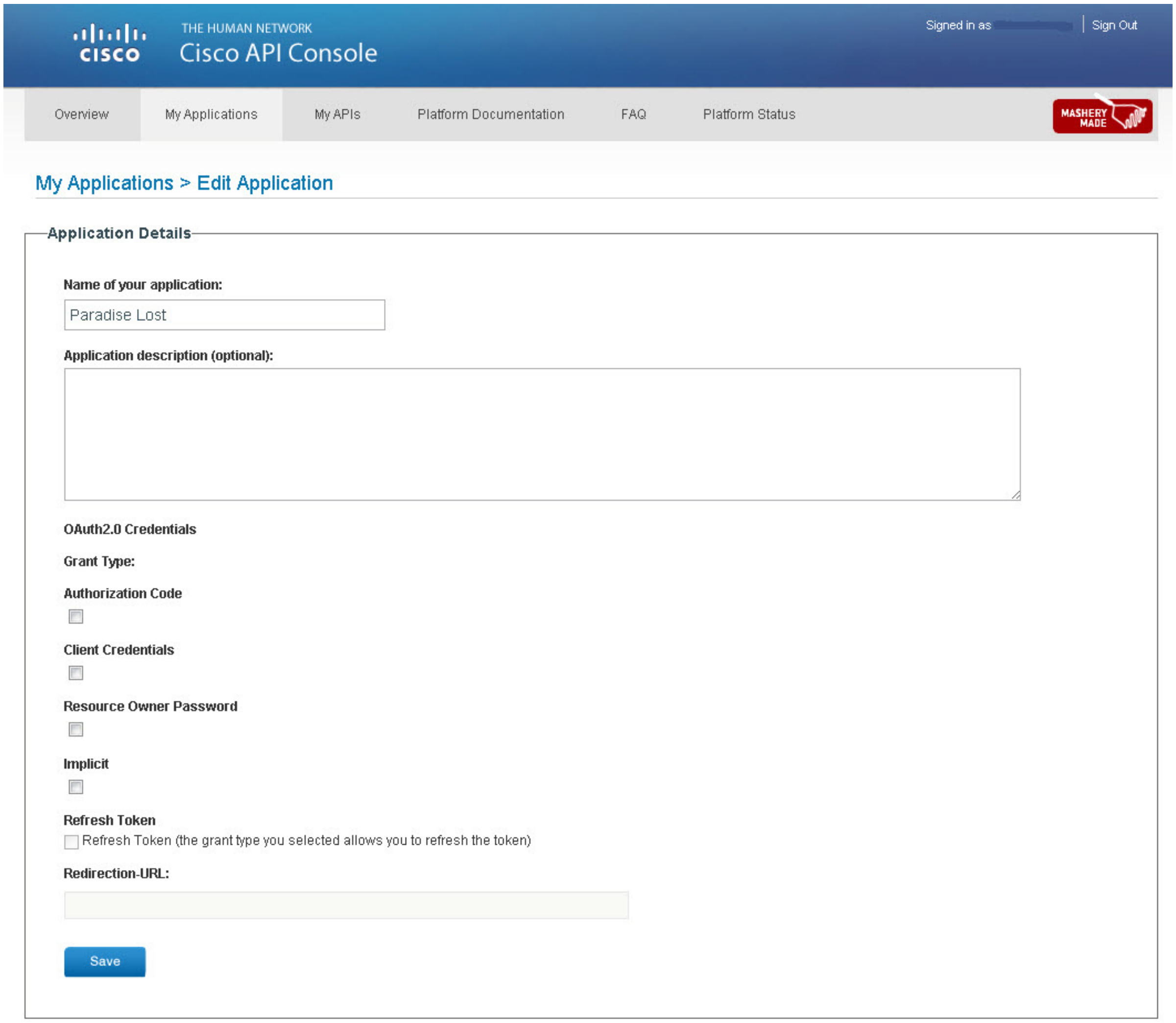
Changing the Name and Description

To edit the name and description information do the following:

Step 1 Navigate to **My Applications**.



Step 2 **Click** on “Edit Application” button in the pane for the application that is to be updated. The “Edit Application” page will open.



Step 3 Complete the "Name" and "Application description" fields with the information to be updated.

Step 4 **Click** "Save."

Changing Grant Types

The APIx platform gives the user the flexibility to change grant types for their application. One example where a user might want to change their grant type is where the user has begun by using one grant type, but after time and usage the use case changes, and as such, the original choice of grant type may need to be updated. For more information on Grant Type selection see "Register an Application" section on page 3-3. To change a grant type complete the following steps:

Step 1 Navigate to the "My Applications" page.

Step 2 In the application frame to be edited, **click** "Edit Application." The "Edit Application" page will be displayed.

Step 3 Select the OAuth2.0 Grant Type (see the Glossary for expanded explanations of the OAuth2.0 Grant Types) to be used with the application. The available choices are:

- **Authorization Code**
- **Client Credentials**
- **Implicit**
- **Resource Owner Credentials**
- **Refresh Token (Token Validation)–Only valid for Authorization Code or Resource Owner Credential grant types.**
- **Register Callback URL**

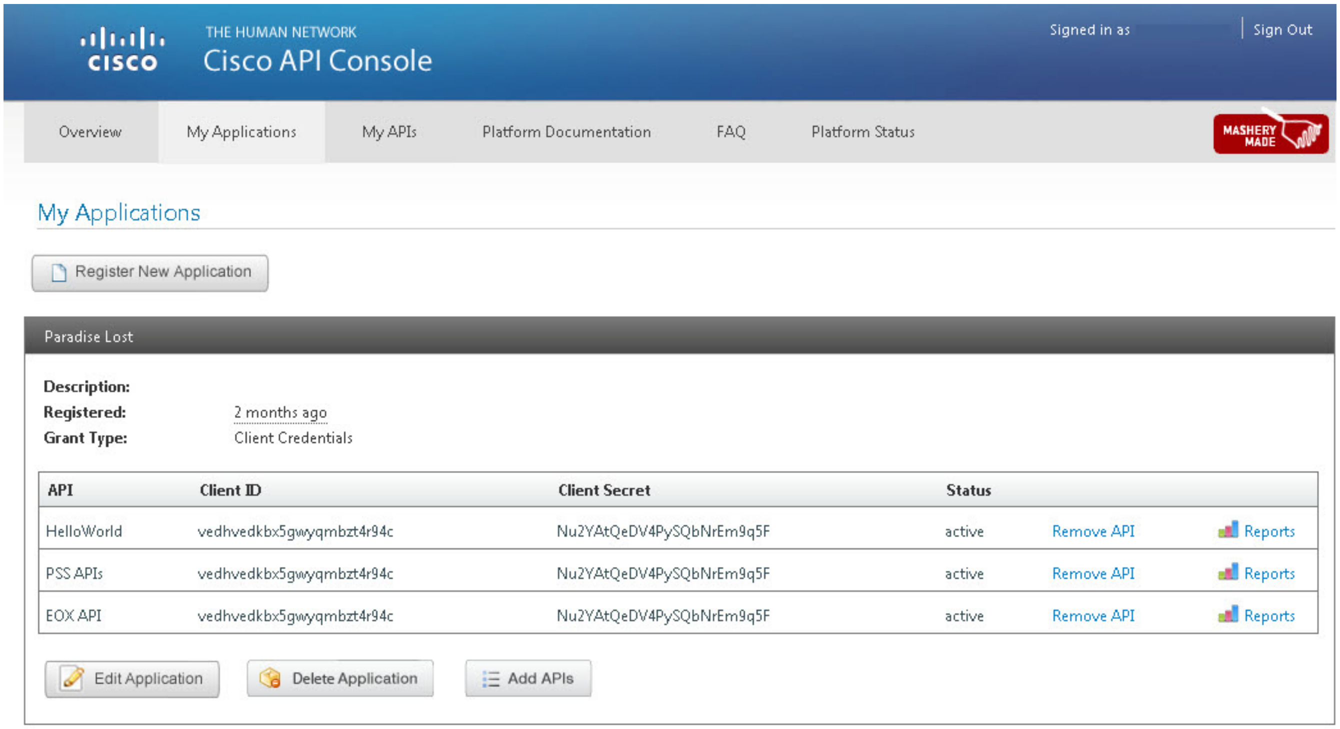
Step 4 **Click** “Save.”

Delete an Application

The user can delete an application depending upon their needs. To delete an application, use the following steps:

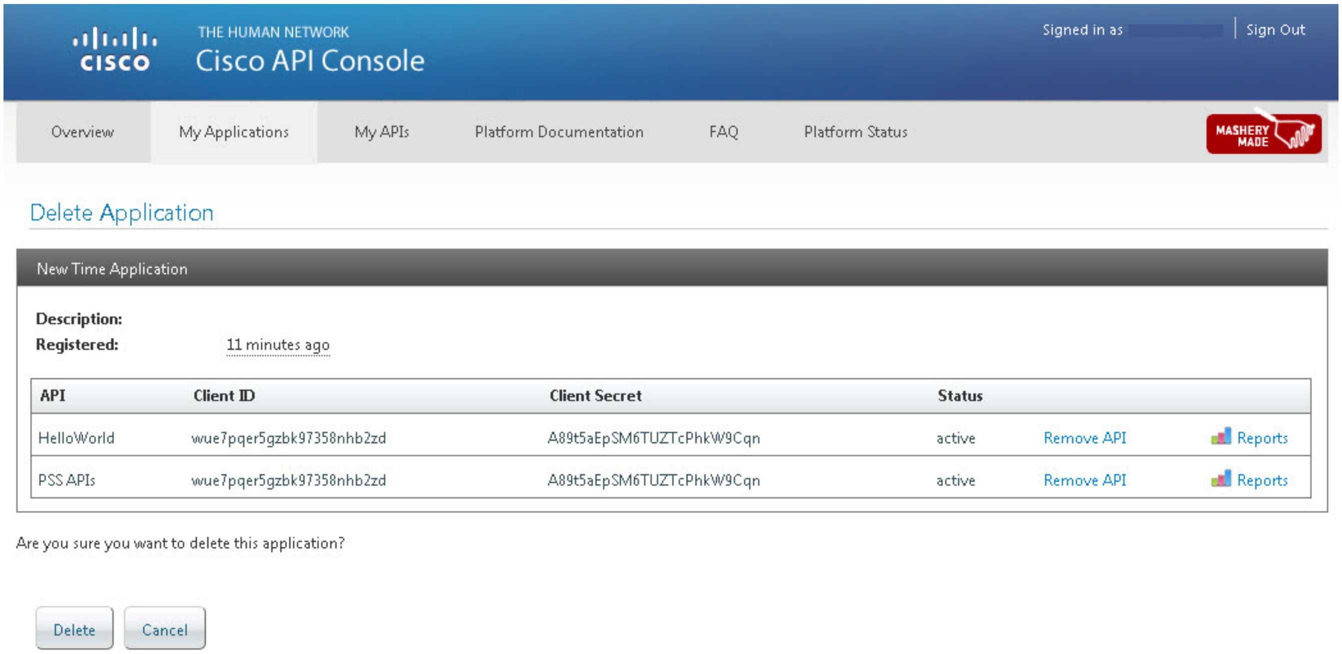
Note If the user decides to delete an application, be aware that this will delete all of the files associated with the application, including the Client ID/Client Secret. Once the application has been deleted, the Client ID/Client Secret will no longer be valid and can not be used for another application.

Step 1 Navigate to the “My Applications” page. The page should display all of the applications currently registered with the Platform and all APIs associated with that application.

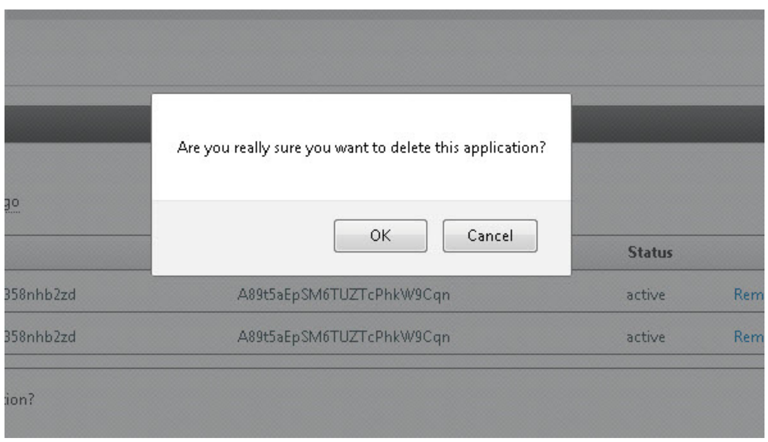


Step 2 Choose the application to be deleted. For this example we will choose the "Anywhere Application."

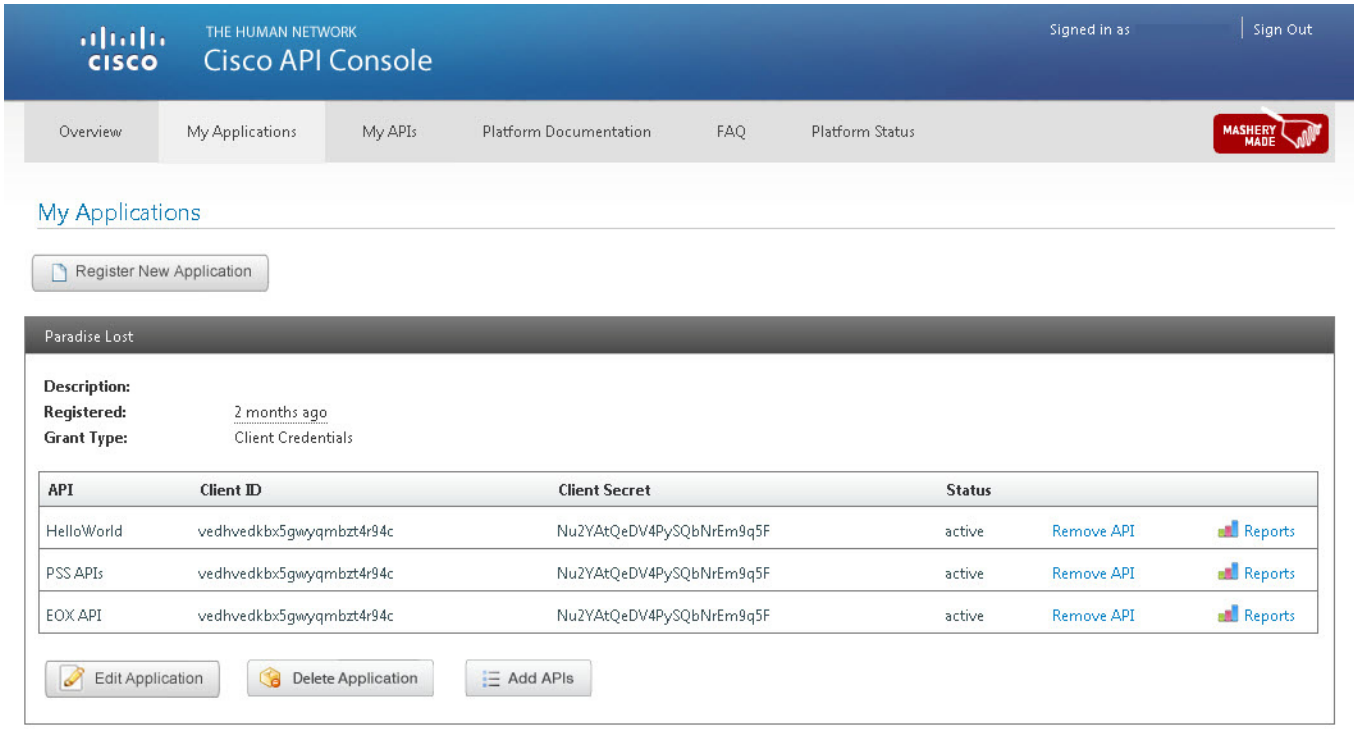
Step 3 **Click** the "Delete Application" button. The "Delete Application" page will be displayed.



Step 4 **Click** "Delete." A new window will appear requesting a delete confirmation.



Step 5 **Click** "OK." The "My Applications" page will be displayed showing the remaining registered applications (if there are any), or a blank page if there was only one registered application.

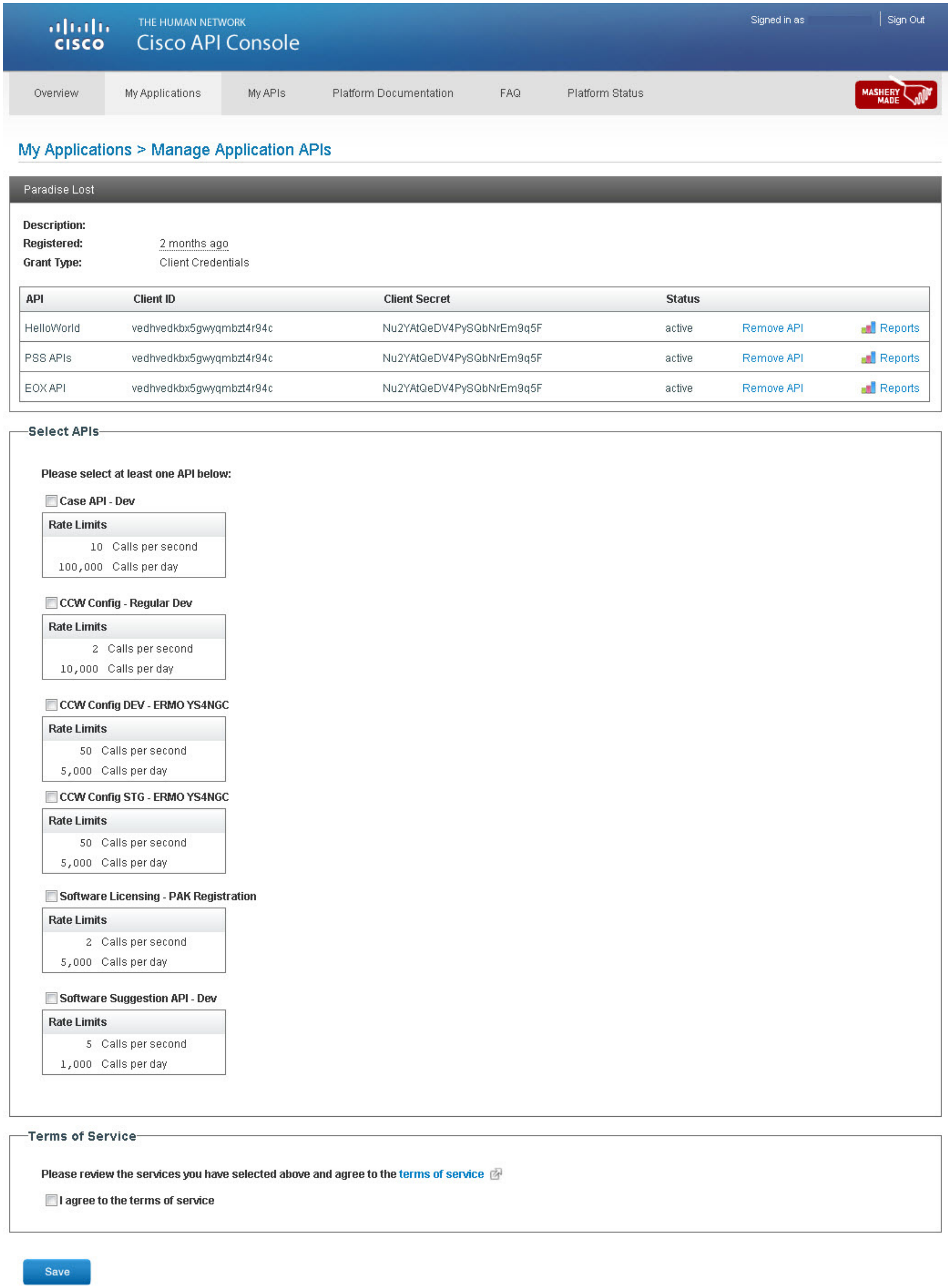


Add APIs

An application may use different services which will require the addition of different APIs. However, the initial grant type chosen when registering the original application will remain the same. Therefore, if a grant method was chosen for a web based application, then the newly added APIs will only be available for a web based application. As stated above in the "Register an Application" section on page 3-3, if the application is to be used for a different purpose than the original grant type, the user must register a new application for that grant type.To add APIs to an already registered application, do the following:

Step 1 Navigate to **My Applications**.

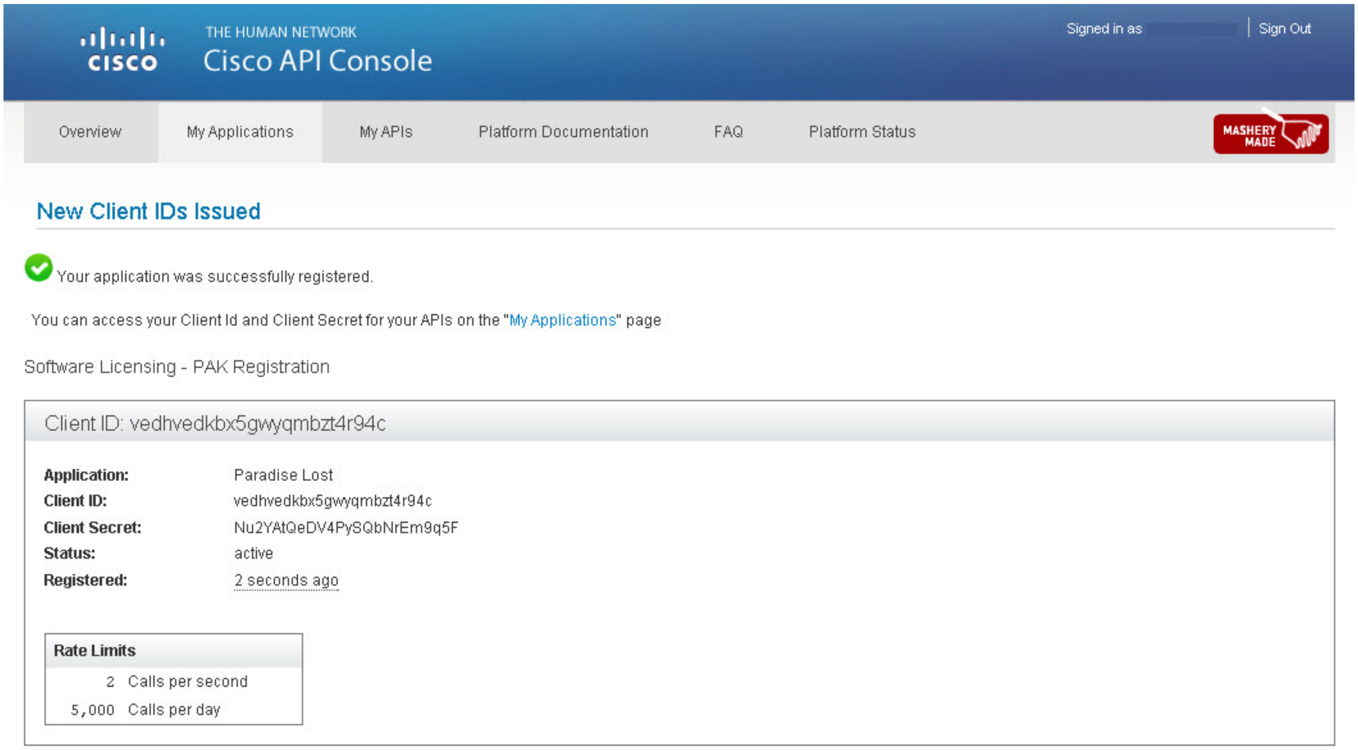
Step 2 In the application pane, **click** "Add APIs." The "Manage Application APIs" page will open.



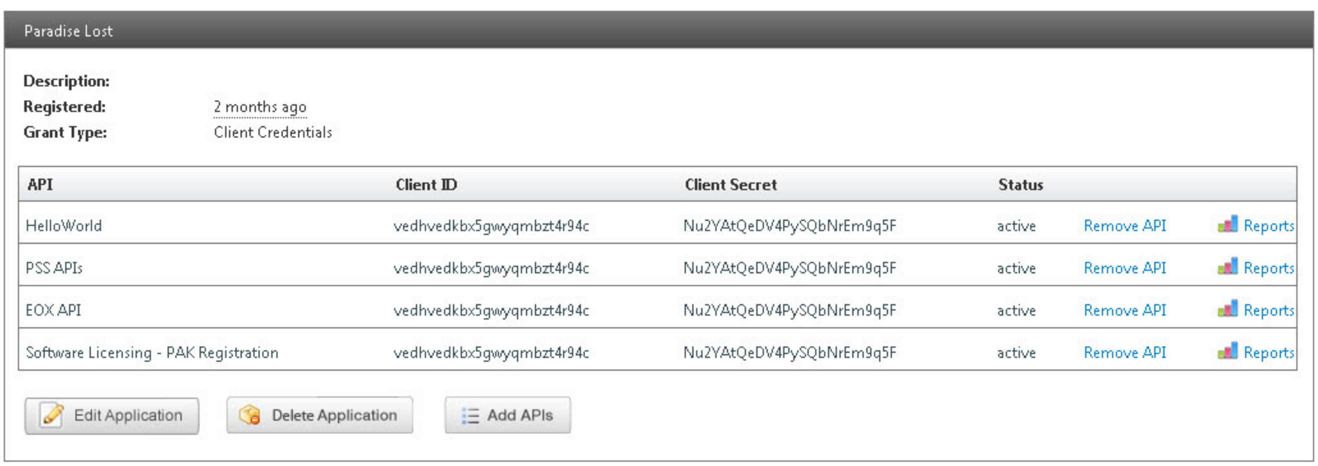
Step 3 **Click** the checkboxes for the APIs to be utilized by the application.

Step 4 **Click** the **I agree to the terms of service** checkbox.

Step 5 **Click** the **Save** button. The “New Client IDs Issued” page will open.



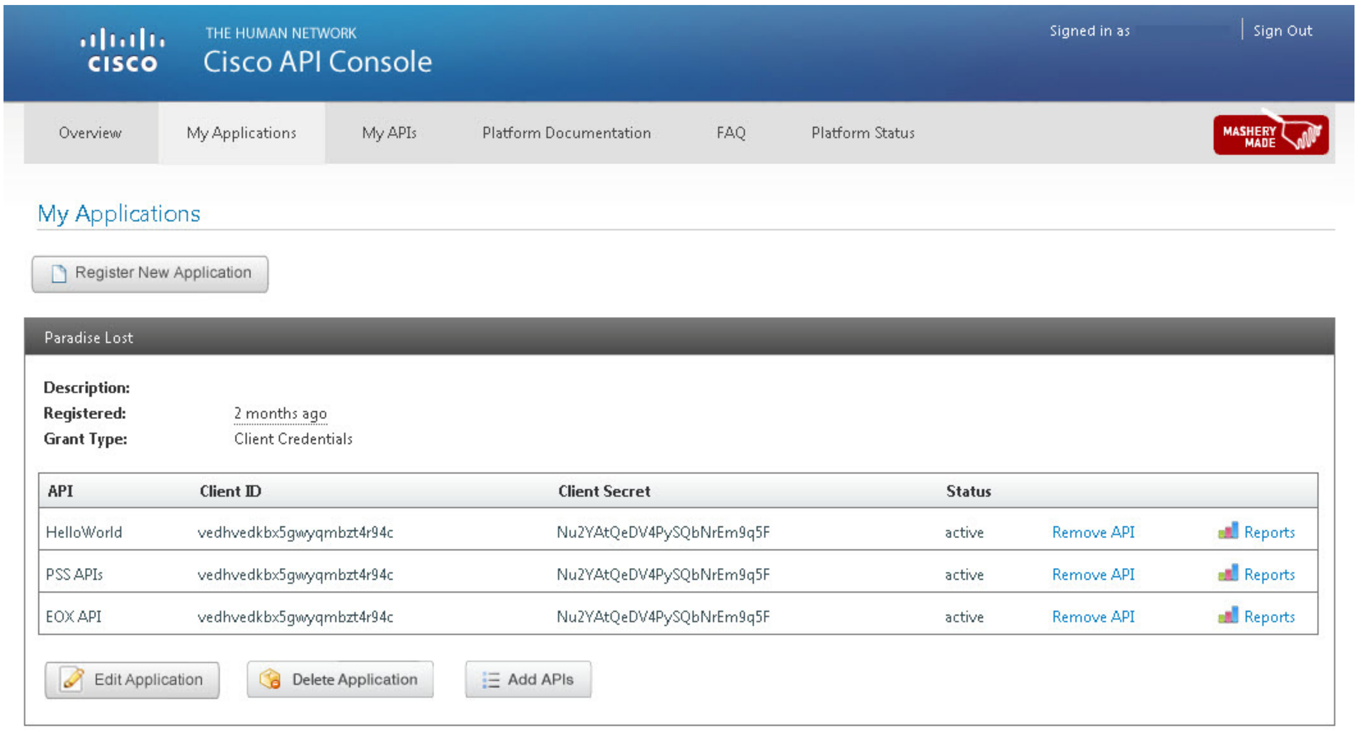
Step 6 **Click** on the “My Applications” link below the “Your Application was successfully registered” statement, or the “My Applications” tabbed link. The “My Applications” page will open displaying the newly added APIs for the application.



Remove APIs from a Registered Application

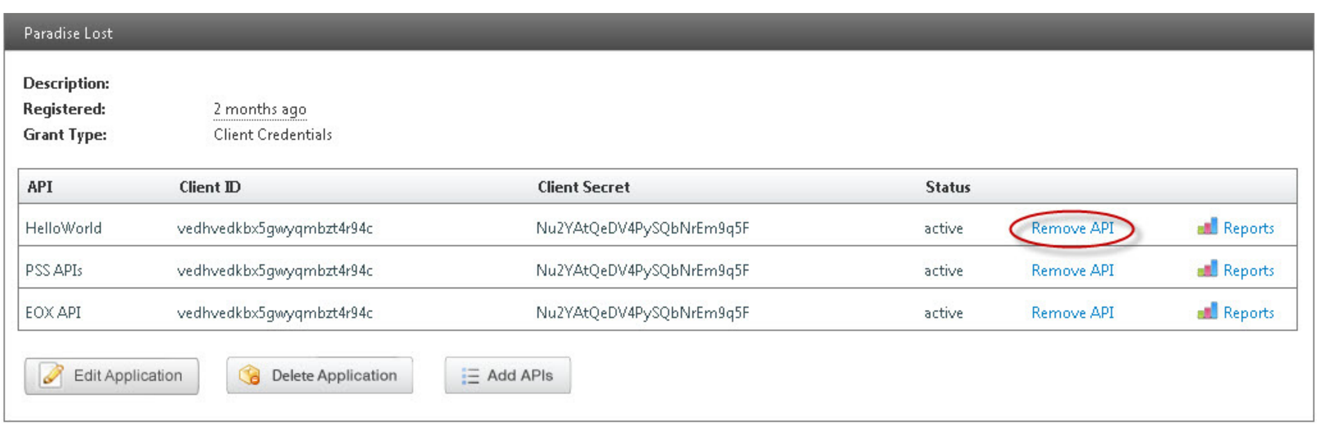
The APIx Platform allows the user the ability to remove specific APIs from any registered application. The following steps will only remove the APIs, if the user requires deletion of the application, follow the steps in the "Delete an Application" section on page 3-12. To remove APIs from a registered application do the following:

Step 1 Navigate to the "My Applications" page. The Page will show all of the currently registered applications.

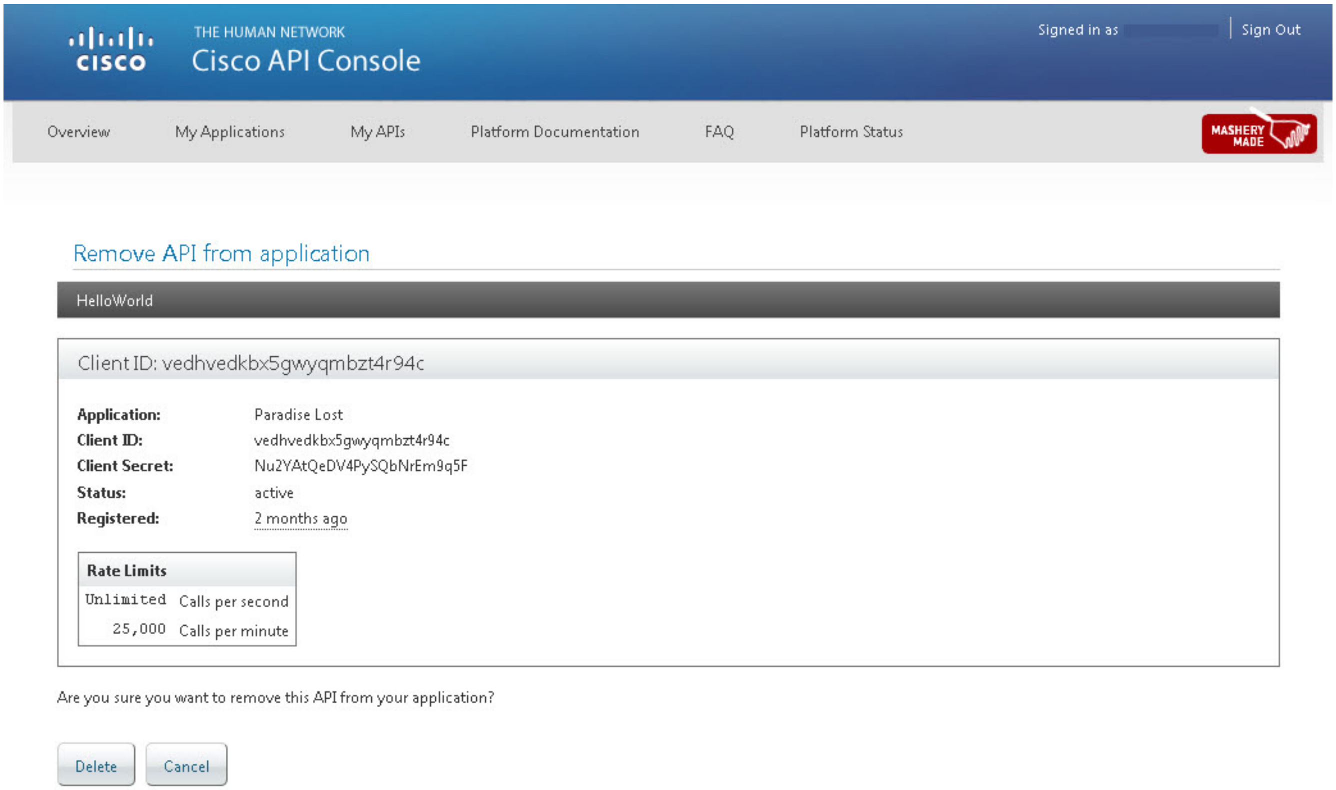


Step 2 Choose the APIs to be removed from the application. For this example we will remove the "HelloWorld" API from the "Paradise Lost" application.

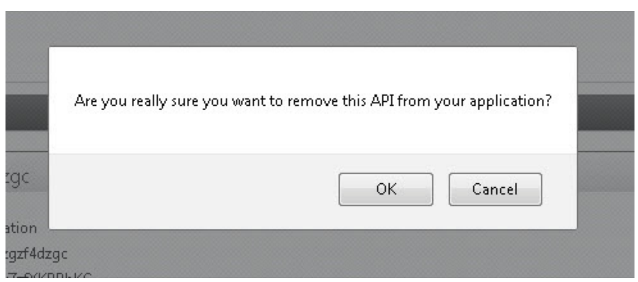
Step 3 **Click** on the "Remove API" link to the right of the "Status" column.



Step 4 The "Delete Client ID" page will be displayed.



Step 5 **Click** "Delete." A new window will appear requesting a delete confirmation.



Step 6 **Click** "OK." The "My Applications" page will be displayed showing the remaining associated APIs (if there are any), or a registered application frame with no associated APIs.

My APIs

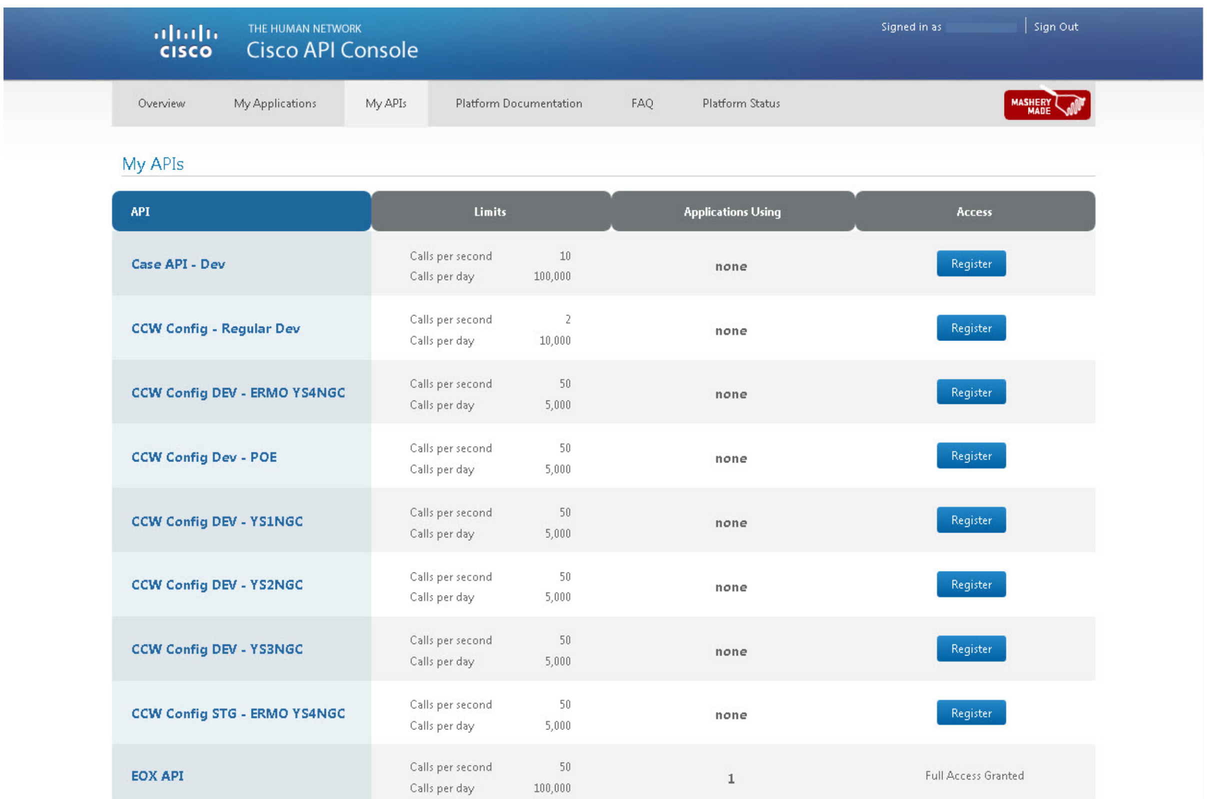
The My APIs page displays all of APIs the user is currently registered for, the access level of the APIs, and any other APIs available for registration by the user. The My APIs page is divided into four columns: API, Units, Application Using, and Access.

Table 3-1 My API Column Headings and Descriptions

Heading	Description
API	The specific API offered by a tenant on the APIx platform.
Limits	Describes the number of calls per second, and calls per day for each of the API offerings. These limits are set by the individual tenants offering the API, not the platform.
Application Using	Shows the number of applications the user has registered to use the specific API.
Access	Shows the level of access granted to the user for the registered API.

Figure 3-1 gives an example of what a user may see when viewing the My APIs page.

Figure 3-1 My APIs Page



Notice there are several APIs which have “Register” next to them, while the EOX API at the bottom shows “Full Access Granted.” These statuses inform the user that they have full privileges to the EOX API, and may also register the other APIs for a current, or new, application.

Platform Status

The Platform Status page gives the user updates on Alerts, Notifications/Announcements (archived and current), and API Availability Status.

Support

Support for each tenant's API can be found in the API Availability section of the Platform Status page under the heading "Support Tools":

Support Tools:			
CASE API	API is Operating Normally	N/A	ssapi-pilot-help@external.cisco.com
EOX API	API is Operating Normally	N/A	ssapi-pilot-help@external.cisco.com
Service Order Return API	API is Operating Normally	N/A	ssapi-pilot-help@external.cisco.com
Software Information And Delivery	API is Operating Normally	N/A	
Software Information And Delivery - POE	API is Operating Normally	N/A	
Software Suggestion API	API is Operating Normally	N/A	ssapi-pilot-help@external.cisco.com

Note If there is no support contact listed for a tenant, please contact your business operations manager, or liaison.

GLOSSARY

Revised: October 3, 2013

A

AAA

Standsforauthentication,authorization,andaccounting.Formoreinformation,refertoAAAprotocol on the Wikipedia web site.

Authorization Code Grant Type

The authorization code grant type is used to obtain both access tokens and refresh tokens and is optimized for confidential clients. As a redirection-based flow, the client must be capable of interacting with the resource owner's user-agent (typically a web browser) and capable of receiving incoming requests (via redirection) from the authorization server.

C

Client Credentials Grant Type

The client can request an access token using only its client credentials (or other supported means of authentication) when the client is requesting access to the protected resources under its control, or those of another resource owner which has been previously arranged with the authorization server (the method of which is beyond the scope of this specification).

The client credentials grant type MUST only be used by confidential clients.

I

Implicit Grant Type

The implicit grant type is used to obtain access tokens (it does not support the issuance of refresh tokens) and is optimized for public clients known to operate a particular redirection URI. These clients are typically implemented in a browser using a scripting language such as Java Script.

R

Refresh Token

Refresh tokens are credentials used to obtain access tokens. Refresh tokens are issued to the client by the authorization server and are used to obtain a new access token when the current access token becomes invalid or expires, or to obtain additional access tokens with identical or narrower scope (access tokens may have a shorter lifetime and fewer permissions than authorized by the resource owner). Issuing a refresh token is optional at the discretion of the authorization server. If the authorization server issues a refresh token, it is included when issuing an access token.

A refresh token is a string representing the authorization granted to the client by the resource owner. The string is usually opaque to the client. The token denotes an identifier used to retrieve the authorization information. Unlike access tokens, refresh tokens are intended for use only with authorization servers and are never sent to resource servers.

Resource Owner Credentials Grant Type

The resource owner password credentials grant type is suitable in cases where the resource owner has a trust relationship with the client, such as the device operating system or a highly privileged application. The authorization server should take special care when enabling this grant type, and only allow it when other flows are not viable.

The grant type is suitable for clients capable of obtaining the resource owner's credentials (user name and password, typically using an interactive form). It is also used to migrate existing clients using direct authentication schemes such as HTTP Basic or Digest authentication to OAuth by converting the stored credentials to an access token.

INDEX