



Security Administration Form eRepository (SAFE) User's Guide

Version 3.4.3

© Copyright 2020-2023, Atos. All rights reserved. Reproduction in whole or in part is prohibited without the prior written consent of the copyright owner.

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	3
Introduction.....	3
Accessing the eRepository.....	5
Selecting & Submitting a Form.....	8
Understanding Your Form Status.....	13
Viewing and Modifying Your Profile.....	13
Searching Forms	14
Updating Forms – Adding Additional Users.....	15
Updating Forms – Updating Help Desk Information	16
Managers Section	17
Overview.....	17
Managing Approvals	17
Accessing & Updating Forms	19
Auditor’s Section	20
Overview.....	20
Support	22
Appendix A: Powerful User Access Request Options (User Types & Platforms)	23
Appendix B: Powerful User Access Request Options (Platforms & Roles).....	24

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?

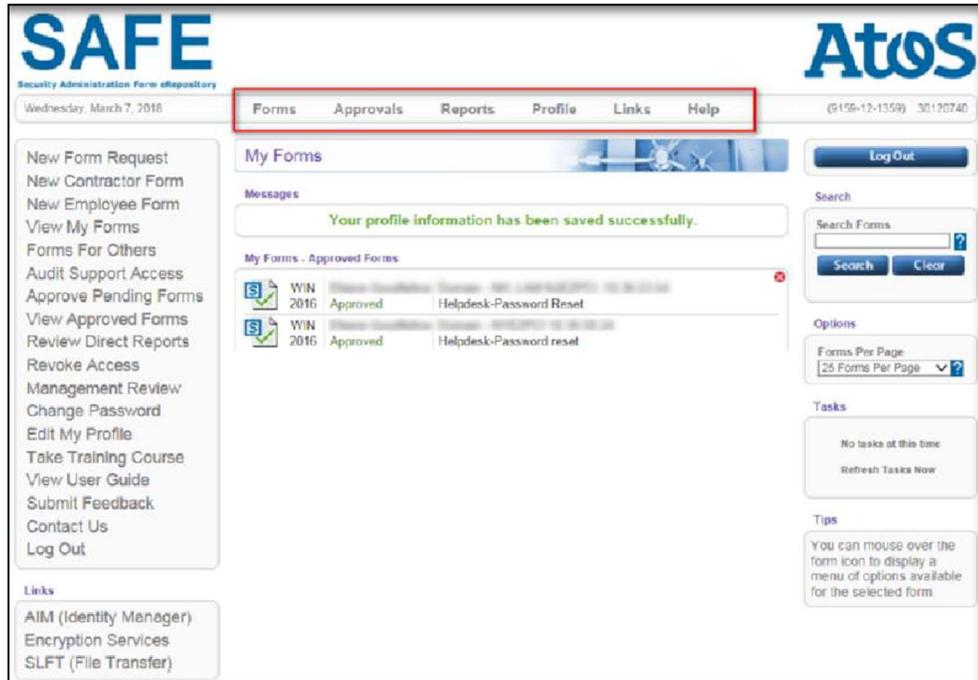
Anyone who has powerful user access should use SAFE. This application enables users to request access for themselves and allows managers to request access for their employees.

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.

SAFE
Security Administration Form eRepository

Atos

Wednesday, March 7, 2018 Not Logged In

Change Password
Take Training Course
View User Guide
Contact Us

Links

Encryption Services
SLFT (File Transfer)
AIM (Identity Manager)

Security Administration Form eRepository (SAFE)

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 user's to request access for themselves and allows managers to request access for their employees.

© 2008-2018 Atos. All rights reserved.

Log In

User ID

Password

Tasks

Log in to view more tasks
Read SAFE User Guide
Take SAFE Training

Tips

Better SAFE than sorry.

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.

The screenshot shows the SAFE system interface. At the top, there is a navigation bar with the SAFE logo on the left and the Atos logo on the right. Below the logos, there is a date (Wednesday, March 7, 2018) and a set of navigation links: Forms, Approvals, Reports, Profile, Links, and Help. On the right side of the navigation bar, there is a user ID (0150-12-1256) and a date (3/12/18). The main content area is titled "Is Your SAFE Profile Up To Date?" and features a "Yes" button. Below this, there is a "My Profile" section with a form containing the following fields: First Name (filled with "Test"), Middle Initial, Last Name (filled with "User"), Email Address, Alternate Email Address, Phone Number, Position/Title, Department/Group/Client/SBU, and Supervisor/Manager Email Address. A note below the form states: "Note: The supervisor/manager listed above will be your primary approver of forms in this system." There are "Submit" and "Cancel" buttons at the bottom of the form. To the right of the form, there is a "Log Out" button, a search box, and a "Tasks" section. The left side of the page has a navigation menu with various options like "New Form Request", "View My Forms", and "Contact Us".

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”.

The screenshot shows the SAFE web interface. The left navigation menu has a red arrow pointing to "New Form Request". The main content area is titled "New Form Request" and contains a form with the following fields:

- 'Request Access For:' dropdown menu with 'Myself' selected.
- 'Platform:' dropdown menu with '[Choose One]' selected.
- 'Environment Details:' text input field.
- 'Role Details:' dropdown menu.

Below the form are 'Submit' and 'Cancel' buttons. The right-hand side of the page features a search bar, an options section with a 'Forms Per Page' dropdown set to '25 Forms Per Page', and a tasks section showing 'No tasks at this time' and a 'Refresh Tasks Now' button. The top navigation bar includes 'Forms', 'Approvals', 'Reports', 'Profile', 'Links', and 'Help'.

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)

SAFE Powerful User Access Request
SAFEID-9159-11-14-7

IF YOU ARE AN EMPLOYEE OR CONTRACTOR OF Xerox:
As an Xerox employee or contractor ("Xerox Worker"), your work with Xerox requires you to have access to critical Xerox-owned or managed IT networks and systems as well as confidential and personal information ("Systems and Information").

IF YOU ARE AN EMPLOYEE OR CONTRACTOR OF AN Xerox CLIENT:
Xerox provides information technology services to its client ("Xerox Client"), including administration of access controls to IT networks and systems that may be owned or managed by Xerox. Xerox has been informed that you are required to have access to these IT networks and systems as well as confidential and personal information ("Systems and Information") in your capacity as an employee or contractor for Xerox Client.

Because of the critical and highly sensitive nature of Systems and Information you will have access to, Xerox requires your specific acknowledgement of the added responsibility related to such access. Upon receipt of your signature below indicating agreement with the provisions of this form, Xerox may provide you with "Powerful User" access to and use of certain designated Systems and Information.

You acknowledge that:

- Powerful User access provides special privileges which may include direct and increased access to and use of critical Xerox-owned or managed Systems and Information.
- Designation as a Powerful User requires your commitment to an increased level of awareness and alertness in protecting and securing Systems and Information.
- You have received from Xerox and/or Xerox Client and understand applicable policies, standards, procedures, guidance and directives ("Policies") related to your access and use, and that such Policies may be modified at any time, and
- Xerox may terminate Powerful User access at any time for any reason. Upon such termination, you agree not to make any effort to access or use Systems and Information as a Powerful User.

As a Powerful User you will, at a minimum:

- Only access and use Systems and Information for authorized purposes.
- Never access or use Systems or Information without authorization.
- Always safeguard Systems and Information including but not limited to all User IDs, passwords, IP addresses and similar information with the same degree of care as: (i) for Xerox Workers, you are required to use for protection of Xerox confidential information that Xerox does not wish to have disclosed or misused, or (ii) for Xerox Client employees or contractors, you are required to protect other Xerox information under the contract between Xerox and Xerox Client, but in any event no less than a reasonable level of care.
- Adhere to all Policies and applicable laws, and
- Immediately report to Xerox any issues of which you become aware that may affect the security or integrity of Systems and Information or any activity, whether by you or anyone else, which possibly may violate the terms of Powerful User access.

You agree that at all times you will hold in strict confidence and will not disclose, publish or use in any manner not authorized by Xerox any Xerox confidential information. "Confidential Information" means information in any form that may be disclosed to you by Xerox or which you may otherwise learn through access to Systems and Information that relates to the business of Xerox, any customer or supplier of Xerox, or any other party for which Xerox has an obligation to hold information in confidence. Confidential Information includes, but is not limited to, technical information, marketing and business strategies, product plans, business processes and techniques, lists of suppliers, customer names and requirements, pricing and bidding strategies and techniques, financial data, personnel information regarding the skills and compensation of other employees of Xerox, personally identifiable information about any individual, and any intellectual property of Xerox or a third party. The provisions of this form supplement but are not intended to amend or supersede any other written agreement you may have with Xerox or Xerox Client.

I, _____ acknowledge that I have read, understand and agree to comply with the terms of this Powerful User form.

Buttons: Add Approver, Edit HelpDesk, Email Form Info, Close Form

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.

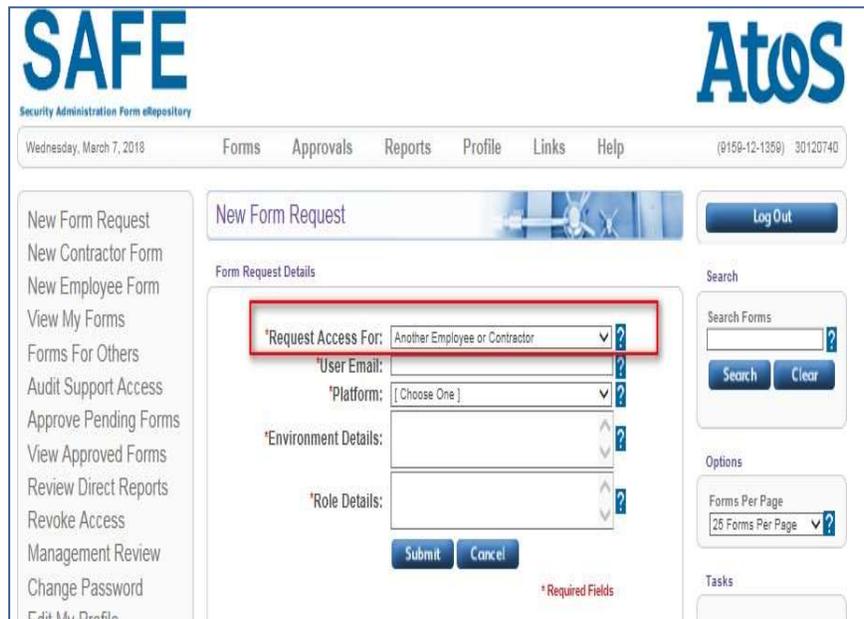
Completing a Powerful User Access Request – Another Employee

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:

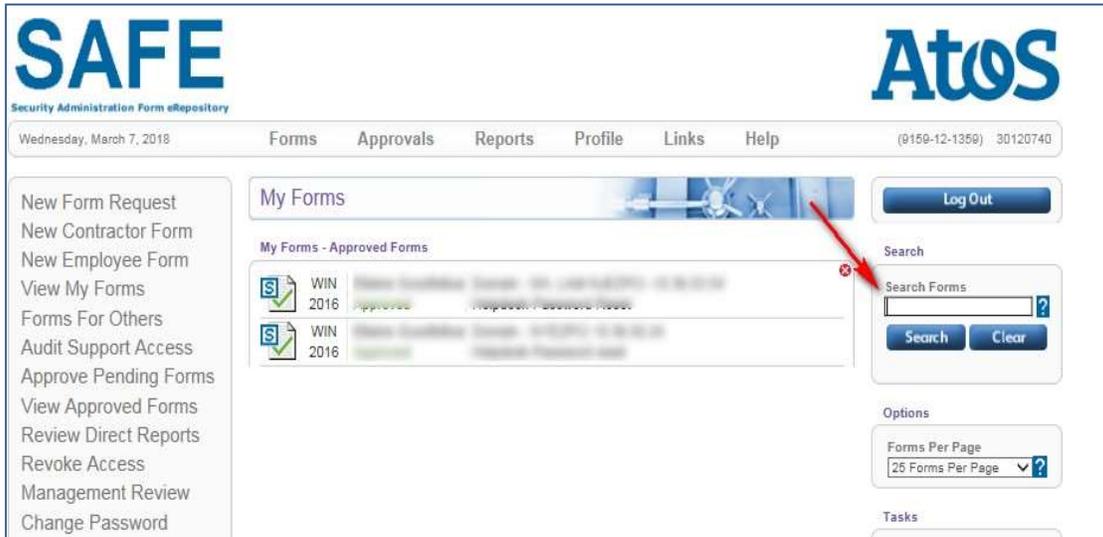
1. Click the Profile tab.
2. Type any necessary changes to your information.
3. Click Submit.

Searching Forms

It is possible to have hundreds of form requests under your My Forms view, searching for specific forms can be difficult. To simplify 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.



The screenshot displays the SAFE (Security Administration Form eRepository) web interface. At the top left is the 'SAFE' logo, and at the top right is the 'Atos' logo. Below the logos is a navigation bar with links for 'Forms', 'Approvals', 'Reports', 'Profile', 'Links', and 'Help'. The date 'Wednesday, March 7, 2018' and user information '(9159-12-1359) 30120740' are also visible. On the left side, there is a vertical menu with options like 'New Form Request', 'View My Forms', and 'Approve Pending Forms'. The main content area is titled 'My Forms' and shows a list of 'Approved Forms'. A search box labeled 'Search Forms' is located on the right side of the 'My Forms' section, with a red arrow pointing to it. Below the search box are 'Search' and 'Clear' buttons. There is also an 'Options' section with a 'Forms Per Page' dropdown set to '25 Forms Per Page'.

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.

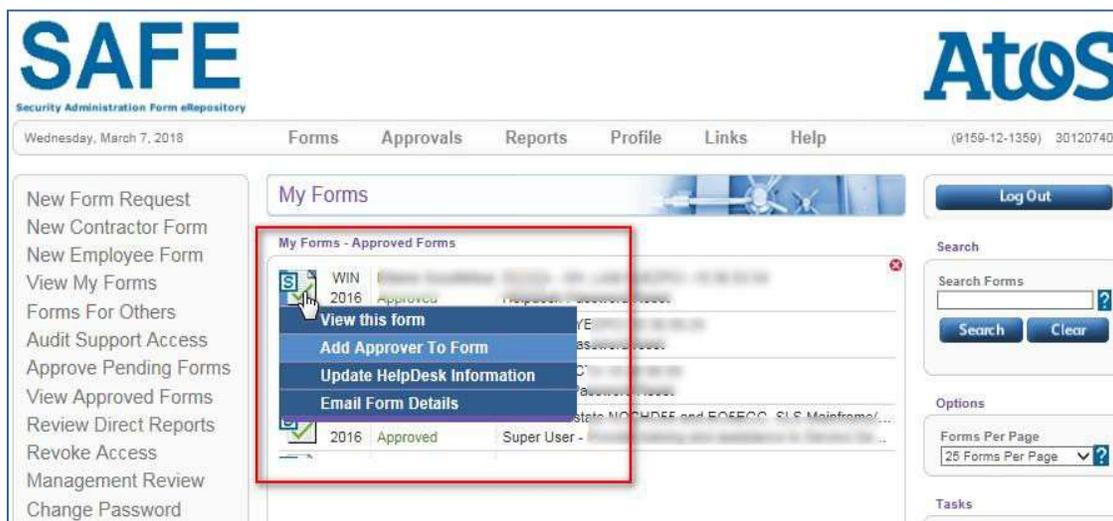
Updating Forms – Adding Additional Approvers

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.

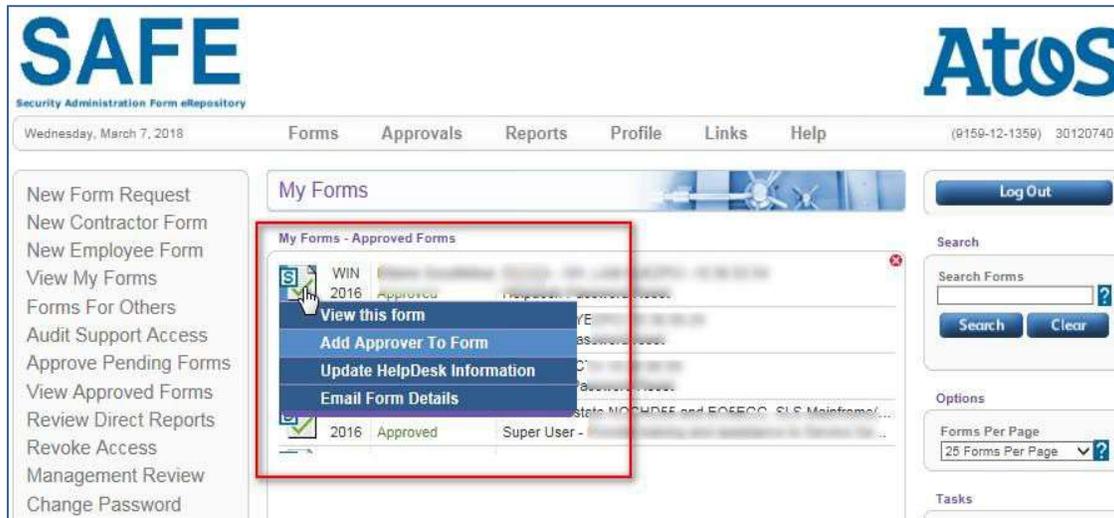


3. Click the **Yes** button to “Would you like to add an additional approver?”
4. Enter the approver’s first and last name. Then, enter their email address and click **Search**.
5. Click **Select** to choose the correct approver.

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.

SAFE Request ID:	SAFEID-10104-4-1-4-1
Requestor WIN Number:	11023288
Requestor Full Name:	Megan M. Christian
Requestor Business Unit/Group:	Schoole
Requestor Job Title:	Drama Queen
Requestor Email Address:	megan@ctxb.com
Requestor Phone Number:	123.123.1234
Specified Helpdesk Email:	None Specified
Assignment Group:	None Specified
Platform:	SAFE
Environment:	Other - Details: Test
Role(s):	Audit Support Access - Details: Test
Request Status:	Awaiting Approval @ 2012-05-31 16:15:22
Approver:	Latonya Sneed (LaTonya.Sneed@acs-inc.com): Awaiting Approval @ 2012-05-31 16:15:22
Approver:	Shantress Williams (shantress28@hotmail.com): Awaiting Approval @ 2012-05-31 16:16:10

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).

SAFE
Security Administration Form eRepository

Wednesday, November 20, 2019 Forms **2** Approvals Reports Profile Links Help (32744-1-28584) 52109792

Atos

Log Out

Search

Search Forms

Search Clear

Options

Forms Per Page

25 Forms Per Page

Tasks

No tasks at this time

Refresh Tasks Now

Management Review

Management Review - Pardhu Gudavarthi

	WIN 9/11 Approved	Pardhu Gudava...	itocservices.com (ITOC) - Provide access for ITOC_VPN gr... Remote Desktop User - Provide access for ITOC_VPN group	Mark Section As Reviewed
View this form				
Email Form Details				
Transfer User Forms To Another Manager				
Revoke Form				
Revoke All Forms For User				
Mark Form As Reviewed				
Mark All Forms For User As Reviewed				

Mark Section As Reviewed

Mark Section As Reviewed

Mark Section As Reviewed

Mark Section As Reviewed| | WIN 9/05 Approved | Ramesh Yadav ... | itocservices.com (ITOC) - Provide access for ITOC_VPN group Remote Desktop User - Provide access for ITOC_VPN group | **Mark Section As Reviewed** |

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: <ul style="list-style-type: none"> • 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 Administrator	
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