SCM6 Institutional Administrator
Dashboard User Guide

Version 6.0
Last Updated: January 2019

Confidential
and
Proprietary

DO NOT DISTRIBUTE

TABLE OF CONTENTS

1. INTRODUCTION

The institutional administrator dashboard allows librarians and other authorized personnel access to information about their institution's account with the ability to edit a portion of the details, if the publisher allows it. This document explains how the dashboard works from a general sense, but your settings may be different depending on which features the publisher has elected to show and utilize.

1.1 SIGN IN

Your publisher will provide you with the URL and sign in credentials to access the institutional dashboard.

Your publisher may have single sign-on enabled, meaning you do not have to log into the institutional dashboard separately. If your publisher does not have this feature enabled, you must log into the institutional dashboard separately from your website. To do so, enter your Username and Password into the boxes provided and click the "Sign In" button.

1.2 NAVIGATION

Once you are signed in, the name of your institution appears in the masthead. Additionally, you will see your administrator name in the top right hand corner next to a "Logout" button. If you want to sign out of the institutional dashboard, click the "Logout" button.

The structure of the institutional dashboard is fairly simple. Various information pertaining to your institution is housed in 5 separate tabs: Institutional Summary, Access Options, COUNTER Release 4 Reports, COUNTER Release 5 Reports, and Other Reports (if applicable for publisher). See the sections below for details on the information these tabs contain.
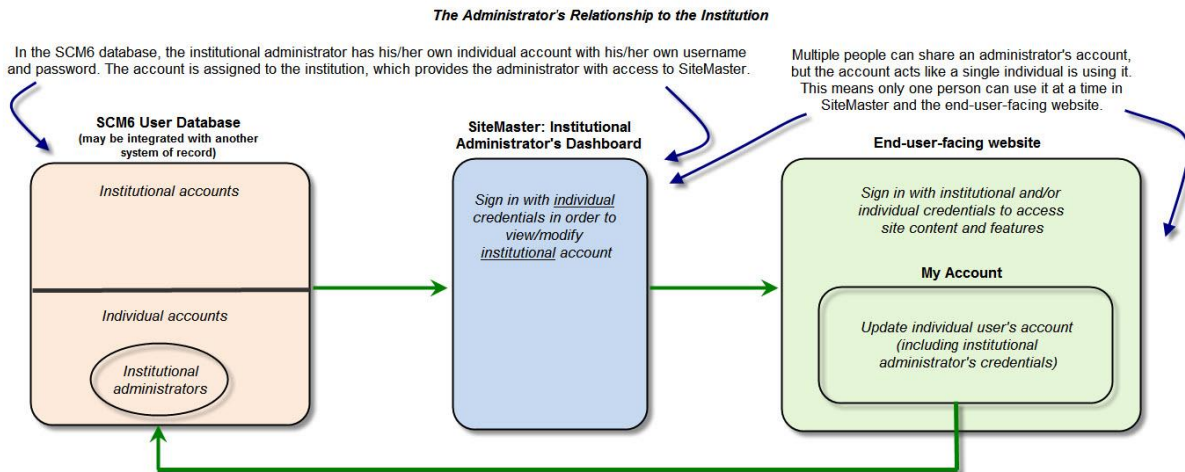
2. INSTITUTIONAL SUMMARY TAB

2.1 GENERAL INFORMATION

This section of the Institutional Summary is a snapshot of the basic institutional details. If the publisher has elected to allow institutional administrators the ability to edit their institution's general information, then an Edit button will appear. If this section appears as read-only, you must contact your publisher to change the information.

Clicking on the Edit button will take you to a page where all of the basic institutional account information can be edited with the exception of the Vendor ID. Once your changes are made, click the "Save Changes" button and you will be returned to the Institutional Summary where all of the General Information will be updated per the changes that you made. Clicking "Cancel" will return you to the Institutional Summary and none of your changes will be saved.

2.2 ADMINISTRATIVE CONTACT

This section lists the Administrative Contact details for the institutional administrator. You must contact your publisher to change this information. The diagram below further details the relationship between the administrator and the institution:

The Administrator's Relationship to the Institution

In the SCM6 database, the institutional administrator has his/her own individual account with his/her own username and password. The account is assigned to the institution, which provides the administrator with access to SiteMaster.

Multiple people can share an administrator's account, but the account acts like a single individual is using it. This means only one person can use it at a time in SiteMaster and the end-user-facing website.

SCM6 User Database
(may be integrated with another system of record)

Institutional accounts

Individual accounts

Institutional administrators

SiteMaster: Institutional Administrator's Dashboard

Sign in with individual credentials in order to view/modify institutional account

End-user-facing website

Sign in with institutional and/or individual credentials to access site content and features

My Account

Update individual user's account (including institutional administrator's credentials)

2.3 CONSORTIA INFORMATION

This section shows whether the institution is a consortium master and if it is a member of any consortia. In the context of the SCM6 platform, a consortium is a group of related institutions whereby the members can inherit the master's subscriptions and concurrency. Consortium relationships are set up by your publisher and include a master account that contains the subscriptions(s) that are passed down to member accounts. Once the relationship has been established between master and member by your publisher, the member institution will share the subscriptions loaded into the master account. A consortium master account can have multiple member accounts and levels of members, and a consortium member account can belong to multiple consortia.

If your institution is designated as the consortium master, you are able to view all member accounts within all layers below you on the consortia tree. To do this, select the link "View Members" and click on the name of the member institution you want to view. This will take you to the institutional dashboard for that institution. You can always return to the master account dashboard by clicking on the "My Institutional Summary" link.

If your institution is a consortium member of one or more consortia, you are only able to view the names of your consortium master(s) in the Consortia Information section of your institutional dashboard, but you cannot access the institutional dashboard for your consortium master(s).

2.4 INSTITUTIONAL LOGO

This area of the Institutional Summary Tab will display an institution's logo. It may also provide functionality to add or remove an institutional logo, depending on the publisher's preferred configurations.

The institutional logo that appears in this section may be displayed on the publisher's website (likely the homepage and possibly other pages) when a user is authenticated at that institution.

The publisher may provide Institutional Administrators with the ability to have a read-only view of the logo, or may also provide the ability to add/replace or remove a logo.

If a publisher has enabled the Institutional Administrators to edit their institutional logo, as opposed to having a read-only view, you have the following options:

- Add or replace an image:
    1. Hit the "Edit" button to add an image or replace an existing image (when "replacing" an image, you may want to remove the initial image first.)
    2. When you click the "Edit" button, a modal will appear asking you to browse to the image on your computer and upload it.
- Remove an image:
    1. If you prefer to have no institutional logo appear for that institution, simply hit the red "x" to delete the image. NOTE: There will **not** be a warning or a confirmation when you hit the red "x" – the image will be immediately removed and this action cannot be undone.

An institution can have one logo.

- The vendorID must be used as the filename.
    1. For example, for an institution with VendorID 000123456, the image filename should be **000123456.jpg**.
- Size restrictions are 300 pixels wide by 100 pixels high.
- Acceptable file types are JPG, PNG and GIF.

2.5 ACCESS OPTIONS

This section lists the Access Options that have been configured for your institution. Clicking on "Manage Access Options" will take you to the Access Options Tab. See the Access Options Tab section for more information.

2.6 INSTITUTIONAL LINKS

This section lists any important external links your publisher has designated. If this section does not appear, your publisher has chosen not to include any links.

2.7 CURRENT SUBSCRIPTIONS

This section lists the institution's current subscriptions and their expiration dates and is not editable. Please contact your publisher if you need to renew or cancel your subscription.

3. ACCESS OPTIONS TAB

The access options for institutional accounts are as follows:

- Master Username/Password Login
- Referring URL
- IP Address
- Athens ID
- Shibboleth Information
- OpenURL (outbound)

The publisher may allow institutional administrators to modify the values for some of these settings. If they have chosen to not allow institutional administrators to edit these fields, they will be read-only and you must contact your publisher to change the information.

3.1 MASTER USERNAME/PASSWORD LOGIN

3.1.1 MASTER USERNAME/PASSWORD DEFINITION

The Master (or shared) Username and Password are the login credentials that an end-user inputs to access an Institutional Account on the front-end website.

3.1.1.1 EMBEDDED LOGIN

SCM6 supports embedded login to satisfy customers who do not wish to use IP authentication, but do not want their customers to have to enter a master username/password each time they sign in. If this feature is enabled on a site, a Master UN/PW needs to be configured in SiteMaster. Then, the URL will need to be created based on the following syntax: http://[siteURL]/index.aspx?username=[USERNAME]&password=[PASSWORD]

3.1.2 ADDING/EDITING/DELETING MASTER USERNAME/PASSWORD

If the publisher has chosen to allow institutional administrators to modify the Master Username/Password, then the following fields can be added by clicking on the "Add Master UN/PW" button:

- Username (four characters minimum, *not* case sensitive)
- Password (must be at least six characters long and must contain: at least one lowercase letter, at least one uppercase letter, and at least one digit)
- Confirm password

If a Master Username/Password already exists for the account, you can click on the "Edit Username" or "Edit Password" button to modify the credentials. Once you have made your changes, click "Save." If you want to remove the Master Username/Password from the institutional account, you may delete it by clicking on the red X icon.

Only one Master Username/Password can be used for an institutional account.

3.2 REFERRING URL

3.2.1 REFERRING URL DEFINITION

Referring URL, sometimes known as Referrer Based Access Control (RBAC) is the URL from which the end-user enters the website and automatically becomes authenticated by the institution for which the referring URL was added.

For example, if an institutional account for the University of Virginia is set up with a Referring URL of www.virginia.edu and a link to the publisher's front-end website is placed on the actual URL for www.virginia.edu

(or one of its sub-domains), a user clicking on the link will be taken to the front-end website and be automatically authenticated by the University of Virginia's institutional subscription.

Though an institution can configure an unlimited number of referring URLs, they must unique across institutions; validation allows for forward-slash variances between institutions. For example, Institution A may use www.silverchair.com/jobs whereas Institution B may use www.silverchair.com/marketing.

3.2.2   ADDING/EDITING/DELETING REFERRING URL

To add a Referring URL, click the "Add a New URL" button which will produce a dialog where the referring URL can be entered. Once entered, click the "Save" button. The URL should now appear in the list. Multiple referring URLs can be entered for an institution, but they must be unique across all institutions for your publisher.

To edit an existing URL, simply click the "Edit" button and modify the URL as you wish. To delete an existing URL, click the red X icon.

3.3 IP RANGES

3.3.1   IP RANGE FORMATS

IP ranges may be associated with institutional accounts. The following formats are accepted:

xxx.xxx.xxx.xxx (single IP address)

xxx.xxx.xxx.xxx-yyy (a few contiguous IP addresses)

xxx.xxx.xxx.* (a single class C range)

xxx.xxx.. (a single class B range)

xxx.xxx.xxx-yyy.* (multiple contiguous class C ranges)

xxx.xxx-yyy.. (multiple contiguous class B ranges)

The same IP address cannot be assigned to multiple accounts, nor any overlapping of IP addresses within a range. An account can have multiple IP addresses or IP ranges, and there is no limit to the number of ranges that can be associated with an institutional account. If the account that you are viewing has country-wide access, then IP ranges will not be editable.

3.3.2   SINGLE IP INPUT

When adding a single IP address or range, click the "Add a New IP" button. Enter the address or range using one of the formats listed above and click Save. Once entered you can edit the IP range by clicking the "Edit" button or delete it by clicking on the red X icon.

3.3.3   BULK IP UPLOAD

If you have multiple IP addresses or ranges that you would like to add in bulk, you can use the bulk IP upload functionality. First, download your current list of by clicking on the "Download Current IP File." This will open a

.CSV file that contains either a list of your already configured IP addresses/ranges or a blank template that contains a header column.

Add, modify, or delete the IP addresses so that the list contains all of the IP addresses that you want included. Save the file to your computer as a .CSV file. Click on the "Upload Bulk IP" button. Click the "Browse" button and navigate to where you saved the .CSV file. Click "Upload File". A confirmation message will appear for you to confirm that you want to replace all of the existing IP addresses with those that are on your file. **PLEASE NOTE: The IP addresses or ranges that are uploaded using the bulk IP upload functionality will *replace* the entire list of those already configured for an institution. So your file should include all IPs that need to exist for that institution.**

If the IP addresses in your file are valid, they will be added to the screen. If they are invalid, you will receive an error message. Possible reasons an IP address or range is invalid are as follows:

- IP address or range is a Private IP address, which are not allowed
- IP address already exists on another institution
- IP address is in an invalid format

3.3.4 SETTING UP TRUSTED PROXIES

If your publisher has Institutional IP Proxy Whitelisting enabled, you will either be able to have a read-only view of whether an IP address is for a trusted proxy, or a view along with the ability to designate an IP as belonging to a trusted proxy.

In order to check the Proxy checkbox to add the IP of a trusted proxy server used by an institution, click on "Manage Access Options" from the Institutional Summary Dashboard. Click the "Add a New IP" button check the Proxy check box under the entered IP Address. Press "Save Changes" to save your selection. This checkbox can also be edited for IP address(es) previously specified for this account.

When traffic comes from an IP address identified as a trusted proxy for the institution, then (and only then) we will examine the X-Forwarded-For header fields in the request header. These header fields will be trusted will be trusted and checked against the known IP addresses for that institution. This allows institutional access to again be compared against the true IP addresses belonging to the institution via X-Forwarded-For headers, but only when those X-Forwarded-For headers are known to be from a trusted source.

3.4 SHIBBOLETH INFORMATION

Shibboleth Information will be available for Institutional Administrators to see and possibly edit within the Access Options page, if the publisher has at least one federation set up. If the publisher has not set up any federations, a message will display, saying that Shibboleth access is not available at this time.

If your publisher has federations set up, and your institution is a member of one of those federations, you will either be able to have a read-only view of your Shibboleth information, or a view along with the ability to add, edit and remove your own Shibboleth information. If you do not see the edit and remove buttons, you will need to contact your publisher to have them add, edit, or remove your Shibboleth information.

Figure: Shibboleth Information is displayed, along with Edit and Remove buttons

Adding or Editing Shibboleth Information

To add or edit your institution's Shibboleth Information, simply click the "edit" button. Within the modal box for editing are instructions on which fields are required, the format, and an example. Make sure to remove any additional spaces at the end of each field if you are copying/pasting. Any unintentional spaces will prevent the Institution from having Shibboleth access. If you do not enter your Shibboleth information completely or accurately, your Shibboleth access will not work properly. Only the federations that your publisher has set up will be available within the Federation drop-down. You can only select a federation that your publisher has set up. Required fields are Federation, Shibboleth Entity ID, and at least one of the three SSO attributes (eduPersonScopedAffiliation, eduPersonAffiliation, eduPersonEntitlement).

Note: For institutions using OpenAthens as the method of access, the Federation is either UK Access Management Federation **OR** OpenAthens Federation, the Shibboleth Entity ID is the OAFed Entity ID, and the eduPersonScopedAffiliation is the Federation Scope with a 'member@' prefix appended to the value.

Removing Shibboleth Information

When the red "x" is clicked to remove all of your Shibboleth information, you will a popup asking you to confirm your decision to remove everything in Shibboleth Information. This action cannot be undone. You can simply close the popup if you do not wish to remove all of your Shibboleth information.

3.5 OPENATHENS

Silverchair has set up access to Eduserv's OpenAthens via the OpenAthens Federation. To input OpenAthens access data, follow the mapping table below to input the values into the relevant Shibboleth fields that exist in SiteMaster.

Note: Due to the Silverchair migration that allows our applications to leverage the advantages of 64-bit architecture, OpenAthens Service provider software has been combined with Shibboleth. The OpenAthens federation still provides normal OpenAthens access. There is no change in OpenAthens access for institutions, but the set up process will use Shibboleth terminology. This signifies that OpenAthens information is not explicitly

present in SiteMaster, but is used in combination with Shibboleth Information. If you have any questions about OpenAthens, please consult this link: https://auth.athensams.net/list_orgs.php. Please reference that page to find the available values for OpenAthens.

Name (OpenAthens)	Name (Shibboleth)
OAFed Entity ID	Shibboleth Entity ID
Federation Scope	'member@' + 'eduPersonScopedAffiliation'
Federation	UK Access Management Federation OR OpenAthens Federation

3.6 OPENURL (OUTBOUND)

3.6.1   OPENURL (OUTBOUND) DEFINITION

OpenURL is a standardized syntax for transferring metadata describing an article or chapter. It is a way of organizing data in a URL and pointing it to a destination. When an OpenURL is configured, a link is provided in the References tab of an article or chapter that lets the end user know if the institution they are accessing has the article or chapter being cited.

3.6.2   ADDING/EDITING/DELETING OPENURL (OUTBOUND) DEFINITION

When adding an OpenURL in SiteMaster, the popup dialog contains fields for the resolver base URL, link text, and an image. You may browse your own files and upload your own image, or the default image can be used. The system will validate the uploaded image's size and dimensions. Images must have a maximum file size of 5KB and maximum dimensions of 150px wide x 30px high. As indicated above, this image will appear in an article/chapter's References section as the institutional link resolver.

The system will pass in the DOI of the article or chapter being cited at the end of the resolver base URL. Therefore, the URL must be entered exactly how it would appear in the address bar minus the DOI (for example https://resolverbaseurl/doi=).

4   COUNTER REPORTS TAB (RELASE 4 AND RELEASE 5 FORMATS)

Counting **O**nline **U**sage of **N**e**T**worked **E**lectronic **R**esources (COUNTER) Reports are a standardized way that librarians and other institutional personnel can see how products they purchase are being utilized. The COUNTER Reports tab contains the COUNTER Release 4 reports for a given institution in Excel (XLSX) format. Institutional Administrators can generate COUNTER Reports for their Institution and if they are a master consortia, relevant consortia reports.

COUNTER Release 5 reports for an institution can be accessed by selecting **COUNTER Release 5 REPORTS** tab (if enabled for the Sitemaster site). Each report is available for download in TSV format and accessible via the COUNTER SUSHI API. This file by default opens in Notepad. When opened by Excel, the Text Import Wizard is

started, and the result does not include formulas. For more information on the formatting and delivery of these reports, please go to: https://www.projectcounter.org/code-of-practice-five-sections/5-delivery-counter-reports/

The following reports are available for **COUNTER Release 5 Reports**, depending on the publisher's site and content. A change in this release is that all reports that Silverchair supports on the Silverchair Platform will appear in Sitemaster. This is a requirement from COUNTER. The report interface MUST offer all Standard Views the content provider is required to provide.

REPORT NAME	DESCRIPTION
TR Title Master Report	Provides comprehensive information about activity at the "Title" level and includes all metrics and attributes relevant to any of the "Title Standard Views" This is a flexible report that allows the user to customize columns, attributes and filters as desired.
TR_J1 Journal Requests (Excluding "OA_Gold")	Reports on usage of non-Open Access Gold journal content as "Total_Item_Requests" and "Unique_Item_Requests". The "Unique_Item_Requests" provides comparable usage across journal platform by reducing the inflationary effect that occurs when and HTML full text automatically displays and then access the PDF version. The "Total_Item_Requests" shows overall activity.
TR_J2 Journal Access Denied	Reports on "Access Denied" activity for journal content where users were denied access because simultaneous-use licences were exceeded or their institution did not have a license for the title
TR_J3 Journal Usage by Access Type	Reports on usage of journal content for all metric types broken down by "Access_Type"
TR_J4 Journal Requests by YOP (Excluding "OA_Gold")	Breaks down the usage of non-Open Access Gold journal content by year of publication, providing counts for the "Metric Types"; "Total_Item_Requests" and "Unique_Item_Requests". Provides the details necessary to analyze usage of Backfiles content or content covered by perpetual-access agreement. Note: COUNTER reports do not provide access model or perpetual access rights details.
TR_B1 Book Requests (Excluding "OA_Gold")	Reports on full text activity for non-Gold "Open Access" books as "Total_Item_Requests" and "Unique_Title_Requests". The

REPORT NAME	DESCRIPTION
	"Unique_Title_Requests" provides comparable usage across book platforms. The "Total_Item_Requests" shows overall activity; however, numbers between sites will vary significantly based on how the content is delivered (e.g. delivered as a complete book or by chapter).
TR_B2 Book Access Denied	Reports on "Access Denied" activity for books where users were denied access because simultaneous-use licences were exceeded or their institution did not have a license for the book
TR_B3 Book Usage by Access Type	Reports on book usage showing all applicable metric types broken down by "Access_Type"
PR Platform Master Report	A customizable report that summarizes activity across a provider's platforms and allows the user to apply filters and select other configuration options
PR_P1 Platform Usage	A Standard View of the Platform Master Report offering platform-level usage summarized by metric type
IR Item Master Report	A granular, customizable report showing activity at the level of the "Item" (article, chapter, media object, etc.) that allows the user to apply filters and select other configuration options
IR_A1 Journal Article Requests	Reports on journal article requests at the article level. This report is limited to content with a data type of "Journal"; section type of "Article", and metric type of "Total_Item_Requests" and "Unique_Item_Requests"
IR_M1 Multimedia Item Requests	Reports on multimedia requests at the "Item" level

The following reports are available for COUNTER Release 4 Reports, depending on the publisher's site and content. Only reports that apply to the specific publisher will appear in SiteMaster.

REPORT NAME	DESCRIPTION
Book Report 1	Number of Successful Title Requests by Month and Title
Book Report 2	Number of Successful Section Requests by Month and Title
Book Report 3	Access Denied to Content Items by Month, Title and Category
Consortia Report 1	Number of Successful Full-Text Journal Article of Book Chapter Requests by month and title
Journal Report 1	Number of Successful Full-Text Article Requests by Month and Journal
Journal Report 1a	Number of Successful Full-Text Article Request from an Archive by Month and Journal
Journal Report 2	Access Denied to Full-Text Articles by Month, Journal and Category
Journal Report 5	Number of Successful Full-Text Article Requests by Year-of-Publication (YOP) and Journal
Multimedia Report 1	Number of Successful Full Multimedia Content Unit Requests by Month and Collection
Platform Report 1	Total Searches, Results Clicks and Record Views by Month and Platform

4.6 EXCEL

Select the desired date range and click on the Update Date Range button. Once the desired date range has been selected, click on the 'Download XLSX' button of the report and the report will generate.

4.7 SUSHI

The SUSHI Version 1.6 protocol is a standard client/server web service utilizing a SOAP request/response to retrieve the XML version of a COUNTER report. Please use the following instructions to access the SUSHI Service in order to obtain COUNTER Release 4.0 reports in XML format.

You must have a SUSHI client to use the Silverchair SUSHI service. For more information, visit http://www.niso.org/workrooms/sushi/.

WSDL SUSHI Service address: http://sushi.silverchair.com/SUSHIservice.svc?wsdl

Listed below are the following parameters needed in order to generate a COUNTER Report in XML format using the SUSHI service.

Parameter	Definition
RequestorID	The UserID of the user requesting report
Email	The SiteMaster Password of the user requesting report
CustomerReferenceID	The SiteMasterID of the Institution for requested report
ReportName	COUNTER Report Name
ReleaseNumber	Current COUNTER release version supported (4)
BeginDate	The beginning of the month for the reporting period in format YYYY-MM-DD (example - 2014-01-01 for January 1, 2014)
EndDate	The end of the month for the reporting period in format YYYY-MM-DD (example - 2014-02-28 for February 28, 2014)

This information can be obtained from clicking on the **How do I use SUSHI to generate COUNTER Reports?** link at the bottom of the COUNTER Reports tab.

For COUNTER 5 Release Reports, The SUSHI REST API for COUNTER Release 5 retrieves the JSON version of a COUNTER report. You may use the instructions accessible via clicking the link 'How do I use SUSHI to generate COUNTER Reports?' on the COUNTER Release 5 reports tab. This will allow users to access the SUSHI REST API in order to obtain COUNTER Release 5 reports in JSON format.

Please see the COUNTER SUSHI specification for interactive assistance in creating REST API request URLs.

5   OTHER REPORTS TAB

The Others Reports tab is a configurable option for publishers to turn on so that institutional administrators can access additional non COUNTER Reports.

6   ABUSE LOG TAB

If your site has the abuse monitoring feature enabled and activity has been traced to an IP address associated with your institutional account, you will see the Abuse Log tab in the institutional admin dashboard. On this page, you will see a listing of the IP addresses associated with your institution that have hit the threshold and their current status. Here is a description of the various statuses:

- **Suspended:** A user coming from the IP address indicated has exceeded the pre-defined threshold and can no longer access paid content or the entire site (depending on the publisher's preference)
- **Pending:** An institutional administrator for the IP address in question has submitted a reinstatement request
- **Reinstated:** The publisher has reinstated the IP address and it is no longer blocked from accessing paid content or the site.

If the IP address is associated with your institution and has a status of "Suspended," you will be able to click a link to request reinstatement. The reinstatement request is sent to the publisher where they can choose to accept the request and reinstate the IP address or they can deny the request, which will leave it in a "Suspended" status.