Security Administration Form eRepository (SAFE) User's Guide

Version 3.4.3

Document Details

Document properties

Name	Detail
Author	Sean Christian & Latonya Sneed
Developer	Sean Christian, Principle Developer
Document Date	02/21/2023
Version	3.4.3
Source	Atos
Version	Final

Table of Contents

General Section

Introduction

What is SAFE?

The Security Administration Forms eRepository is a web based application that allows users to create and submit requests for powerful user access. Powerful User access enables an individual to take actions which may affect computing systems, network communication, or the accounts, files, data, or process of other users.

Approval requests will be automatically sent to the requestor's manager, who will then be notified by email. Managers can approve, reject and review requests for access; as well as generate detailed reports. To ensure compliance, a powerful users request can be tracked throughout its entire life cycle using SAFE.

Who should use SAFE?

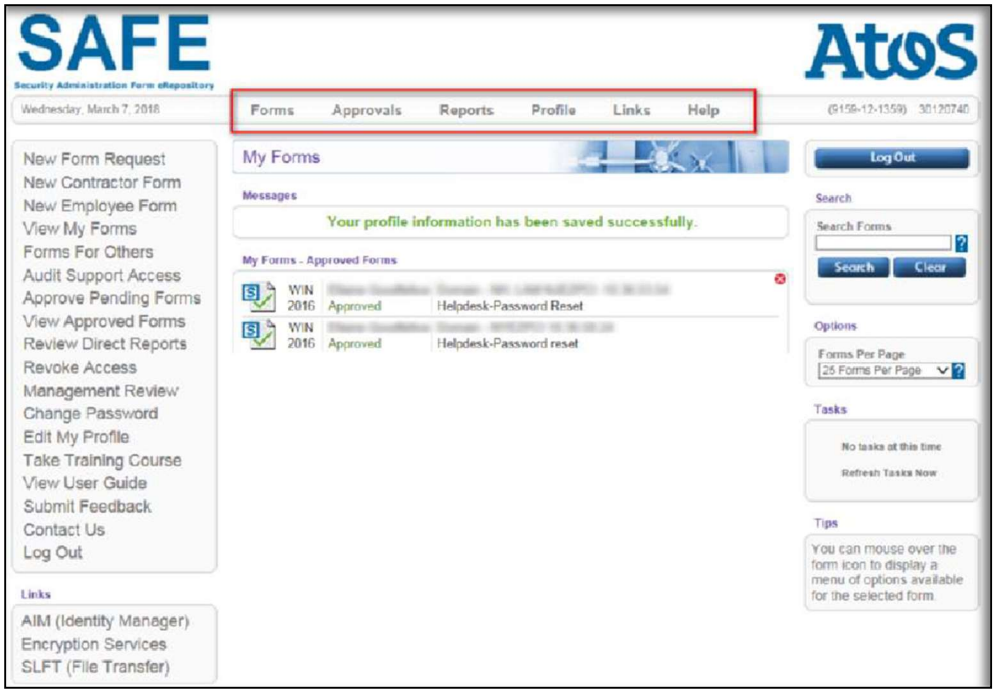
Anyone who has powerful user access should use SAFE. This application enables users to request access for themselves and allows managers to request access for their employees.

What are the Benefits?

- Requests can be tracked and monitored
- Managers can generate reports to audit employees' access
- Easy to use
- Web interface can be accessed globally

Understanding the Interface

Each section of SAFE has a floating menu. To see the menus for each section, mouse over each tab to see which options are available.



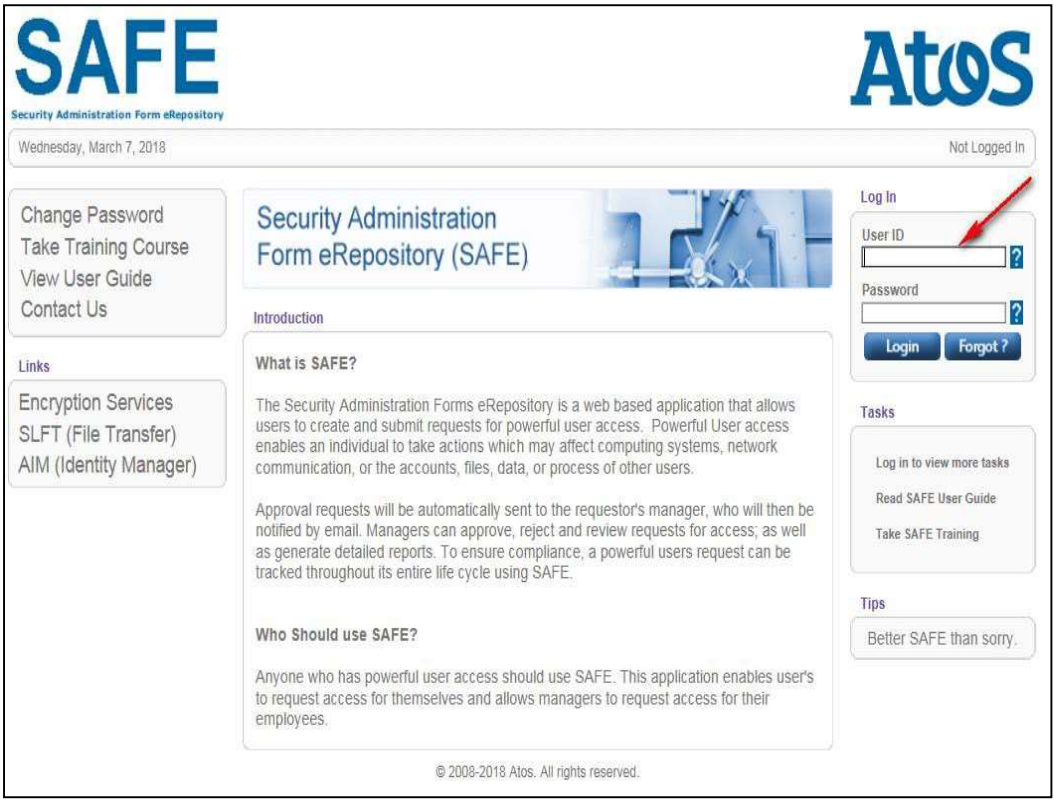
Section	Definition
Forms	In this section, you can create new requests for employees, contractors and vendors. You can also view the status of the forms that you have already submitted. You can also create multiple request forms for one employee, contractor or vendor.
Approvals	This section allows managers with the proper access to view the status of all forms requested.
Reports	Use this section to manage access you have already approved for your direct reports.
Profile	Use this section to edit your user information. You will be required to review and submit this information each time you log in.
Links	Use the links to go to other Encryption Services' documentation and applications.
Help	Use this section to get answers to your SAFE questions and access the SAFE eLearning module.

Accessing the eRepository

There are three ways to log into the SAFE application. If you are a Conduent Employee, use your WIN ID and the password you use to access the network. Contractors can log in with their CID also through the main log in page. Other users will be directed to a different login page. On this page, they can enter the PIN that was assigned to them.

To log into SAFE:

1. Go to https://safe.atos-nao.net/
2. Type your User ID (Win ID) or email address in the User ID field. Note: Your email address will work only if it is your actual login ID.
3. Type your password in the field provided.
4. Click the Logon button.



Forgotten Passwords

If you forget your password for the SAFE system:

1. Type your WINID or email address in the user ID field. Note: Your email address will work only if it is your actual login ID.

2. Click the “Forgot?’’ link.

NOTE: For additional assistance with your account. Contact the DL listed under the Contact Us link in the left side navigation panel.

Registering to Use the System

The first time you log into the application, you must register as a user. Each time you log in, you will be required to review and submit your user information to ensure that your information is kept up to date.

To register as a user:

1. Complete the entire User Registration Information form.
2. Click Submit.

Note: If you have multiple work email addresses, enter an alternative email address in the Alternate email address in the Alternate Email Address field.

Client Approvers and Non-Employees

If a client needs access to SAFE, they must be listed as an approver on a Powerful User request form. Client approvers will receive two emails. One will contain a link to SAFE and the other will contain a PIN for creating their account in SAFE.

To obtain your password:

1. Click on the link provided in your email.

A form has been submitted for your approval in the Security Administration Form eRepository (SAFE) system.

If you have a valid Services Single Sign-on account (i.e. SSPR Login), use the link directly below.

https://safe.atos-nao.net/

If you do not, please login using the link provided in the email sent from the SAFE system.

Note: Your PIN number for accessing the system was sent in a separate email.

1. Enter the PIN number that was emailed to you.
2. Click the Login button.
3. Type your new password.
4. Type your password again to verify.
5. Click Submit.

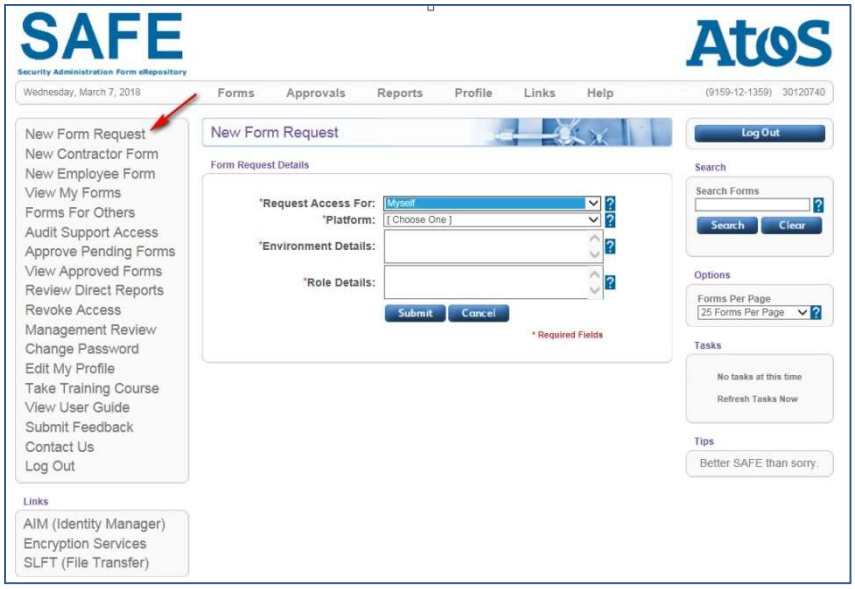
Selecting & Submitting a Form

Completing a Powerful User Access Request for Yourself

Requests for powerful user access can be created and submitted through the Forms menu. Your existing forms can be viewed by selecting “View My Forms” from the side menu.

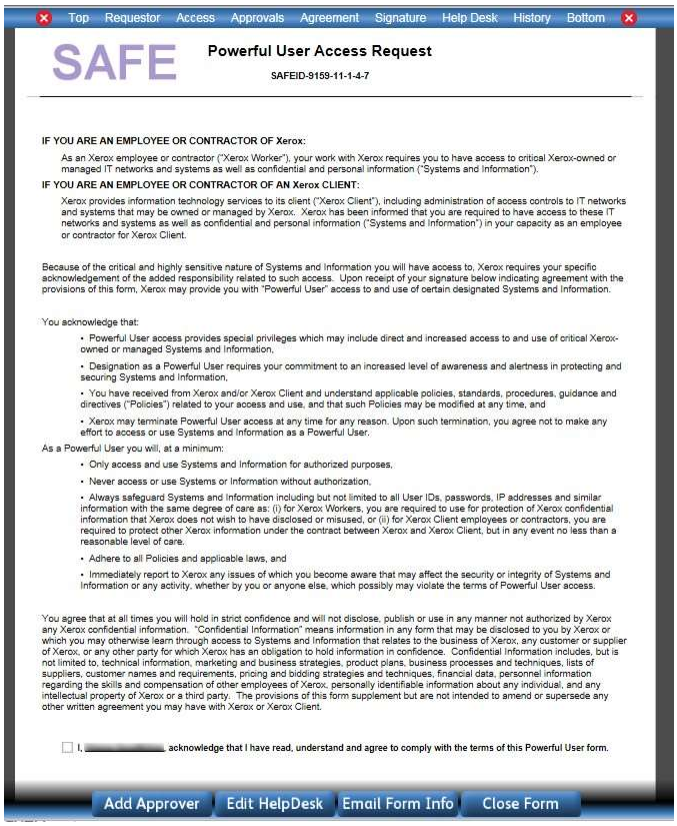
To request access:

1. Select “New Form request”.



2. Select “Myself” from the Request Access For drop -down menu.
3. Select the Platform. (See Appendix A for user type and platform options).
4. Enter the Environmental Details in the text box provided.
5. Select the appropriate Role(s).
6. Enter the role details.
7. Click Submit.

8. Review the document for accuracy.
9. Select the check box next to the statement acknowledging that you have read and reviewed the document. (Note: To continue you must scroll down and click the acknowledgement)



10. Click Submit Form.

Your form will appear with the current status in the My Forms- Forms Waiting for Approval.

Once the request has been saved, you can email the form details to yourself or another individual.

Note: Click the Cancel button to cancel the form. Only forms that have NOT been approved can be cancelled.

To email the form details:

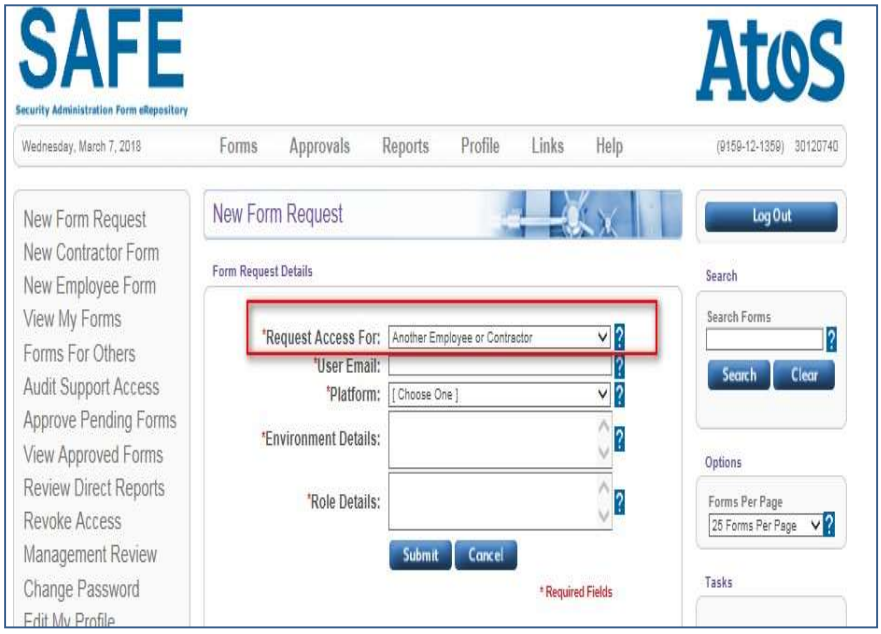
1. Click “Email Form Info” from the menu located at the bottom of screen.
2. Select “Send to Myself” or “Specified Address” from the drop-down list. Click Submit.

Completing a Powerful User Access Request – Another Employee

To request access for another employee:

1. Select “New Employee Form”.

2. Select Another Employee or Contractor from the Request Access For drop-down menu.



3. Click in Use Email field.
4. Enter the user’s First and Last name. **If the employee exists within the database, their name will appear in the search results.**
5. Type the user’s Email Address.

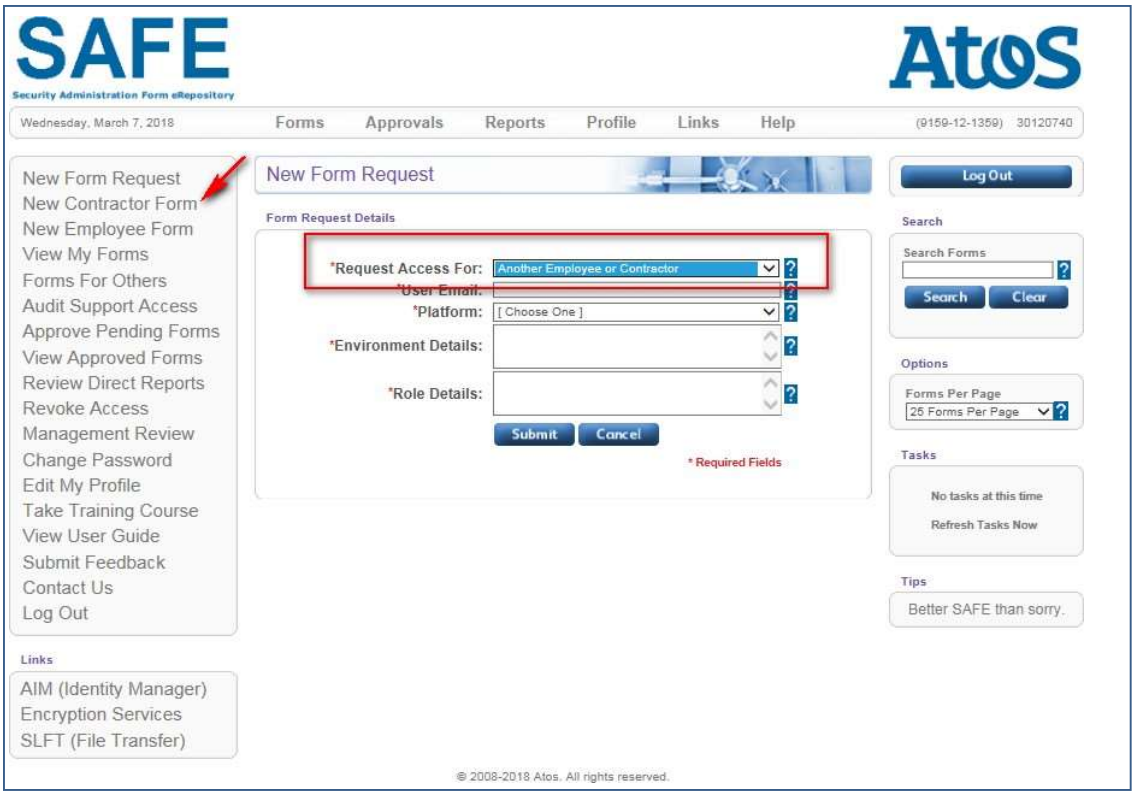
6. Click the Search button.
7. Select the employee's name.
8. Select the appropriate Platform. (See Appendix A for user type and platform options).
9. Enter a description of the environment in the Environmental Details text box provided.
10. Enter a description of the role in the Role(s) text box.
11. Enter the role details.
12. Click Submit.

The form will appear under "Forms I Created for Others" and awaiting signature. The user will receive an email notification stating that a form has been submitted for them. Their form will appear under the "My Forms" section. Once they click on their form, they will be prompted to select the check box next to the statement acknowledging that they have read and reviewed the document. To complete the process, they must click Submit Form.

Completing a Powerful User Access Request – Contractor

To request access for a Contractor:

1. Select “New Contractor Form.”



2. Enter User’s Email.
3. Enter User’s First and Last name.
4. Type the user’s Email Address.
5. Select the appropriate Platform. (See Appendix A for user type and platform options)
6. Type a description of the environment in the Environmental Details text box provided.
7. Type a description of the role in the Role(s) text box.
8. Enter the role details.
9. Click Submit.

The form will appear under “Forms I Created for Others” and awaiting signature. The user will receive an email notification stating that a form has been submitted for them. Their form will appear under the “My Forms” section. Once they click on their form, they will be prompted to select the check box next to the statement acknowledging that they have read and reviewed the document. To complete the process, they must click Submit Form.

Understanding Your Form Status

Review of Definitions

The status of your request can always be viewed on the Forms tab. Once your request has been submitted, one of the following will be assigned:

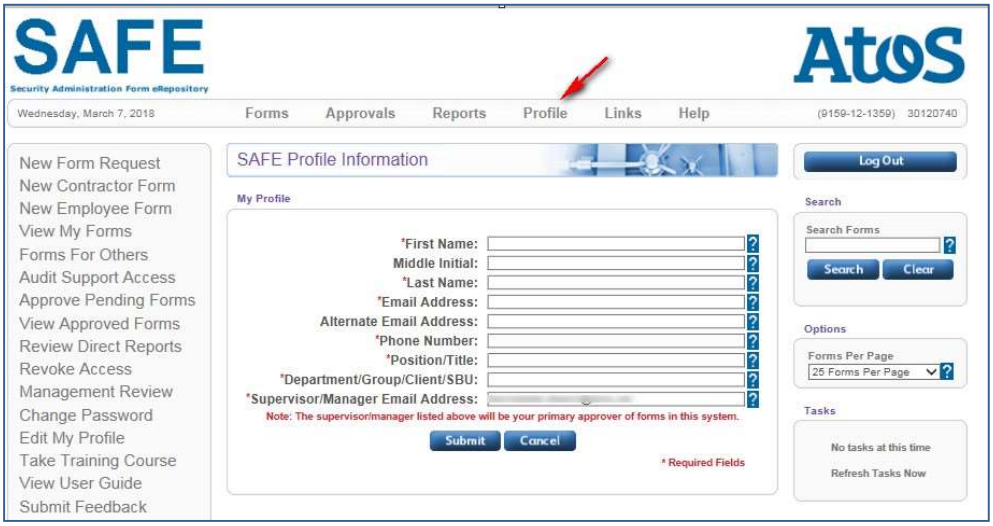
Status	Definition
Awaiting Signature	Your request is waiting for you to acknowledge the legal agreement and submit for approval
Awaiting Approval	Your request is pending approval.
Approved	Your request has been approved.
Rejected	Your request has not been approved.
Revoked	A request that has been previously approved but has been terminated for various reasons.
Management Transfer	A request that was previously approved but Is being transferred to another manager.

Viewing and Modifying Your Profile

How to Update Your Profile

It is important to keep your user registration information in SAFE up to date. The Profile tab allows you to edit any of your user registration information. To view or modify your profile:

1. Click the Profile tab.
2. Type any necessary changes to your information.
3. Click Submit.

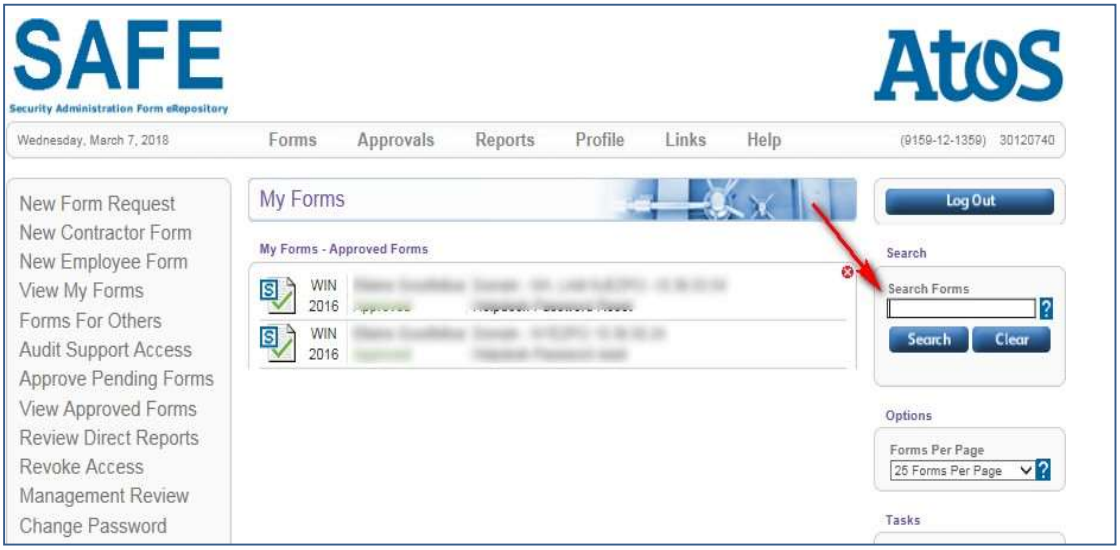


Searching Forms

It is possible to have hundreds of form requests under your My Forms view, searching for specific forms can be difficult. To simply your search, use the search field feature.

To search for forms:

1. Type your search criteria in the Search Forms field and click the search button.



Your query results will appear if there is a match. Note: To see all of your forms, click on the Forms link at the top of the page.

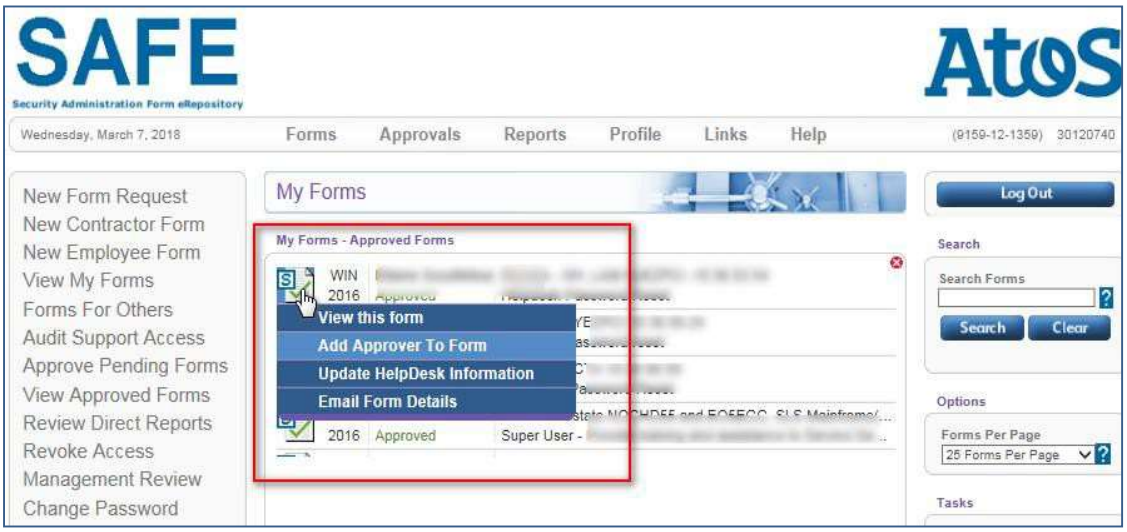
Updating Forms – Adding Additional Approvers

Updating your forms in SAFE is very simple. On the Forms tab, use the drop- down list provided to update your form.

NOTE: Atos privileged access only requires one approval from the manager or designee.

To add additional approvers:

1. Mouse over the form icon.
2. Select “Add additional approver from the drop down menu.

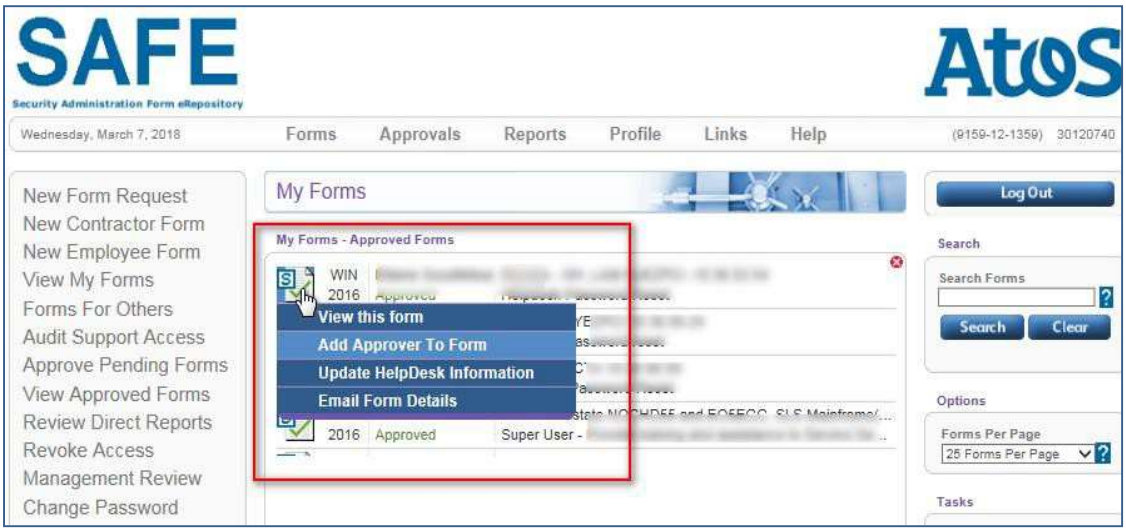


3. Click the **Yes** button to “Would you like to add an additional approver?”
4. Enter the approver’s first and last name. Then, enter their email address and click **Search.**
5. Click **Select** to choose the correct approver.

Updating Forms – Updating Help Desk Information

To update Help Desk Information:

1. Mouse over the form icon.
2. Select “Update Helpdesk Information” from the drop down menu.



3. Select the appropriate help desk from the drop down menu.
4. Select the ticket assignment group or enter manually.
5. Click Submit.

Managers Section

Overview

In the Security Administration Forms e-Repository (SAFE), authorized managers can approve, reject, view and query Powerful User Access forms.

Managing Approvals

Managers with the proper access can view the status of all forms requested and make decisions on the future status of those forms.

Forms in the repository can have the following statuses:

- Pending Approvals – forms that are awaiting your approval
- Previous Approvals – forms that you have previously approved
- Previous Rejections – forms that you have previously rejected
- Revokes / Transfers – forms that have been previously approved / reviewed and the status have now been changed to revoked or transferred.

Approving a Form

As the approving manager, you will make most of your approvals from the Approve Pending Forms section. You can manage and make approvals by using the following steps:

To approve a form request:

1. Select the form by clicking on the form icon.
2. Read all information on the form, including Requester's information and access requested.
3. Select **Approve Form**.
4. Select **Yes** or **No** to add additional approvers.
5. Select **Yes** to approve form.

Note: If a helpdesk was not initially selected, you may be asked to update the Helpdesk information.

To reject a form request:

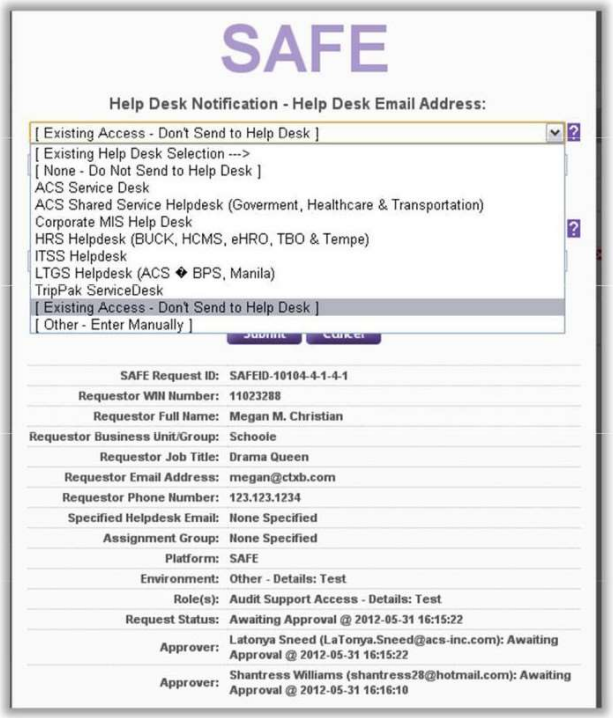
1. Select the form by clicking on the form icon.
2. Click the **Reject Form** button.
3. Click **Yes** to reject the form and enter the reason for the rejection.

Your rejected for will appear in the “Forms I Created for Others”

Existing Access (For Record Keeping Purposes)

To approve existing access request:

1. Click on the form request.
2. Read all information on the form, including Requester’s information and access requested.
3. Click the **Approve Form** button at the bottom of the page.
4. Select “Existing Access – Do not send to Helpdesk” from the drop-down menu.



5. Click the **No** button for additional users.
6. Click **Yes** to approve the form.

Accessing & Updating Forms

The My Reports section in the Security Administration Forms e-Repository (SAFE) allows managers with the proper access to view and update the status of previously approved forms. This section allows the managers to continually review and check the status of their approvals. The three actions available in the My Reports section are:

Action	Definition
Revoked – Termed	This selection means the form has been revoked and should be terminated by a specific date.
Revoked – No Longer Needed	This selection means the form has been revoked and is no longer needed.
Management Transfer	This selection means the form has been transferred to another approving manager.

Making a Change on a Form's Status:

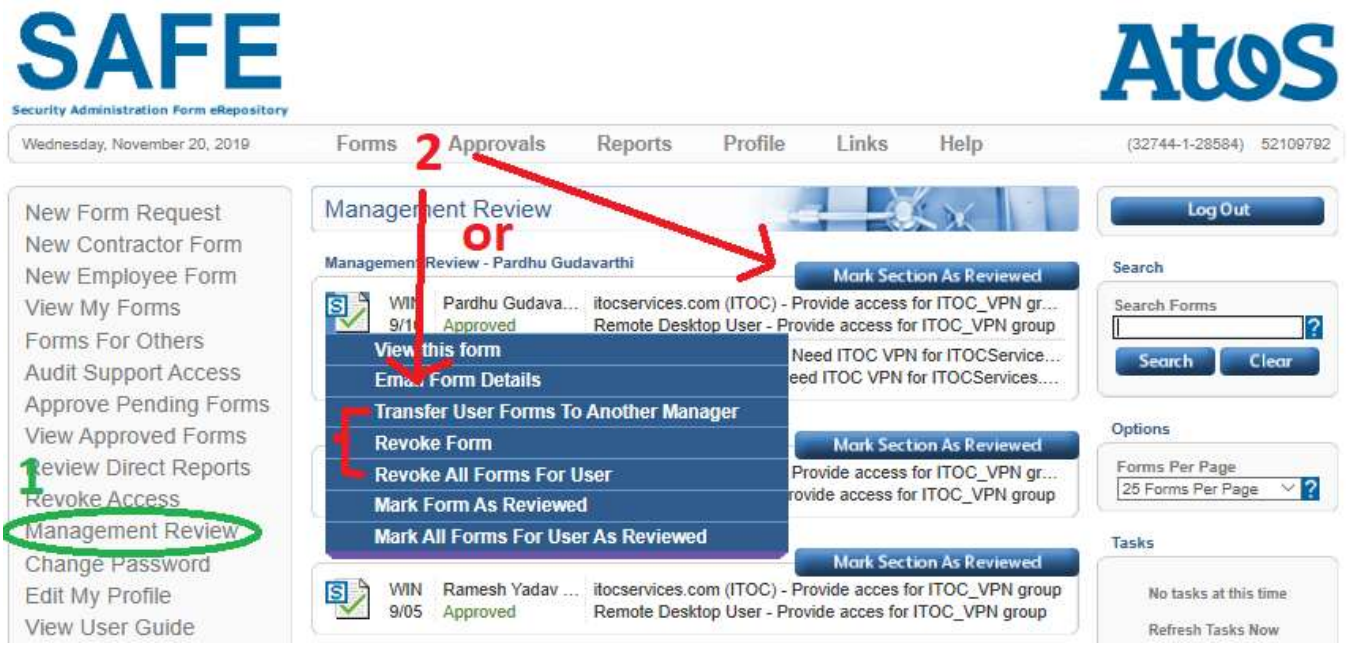
1. Place your pointer on the Reports tab.
2. Click "Review forms that I have previously approved"
3. Place your pointer on the form icon.
4. Select the correct status for the form.

If you selected…..	Then…
Revoked – Termed	You can enter Help Desk Notification Information.
Revoked – No Longer Needed	You can enter Help Desk Notification Information
Management Transfer	Enter the new managers information

Management Reviews

It is an audit requirement that all forms for elevated access are reviewed quarterly by the user's manager. The managers are notified twice a month if they have outstanding forms in the SAFE system that need reviewed. If forms are not reviewed within 120 days, there is an automated process that may auto-revoke these forms and create SNOW tickets to have the associated access listed the non-compliant forms removed. Please follow the steps below to complete your reviews in a timely manner and prevent forms from being revoked which can lead to access being removed.

When you log into the system you should automatically be taken to the management review screen after reviewing your profile information if you have forms that are due for review. If you need to navigate to the management review page, click the Management Review link in the left navigation bar (see #1 in diagram below). If all the access is still valid for the listed user, simply click the Mark Section As Reviewed button (see #2 in the diagram below) or if you need to take other actions on the listed forms, mouse over the form icon to pull up the action menu for the form and select and appropriate action such as transferring the employee or revoking the user's form(s).



Auditor's Section

The auditors section allows any person who has proper access to query and review all transactions that have been processed. As an auditor you will only be able to view selected forms.

To access the auditors section of the SAFE application:

1. Place your mouse cursor on the Reports
2. Select "Search forms for all users (Auditor Support).

3. Enter your Search criteria in Search Form text box.

4. Click the **Search** button. If there are forms with your selected search criteria, your search results will be displayed.
5. Click the appropriate form in the table to view

All requests for auditing rights should be sent via email to dl-bds-safe@atos.net. To obtain auditor rights, your Manager must provide your Name, Win ID and Email address. Requests for auditing rights will be reviewed and approved by the Information Security Services (ISS) office. If your request has been approved, it will be routed to the appropriate persons for processing.

Support

Contacts

For issues or problems with the SAFE application, send an email to dl-bds-safe@atos.net.

Appendix A: Powerful User Access Request Options (User Types & Platforms)

Field	Definition	Myself	Another Conduent Services Employee	Another Non-Conduent Services
Request Access For:	Select for whom this form is being created. Note: Your selection for this field will determine your following entry field choices.	x	x	x
User WIN Number:	Enter the WIN (Conduent Employee Number) of the user this form is being created for.		x	
User First Name:	Enter the first name of the user this is being created for.		x	x
User Last Name:	Enter the last name of the user this is being created for.		x	x
User Email:	Enter the e-mail address of the user this form is being created for. Note: This		x	x
Platform:	Select the appropriate platform (Operating System) that access is being requested for. Platforms Examples: • Wintel – Windows • AS/400 – iSeries • Network Novell – Netware • VMS • UNIX - Linux • Novell – Netware • Telecom • Network • RSA SecurID • RSA envision	x	x	x
Environment:	Select the appropriate environment (Scope) of access that is being requested for.	x	x	x
Environment Details:	Describe the environment (Scope) of where the requested access will cover.	x	x	x
Role(s):	Select the appropriate role(s) (Group/Rights) for the requested access. Note: To select multiple roles hold down the [Ctrl] key while clicking your selections.	x	x	x
Role Details:	Describe the role(s) for the requested access.	x	x	x

Appendix B: Powerful User Access Request Options (Platforms & Roles)

Platform Name	Available Roles
AS/400 - iSeries	Other
	Super User
Build-Team-Infra	AD Group Creation
	AD Group Update
	AD Service Account Creation
	AD Service Account Update
Conduent Active Directories	Account Operator
	Admin (Domain Based)
	AppDynamics
	Backup Operator
	Database Administrator
	Desktop Administrator
	DHCP Admin
	Distributed COM User
	DNS Admin
	Domain Admin
	Enterprise Admin
	Local Admin Access
	Other
	OVM Support
	Perf Log User
	Perf Monitor User
	Print Operator
	Remote Desktop User
	Server Operator
	Solar Winds Group Access
	SSH Access
	SUDO Access
	Windows Auth Access Group
Enterprise Data Protection	Data Protection Administration
	Data Protection Engineering
Enterprise Storage	Storage Administration
	Storage Engineering
HAWK SIEM	HAWK SIEM Engineer
	HAWK SOC User
Mainframe	Database Administrator
	Group Auditor
	Group Operations/Non-Cncl/Nodsnchk

	Group Security Admin
	Other
	System Auditor
	System Operations/Non-Cncl/Nodsnchk
	System Programmer
	System Security Admin
	UNIX Superuser
MyStats	Account Leader
	Admin - Developer
	Admin - Support
	Agent
	Local Support (WFM/Quality/Training)
	Manager
	Supervisor
Network	Other
NJTransit	Administrator
	CSR - Agent
	CSR - Supervisor
	Linux/Solaris/Storage sudo
	MySQL DB Admin
	xMS Oracle DB Admin
Novell - Netware	Other
OCI Transit-SimpliGo	Admin access for BOS applications
	Administrator
	DBA access
	Read Only
	Server Administrator
	Server Administrator - sudo
	Support access
RSA enVision	enVision Administrator
	enVision Client Administrator
	enVision Client User
	enVision SOC Administrator
	Other
	Windows Domain Administrator
	Windows Domain Server Operator
	Windows Local Administrator
	Windows Local Power User
	Windows Local User
RSA SecurID	Enterprise
	Helpdesk
	Other
	Privileged Helpdesk

	Super Admin
SAFE	Audit Support Access
Service Account in a Conduent Directory	Owner and Co-Owner
Service Principal in a Conduent Directory	Owner and Co-Owner
TCLG Vector	Configuration Management
	CRM Developer
	Crystal Administrator
	CSC LAN/Desktop Administrator
	Development DBA
	Development Manager
	Images Developer
	IVR Administrator
	IVR Developer
	Lane Developer
	Level 1
	Level 2
	Level 3
	Linux Administrator
	PBX Administrator
	Production Control
	Production DBA
	Reports Developer
	Siebel Administrator
	Software Tester
	Software Testing Manager
	System Account
	Temporary Privileges
	TPMS Developer
	Web Developer
	Websphere Administrator
	Windows/LAN Adminstrator
Telecom	Other
Time Tracking Applications	Administrator
UNIX - Linux	Database Administrator
	Other
	SUDO Access
VMS	Other
	SYSTEM Level Access
Wintel - Windows	Account Operator
	AD Group Creation
	AD Group Owner Update
	Admin (Domain Based)
	AppDynamics

	AppDynamics
	Backup Operator
	Database Administrator
	Desktop Administrator
	DHCP Admin
	Distributed COM User
	DNS Admin
	Domain Admin
	Domain Admin
	Domain Admin
	Enterprise Admin
	Enterprise Admin
	Local Admin Access
	Local Admin Access
	Other
	OVM Support
	OVM Support
	Perf Log User
	Perf Monitor User
	Print Operator
	RDP Access Only
	Remote Desktop User
	Server Operator
	Solar Winds Group Access
	Solar Winds Group Access
	SSH Access
	SSH Access
	SUDO Access
	SUDO Access
	VDI Local Admins
	VDI Local Admins
	VPN Group Access
	Windows Auth Access
	Windows Auth Access Group
	Windows Auth Access Group
WSP Elevated Access for Atos Personnel	AD Admin
	Application Packaging
	AV / Malware Admin
	Azure Automation Coordinator
	Azure Contributor
	Azure Owner
	Backup Admin
	Beatbox Admin

	BPS Developer
	Bridge Team
	CES Admin
	Citrix Admin
	Client Side Support (Africa,India,ME)
	Client Side Support (Australia,NZ,Asia)
	Client Side Support (CAN,LATAM,USA)
	Client Side Support (CE, Nordics, UK)
	DNS External Admin
	DSE Admin
	DSE Admin / Azure Contributor
	DSE Admin / DSE AD Admin
	DSE Admin / DSE AD Admin / Azure Contributor
	DSE SCCM Patching Admin
	DSE Supervisor
	DSE Supervisor / Azure Owner
	DSE Supervisor / DSE AD Admin / Azure Owner
	EOC Admin
	Exchange / Skype / O365 Admin
	Exchange / Skype / SharePoint Admin
	Exchange / Skype Admin
	Exchange / Skype Admin / Azure Owner
	Exchange Admin
	Flexera Admins
	Flexera Operators
	HCI Admin
	HCI Operator
	IAM Admin
	IAM Admin / PKI Admin / PKI External Admin
	Intune Admin
	IPAM Admin
	Linux Admin
	M and A Admin
	M and A Tester
	Network Admin
	Network Tools Admin
	O365 License Admin
	PKI Admin
	PKI External Admin
	PTM Admin
	Remote Resolution Team
	RPA Admin
	RPA Developer

	SCCM Admin
	SCOM Admin
	Server Virtualisation Admin
	Service Desk Level 1
	Service Desk Level 2
	Service Desk Supervisor
	Service Now Admin
	SharePoint / O365 / Yammer Admin
	SharePoint / Yammer Admin
	SharePoint Admin
	Sitecore Developer
	Skype Admin
	SN eDiscovery Admins
	SQL Admin
	Storage Admin
	User Management Admin
	VDI Admin
	Voice Admin
	Yammer Admin
	Zscaler Admin