Managed Access Gateway

HII Request Management Guide

(For Administrators)

HII Version
Exostar, LLC
February 14, 2012

Table of Contents

Purpose

This guide has been created for the designated Organization and Application Administrators. This guide will provide you information on the administrative tasks that you need to perform complete subscription requests for users within your organization to HII SCP and HII Information Manager. You can access MAG by logging on to: https://portalvs.exostar.com.

NOTE: This guide does not include information on managing users. Please refer to the User Management Guide for information related to processing all user management requests. This guide will provide you information on all the tasks under the Registration Requests tab that are performed by the Organization and Application administrators.

Important URLs:

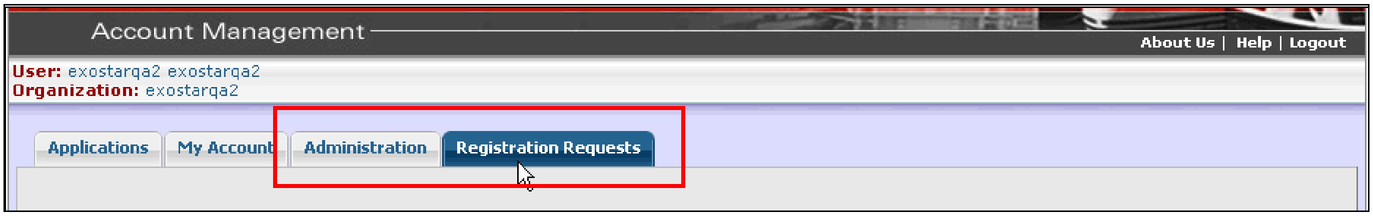
- MAG information: http://myexostar.com/myexostarAll.aspx?id=550
  - User Guides: http://myexostar.com/myexostarAll.aspx?id=1026
  - Administration Guides: http://myexostar.com/myexostarAll.aspx?id=1024
- FIS Information: http://myexostar.com/myexostarAll.aspx?id=534
  - FIS Administration Guide: http://myexostar.com/WorkArea/showcontent.aspx?id=900

Overview

An organization account for Exostar MAG requires that two types of administrators are created:

1. Organization Administrators; and
2. Application Administrators

Organization Administrators are individuals who are designated to perform administrative activities on behalf of their organization (in addition to administering their own accounts as regular users). Upon successful login, the Exostar MAG will automatically recognize your designation as an Organization Administrator, and your view of the dashboard will include the *'Administration'* Tab and 'Registration Requests' tab in addition to the general *'Applications'* and *'My Account'* tabs.

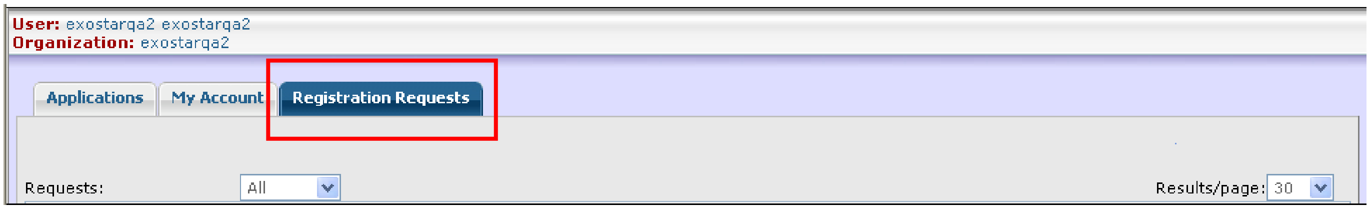


User: exostarqa2 exostarqa2
Organization: exostarqa2

Application Administrators are individuals of an organization who are designated within MAG to perform administrative activities for an application. An Application Administrator has the ability to perform the following functions:

- Authorize a user's request to access an application.
- Authorize user for FIS (digital certificates)
- Revoke User's Digital Certificates (FIS-issued only)

Upon successful login, the system will automatically recognize your designation as an Application Administrator, and your view of the dashboard will include the *'Registration Requests'* tab in addition to the general *'Applications'* and *'My Account'* tabs.


User: exostarqa2 exostarqa2
Organization: exostarqa2

Requests: All
Results/page: 30

NOTE: For some organizations, an organization administrator may also perform application administrator functions. These administrators will see all the tabs and sub-tabs that are individually available to the organization and application administrators.

This guide is divided into three chapters as follows:

- Organization Administrator tasks;
- Application Administrator tasks; and
- FIS administrator tasks[1]

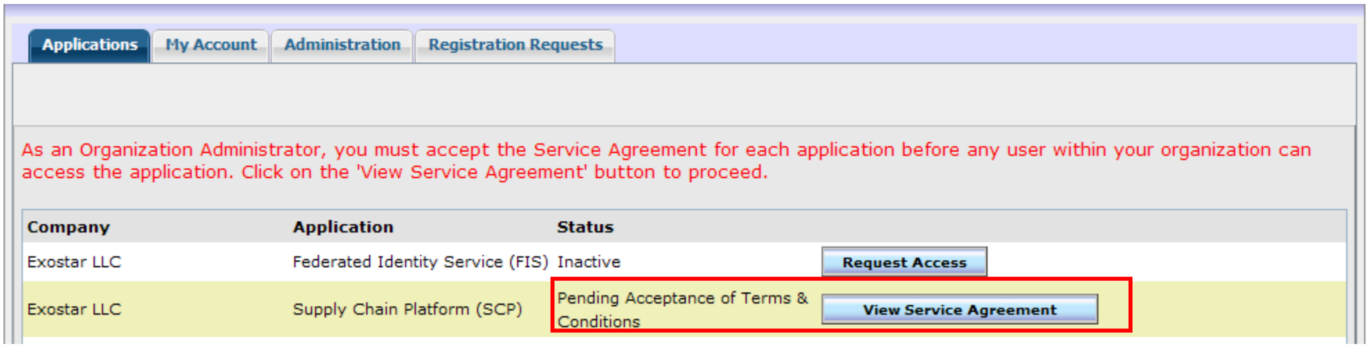
[1] FIS Administrators are application administrators who perform specific tasks to authorize users to receive digital certificates.

Organization Administrator Tasks

Accept Terms and Conditions

Once the Organization Administrator receives the approval notification from Exostar, they will need to accept the Terms & Conditions online. If the organization has multiple Organization Administrators, these terms & conditions may be accepted by any ONE Organization Administrator. To sign-off on Terms & Conditions:

1. Login to your MAG account by accessing the following URL: **https://portalvs.exostar.com**.
2. On the Applications tab, the status for the application(s) will be *'Pending Acceptance of Terms & Conditions'*.
3. Click on *'View Service Agreement'* next to the application name.



As an Organization Administrator, you must accept the Service Agreement for each application before any user within your organization can access the application. Click on the 'View Service Agreement' button to proceed.

Company	Application	Status	
Exostar LLC	Federated Identity Service (FIS)	Inactive	Request Access
Exostar LLC	Supply Chain Platform (SCP)	Pending Acceptance of Terms & Conditions	View Service Agreement

4. Click on *'Accept'* to complete the sign-off.

For detailed information on the application status, refer to section *User Application Subscription Status Information*.

Once the Organization Administrator accepts the Terms & Conditions, the application status changes to 'Active' and the application administrator is now able to approve user subscription requests. The Organization Administrator(s) will receive an Adobe PDF version of the agreement via email on completion of the acceptance.

After your organization is subscribed to an application, users within your Organization can request access to the application.

Application Administrator Tasks

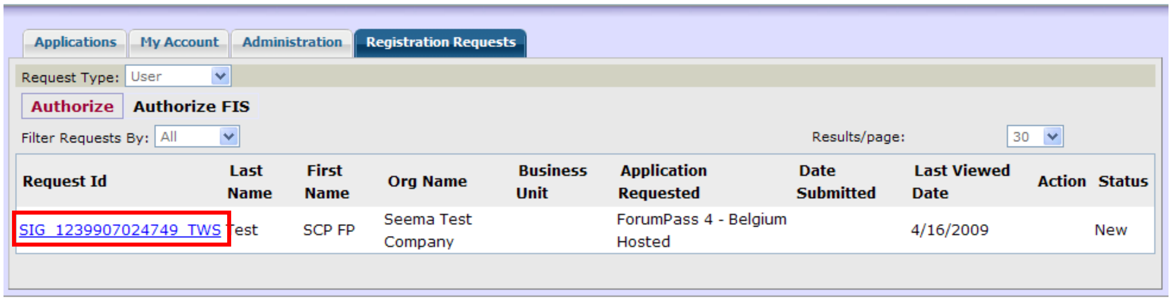
Authorize User's Access to HII SCP or Information Manager

An Application Administrator’s role is to authorize a user's access to the applications. Every user, once added to the account, must be authorized by an Application Administrator before they can access the applications.

1. On the *'Registration Requests'* tab, click on the *'Authorize'* link and you will see the list of requests awaiting your authorization. These are the user requests that have been verified by the Organization Administrator. The 'Action' column lists all the requests that need your authorization or activation.

   - You will be able to filter the requests by the status of ‘All’, 'New' and 'Pending'.
   - You will be able sort the table by clicking on the column headers.

2. Select a request that needs authorization by clicking on the Request ID as highlighted below.



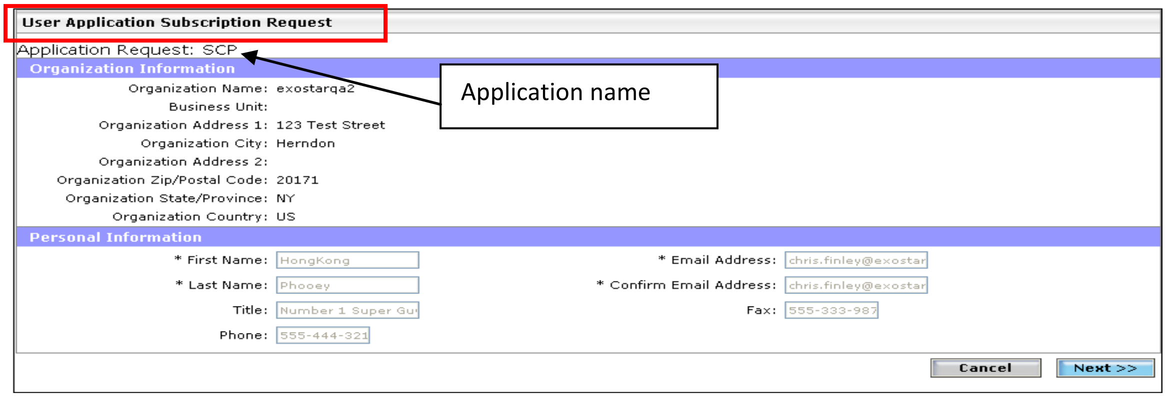
Request Type: User

Filter Requests By: All

Results/page: 30

Request Id	Last Name	First Name	Org Name	Business Unit	Application Requested	Date Submitted	Last Viewed Date	Action	Status
SIG_1239907024749_TWS	Test	SCP FP	Seema Test Company		ForumPass 4 - Belgium Hosted		4/16/2009		New

3. The *‘User Application Subscription Request’* page will be presented.
   - In this step, you will see the user's Organization information and personal information in read-only mode.



User Application Subscription Request

Application Request: SCP

Application name

Organization Information

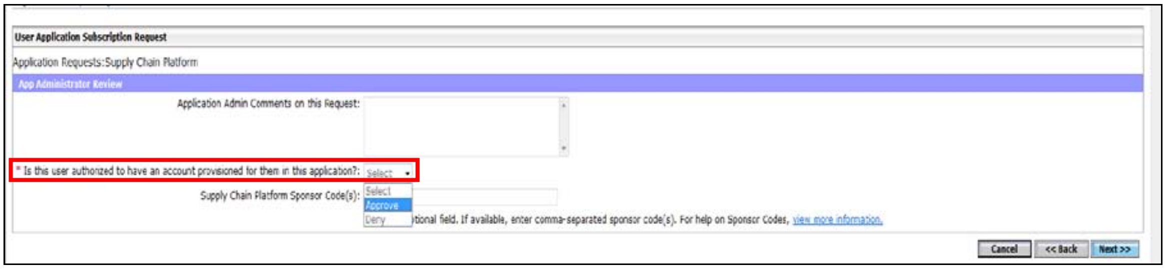
Organization Name: exostarqa2
Business Unit:
Organization Address 1: 123 Test Street
Organization City: Herndon
Organization Address 2:
Organization Zip/Postal Code: 20171
Organization State/Province: NY
Organization Country: US

Personal Information

* First Name: HongKong
* Last Name: Phooey
Title: Number 1 Super Gu
Phone: 555-444-321
* Email Address: chris.finley@exostar
* Confirm Email Address: chris.finley@exostar
Fax: 555-333-987

4. Click on *'Next'* button to go to the next step.

5. You must select to Approve or Deny the request on this page. If you opt to deny this request, you will be prompted to enter comments/reason for denial.



User Application Subscription Request

Application Requests:Supply Chain Platform

App Administrator Review

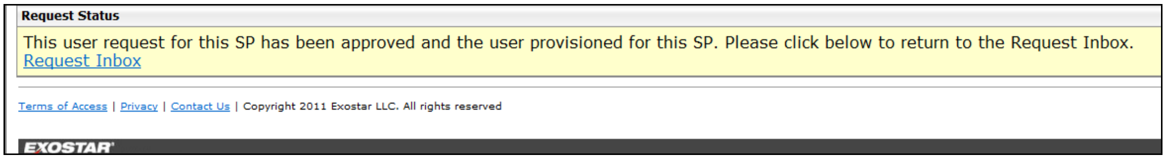
Application Admin Comments on this Request:

* Is this user authorized to have an account provisioned for them in this application?: Select

Supply Chain Platform Sponsor Code(s):

Optional field. If available, enter comma-separated sponsor code(s). For help on Sponsor Codes, view more information.

6. After you approve or deny a request, you will be presented with a confirmation message.



Request Status

This user request for this SP has been approved and the user provisioned for this SP. Please click below to return to the Request Inbox.
Request Inbox

Terms of Access | Privacy | Contact Us | Copyright 2011 Exostar LLC. All rights reserved

The request will be removed from your *'Requests Inbox'* and an email is sent to the user notifying him/her that access to SCP has been granted. The user will be able to login and access the application from the Exostar MAG.

NOTE: Once you have started to process the user's authorization request, ensure that you either complete the process or click *'Cancel'* to ensure that the request is available to other application administrators for further action.

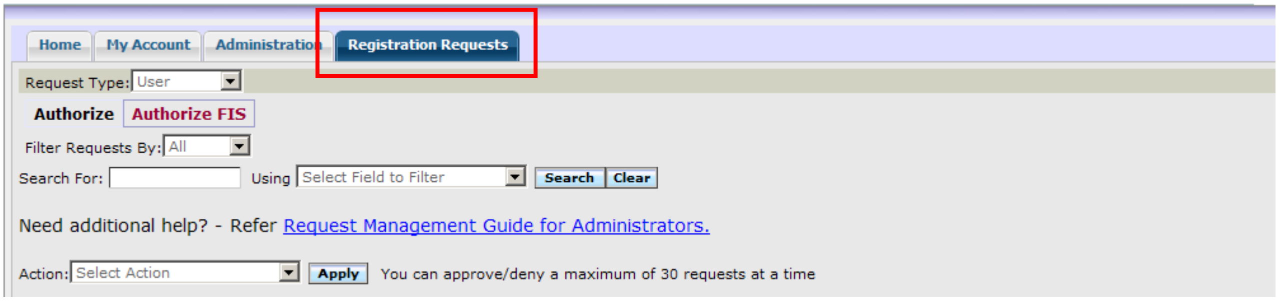
FIS Administrator Tasks

FIS Administrators (or FISA) are individuals of an organization who are designated within Exostar MAG to be Application Administrators for FIS, which issues digital certificates. A FISA performs the following functions:

- Approves all user requests for access to FIS (new digital certificates, renewing digital certificates, etc.)
- Revokes user's Digital Certificates
- Prepares employment authorization letters for users

Note that the FISA is not required to have digital certificates to perform all the roles above.

Upon successful login, the system will automatically recognize your designation as an Application Administrator, and your view of the dashboard will also include the 'Registration Requests' tab as highlighted below.



Request Type: User

Filter Requests By: All

Search For: Using Select Field to Filter

Need additional help? - Refer Request Management Guide for Administrators.

Action: Select Action

You can approve/deny a maximum of 30 requests at a time

Here is a review of the components available on this screen:

NOTE: For some organizations, an organization administrator may also perform FIS Administrator functions. These administrators will see all the tabs and sub-tabs that are individually available to the organization and application administrators.

Administration tab: You can search for users with FIS certificates via this tab. This tab also allows you to view their certificate information and if require, revoke their certificates.
Authorize sub-tab: No information available under this tab if you do not have application administrator rights for an application other than FIS.
Authorize FIS: All FIS requests are available under this tab.
Filter Requests: This filter allows you to filter out the requests in the queue based on the new or pending requests. Note that if you have any requests Pending in your queue, another FIS Administrator will not be able to access those requests. If you will not be taking action on a Pending request in your queue, open the request and release it for another FIS Administrator (if available) to take appropriate action.

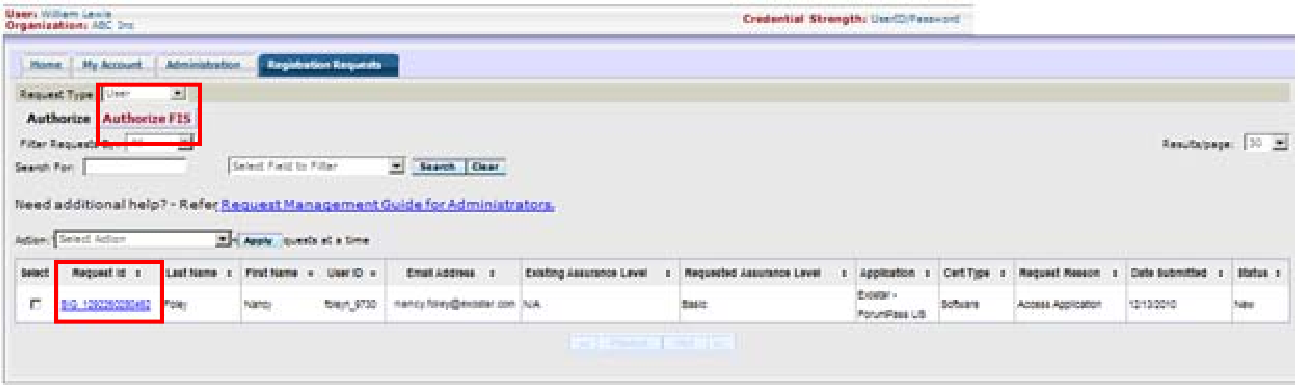
Search: You now have the option to search for a specific user's request by First Name, Last Name, UserID or the Requested Level of assurance.
Action: You are now able to approve/deny up to 30 requests at the same time. More information is provided under section Approving/Denying Multiple Requests.

Medium Level of Assurance

Users within your organization will require Medium Level of Assurance hardware certificates in order to access HII SCP and Information Manager. Note that the Medium level of Assurance Certificate requires that the user goes through the in-person proofing activity. Make sure that you follow step 5 under Authorize User's Access to FIS to approve the user's request appropriately. If you still have questions, you may contact the sponsoring organization for additional information or Exostar Customer Support.

Authorize a User's Access to FIS (new certificate request)

If you are the designated administrator for Federated Identity Service (FIS), you will see the *'Authorize FIS'* sub-tab under *'Registration Requests'*. Here, you will see the list of requests awaiting your authorization for digital certificates. These work in the same way as an Application Administrator authorizing access to other applications in MAG.


User: William Lewis
Organization: ABC Inc
Credential Strength: UserID/Password

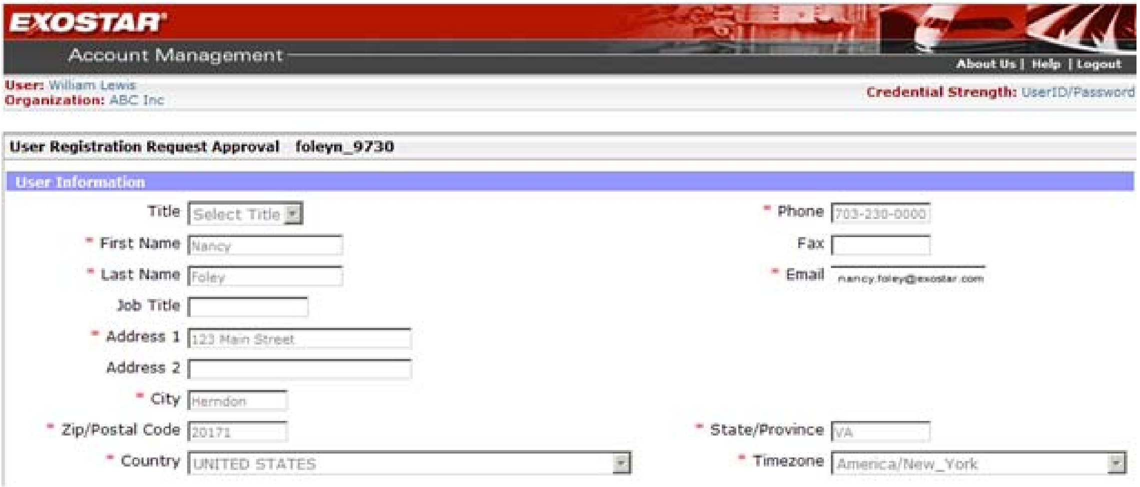
Need additional help? - Refer Request Management Guide for Administrators.

Select	Request Id	Last Name	First Name	User ID	Email Address	Existing Assurance Level	Requested Assurance Level	Application	Cert Type	Request Reason	Date Submitted	Status
□	BIG_129260280462	Foley	Nancy	foleyn_9730	nancy.foley@exostar.com	N/A	Basic	Exostar - ForumPass US	Software	Access Application	12/13/2010	New

- You will be able to filter the requests by the status of 'New' and 'Pending'.
- You will be able sort the table by clicking on the column headers.
- You will be able to search for a user based on the available search criteria.
- You will be able to approve/deny multiple requests. Refer to the Approving/Denying Multiple Requests section for details.

1. Select a request that needs authorization by clicking on the Request Id as highlighted above.
2. You will be presented with the user's approval request screen. The approval screen is divided into 5 sections:
   a. User Information
   b. Products & Services
   c. Organization Information
   d. Org Administrator Comment
   e. FIS Administrator Action

3. Review User Information: In this section, all information is in read-only mode. If any information is incorrect, you can deny the user's request with comments for the user to update the information appropriately and resubmit the request.



User: William Lewis
Organization: ABC Inc
Credential Strength: UserID/Password

User Registration Request Approval foleyn_9730

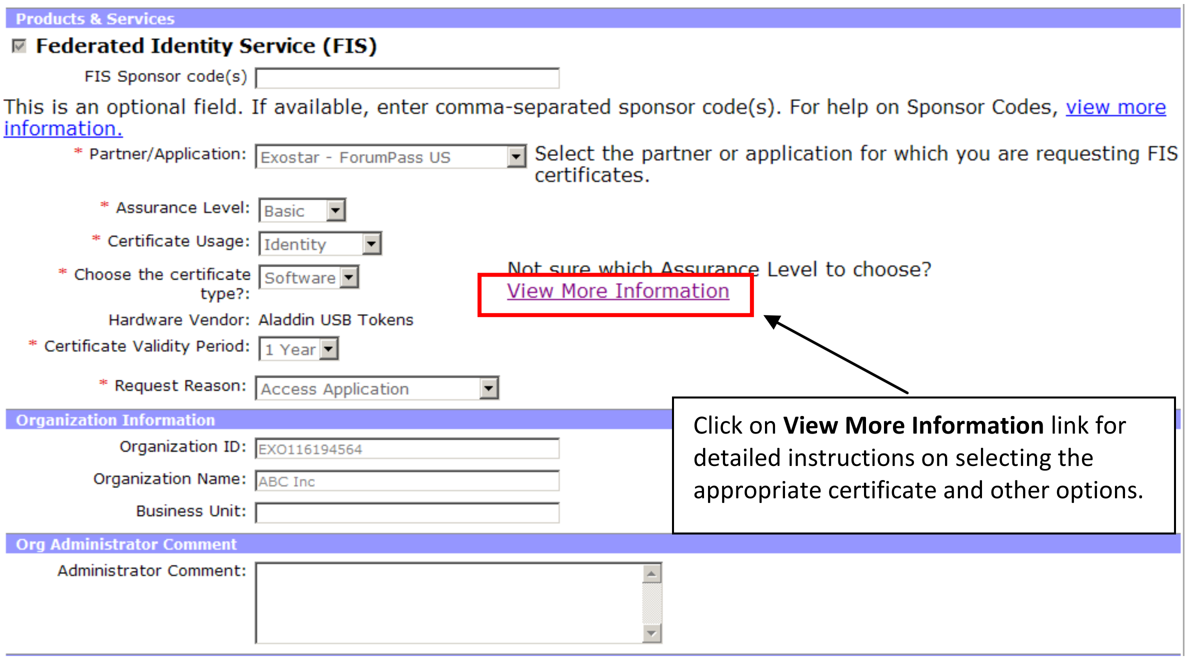
User Information

Title	Select Title	* Phone	703-230-0000
* First Name	Nancy	Fax	
* Last Name	Foley	* Email	nancy.foley@exostar.com
Job Title			
* Address 1	123 Main Street		
Address 2			
* City	Herndon		
* Zip/Postal Code	20171	* State/Province	VA
* Country	UNITED STATES	* Timezone	America/New_York

4. Review Products & Services section: In this section, you will be presented with the information that the user selected at the time of requesting access to FIS certificates.

IMPORTANT:

- Make sure you review and if required update the selected options. If you need additional information on what options to select, access the support link as highlighted on screenshot below for information.
- **Sponsor Code:** This is an optional field and if the user has not input any information and you have not received any information from a partner organization or Exostar, you can leave this field blank.
- **Partner/Application**: Review the information provided by the user and update as needed by selecting from the drop-down list.
- **Assurance Level**: The Medium option will be available only if your Organization is subscribed for MLOA (Software) or MLOA (Hardware). If the user needs an MLOA certificate and the Medium option is not available, deny the user's request and contact the Organization Administrator to complete the Upgrade to MLOA request. Refer to the Upgrade to Medium Software section for details on upgrading your organization's subscription. If your organization account needs to be upgraded to MLOA (Hardware), contact Exostar Customer Support. If the user has selected UNKNOWN as the option, you are **required** to select the assurance level other than UNKNOWN to approve the user's request.
- **Certificate Type:** The Hardware option will be available only if your organization is approved for MLOA Hardware certificates. Contact Exostar Customer Support if you need to upgrade your organization for MLOA Hardware. If the user has selected UNKNOWN as the option, you are **required** to select the certificate type other than UNKNOWN to approve the user's request.
- **Certificate Validity Period:** If the user selected Medium option for the assurance level, the user will have the option of selecting between 1 year and 3 years. Please note that for Medium certificates, the user has to go through in-person proofing irrespective of the validity period. In addition, a 3 years certificate is available at a discounted price. (For price details, contact Exostar Customer Support). If the user has selected UNKNOWN as the option, you are **required** to select the certificate validity period other than UNKNOWN to approve the user's request.
- **Request Reason:** The Unknown option is a valid option for this field.



Products & Services

☑ Federated Identity Service (FIS)

FIS Sponsor code(s)

This is an optional field. If available, enter comma-separated sponsor code(s). For help on Sponsor Codes, view more information.

* Partner/Application:	Exostar - ForumPass US	Select the partner or application for which you are requesting FIS certificates.
* Assurance Level:	Basic	
* Certificate Usage:	Identity	
* Choose the certificate type?:	Software	Not sure which Assurance Level to choose? View More Information
Hardware Vendor:	Aladdin USB Tokens	
* Certificate Validity Period:	1 Year	
* Request Reason:	Access Application	

Click on **View More Information** link for detailed instructions on selecting the appropriate certificate and other options.

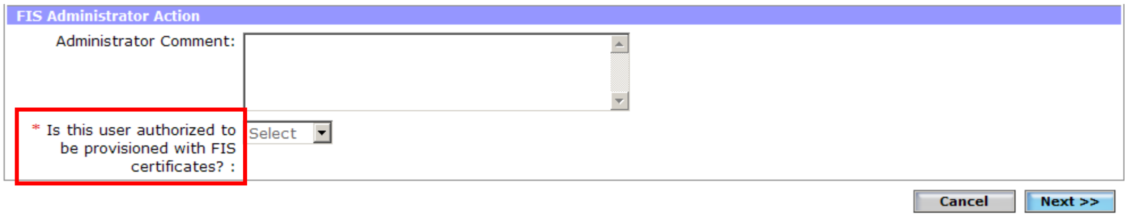
Organization Information

Organization ID:	EXO116194564
Organization Name:	ABC Inc
Business Unit:	

Org Administrator Comment

Administrator Comment:

5. Organization Information section: In this section, you can view your organization's information in read-only mode.
6. Org Administrator section: If the organization administrator entered any comments during user approval process, these will be reflected in read-only mode here.
7. FIS Administrator Action section:
    a. Administrator Comment: If you need to enter any comments, you may enter them here. These comments will be available to Exostar for any additional actions as required for MLOA certificates.
    b. Is this user provisioned…: If you select *Deny* option, you will be presented with a Deny Comments box to input your denial reason. This information will be sent to the user. Select *Approve* to approve the user's request.

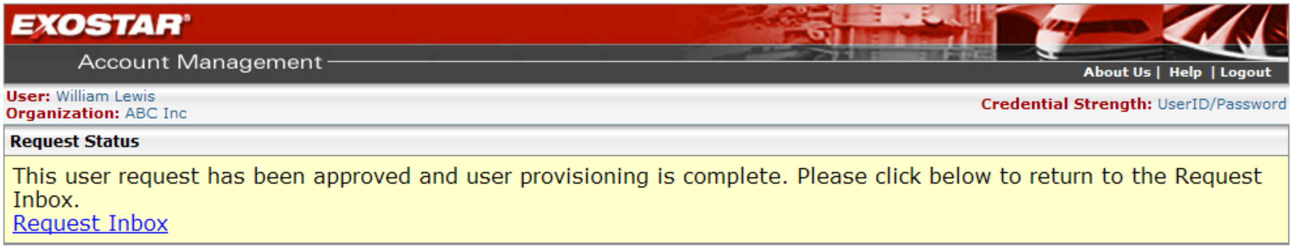


FIS Administrator Action

Administrator Comment:

* Is this user authorized to be provisioned with FIS certificates? : Select

8. Click *Next>>* complete the approval. You will receive a confirmation screen (see below).



User: William Lewis
Organization: ABC Inc
Credential Strength: UserID/Password

Request Status

This user request has been approved and user provisioning is complete. Please click below to return to the Request Inbox.
Request Inbox

Approving/Denying Multiple Requests

You can select up to 30 FIS requests to either approve or deny at a time. To be able to approve or deny, the user needs to have provided information other than UNKNOWN for the following fields:

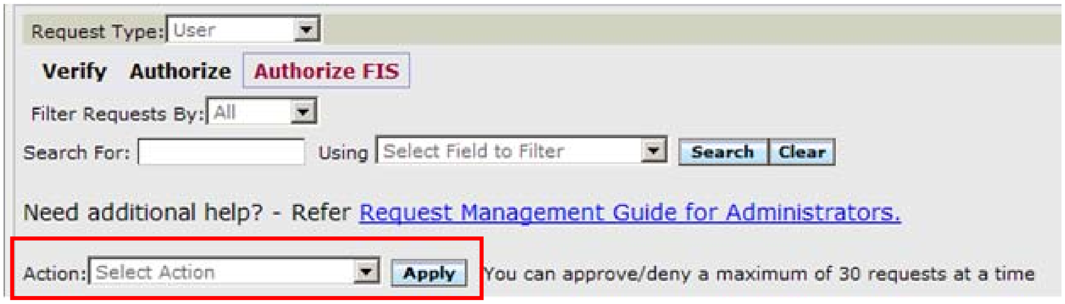
- Assurance Level

- Certificate Usage (for Basic only)
- Certificate Type
- Certificate Validity period

If any of these fields has Unknown as the response, you will be required to access the request individually to approve.

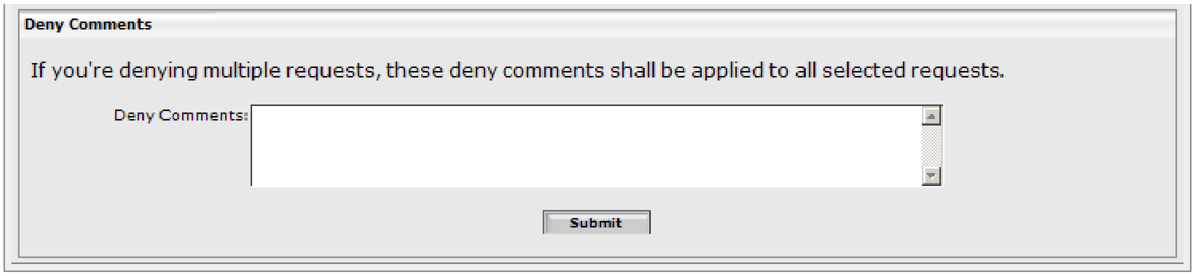
For approval:

Once you have selected the requests for approval, select the *Approve* action from the *Action* drop-down as highlighted below. Click *Apply*. All requests will be approved in a single attempt.


Request Type: User
Verify
Authorize
Authorize FIS
Filter Requests By: All
Search For:
Using Select Field to Filter
Search
Clear
Need additional help? - Refer Request Management Guide for Administrators.
Action: Select Action
Apply
You can approve/deny a maximum of 30 requests at a time

For denying requests:

Once you have selected the requests for denial, select the *Deny* action from the *Action* drop-down as highlighted above. Click *Apply*. You will be prompted to provide the denial reason.


Deny Comments
If you're denying multiple requests, these deny comments shall be applied to all selected requests.
Deny Comments:
Submit

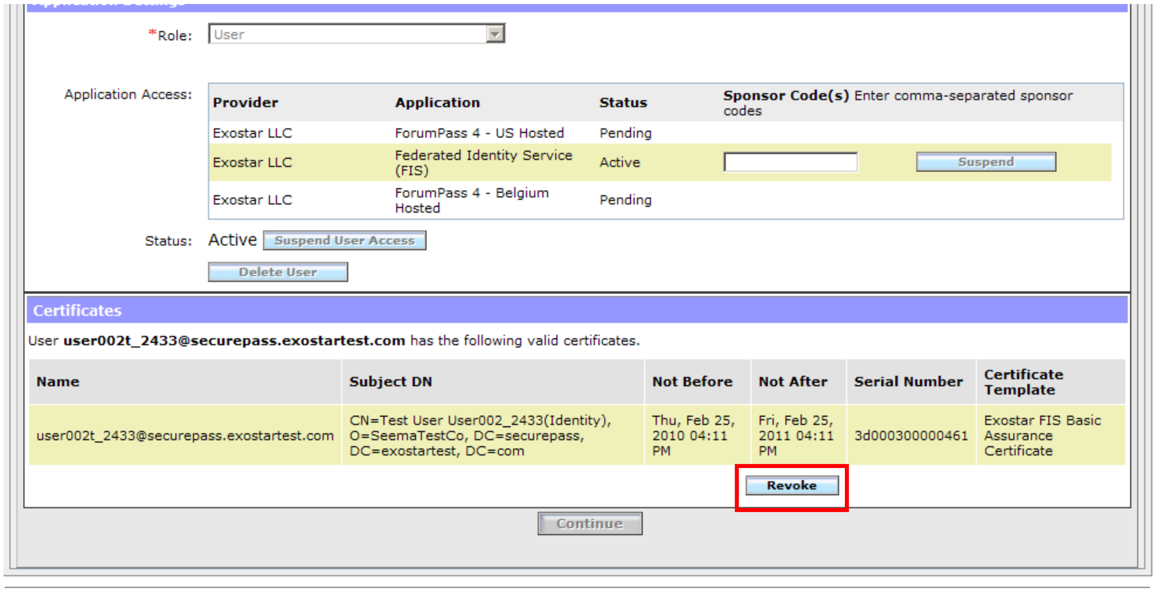
All FIS requests will receive the same denial comments as provided in the Denial comments box above.

Revoke User's Certificates

If you are the designated administrator for Federated Identity Solution (FIS), you will be able to revoke the certificates of users within your organization from the user's profile page.

NOTE: If you started a revocation process and didn't complete it, the requests will be available in the *'Registration Requests'* tab.

1. Select the *'Administration'* tab and then select the option *'View Users'*. You can search for the user that you want to revoke the certificates for by using a search option from the available drop-down.
2. Once you have found the user, click on the *'Details'* button next to the user details.
3. The user's profile will be presented. Scroll to the bottom of the profile screen:



*Role: User

Application Access:

Provider	Application	Status	Sponsor Code(s) Enter comma-separated sponsor codes
Exostar LLC	ForumPass 4 - US Hosted	Pending	
Exostar LLC	Federated Identity Service (FIS)	Active	Suspend
Exostar LLC	ForumPass 4 - Belgium Hosted	Pending	

Status: Active Suspend User Access

Delete User

Certificates

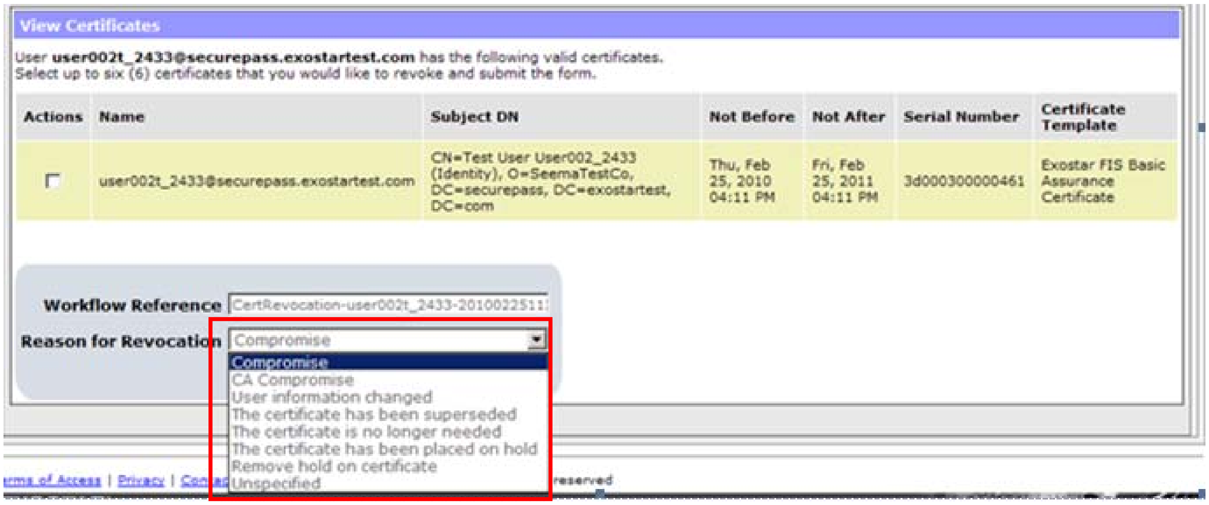
User **user002t_2433@securepass.exostartest.com** has the following valid certificates.

Name	Subject DN	Not Before	Not After	Serial Number	Certificate Template
user002t_2433@securepass.exostartest.com	CN=Test User User002_2433(Identity), O=SeemaTestCo, DC=securepass, DC=exostartest, DC=com	Thu, Feb 25, 2010 04:11 PM	Fri, Feb 25, 2011 04:11 PM	3d000300000461	Exostar FIS Basic Assurance Certificate

4. Click on the *'Revoke'* button as highlighted above.

IMPORTANT: This action will revoke all certificates for the user.

5. Select a request that needs revocation and click on *'Process Request'* to view details and revoke the request.



View Certificates

User **user002t_2433@securepass.exostartest.com** has the following valid certificates.
Select up to six (6) certificates that you would like to revoke and submit the form.

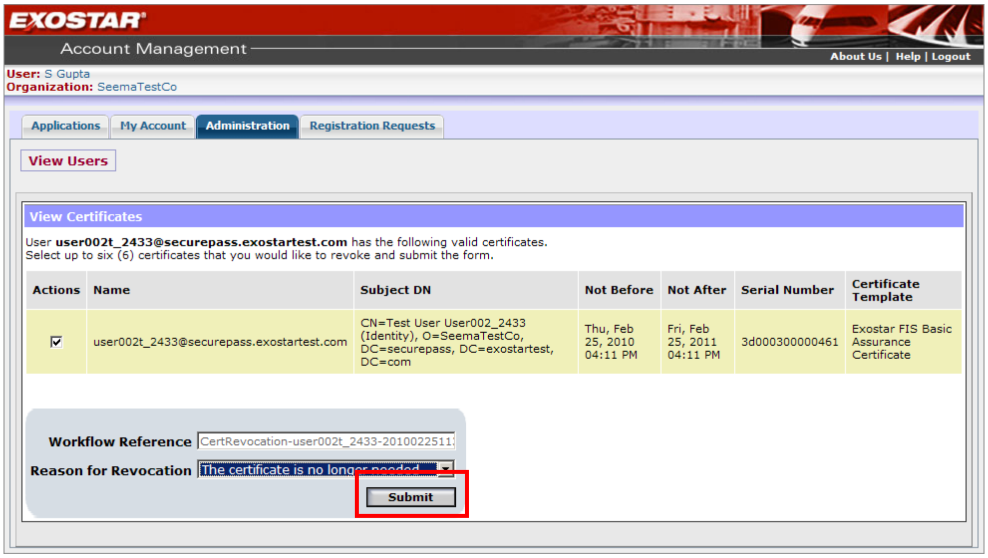
Actions	Name	Subject DN	Not Before	Not After	Serial Number	Certificate Template
☐	user002t_2433@securepass.exostartest.com	CN=Test User User002_2433 (Identity), O=SeemaTestCo, DC=securepass, DC=exostartest, DC=com	Thu, Feb 25, 2010 04:11 PM	Fri, Feb 25, 2011 04:11 PM	3d000300000461	Exostar FIS Basic Assurance Certificate

Workflow Reference CertRevocation-user002t_2433-2010022511

Reason for Revocation Compromise

Compromise
CA Compromise
User information changed
The certificate has been superseded
The certificate is no longer needed
The certificate has been placed on hold
Remove hold on certificate
Unspecified
rms of Access | Privacy | Con
reserved

6. Select the certificates by clicking on the check box against each certificate.
7. From the drop-down list of Reason for Revocation (as highlighted above), select an appropriate reason for revoking all the certificates.



User: S Gupta
Organization: SeemaTestCo

View Certificates

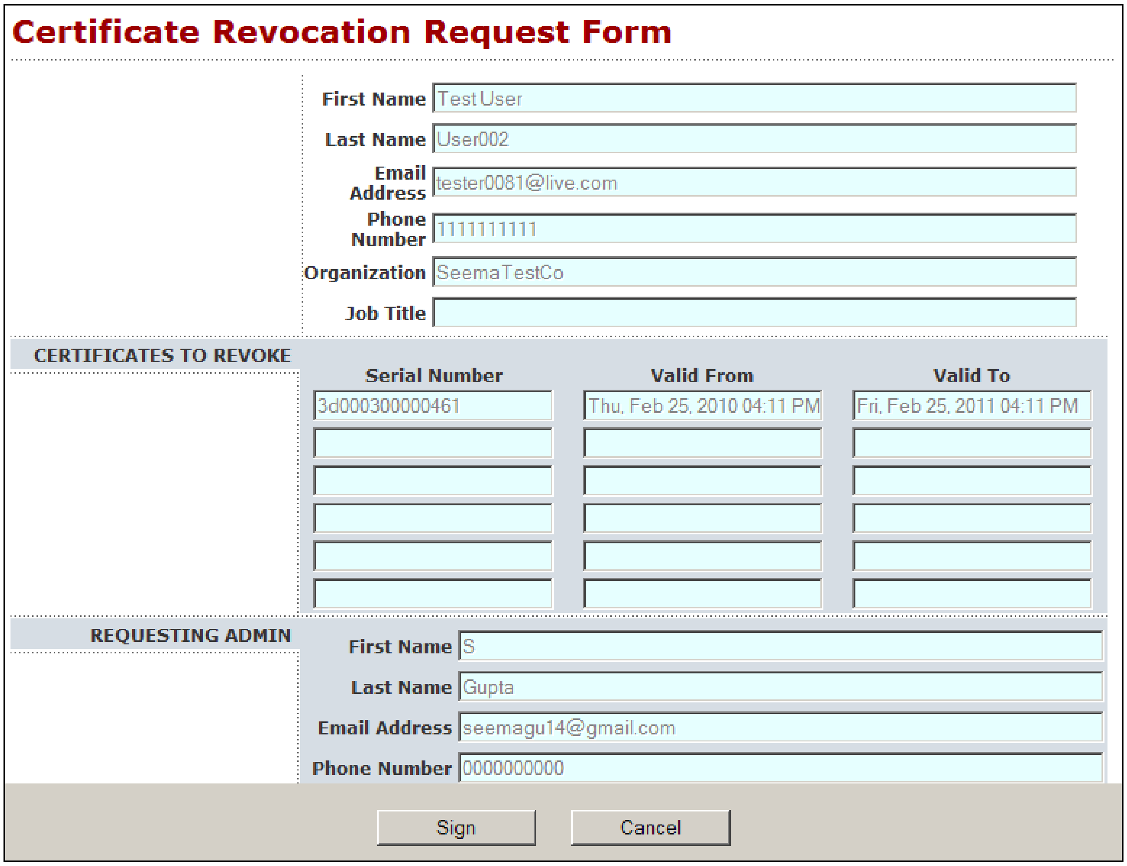
User **user002t_2433@securepass.exostartest.com** has the following valid certificates.
Select up to six (6) certificates that you would like to revoke and submit the form.

Actions	Name	Subject DN	Not Before	Not After	Serial Number	Certificate Template
☑	user002t_2433@securepass.exostartest.com	CN=Test User User002_2433 (Identity), O=SeemaTestCo, DC=securepass, DC=exostartest, DC=com	Thu, Feb 25, 2010 04:11 PM	Fri, Feb 25, 2011 04:11 PM	3d000300000461	Exostar FIS Basic Assurance Certificate

Workflow Reference CertRevocation-user002t_2433-2010022511

Reason for Revocation The certificate is no longer needed

8. Click on *'Submit'*. You will be presented with the confirmation screen.



Certificate Revocation Request Form

First Name	Test User
Last Name	User002
Email Address	tester0081@live.com
Phone Number	1111111111
Organization	SeemaTestCo
Job Title	

CERTIFICATES TO REVOKE

Serial Number	Valid From	Valid To
3d000300000461	Thu, Feb 25, 2010 04:11 PM	Fri, Feb 25, 2011 04:11 PM

REQUESTING ADMIN

First Name	S
Last Name	Gupta
Email Address	seemagu14@gmail.com
Phone Number	0000000000

9. Click on *'Sign'* to complete the revocation process.

Once a user's certificates are revoked, the user will not be able to use those certificates to login and will need new certificates.