

GoAnywhere MFT

Runbook

Author(s): Dalton Hooper
Creation Date: 1/10/2022
Last Saved: 2/4/2022 7:34 PM
Last Saved by:
Version: 1.0

Subject Matter Experts providing input:

Name	Title
[REDACTED]	[REDACTED] Senior Developer
[REDACTED]	[REDACTED] Systems Engineer

History:

Date	Version	Description	Author(s)
01/10/2022	V0.1	Document Creation	Dalton Hooper
02/02/2022	V1.0	Final	Dalton Hooper

Table of contents

ABOUT THIS DOCUMENT	2
<i>Introduction</i>	<i>2</i>
<i>Intended audience.....</i>	<i>2</i>
<i>Purpose</i>	<i>2</i>
<i>Assumptions</i>	<i>2</i>
Requisite knowledge.....	2
Credentials	2
GOANYWHERE MFT – GENERAL INFORMATION.....	3
<i>Logging in</i>	<i>3</i>
<i>The administrator interface.....</i>	<i>7</i>
Customizing the administrator interface.....	7
COMMON GOANYWHERE MFT ADMIN TASKS.....	9
<i>SFTP administration</i>	<i>9</i>
Configure the SFTP service	9
<i>SSH key administration</i>	<i>14</i>
Add key pair	16
Import public key	18
Import private key	20
<i>Gateway administration.....</i>	<i>22</i>
Start / Stop a gateway.....	22
<i>Log file monitoring</i>	<i>24</i>
Log Settings	24
Enabling Tamper-Evident Logging	24
Interpreting Tamper-Evident Logging	27
Audit logs	28
<i>Managing certificates.....</i>	<i>31</i>
Create a new certificate	33
Import a certificate	34
Edit a certificate.....	35
<i>User administration</i>	<i>37</i>
Admin users	37
Add an admin user	37
Edit an admin user	41
Delete an admin user	43
Web users	46
Add a web user	46
Edit a web user	50
Delete a web user	52
<i>Issue Resolution.....</i>	<i>56</i>
Starting and stopping the GoAnywhere MFT application	56
Server post-outage checklist	58
APPENDIX	66
<i>Glossary of terms</i>	<i>66</i>
<i>Admin user roles.....</i>	<i>67</i>
<i>Accessing the [REDACTED] Citrix VDI desktop.....</i>	<i>70</i>

About this document

Introduction

GoAnywhere MFT is the managed file transfer solution utilized by [REDACTED] to automate and secure file transfers. The [REDACTED] implementation includes a GoAnywhere Gateway and an MFT Gateway configuration.

Intended audience

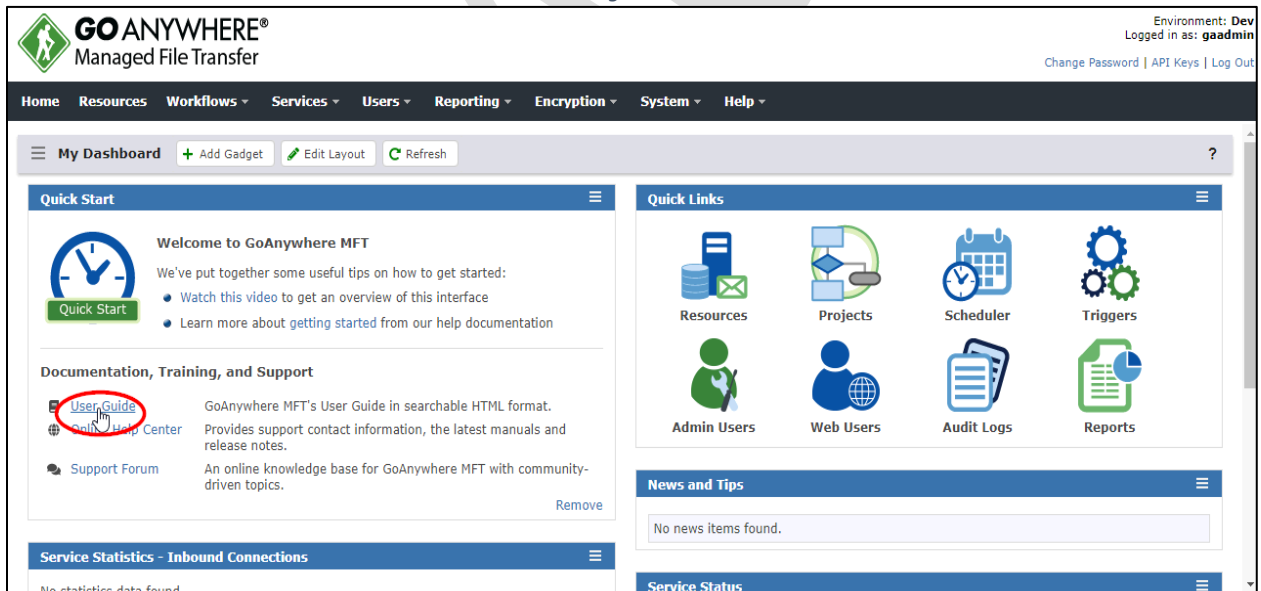
[REDACTED] GoAnywhere MFT administrators.

Purpose

This document is intended to provide the reader with sufficient information to successfully perform routine administrator tasks for the [REDACTED] GoAnywhere MFT application.

Note: This document is intended to assist [REDACTED] administrators with tasks that have been identified as most frequent (i.e., routine tasks). There may be occasions when the reader needs additional information or more detail. In those cases, it is recommended to reference the in-app help provided by the GoAnywhere MFT application. (Figure 1)

Figure 1



Assumptions

This document assumes the following:

Requisite knowledge

- The reader possesses the skillset necessary to read and correctly interpret the information presented within the [REDACTED] *GoAnywhere MFT* application.
- The reader has basic *UNIX/Linux* navigation skills.
- The reader knows how to access the necessary server(s).

Credentials

- The reader has valid [REDACTED] platform credentials.
- The reader has valid *GoAnywhere MFT* credentials at an administrator level.

REDACTED

GoAnywhere MFT – General Information

This section describes the *GoAnywhere MFT* application in general.

Logging in

GoAnywhere MFT must be launched from [REDACTED] desktop (for information on how to access the [REDACTED] desktop, go here.)

1. From the [REDACTED] desktop, if you do not have a *GoAnywhere MFT* shortcut, you can alternatively open a browser and navigate to [REDACTED] (Figure 2 & Figure 3)

Figure 2

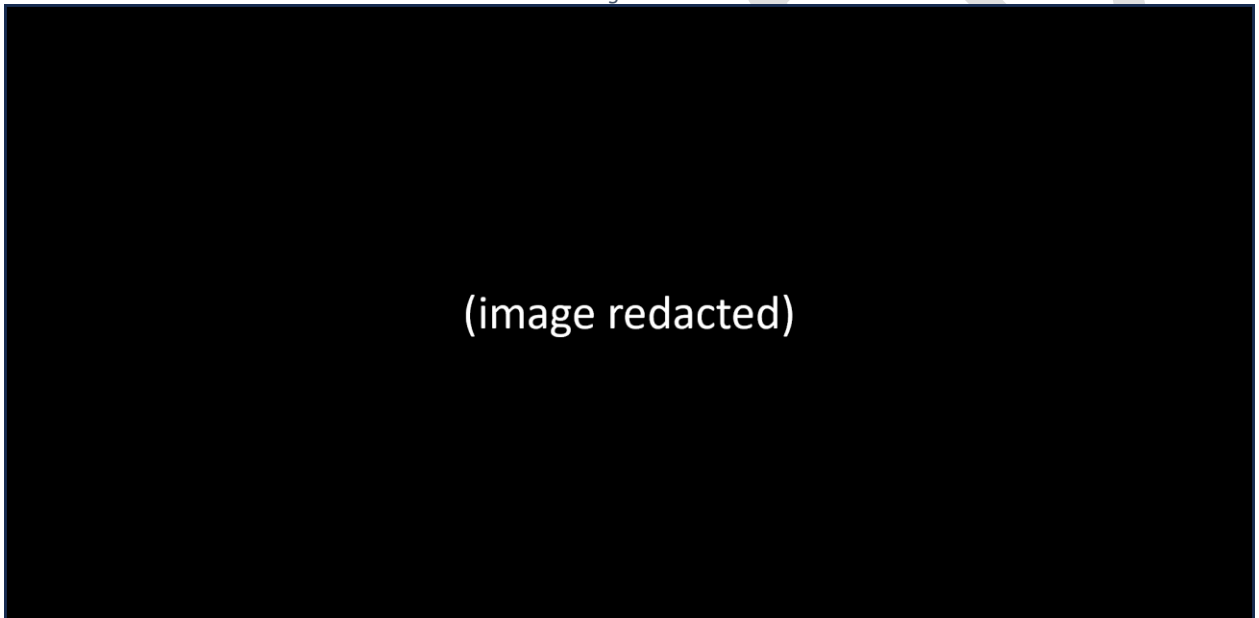
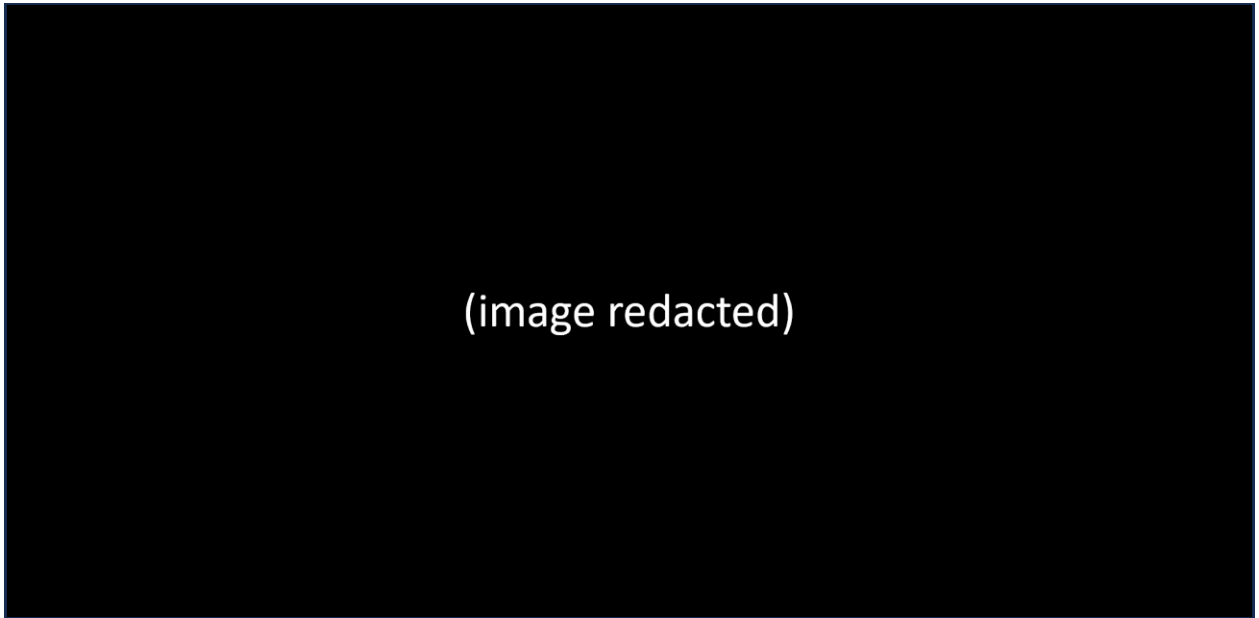
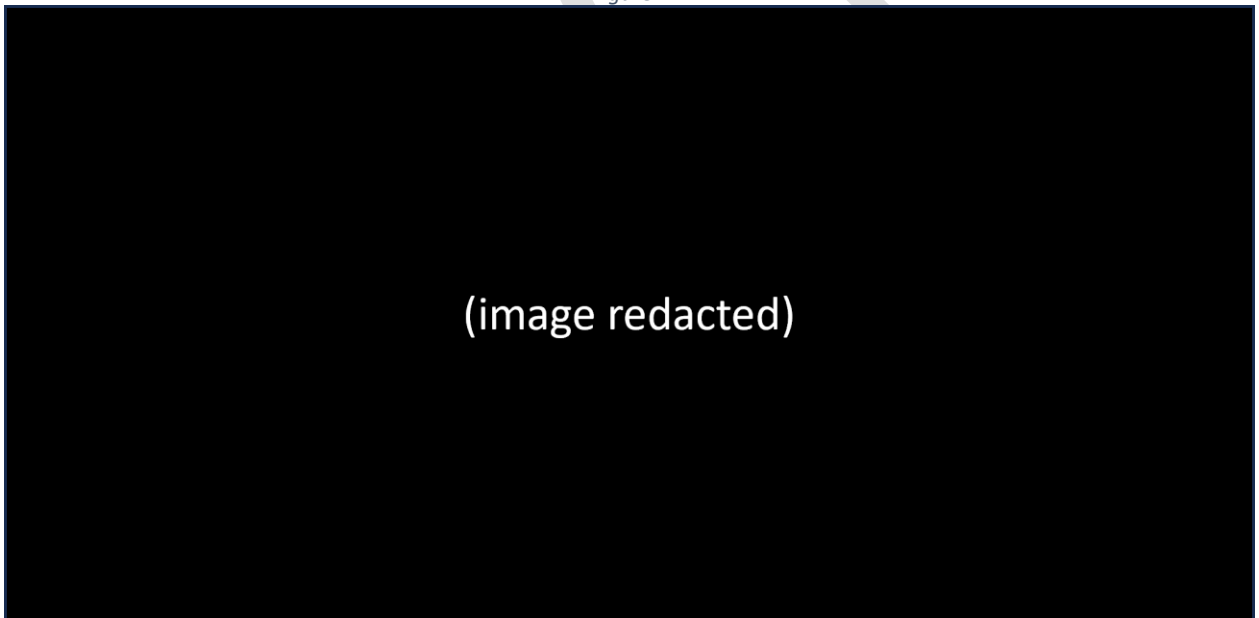


Figure 3



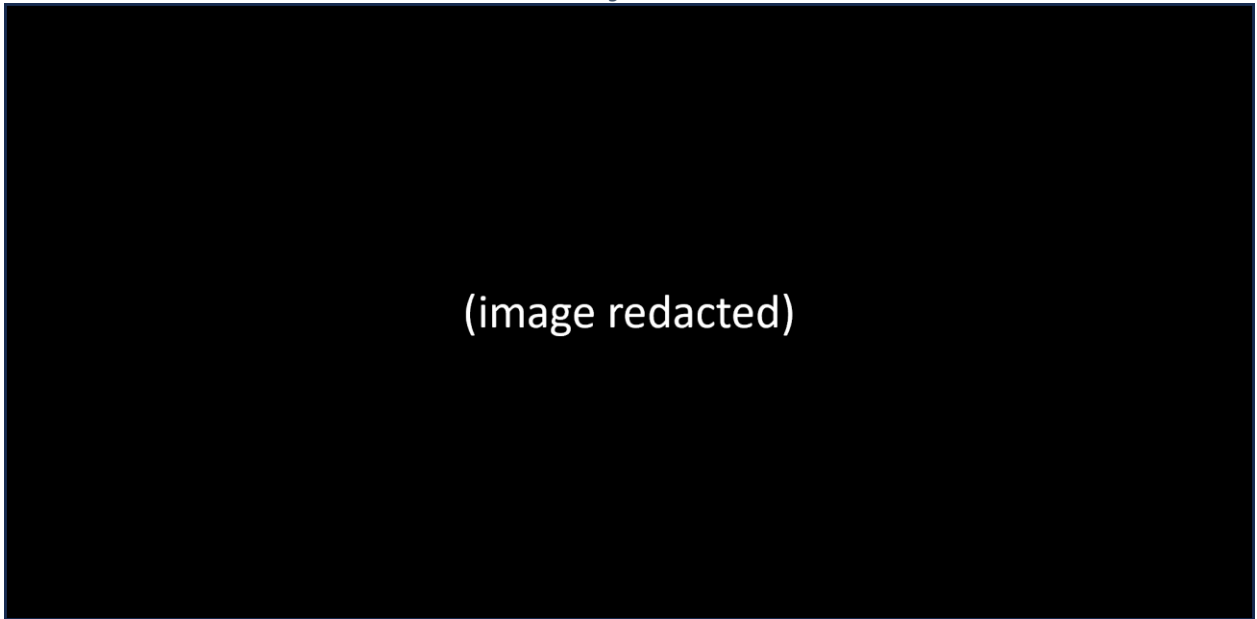
1. If presented, click the *Advanced* button; otherwise, proceed to the next step. (Figure 4)

Figure 4



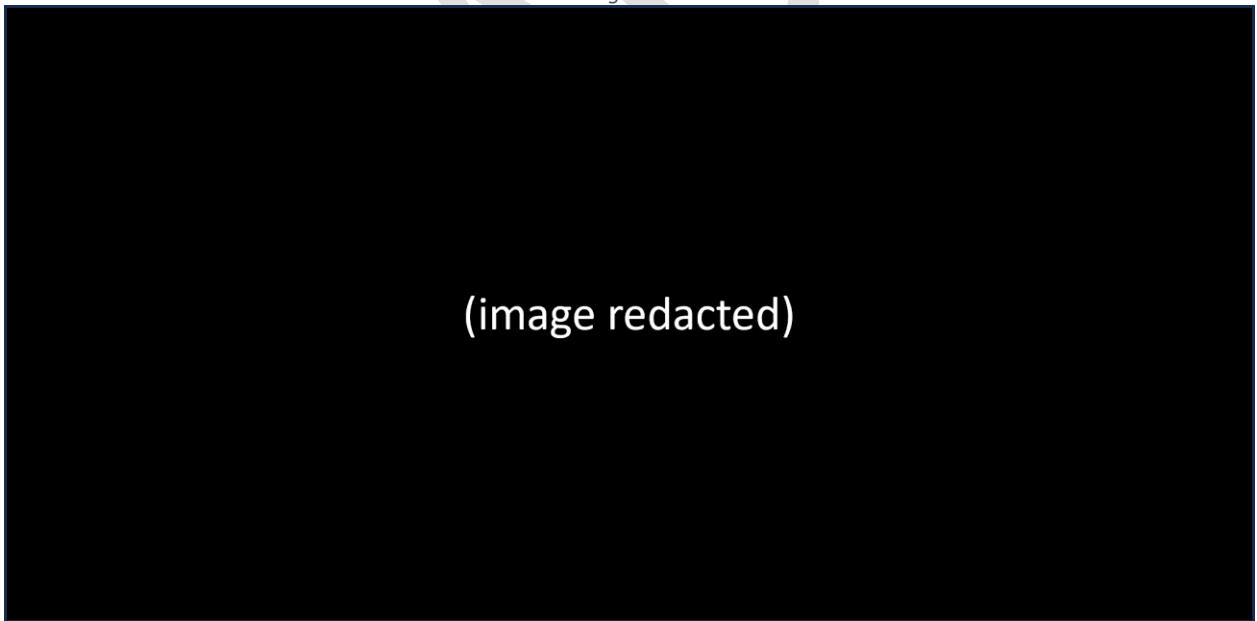
2. If presented, click the [REDACTED] link; otherwise, proceed to the next step. (Figure 5)

Figure 5



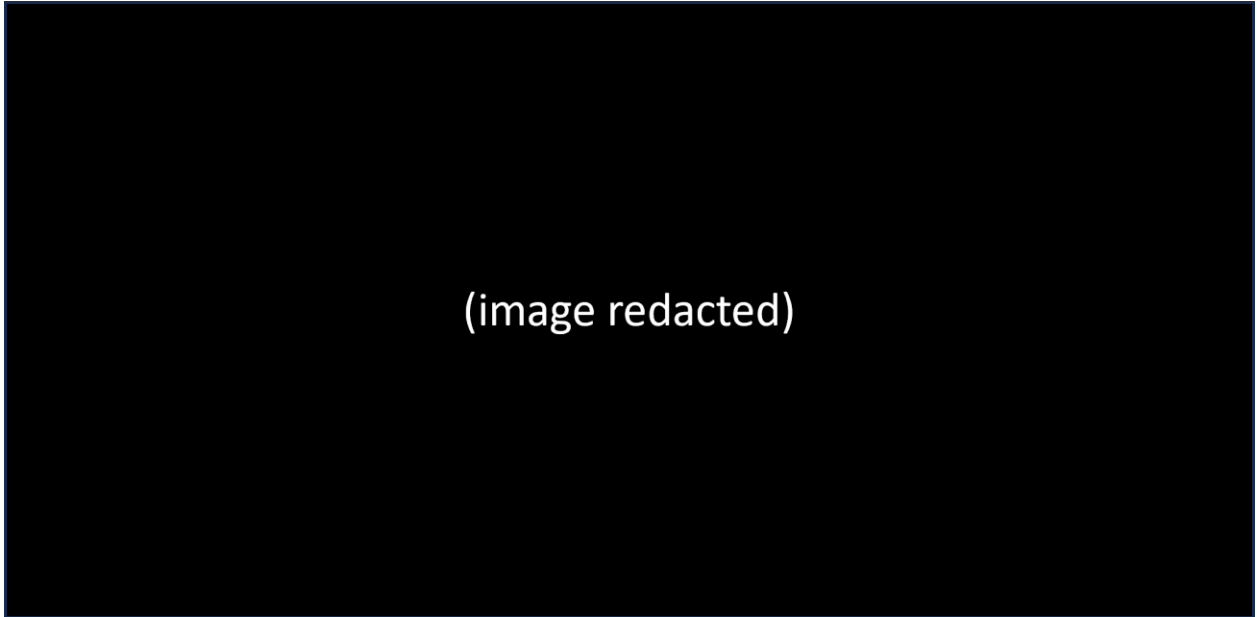
3. Enter your assigned user ID and click the *Next* button. (Figure 6)

Figure 6



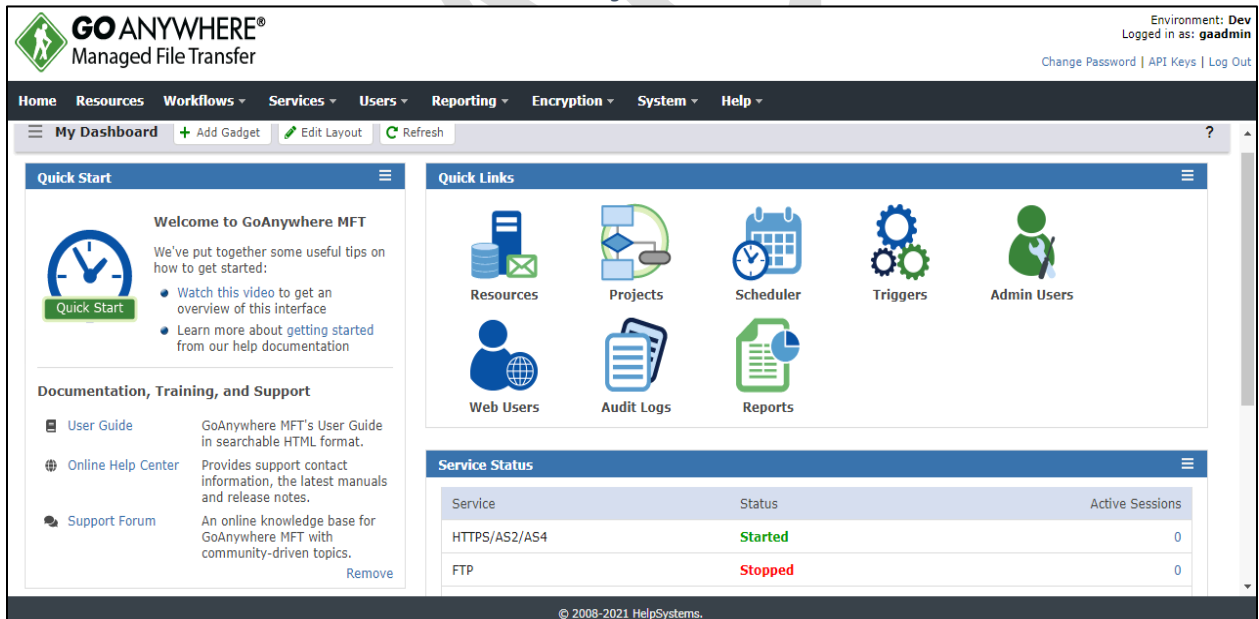
4. Enter your password and click the *Login* button. (Figure 7)

Figure 7



5. If your credentials are valid, you will be taken to the *GoAnywhere MFT Home* page. (Figure 8)

Figure 8



Environment: Dev
Logged in as: gaadmin
Change Password | API Keys | Log Out

Home Resources Workflows Services Users Reporting Encryption System Help

My Dashboard + Add Gadget Edit Layout Refresh

Quick Start

Welcome to GoAnywhere MFT

We've put together some useful tips on how to get started:

- Watch this video to get an overview of this interface
- Learn more about getting started from our help documentation

[Quick Start](#)

Documentation, Training, and Support

- [User Guide](#) GoAnywhere MFT's User Guide in searchable HTML format.
- [Online Help Center](#) Provides support contact information, the latest manuals and release notes.
- [Support Forum](#) An online knowledge base for GoAnywhere MFT with community-driven topics. [Remove](#)

Quick Links

- Resources
- Projects
- Scheduler
- Triggers
- Admin Users
- Web Users
- Audit Logs
- Reports

Service Status

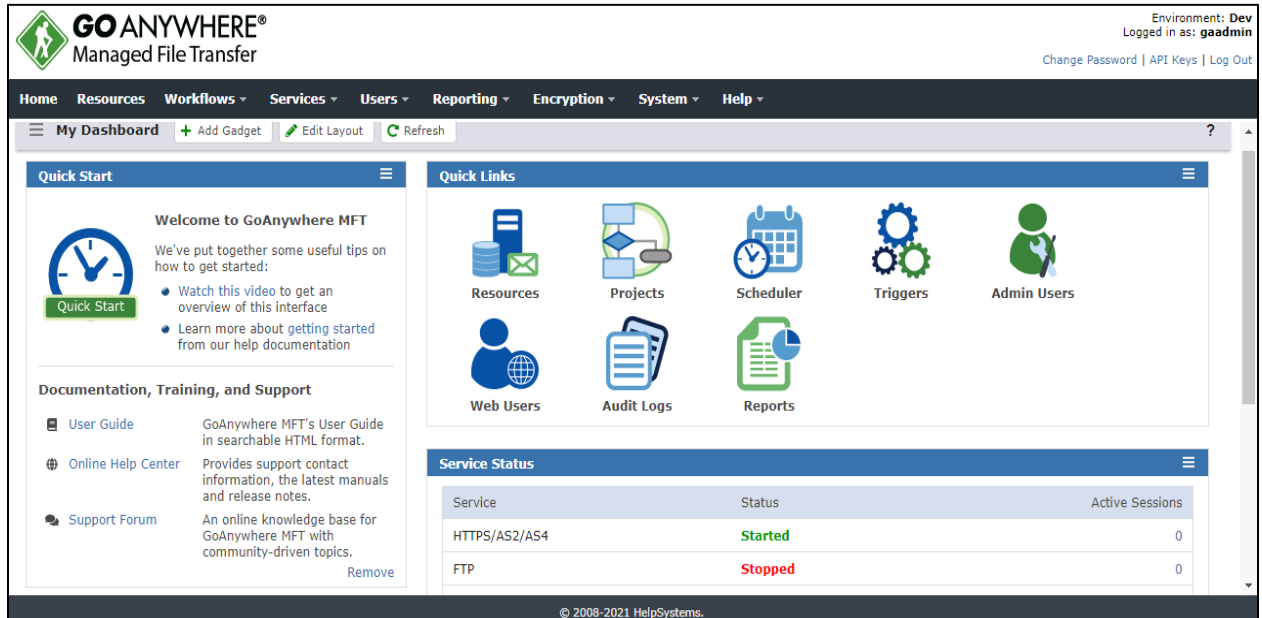
Service	Status	Active Sessions
HTTPS/AS2/AS4	Started	0
FTP	Stopped	0

© 2008-2021 HelpSystems.

The administrator interface

GoAnywhere MFT includes a browser-based administrator interface with a customizable dashboard, advanced graphical components, and drag-and-drop support. The interface is presented upon login (your interface may be arranged differently from the example shown below.) (Figure 9)

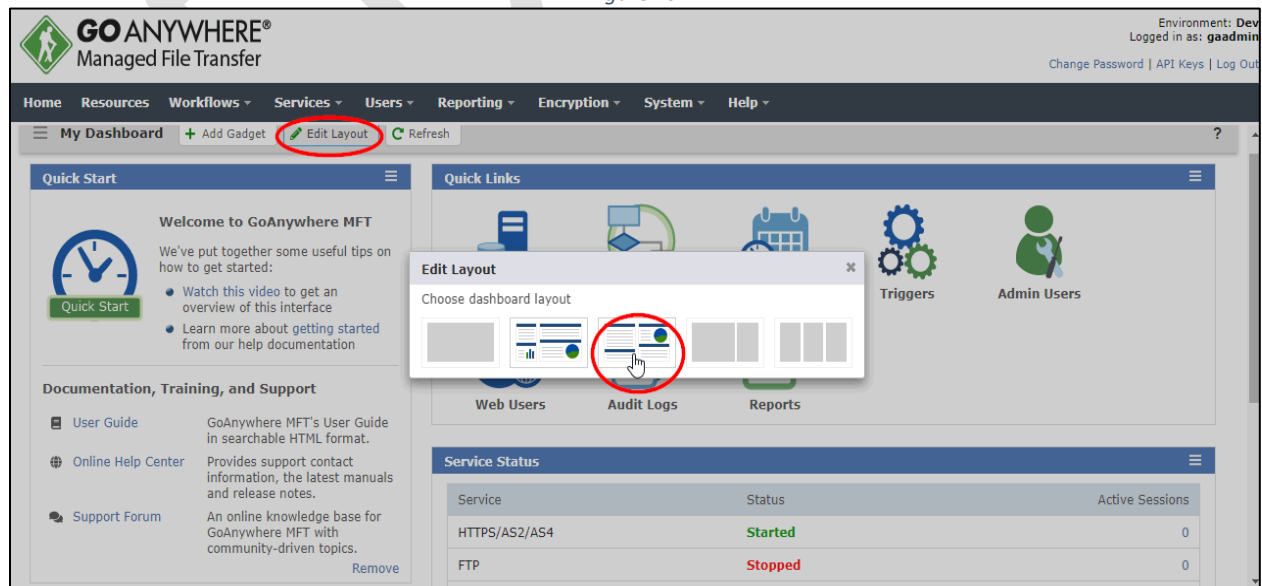
Figure 9



Customizing the administrator interface

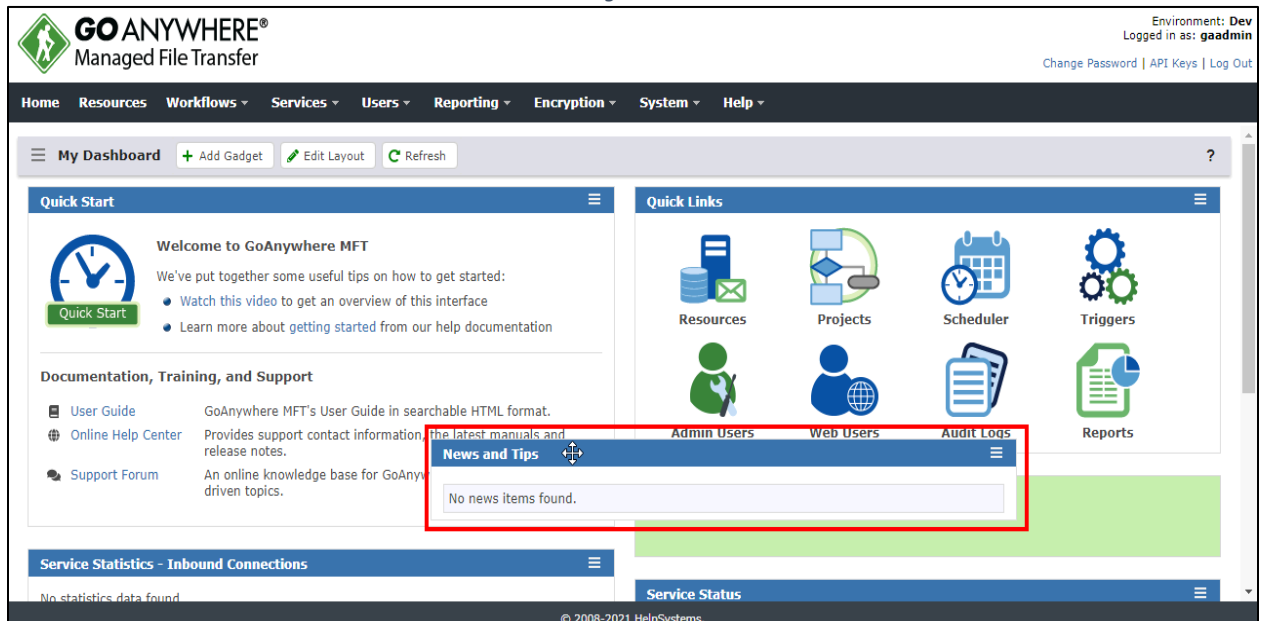
The interface can be customized by first clicking on the *Edit Layout* button and selecting a pre-formatted layout. (Figure 10)

Figure 10



The interface can be further customized by dragging and dropping the individual frames as desired. (Figure 11)

Figure 11



Common *GoAnywhere MFT* Admin Tasks

Typically, there are certain tasks that *GoAnywhere MFT* administrators at [REDACTED] perform more frequently than others. This section addresses those common tasks.

SFTP administration

Configure the SFTP service

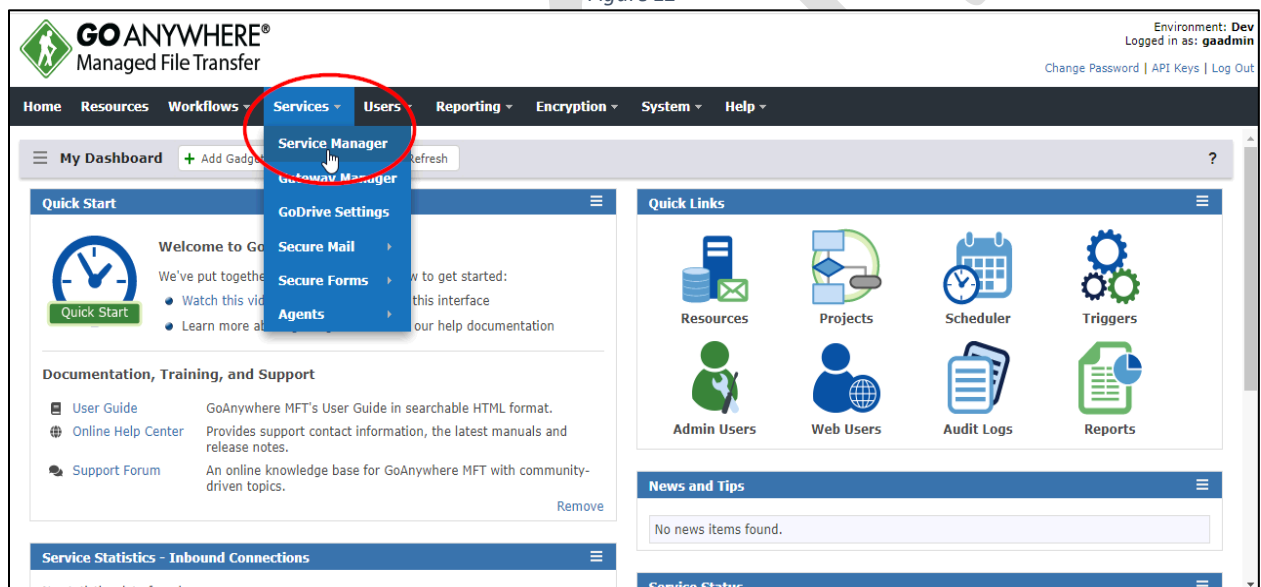
The *SFTP Service Configuration* page provides the configuration options for the *SFTP Service*. From this page, you can modify or add service parameters such as *Login Parameters*, *Port Numbers*, *Listeners*, etc.

1. Log in to *GoAnywhere MFT* as an admin user with the *Product Administrator* role.

Note: If your user account is assigned to a custom admin user role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.

2. From the main menu bar, select *Services > Service Manager*. (Figure 12)

Figure 12



3. Click the action icon (located to the left of *SFTP* in the *Service* column.) (Figure 13)

Figure 13

Environment: Dev
Logged in as: gaadmin
Change Password | API Keys | Log Out

Home Resources Workflows Services Users Reporting Encryption System Help

Service Manager ?

Service	Status	Start Time	Active Sessions
HTTPS/AS2/AS4	Started	01/05/2022 14:19:58	0
FTP	Stopped		0
FTPS	Stopped		0
SFTP	Started	01/05/2022 14:19:59	0
GoFast	Stopped		0
Agents	Started	01/05/2022 14:19:59	1
PeSIT	Stopped		0

4. Select *Edit*. (Figure 14)

Figure 14

Environment: Dev
Logged in as: gaadmin
Change Password | API Keys | Log Out

Home Resources Workflows Services Users Reporting Encryption System Help

Service Manager ?

Service	Status	Start Time	Active Sessions
HTTPS/AS2/AS4	Started	01/05/2022 14:19:58	0
FTP	Stopped		0
FTPS	Stopped		0
SFTP	Started	01/05/2022 14:19:59	0
GoFast	Stopped		0
Agents	Started	01/05/2022 14:19:59	1
PeSIT	Stopped		0

Edit
Stop
Restart

5. From this page you can set or change the *SFTP* configuration elements: (Figure 15)

- Preferences
 - General (Figure 16)
 - Upload Restrictions (Figure 17)
- Server
 - Listener: default (Figure 18)
 - Host Keys (Figure 19)

Clicking any of the above selections will present a form allowing you to change the attributes of that element of the configuration.

Figure 15

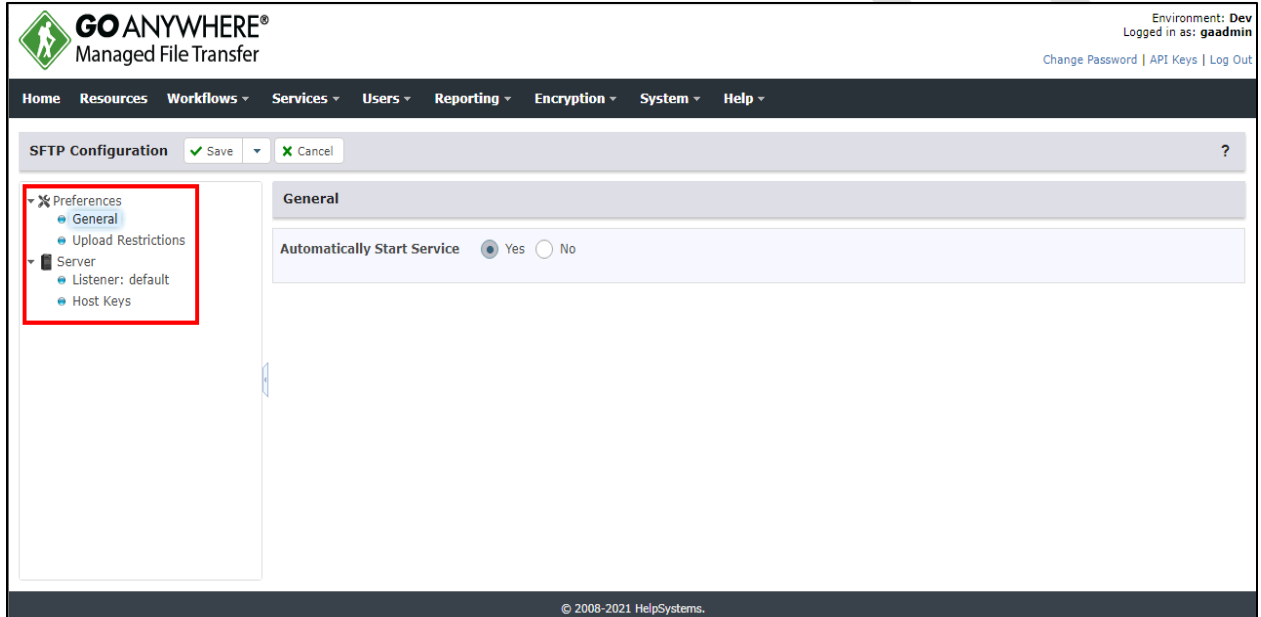


Figure 16

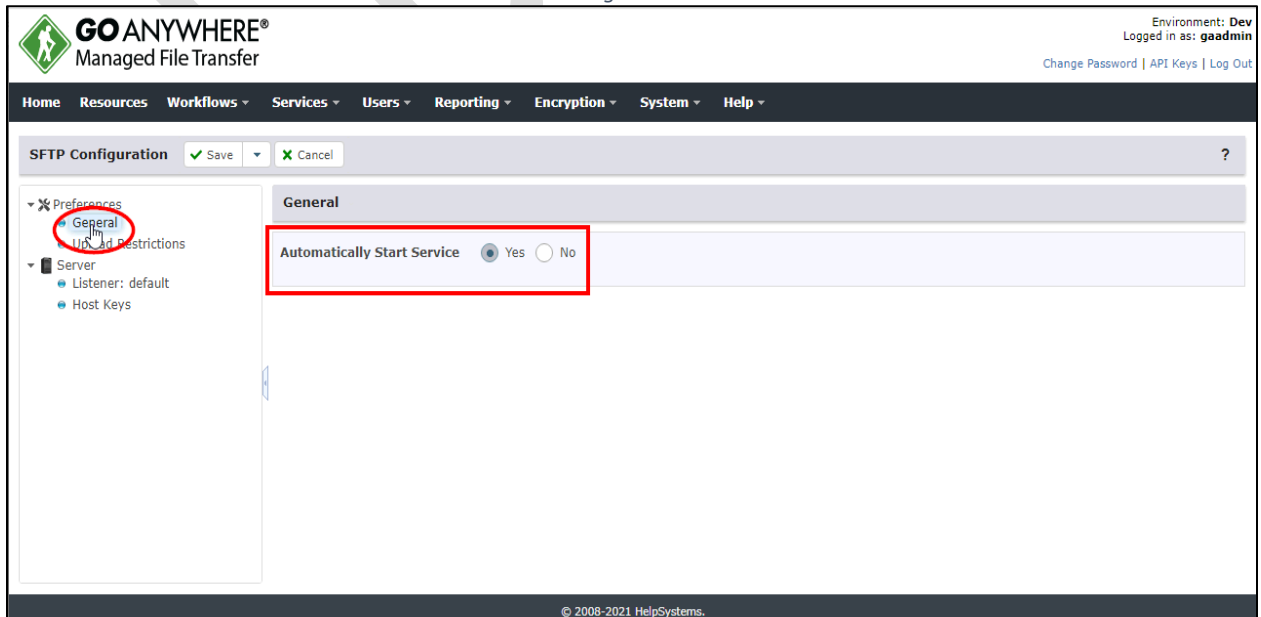


Figure 17

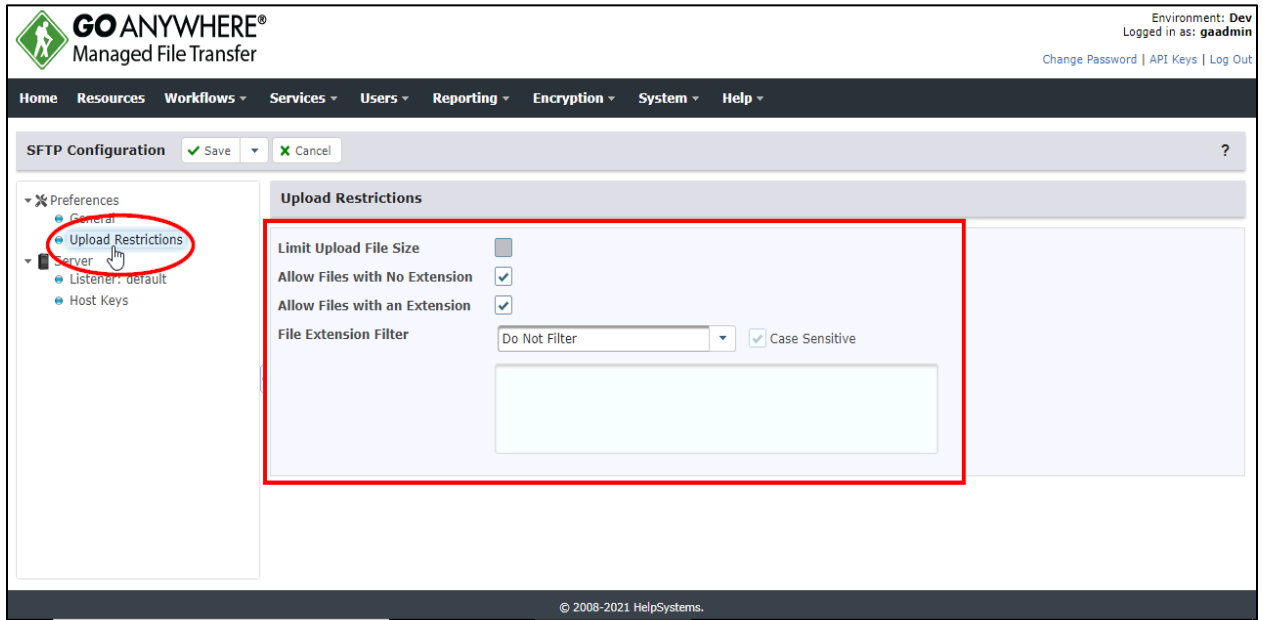


Figure 18

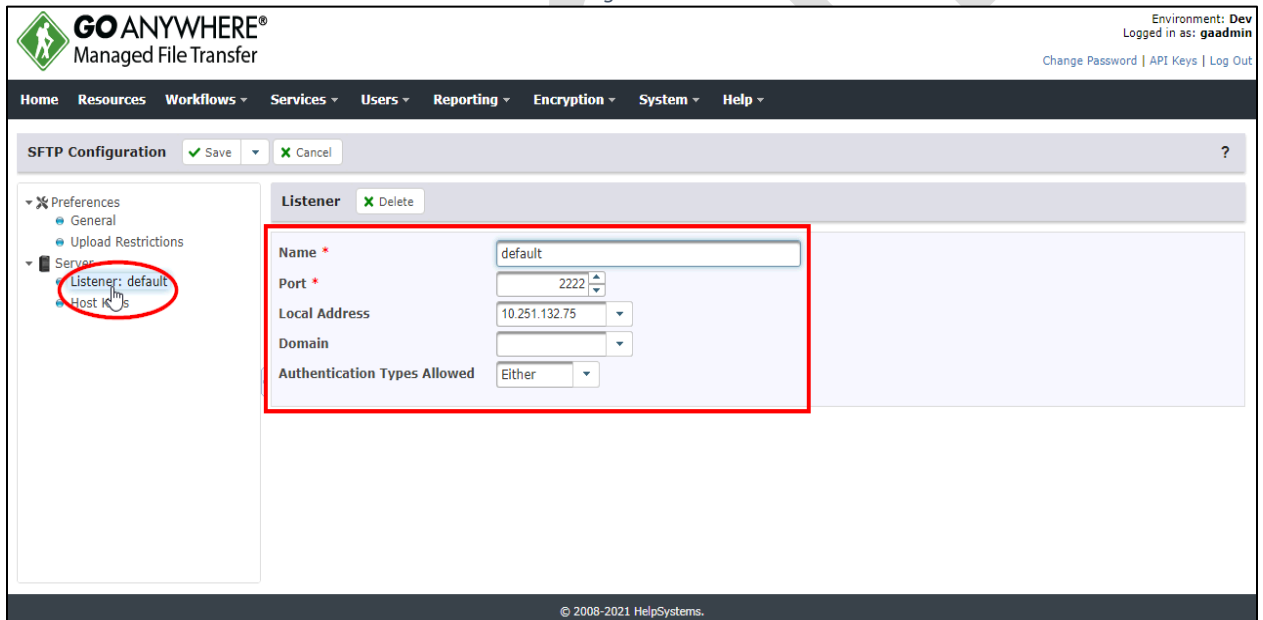
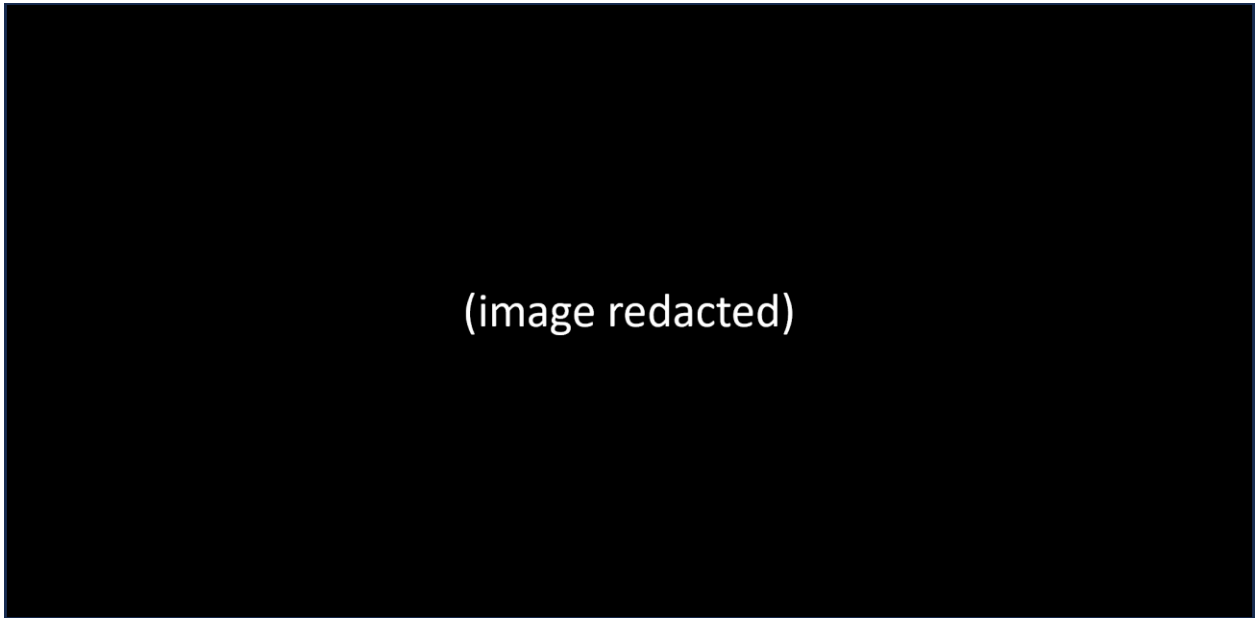
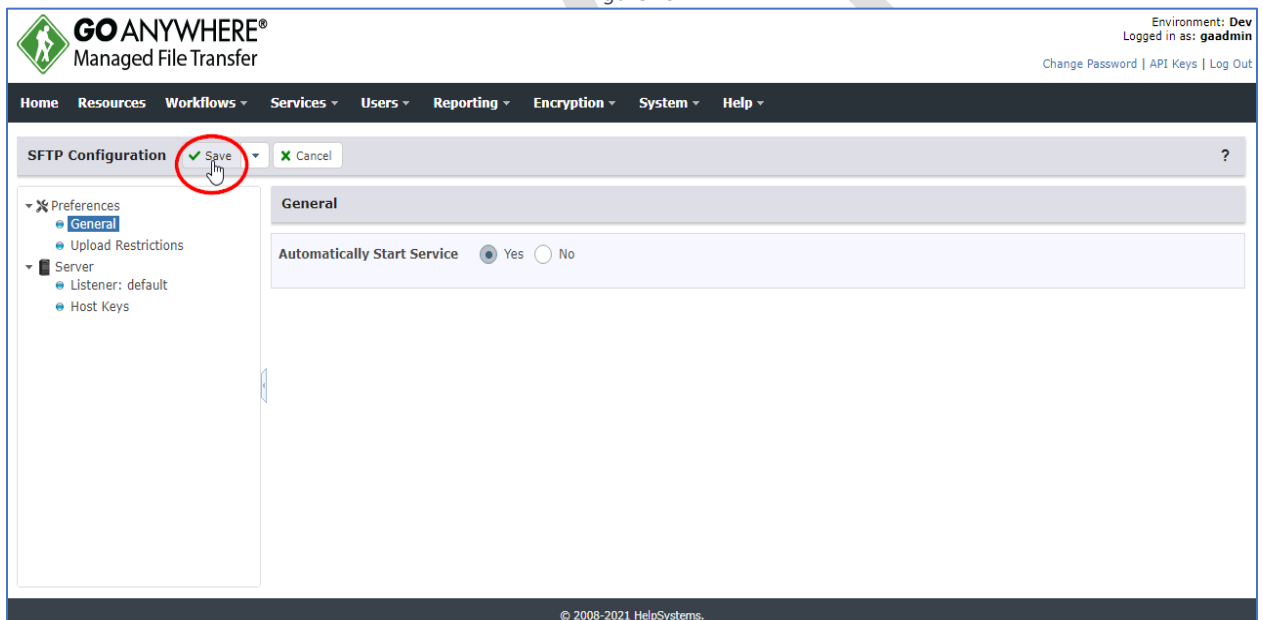


Figure 19



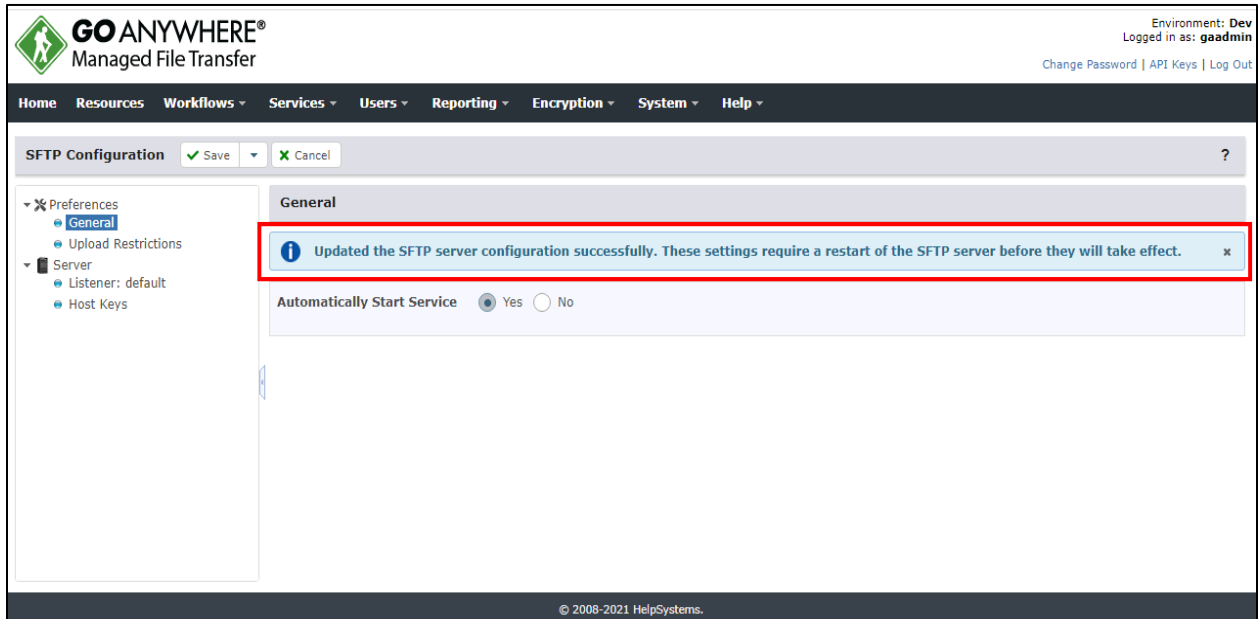
6. Once you have made the desired edits, click the Save button. (Figure 20)

Figure 20



7. Notice that although the edits have been successfully saved, they will not be implemented until after the SFTP server has been restarted. (Figure 21)

Figure 21



SSH key administration

GoAnywhere MFT implements the most current SSH 2.0 protocol standard and includes an integrated key manager for creating and importing SSH public and private keys. The private host keys used by the SFTP server are stored in the *System Key Vault*. Public SSH keys for web user authentication or private keys used for GoAnywhere project tasks should be stored in a key vault associated to a domain.

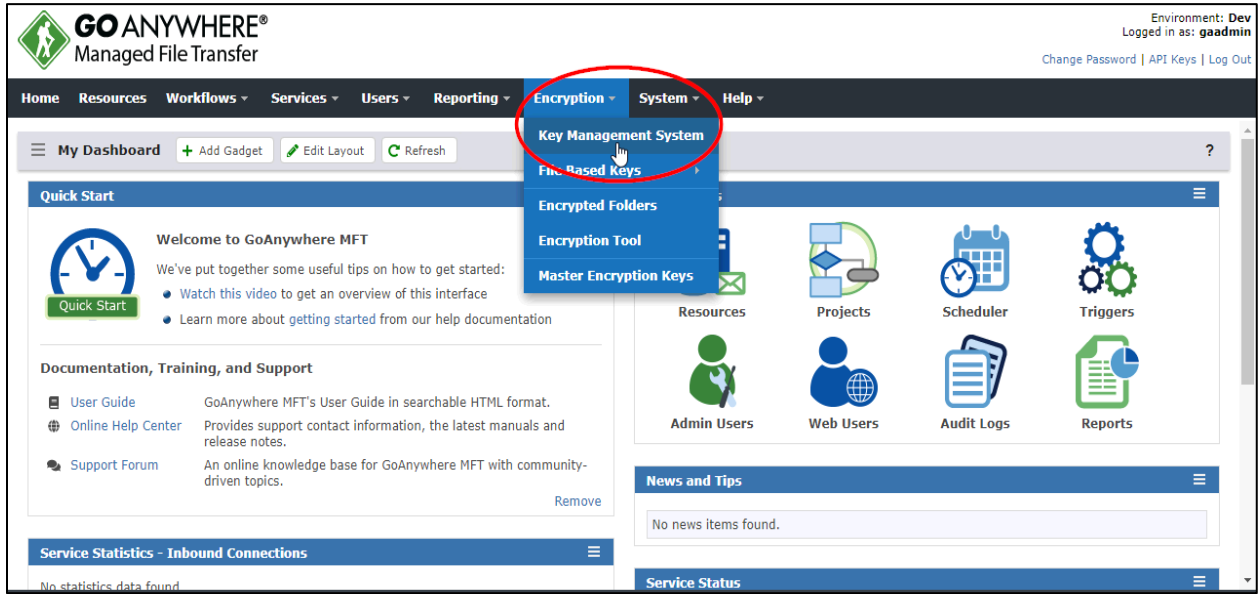
- To manage keys in a **domain's** key vault, log in as an admin user with the Key Manager role.
- To manage keys in the **system** key vault, log in as an admin user with the Product Administrator and Key Manager roles.

Note: If your user account is assigned to a custom admin user role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.

To administer SSH keys, perform the following:

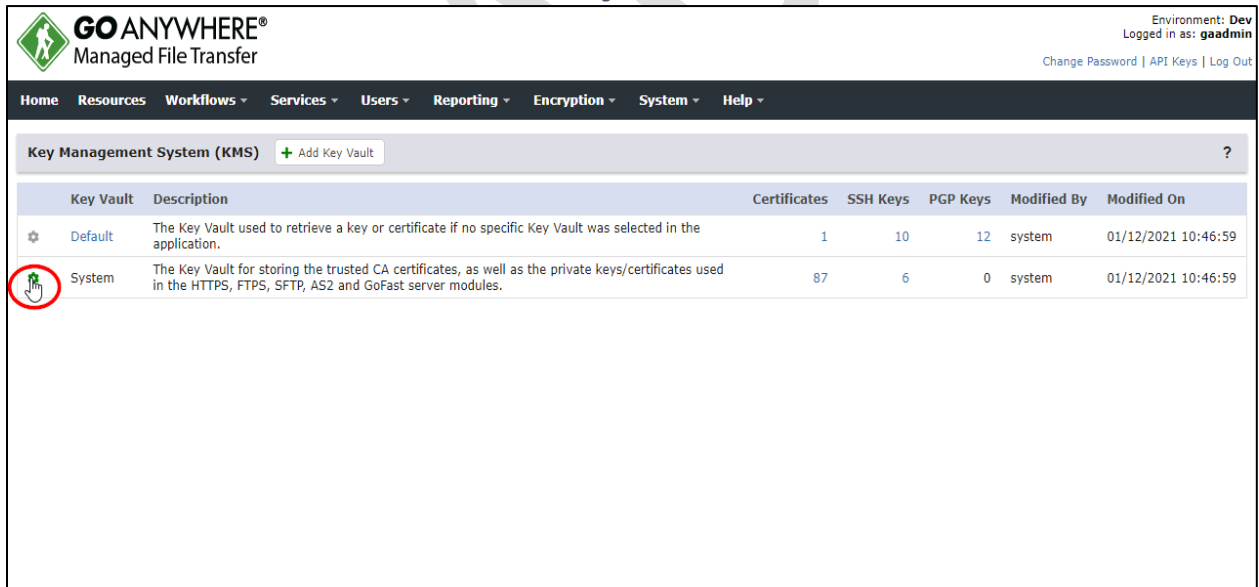
1. From the main menu, select *Encryption* > *Key Management System*. (Figure 22)

Figure 22



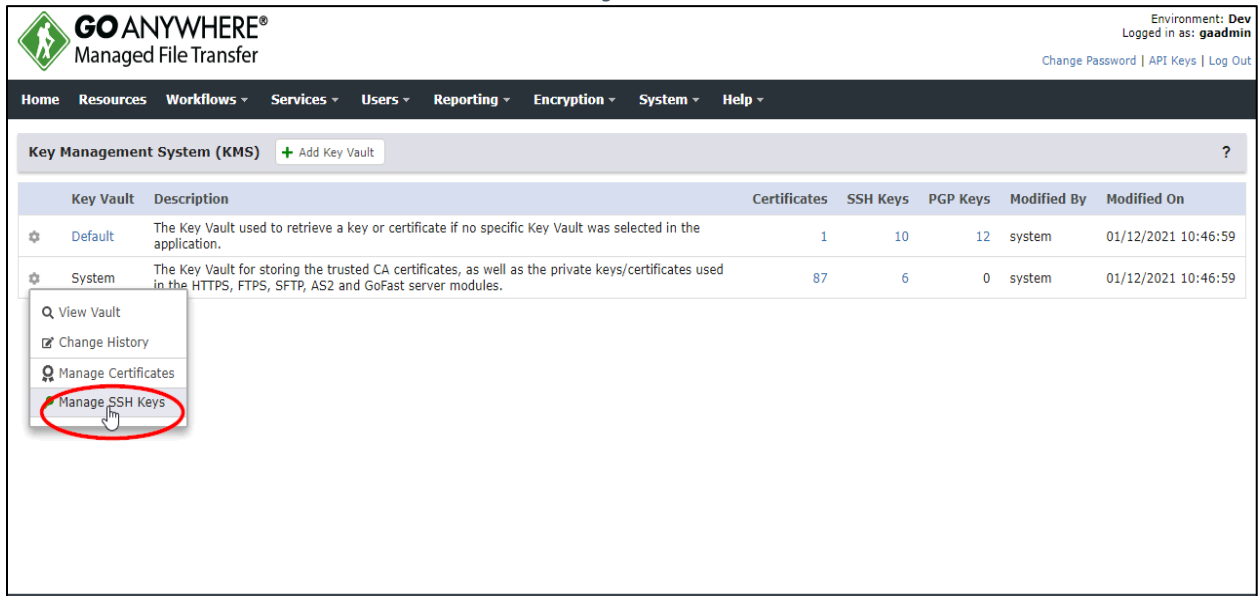
2. When the *Key Management System* appears, click the action icon (located to the left of the *Key Vault* that contains the SSH keys.) (Figure 23)

Figure 23



3. Select *Manage SSH Keys*. (Figure 24)

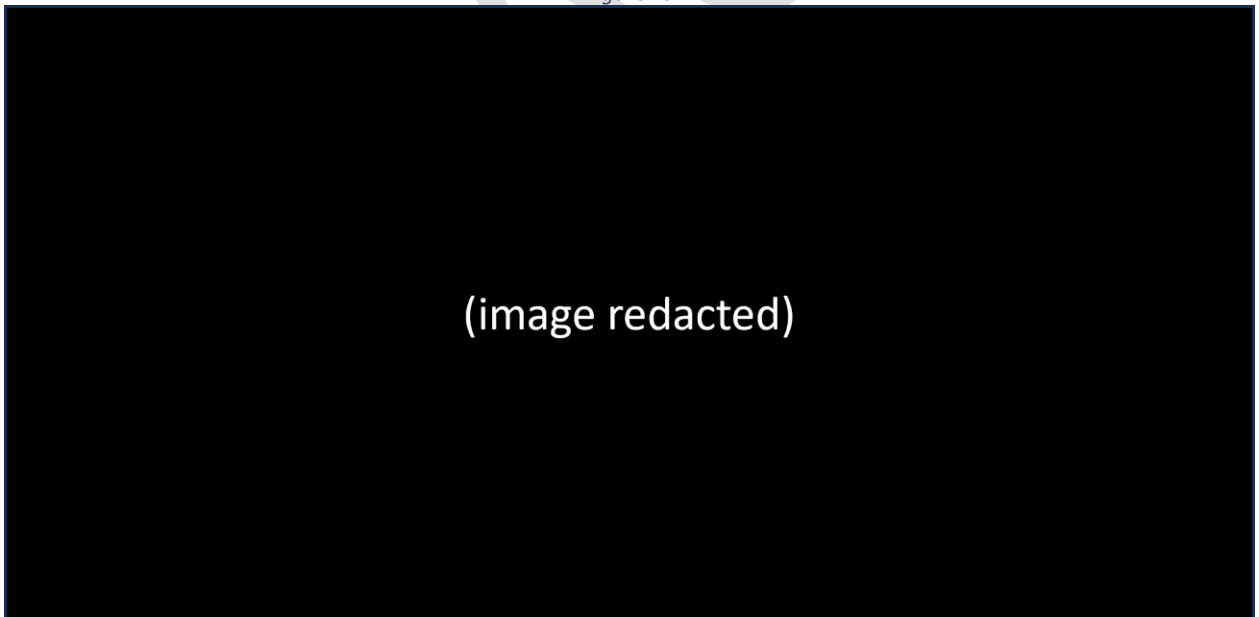
Figure 24



Add key pair

1. On the *SSH Keys* screen, click the *Add Key Pair* button (Figure 25)

Figure 25



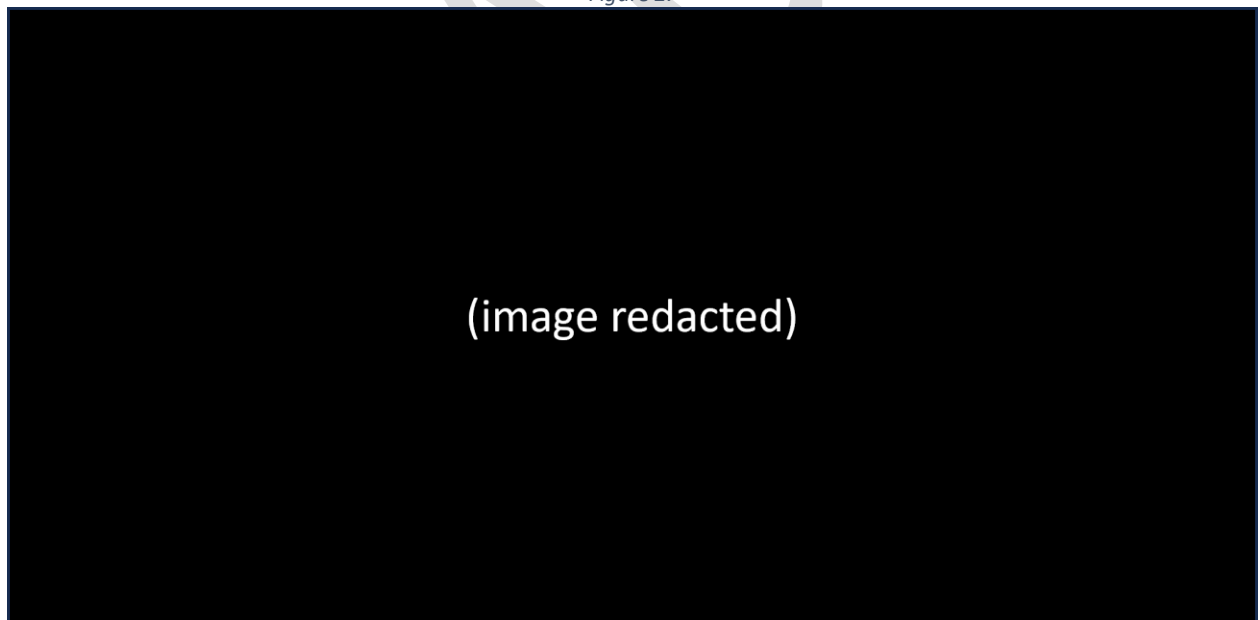
2. After entering the requested information, click the *Save* button. (Figure 26)

Figure 26

The screenshot shows a dialog box titled "Add SSH Key Pair" with a "Save" button circled in red and a "Cancel" button. The form fields are highlighted with a red border. The fields are: Key Vault (System), Name (Demo_Key), Description (This is a test), Algorithm (RSA), Size (2048), Encryption Algorithm (AES128), Password (masked with dots), Confirm Password (masked with dots), Store Password (Yes), and Comments (empty). The dialog box also includes a "Save" button with a checkmark and a "Cancel" button with an 'X'.

3. Notice that a new key pair was successfully created. (Figure 27)

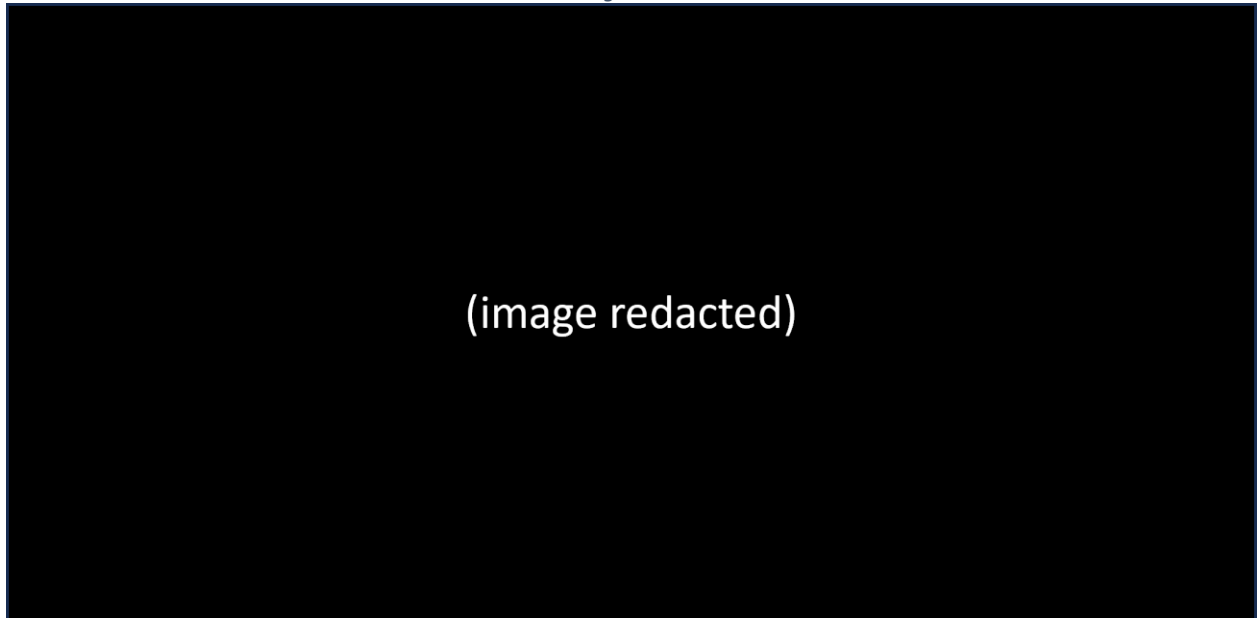
Figure 27



Import public key

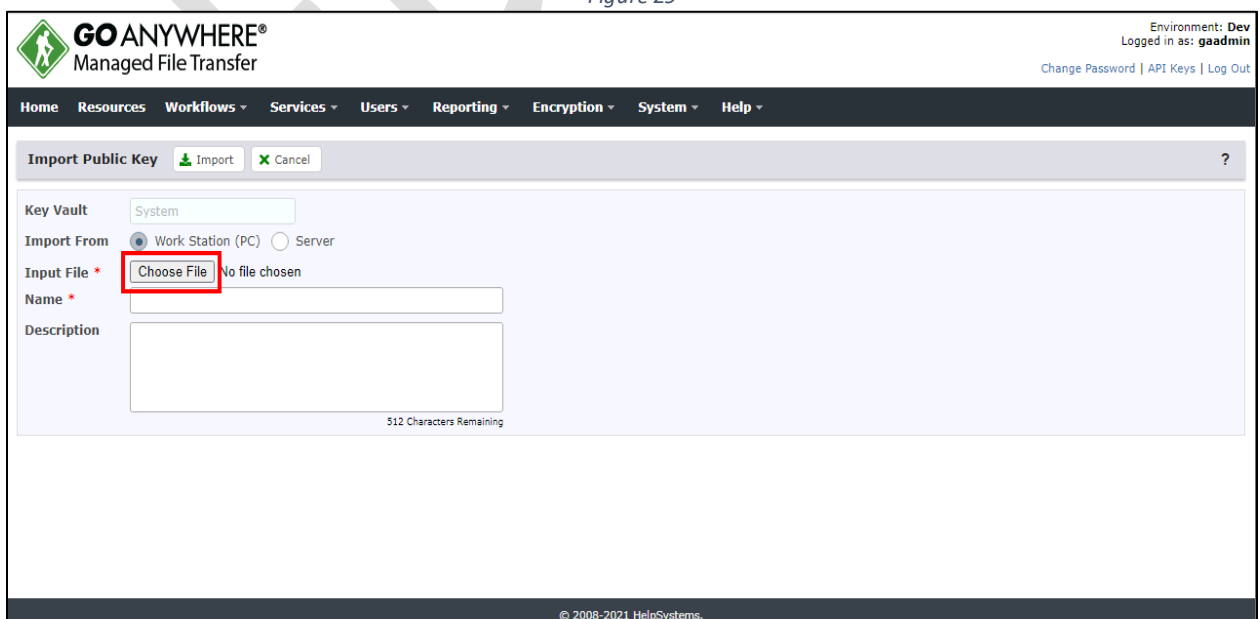
1. On the *SSH Keys* screen, click the *Import Public Key* button (Figure 28)

Figure 28



2. On the *Import Public Key* screen, select the location from which you wish to import a public key.
 - The public key to be imported can be uploaded from one of the two options available (either *Work Station (PC)* or *Server* radio button.)
 - If the *Work Station (PC)* radio button is selected, a button designated as *Choose File* will be displayed. (Figure 29)
 - Clicking this button will allow you to browse the files on your personal work station and select one to be imported.

Figure 29



GO ANYWHERE®
Managed File Transfer

Environment: Dev
Logged in as: gadmin
[Change Password](#) | [API Keys](#) | [Log Out](#)

Home Resources Workflows Services Users Reporting Encryption System Help

Import Public Key Import Cancel ?

Key Vault System

Import From Work Station (PC) Server

Input File * Choose File No file chosen

Name *

Description

512 Characters Remaining

© 2008-2021 HelpSystems.

- If the *Server* radio button is selected, a set of ellipsis points will be displayed. (Figure 30)
- Clicking this ellipsis will allow you to browse the files on the server and select one to be imported.

Figure 30

The screenshot shows the 'Import Public Key' form in the GO ANYWHERE Managed File Transfer application. The form includes a 'Key Vault' dropdown set to 'System', an 'Import From' section with radio buttons for 'Work Station (PC)' and 'Server' (the latter is selected and highlighted with a red box), an 'Input File' field with an ellipsis button (also highlighted with a red box), and fields for 'Name' and 'Description'. The 'Import' and 'Cancel' buttons are at the top. The footer shows '© 2008-2021 HelpSystems.' and the user is logged in as 'gadmin' in a 'Dev' environment.

3. Once the location from which you wish to import a public key has been selected (either *Work Station (PC)* or *Server* radio button), click the *Import* button. (Figure 31)

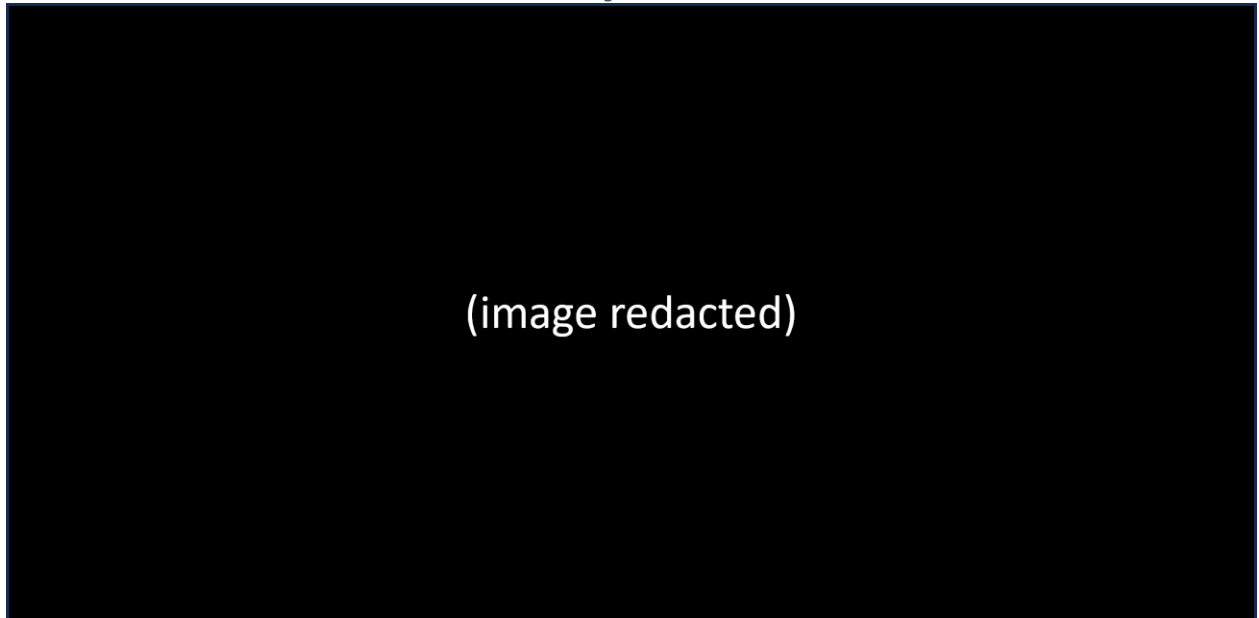
Figure 31

The screenshot shows the 'Import Public Key' form in the GO ANYWHERE Managed File Transfer application. The 'Import' button is highlighted with a red circle, and the 'Server' radio button is highlighted with a red box. The form includes a 'Key Vault' dropdown set to 'System', an 'Import From' section with radio buttons for 'Work Station (PC)' and 'Server' (the latter is selected and highlighted with a red box), an 'Input File' field with an ellipsis button, and fields for 'Name' and 'Description'. The 'Import' and 'Cancel' buttons are at the top. The footer shows '© 2008-2021 HelpSystems.' and the user is logged in as 'gadmin' in a 'Dev' environment.

Import private key

1. On the *SSH Keys* screen, click the *Import Private Key* button (Figure 32)

Figure 32



2. On the *Import Private Key* screen, select the location from which you wish to import a private key.
 - The private key to be imported can be uploaded from one of the two options available (either *Work Station (PC)* or *Server* radio button.)
 - If the *Work Station (PC)* radio button is selected, a button designated as *Choose File* will be displayed. (Figure 33)
 - Clicking this button will allow you to browse the files on your personal work station and select one to be imported.

Figure 33

Environment: Dev
Logged in as: gaadmin
Change Password | API Keys | Log Out

Home Resources Workflows Services Users Reporting Encryption System Help

Import Private Key Import Cancel

Key Vault System

Import From Work Station (PC) Server

Input File * Choose File No file chosen

Password

Store Password Yes

Name *

Description

512 Characters Remaining

© 2008-2021 HelpSystems.

- If the *Server* radio button is selected, a set of ellipsis points will be displayed. (Figure 34)
- Clicking this ellipsis will allow you to browse the files on the server and select one to be imported.

Figure 34

The screenshot shows the 'Import Private Key' form in the GO ANYWHERE Managed File Transfer interface. The form includes the following fields and controls:

- Key Vault:** A dropdown menu set to 'System'.
- Import From:** Two radio buttons: 'Work Station (PC)' (unselected) and 'Server' (selected).
- Input File *:** A text input field with an ellipsis button (three dots) to its right, which is highlighted with a red box.
- Password:** A text input field.
- Store Password:** A dropdown menu set to 'Yes'.
- Name *:** A text input field.
- Description:** A large text area.
- Footer:** '© 2008-2021 HelpSystems.' and '512 Characters Remaining'.

3. Once the location from which you wish to import a private key has been selected (either *Work Station (PC)* or *Server* radio button), click the *Import* button. (Figure 35)

Figure 35

The screenshot shows the 'Import Private Key' form in the GO ANYWHERE Managed File Transfer interface. The form includes the following fields and controls:

- Key Vault:** A dropdown menu set to 'System'.
- Import From:** Two radio buttons: 'Work Station (PC)' (unselected) and 'Server' (selected). The 'Server' radio button is highlighted with a red box.
- Input File *:** A text input field with an ellipsis button (three dots) to its right.
- Password:** A text input field.
- Store Password:** A dropdown menu set to 'Yes'.
- Name *:** A text input field.
- Description:** A large text area.
- Footer:** '© 2008-2021 HelpSystems.' and '512 Characters Remaining'.

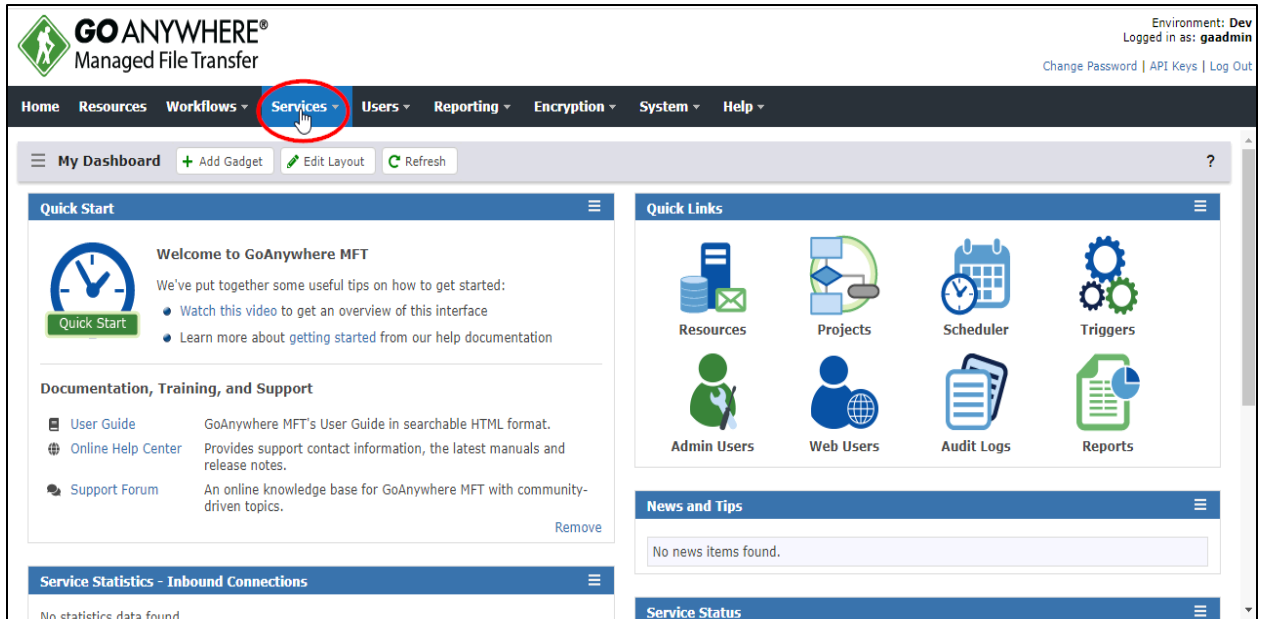
In this screenshot, the 'Import' button (a green arrow icon) is highlighted with a red circle, and the 'Server' radio button is highlighted with a red box.

Gateway administration

Start / Stop a gateway

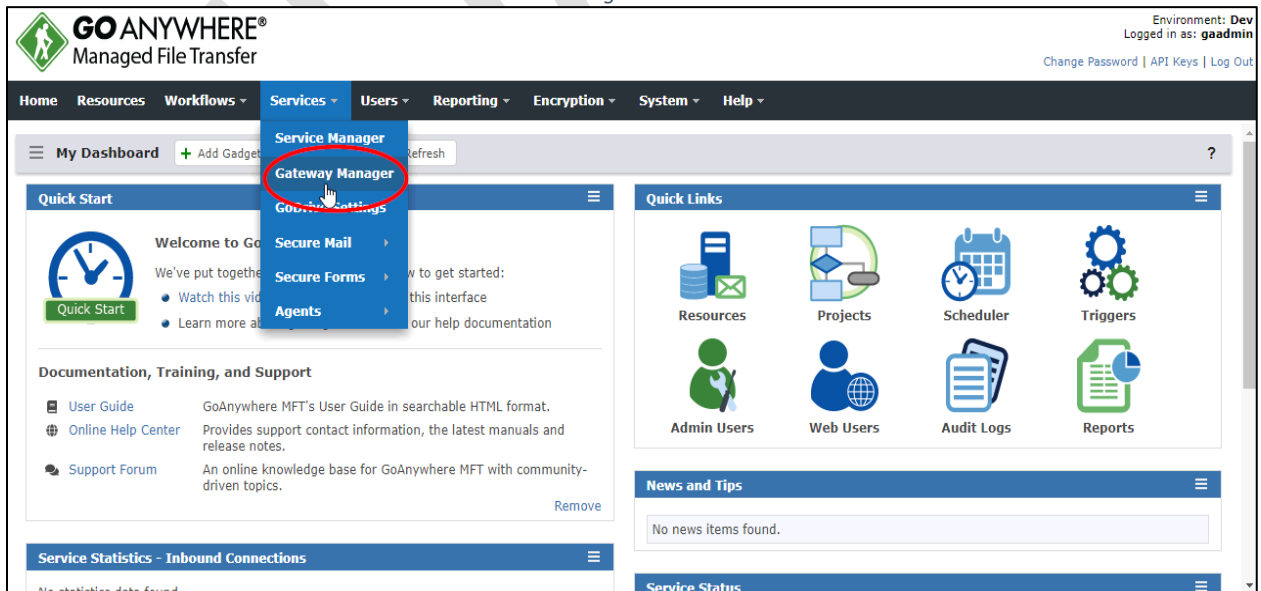
1. From the main menu, select the *Services* tab. (Figure 36)

Figure 36



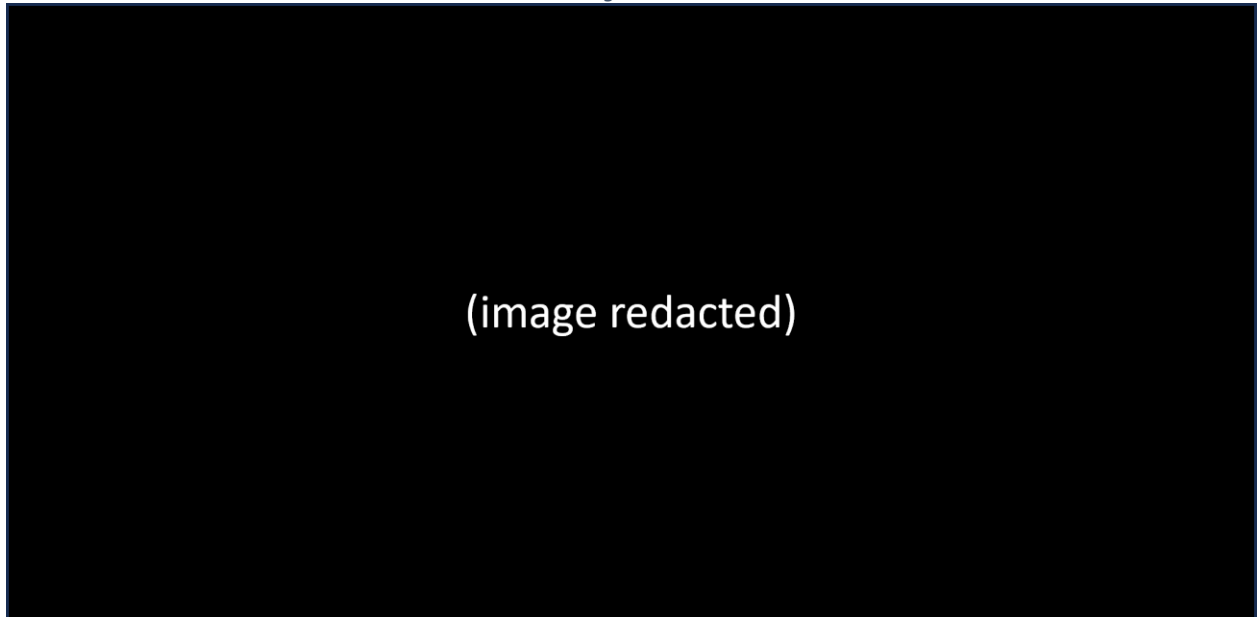
2. Select *Gateway Manager*. (Figure 37)

Figure 37



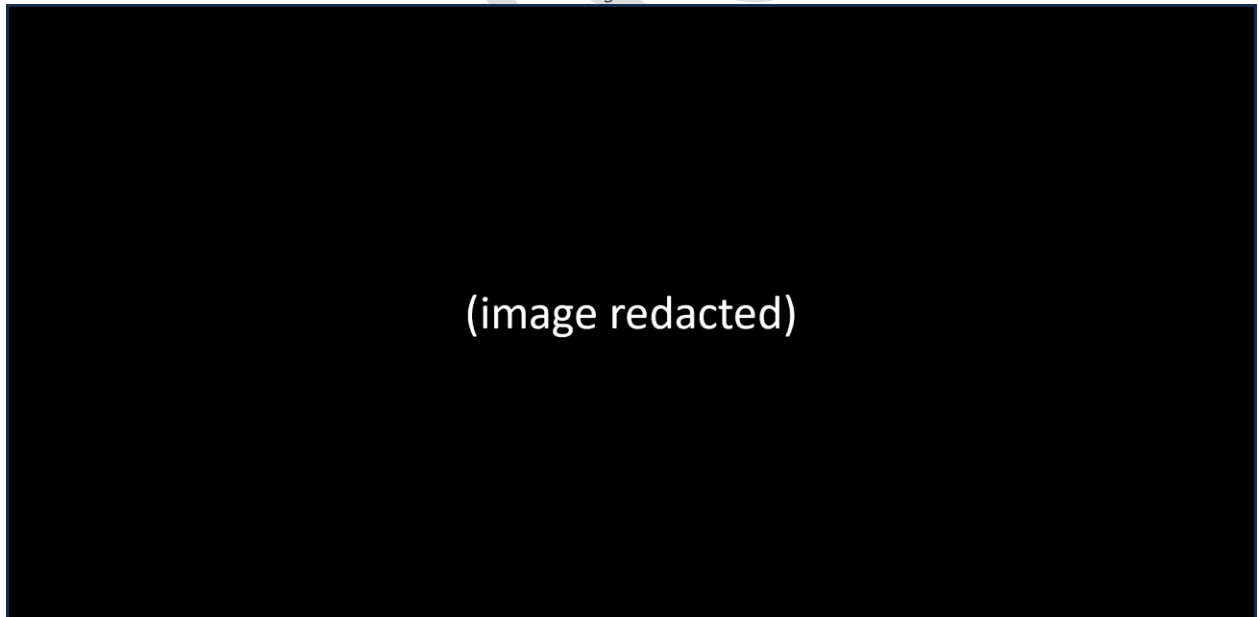
3. The current list of gateways is displayed. (Figure 38)

Figure 38



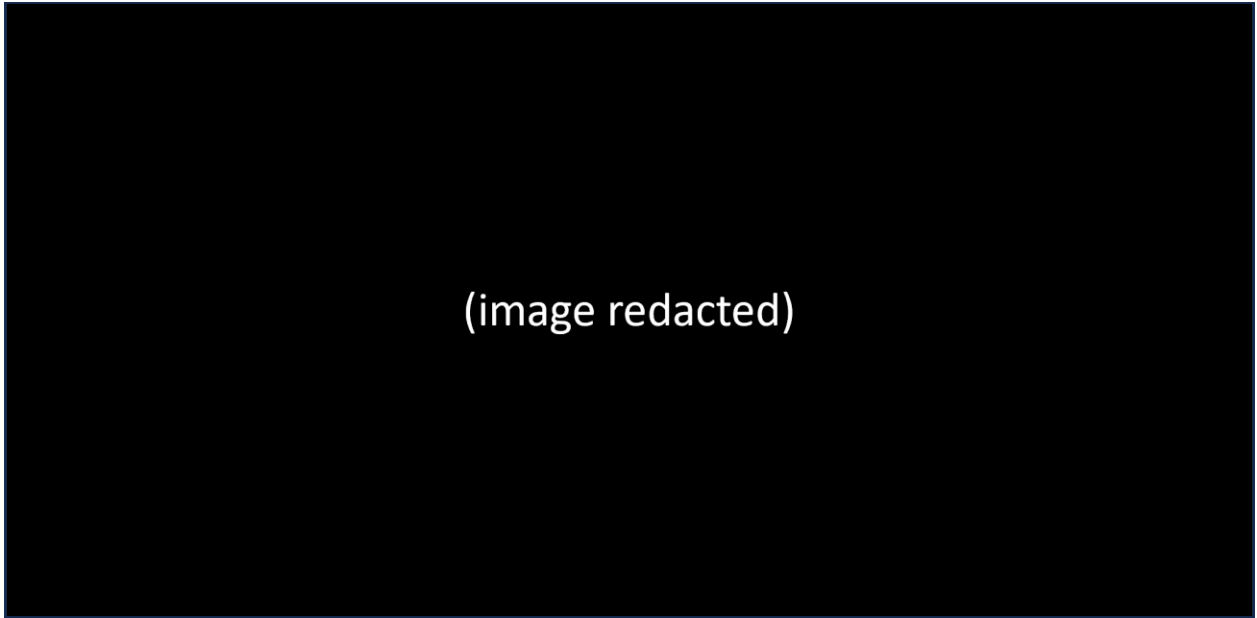
4. If *Enabled* is currently set to "Yes", then hovering over the icon located to the left of the controller address will display a "Stop" tooltip which can be clicked to disconnect (i.e., disable) the gateway. (Figure 39)

Figure 39



5. If *Enabled* is currently set to “No”, then hovering over the icon located to the left of the controller address will display a “Start” tooltip which can be clicked to connect (i.e., enable) the gateway. (Figure 40)

Figure 40



Log file monitoring

One of the responsibilities of a [REDACTED] *GoAnywhere MFT* administrator is to monitor the file logs for any adverse occurrences requiring further investigation.

Log Settings

Enabling Tamper-Evident Logging

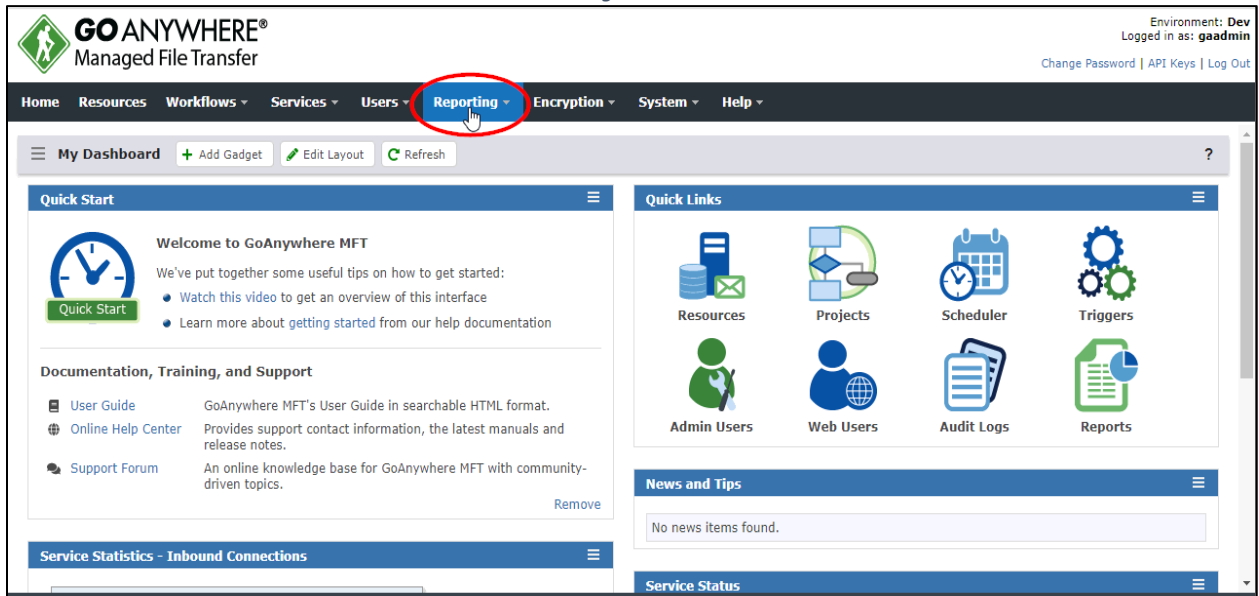
The *Log Settings* page provides central control over all log settings in *GoAnywhere MFT*. The log settings for each service and function within *GoAnywhere MFT* can be configured on the respective tab.

To administer logs, you must be logged in as an admin user with the Product Administrator role.

Note: If your user account is assigned to a custom admin user role, your ability to view, modify, or execute actions are based on the permissions specified for that role.

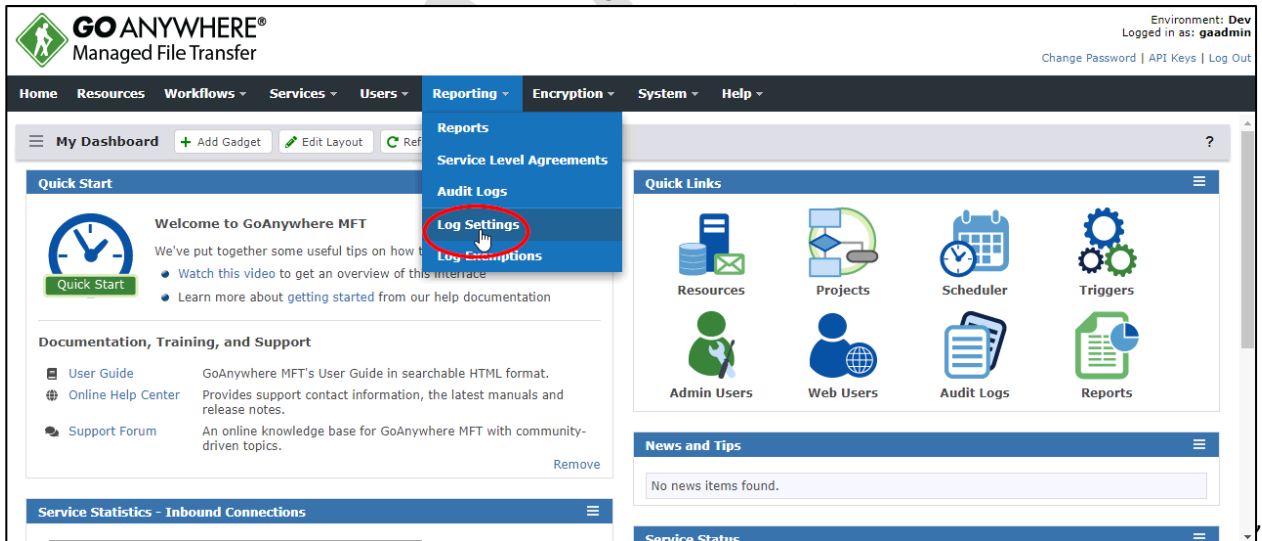
1. From the main menu bar, select the *Reporting* tab. (Figure 41)

Figure 41



2. Select *Log Settings*. (Figure 42)

Figure 42



3. Within the *General* tab, ensure that the *Tamper-Evident Logging Enabled* box is checked. (Figure 43)

Figure 43

The screenshot shows the 'Log Settings' page for 'GO ANYWHERE Managed File Transfer'. The 'General' tab is selected and highlighted with a red box. The 'Tamper-Evident Logging Enabled' checkbox is checked and also highlighted with a red box. Other settings include 'Logs Directory' set to '/mft/logs', 'Default Search Date Range' set to 'Last 7 Days', 'Log Level' set to 'Normal', 'Log File Extension' set to '.log', and 'Maximum Log Size' set to '5 MB'. The page includes a navigation menu at the top, a user login status in the top right, and a copyright notice at the bottom.

Environment: Dev
Logged in as: gadmin
Change Password | API Keys | Log Out

Home Resources Workflows Services Users Reporting Encryption System Help

Log Settings Save Cancel ?

General Syslog Job Logs Services Secure Mail Secure Forms GoDrive Triggers Administration Service Level Agreements

Logs Directory * /mft/logs

Default Search Date Range * Last 7 Days

Tamper-Evident Logging Enabled

Global Log

Log Level Normal

Log File Extension * .log

Maximum Log Size * 5 MB

© 2008-2021 HelpSystems.

Interpreting Tamper-Evident Logging

When a log event is recorded, a checksum value is assigned to the entry for validating the record's accuracy at a later time.

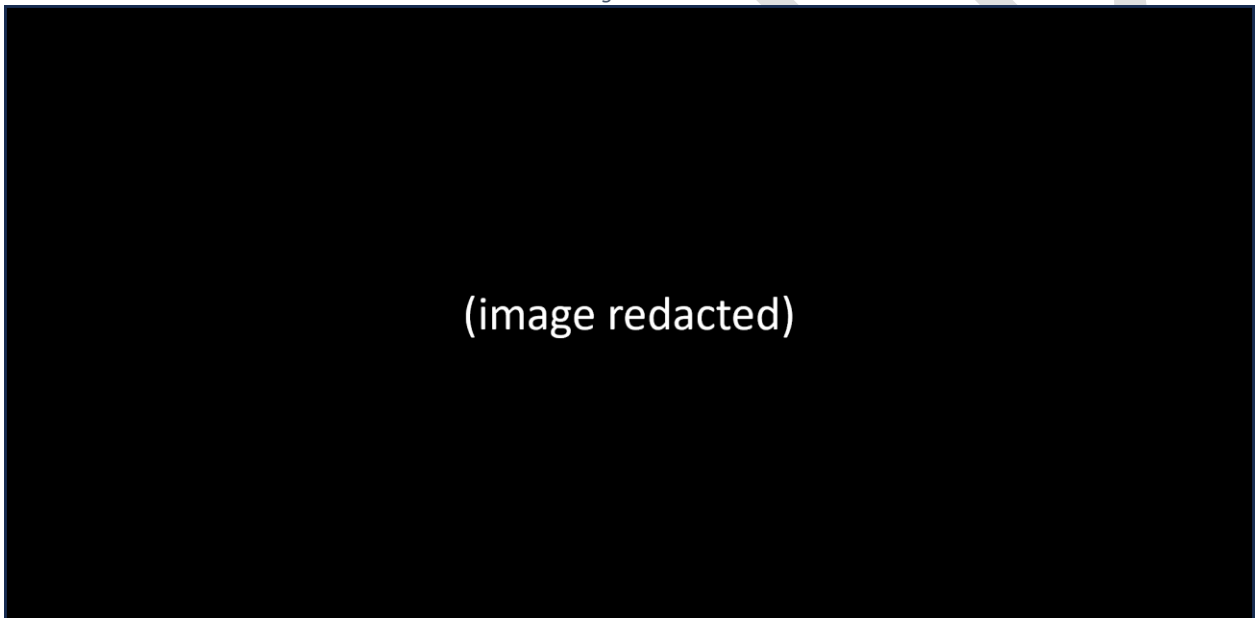
If *Tamper-Evident Logging* is enabled in *Log Settings*, log entries on this page will reflect external alterations to the record or checksum. The state of the log entry is indicated by the following color code: (Figure 44)

White: No tampering evident.

Yellow: The log entry checksum is missing, and the entry cannot be validated, which may indicate log tampering has occurred. Events logged prior to enabling *Tamper-Evident Logging* will not have a checksum value and will be highlighted.

Red: Log tampering has occurred; the data was modified.

Figure 44



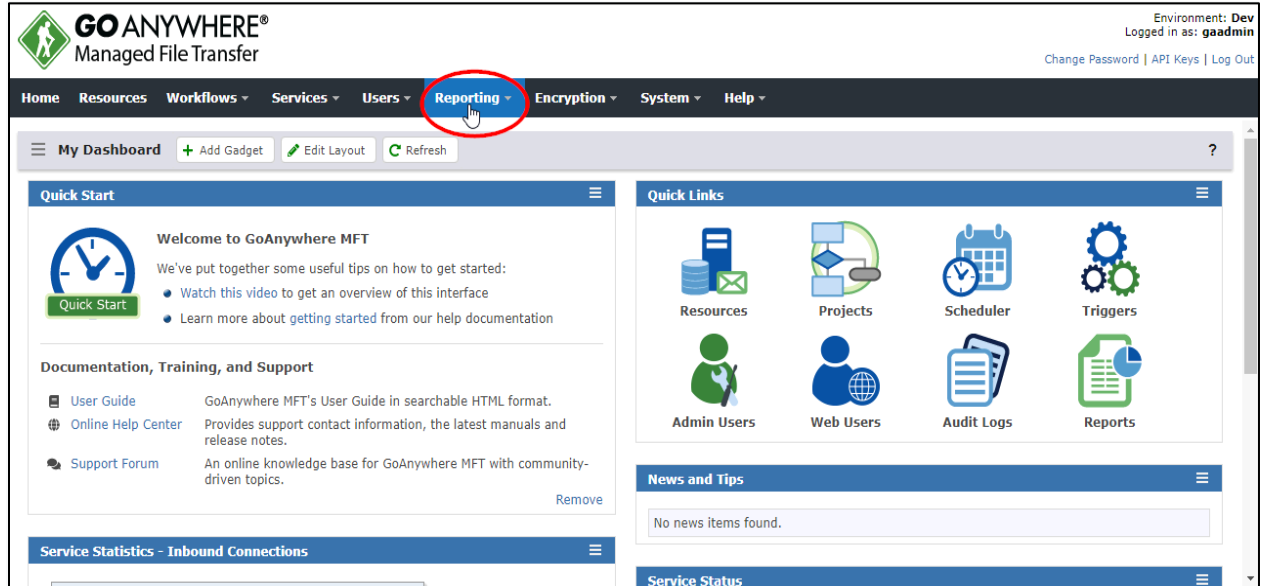
Audit logs

To view the *File Audit Log* in *GoAnywhere MFT*, log in as an admin user with the Auditor role.

Note: If your user account is assigned to a custom admin user role, your ability to view, modify, or execute actions are based on the permissions specified for that role.

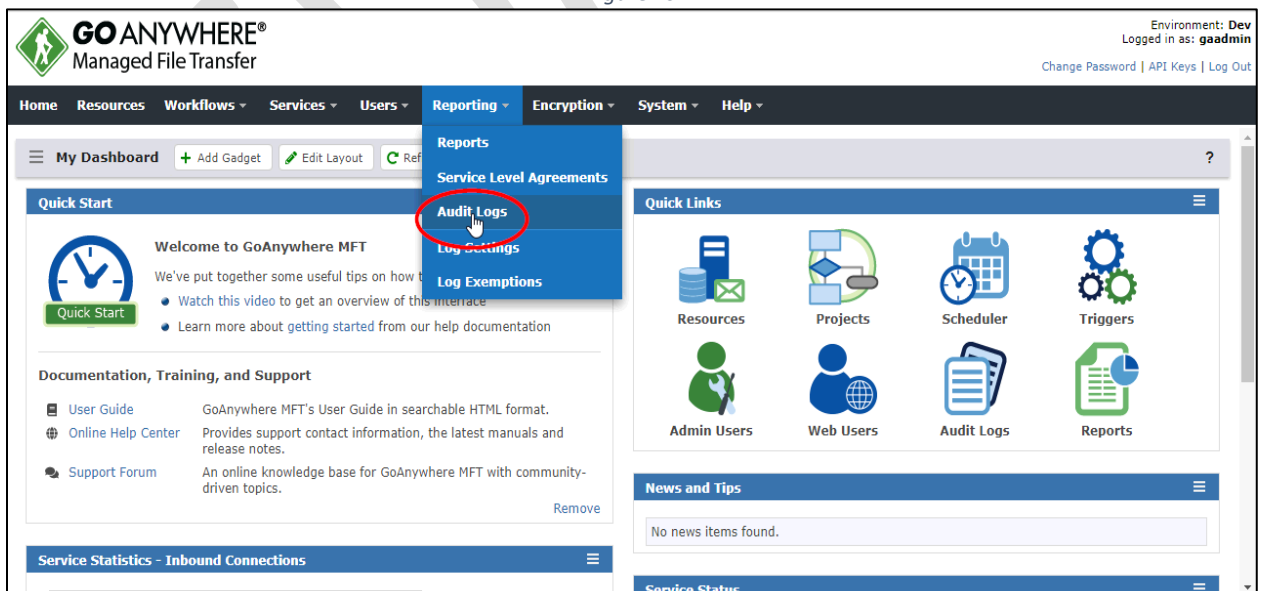
1. From the main menu bar, select the *Reporting* tab. (Figure 45)

Figure 45



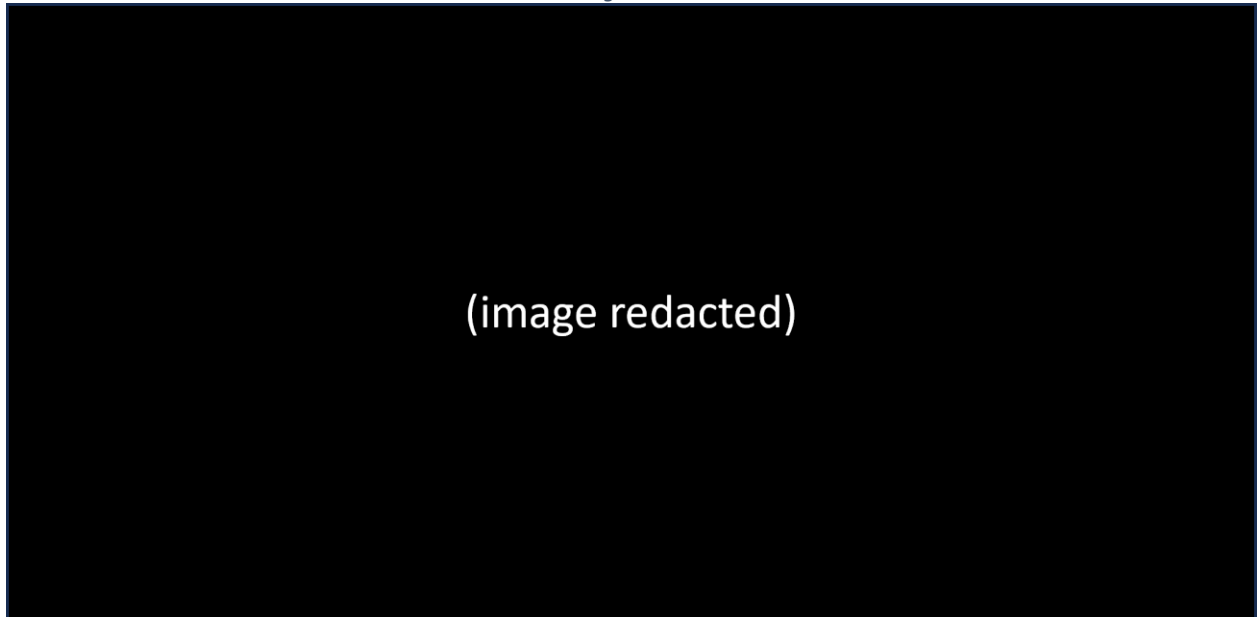
2. Select *Audit Logs*. (Figure 46)

Figure 46



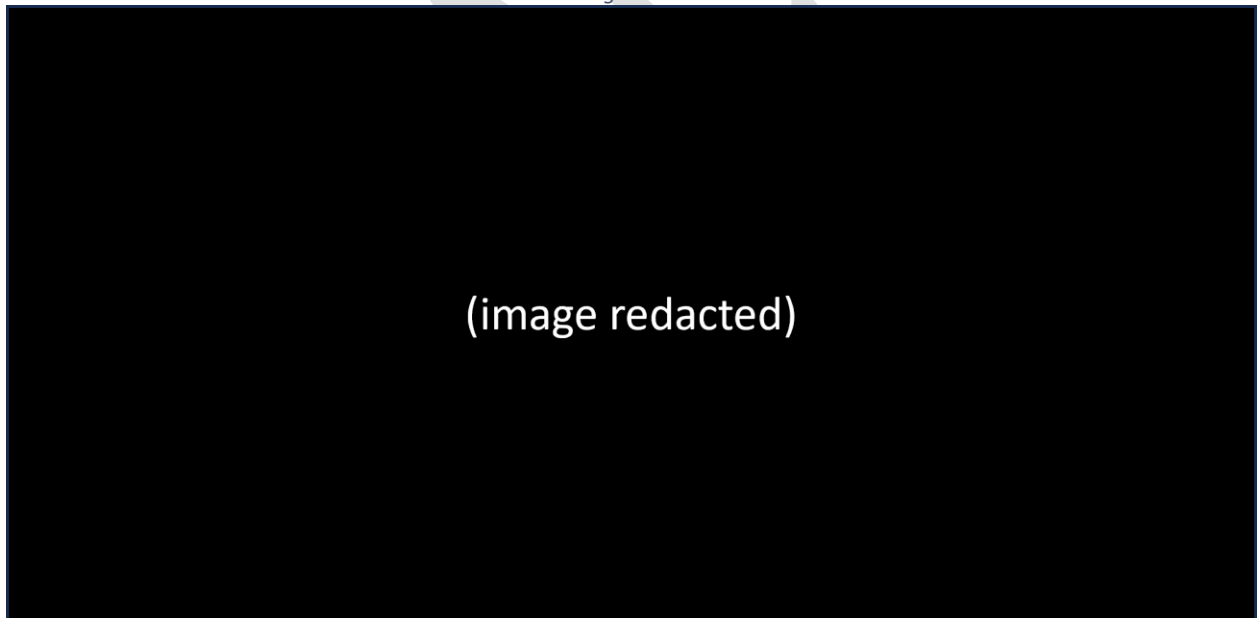
3. Select *File Audit* from the *Job Logs* section in the left pane. (Figure 47)

Figure 47



The *File Audit Log* will appear in the right pane. (Figure 48)

Figure 48



4. View the *Job Details* by clicking the *View* icon. (Figure 49 & Figure 50)

Figure 49

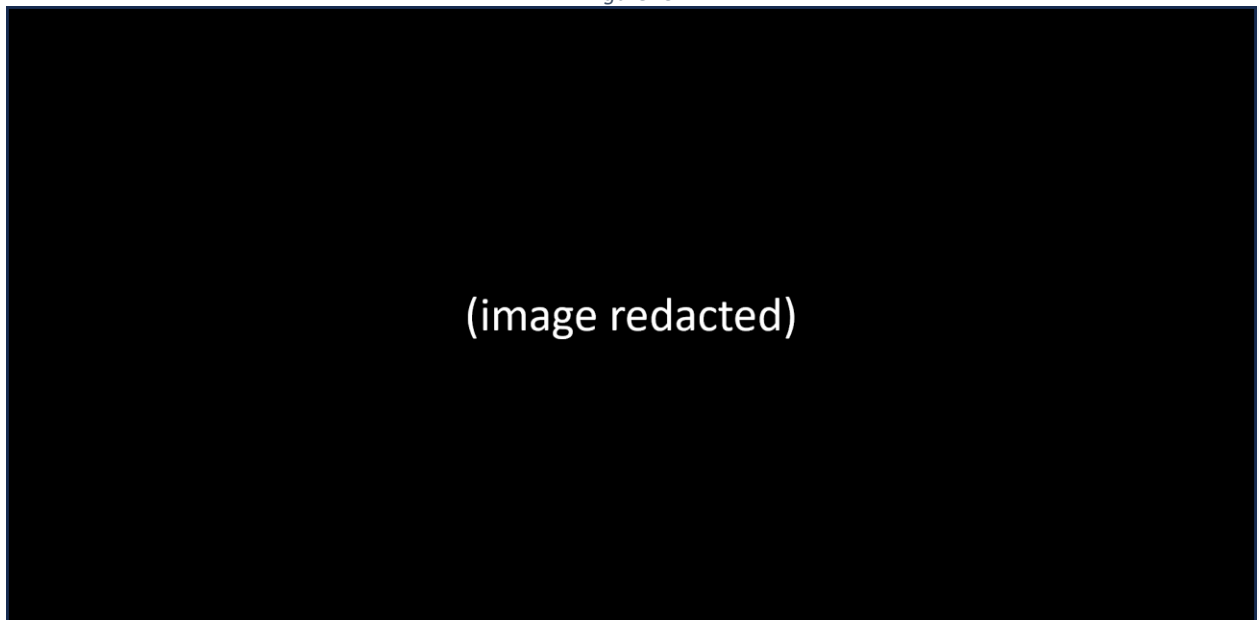
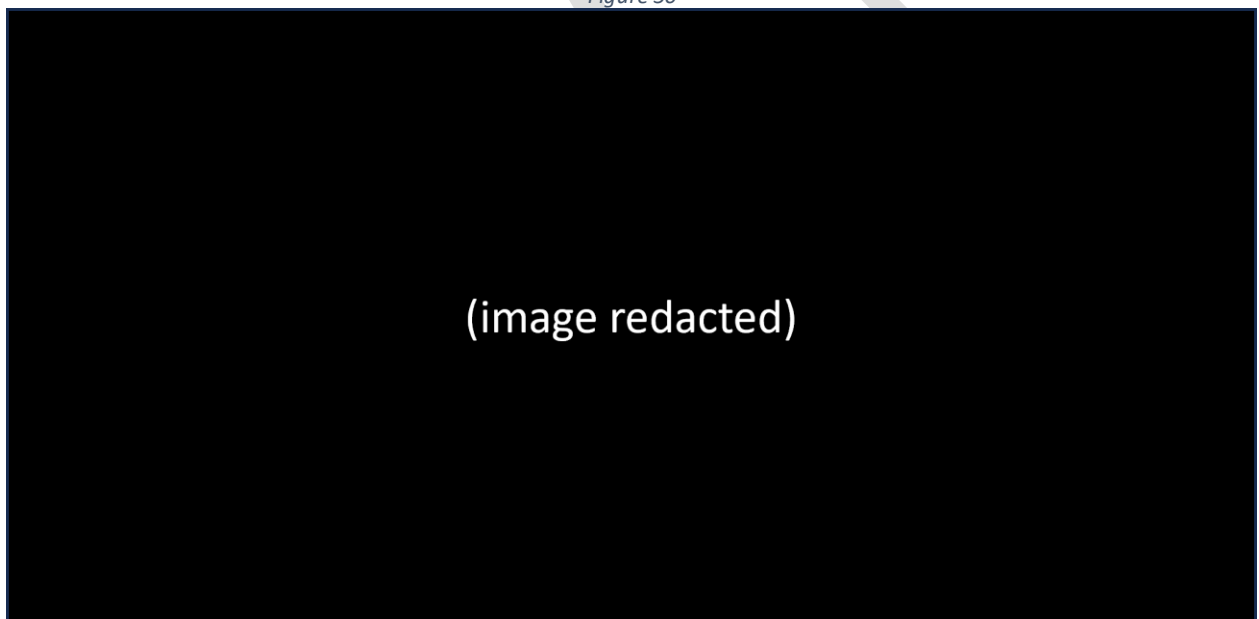


Figure 50



The audit log for each file contains the following information:

- **Event ID:** A unique number assigned to the event. This number is sequential to the order in which the events started
- **Job Number:** A unique job number given to each Project at runtime
- **Start Time:** The date and timestamp of when the job started executing
- **Time (ms) :** The duration of the job run
- **Event Type:** The type of processing that was done to the file
- **Status:** The outcome of the job (Successful icon = Successful, Failed icon = Failed or Canceled icon = Canceled)

- **Source File Name:** The name of the file in the source directory
- **Source File Path:** The path where the file originated
- **Source File Size:** The size of the file before the Job was executed
- **Source Resource Name:** The GoAnywhere Resource that was used to access the file
- **Source Protocol:** The protocol used to access the file
- **Source Server Host:** The host name of the server used to access the file
- **Source Server User:** The Web User account that was used to transfer a file
- **Destination File Name:** The name of the file in the destination directory
- **Destination File Path:** The path where the file is located after the Job completed
- **Destination File Size:** The size of the file after the Job was executed
- **Destination Resource Name:** The GoAnywhere Resource where the file was created or transferred
- **Destination Protocol:** The protocol used to transfer the file
- **Destination Server Host:** The host name of the server used to transfer the file
- **Destination Server User:** The Web user account that received the file
- **Task Name:** The GoAnywhere Project Task name used to process the file
- **Run User:** The user account that was used to submit the job

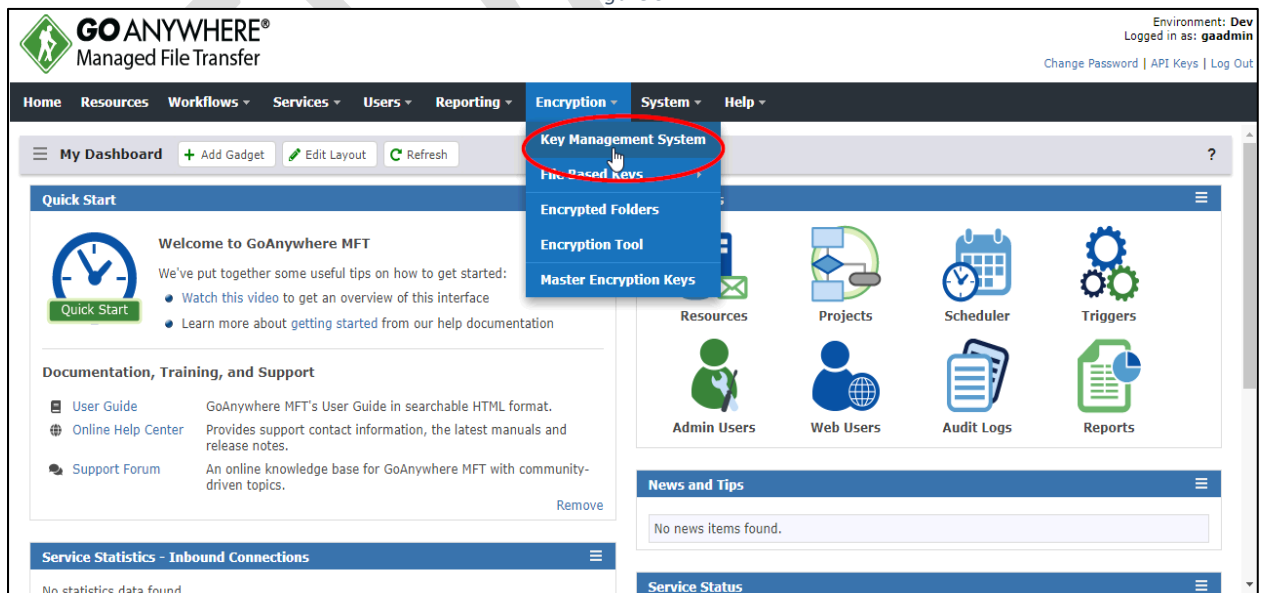
Managing certificates

To manage certificates in a key vault, log in as an admin user with the Key Manager role to manage certificates in a domain's key vault. To manage certificates in the system key vault, log in as an admin user with the Product Administrator and Key Manager roles.

Note: If your user account is assigned to a custom admin user role, your ability to view, modify, or execute actions are based on the permissions specified for that role.

1. From the main menu, select *Encryption*, and then select *Key Management System*. (Figure 51)

Figure 51



2. Click the action icon (to the left of the desired *Key Vault*) and select *Manage Certificates*. (Figure 52)

Note: A certificate shown in red indicates it has expired.

Figure 52

The screenshot displays the GO ANYWHERE Managed File Transfer interface. At the top, the logo and name 'GO ANYWHERE Managed File Transfer' are visible on the left, and the environment 'Dev' and user 'gaadmin' are on the right. A navigation bar includes 'Home', 'Resources', 'Workflows', 'Services', 'Users', 'Reporting', 'Encryption', 'System', and 'Help'. Below this, the 'Key Management System (KMS)' section is shown with a '+ Add Key Vault' button. A table lists two key vaults: 'Default' and 'System'. The 'System' vault is highlighted with a red circle, and its dropdown menu is open, with 'Manage Certificates' also circled in red. The table data is as follows:

Key Vault	Description	Certificates	SSH Keys	PGP Keys	Modified By	Modified On
Default	The Key Vault used to retrieve a key or certificate if no specific Key Vault was selected in the application.	1	10	12	system	1/12/21 10:46:59 AM
System	The Key Vault for storing the trusted CA certificates, as well as the private keys/certificates used in the HTTPS, FTPS, SFTP, AS2 and GoFast server modules.	87	6	0	system	1/12/21 10:46:59 AM

REDACTED

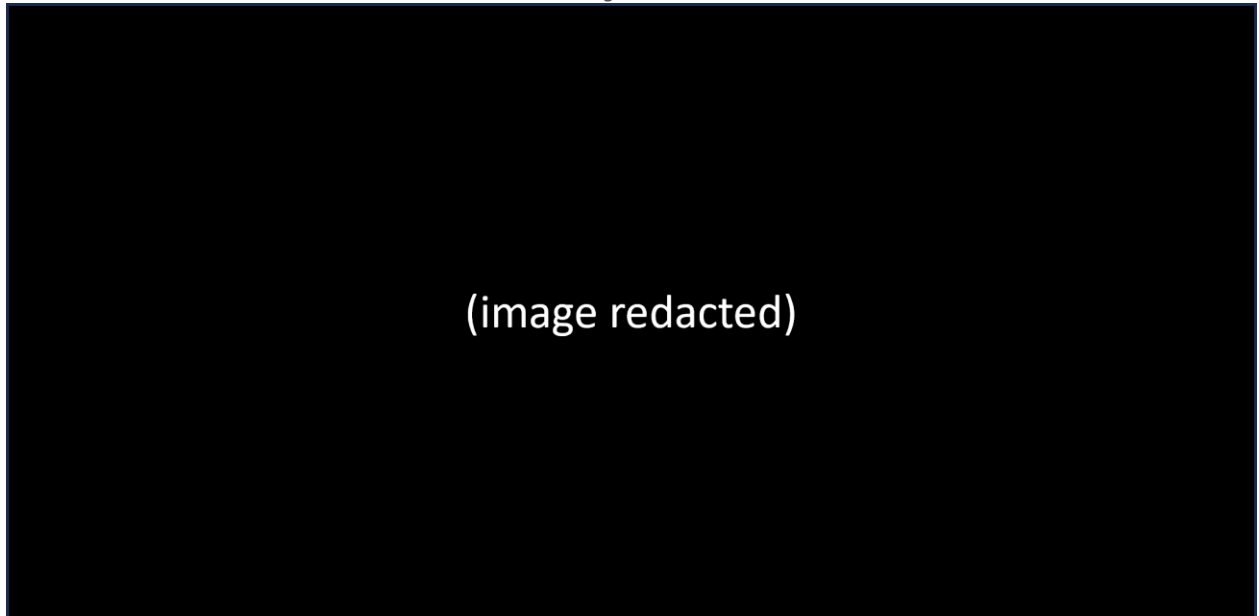
There are two options available to add a certificate – create a new one or import an existing one.

Create a new certificate

To create a new certificate, perform the following:

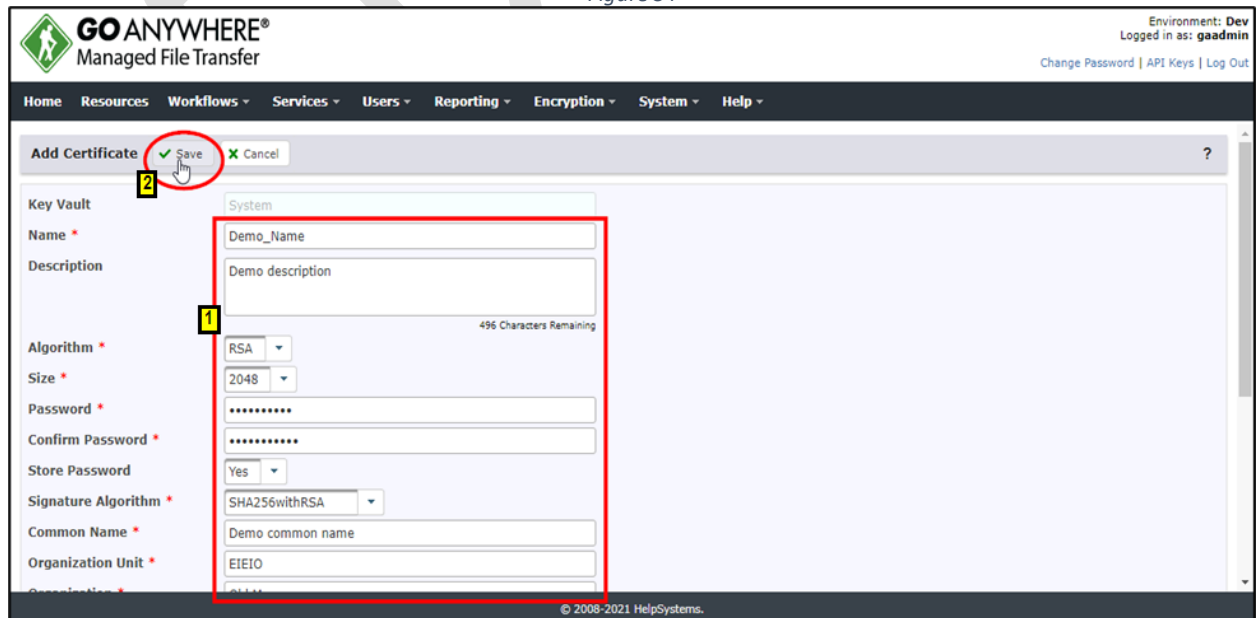
1. From the *Certificates* menu, click the *Add Certificate* button. (Figure 53)

Figure 53



2. Enter the requested information⁽¹⁾. (Figure 54)
3. Click the *Save* button⁽²⁾. (Figure 54)

Figure 54

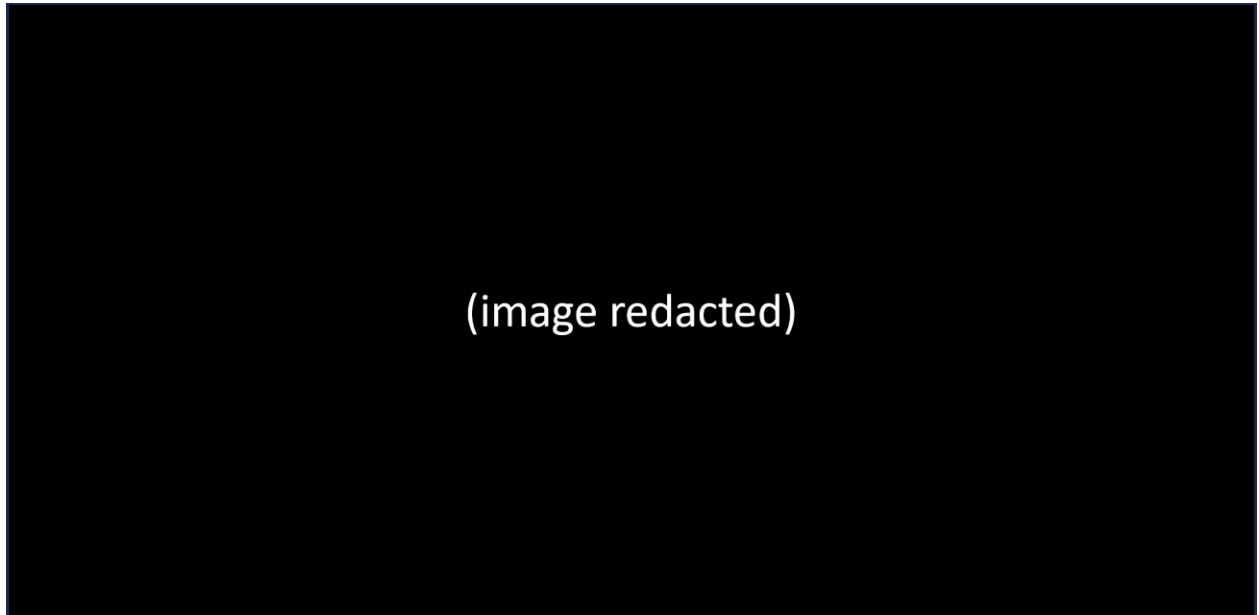


Import a certificate

To import a certificate, perform the following:

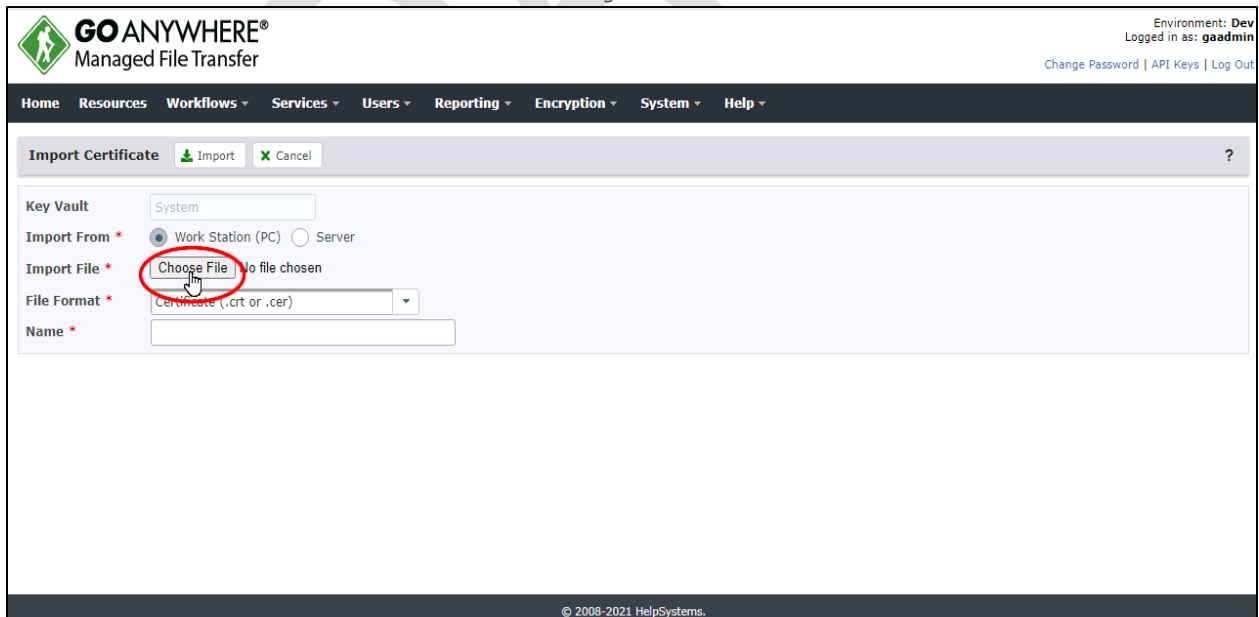
1. From the *Certificates* menu, click the *Import* button. (Figure 55)

Figure 55



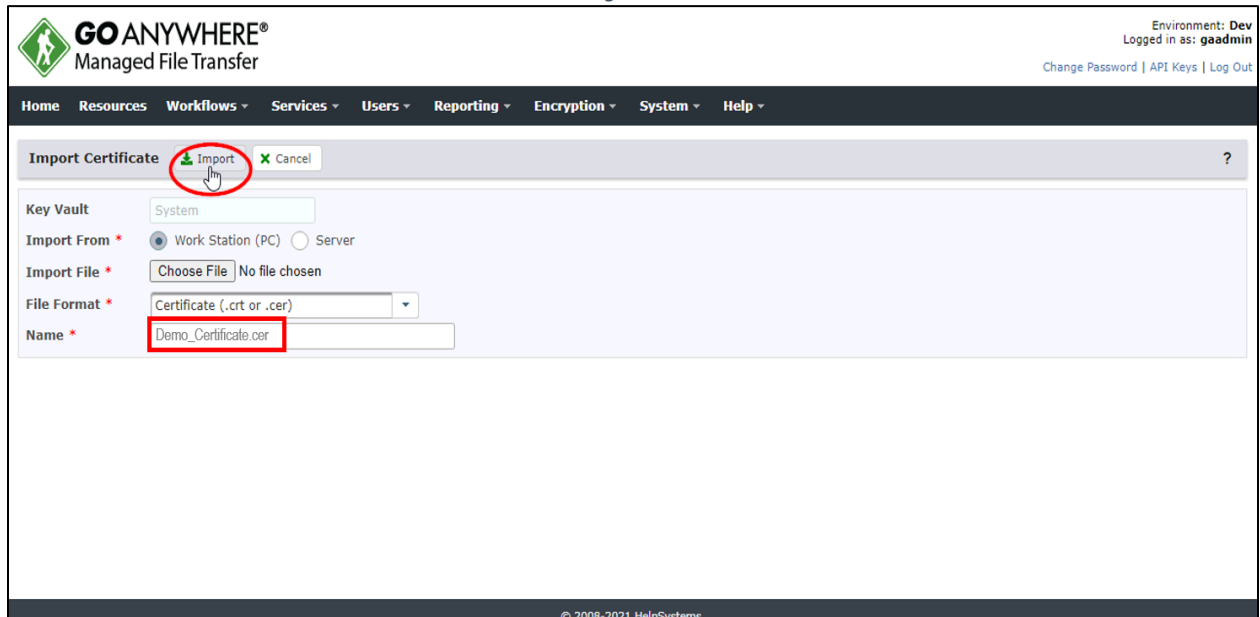
2. Search for and select the file containing the certificate by clicking the *Choose File* button (Figure 56)

Figure 56



3. Once the file has been selected, click the *Import* button to import it. (Figure 57)

Figure 57



Edit a certificate

To edit a certificate, perform the following:

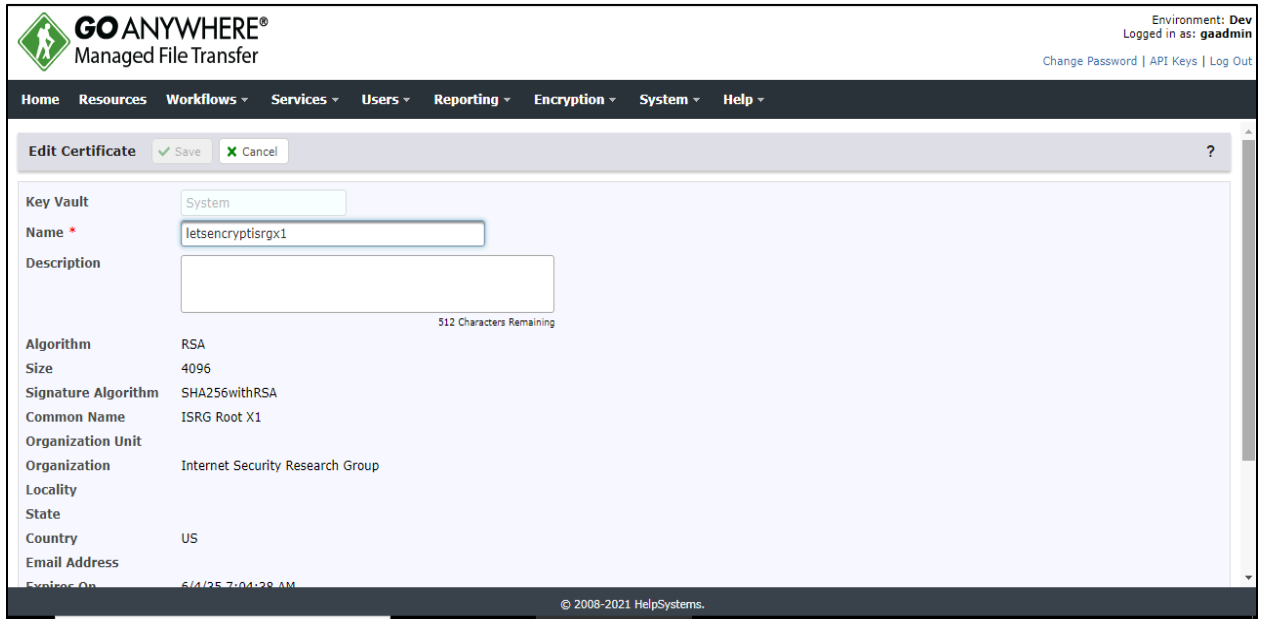
1. Click the action icon⁽¹⁾ (to the left of the desired *Certificate*), then select *Edit*⁽²⁾. (Figure 58)

Figure 58

(image redacted)

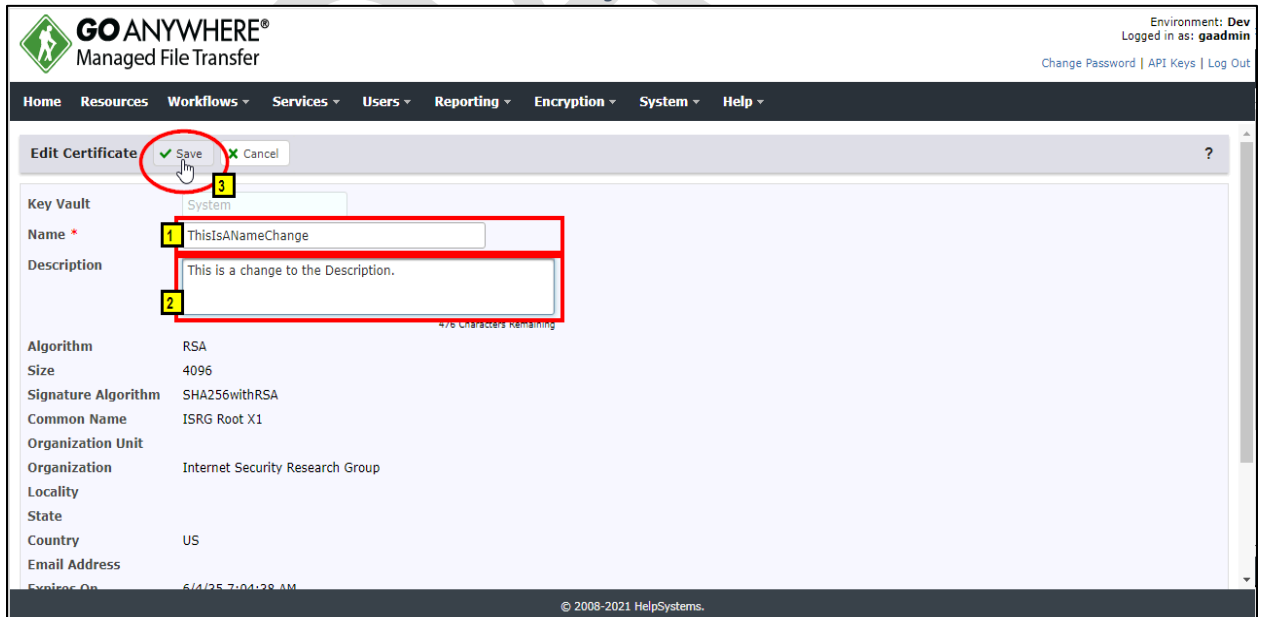
- This page will show the properties for the certificate, such as the *Name*, *Algorithm*, and *Description*. (Figure 59)

Figure 59



- You can now edit the certificate *Name*⁽¹⁾ and the certificate *Description*⁽²⁾. (Figure 60)
- Click the *Save*⁽³⁾ button when finished to save any changes. (Figure 60)

Figure 60



User administration

In general, there are two types of *GoAnywhere MFT* users – admin users and web users.

Admin users

"Administrative level" users have authorization to all functions in *GoAnywhere MFT*. Each admin user may belong to one or more admin user groups. The admin user will adopt the admin roles (authorities) from any admin user group(s) to which they belong. An admin user can also be granted individual admin roles.

Each admin user may also belong to one or more domains. Admin users may only administrate items within the domain(s) in which they are authorized.

To perform administrative functions in *GoAnywhere MFT*, an admin user must log in with a valid username and password. Admin users can be added and managed only by an admin user with the *Security Officer* role.

Note: Roles assigned to an Admin User Group will be adopted by the Admin Users belonging to that group.

Add an admin user

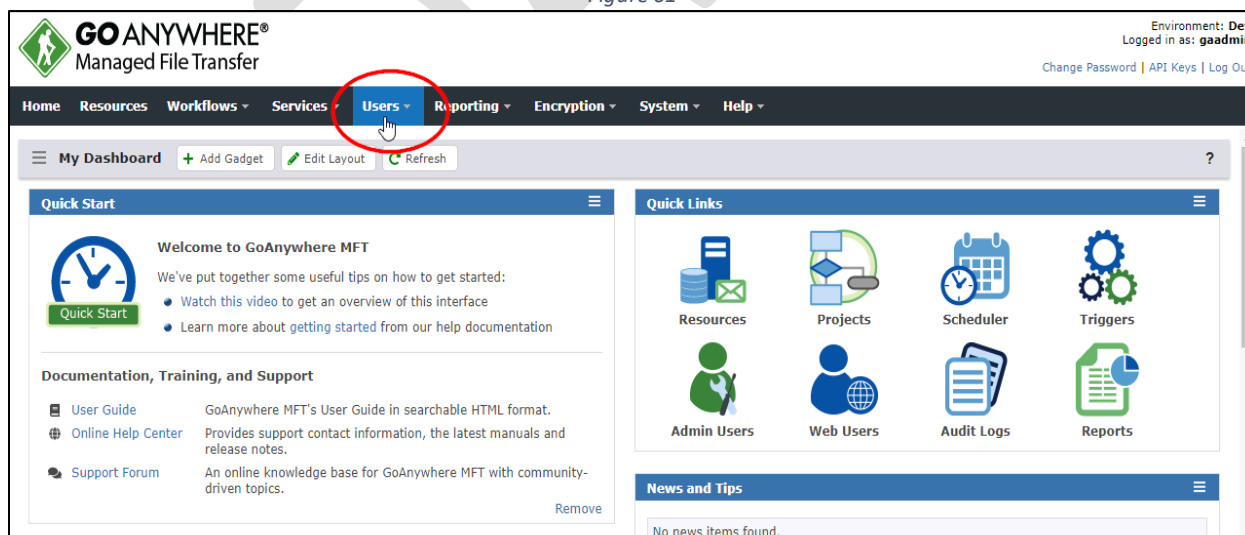
To **add** an admin user, perform the following:

1. Log in as an admin user with the *Security Officer* role

Note: If your user account is assigned to a custom admin user role, your ability to view, modify, or execute actions on this page are based on the permissions specified for that role.

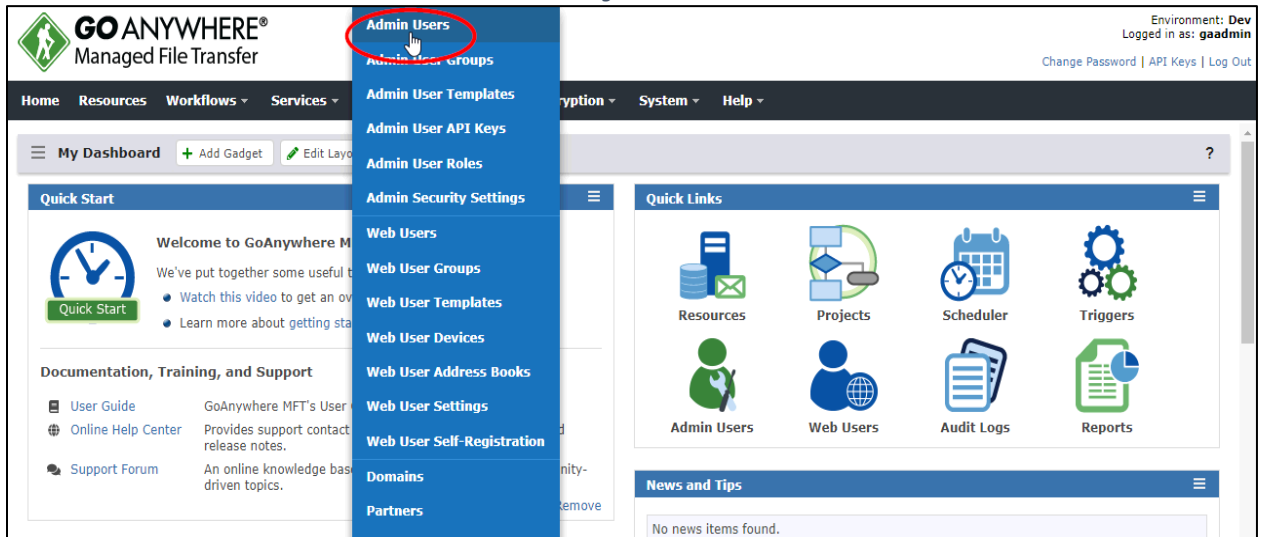
2. From the main menu bar, select *Users*. (Figure 61)

Figure 61



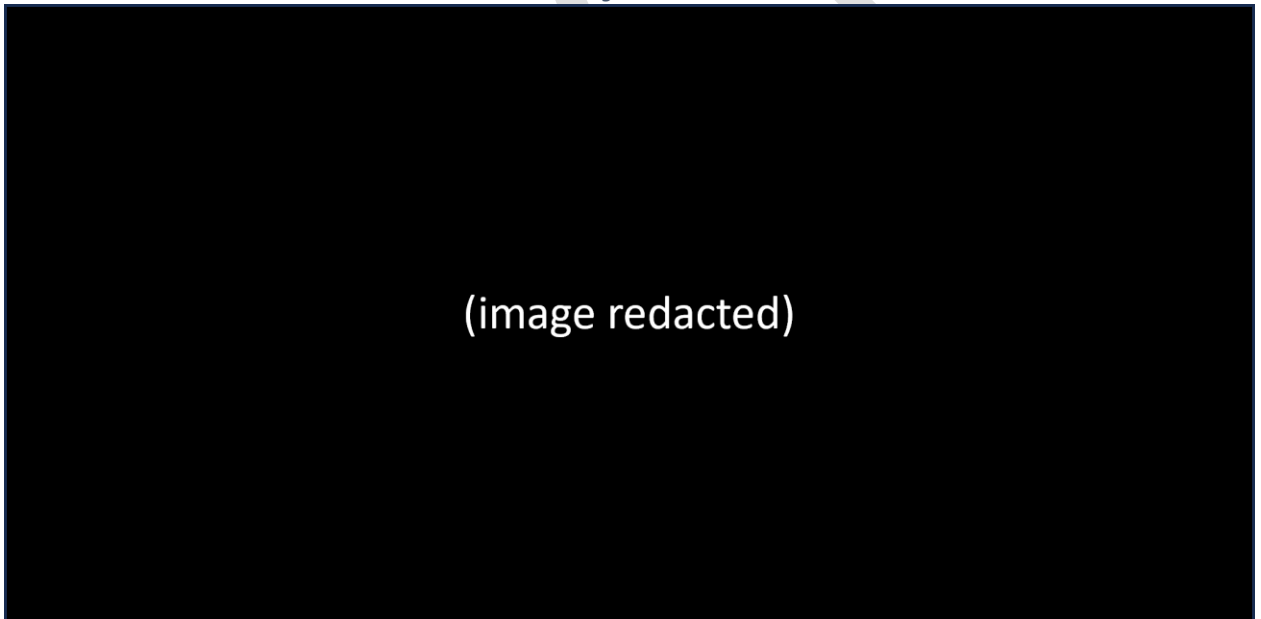
3. Select *Admin Users*. (Figure 62)

Figure 62



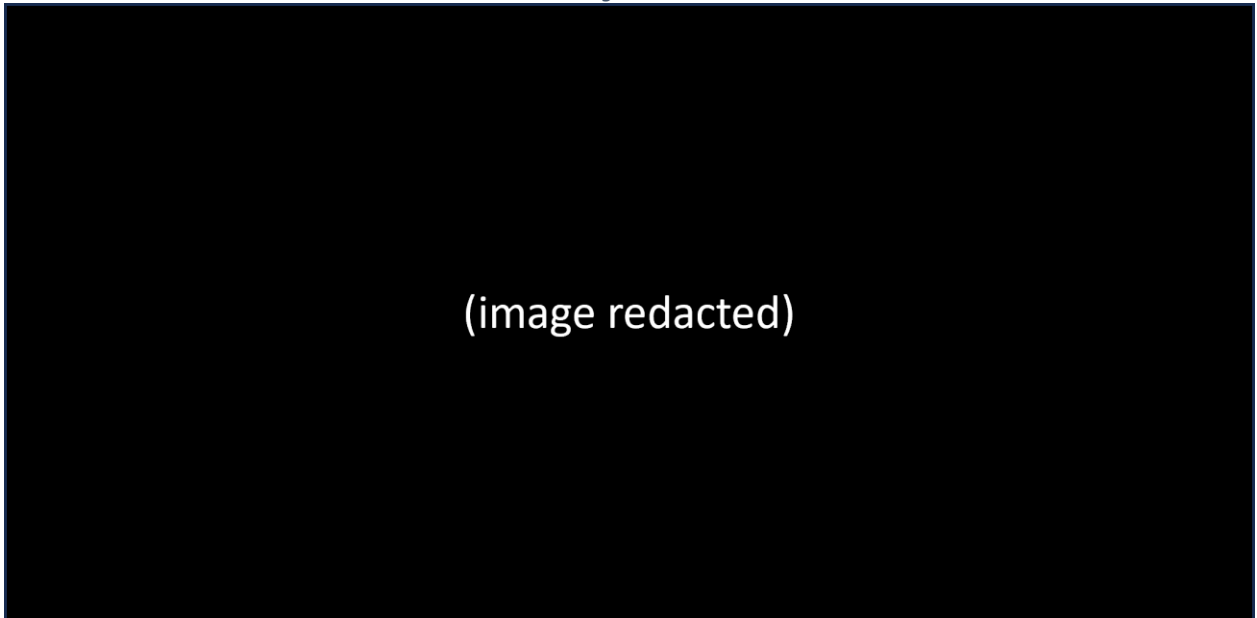
4. Click the *Add Admin User* button. (Figure 63)

Figure 63



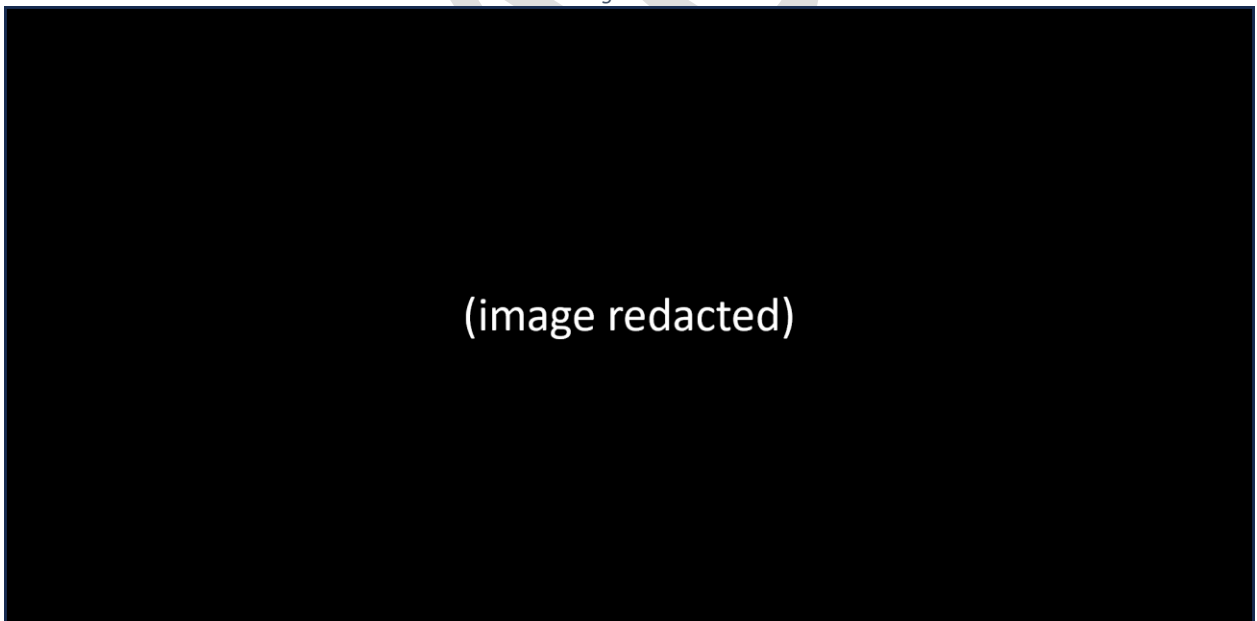
5. Select the *Admin User Template* that will apply default Roles, Admin User Groups, and Domain settings for the admin user. (Figure 64)

Figure 64



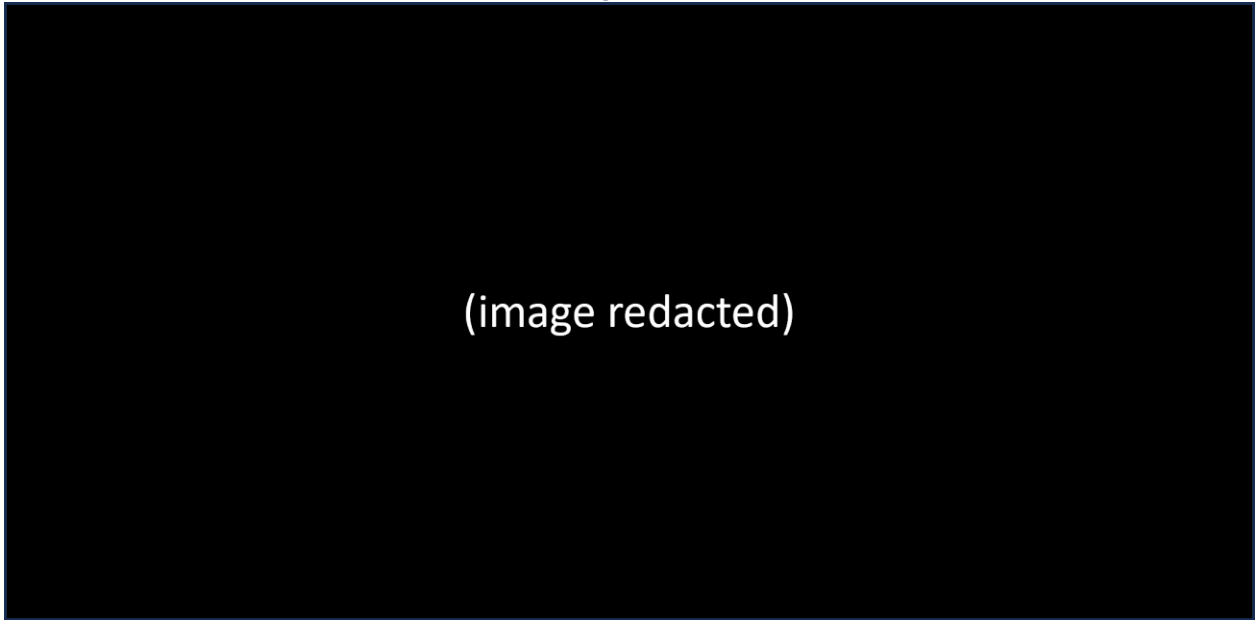
6. Click the *Continue* button. (Figure 65)

Figure 65



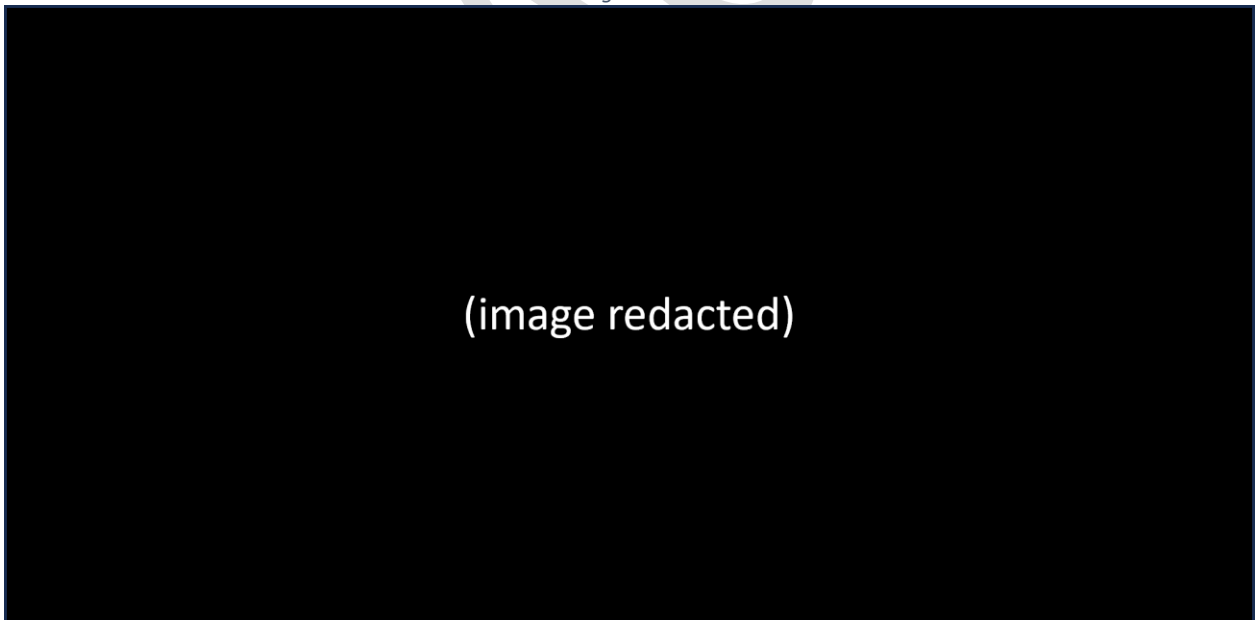
7. Enter the requested information in the *Add Admin User* form^(a). (Figure 66)
8. Click the *Save* button^(a). (Figure 66)

Figure 66



9. Notice the new admin user was added. (Figure 67)

Figure 67

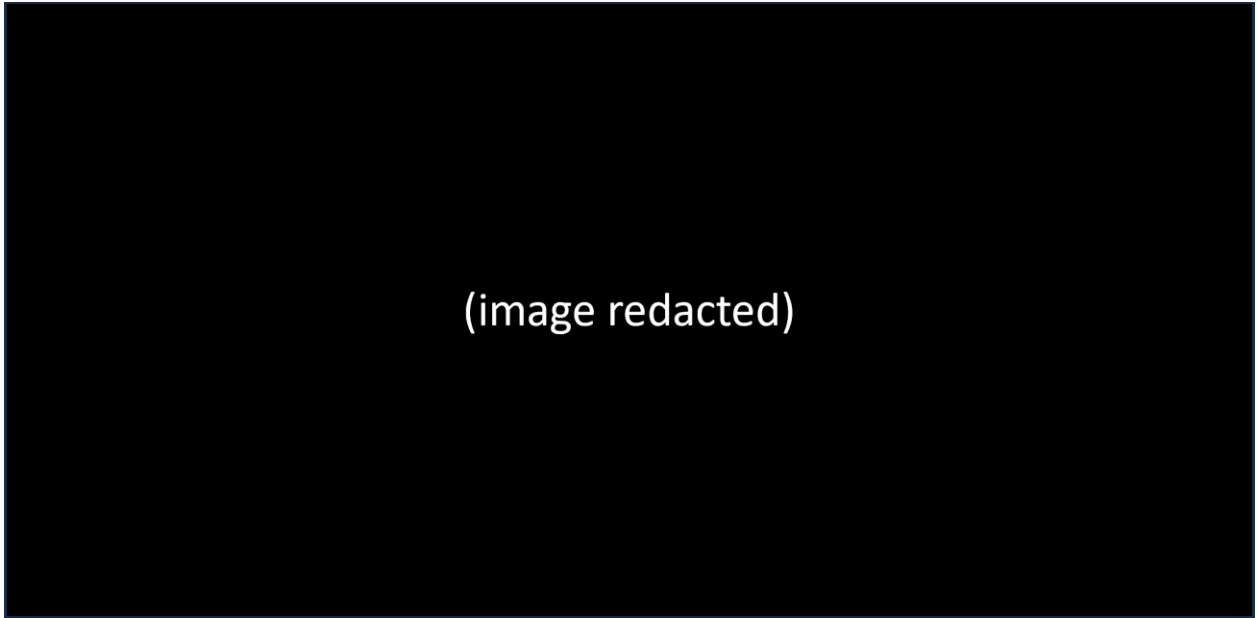


Edit an admin user

To edit an admin user, perform the following:

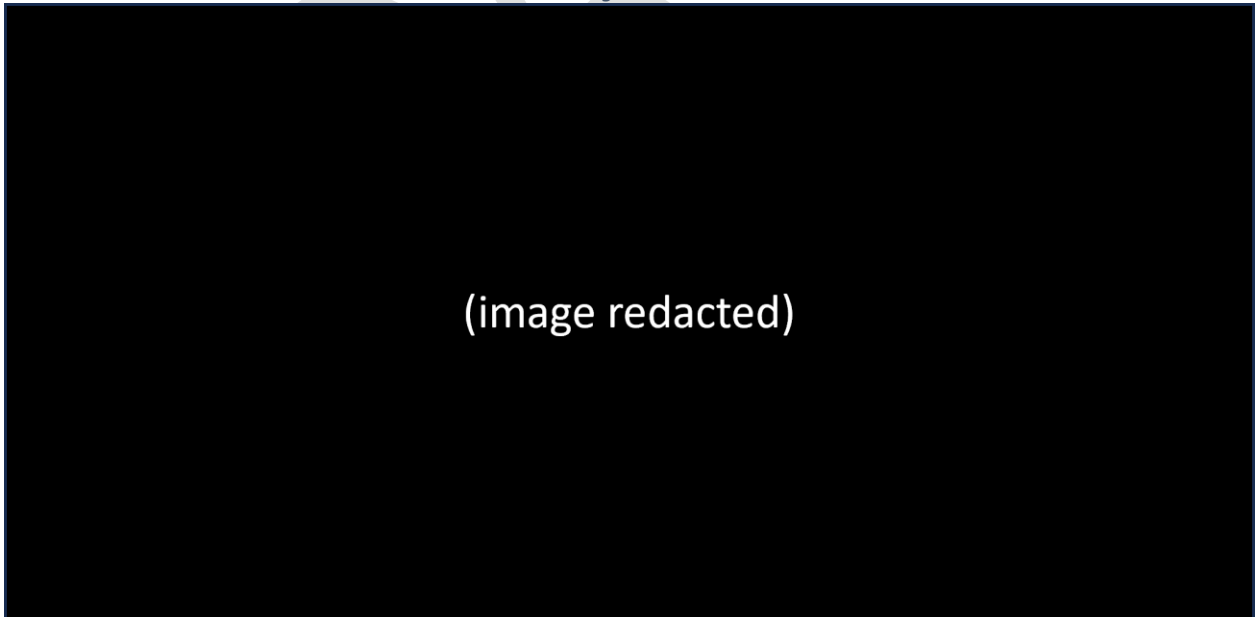
1. Click the action icon (located to the left of the User Name) you wish to edit. (Figure 68)

Figure 68



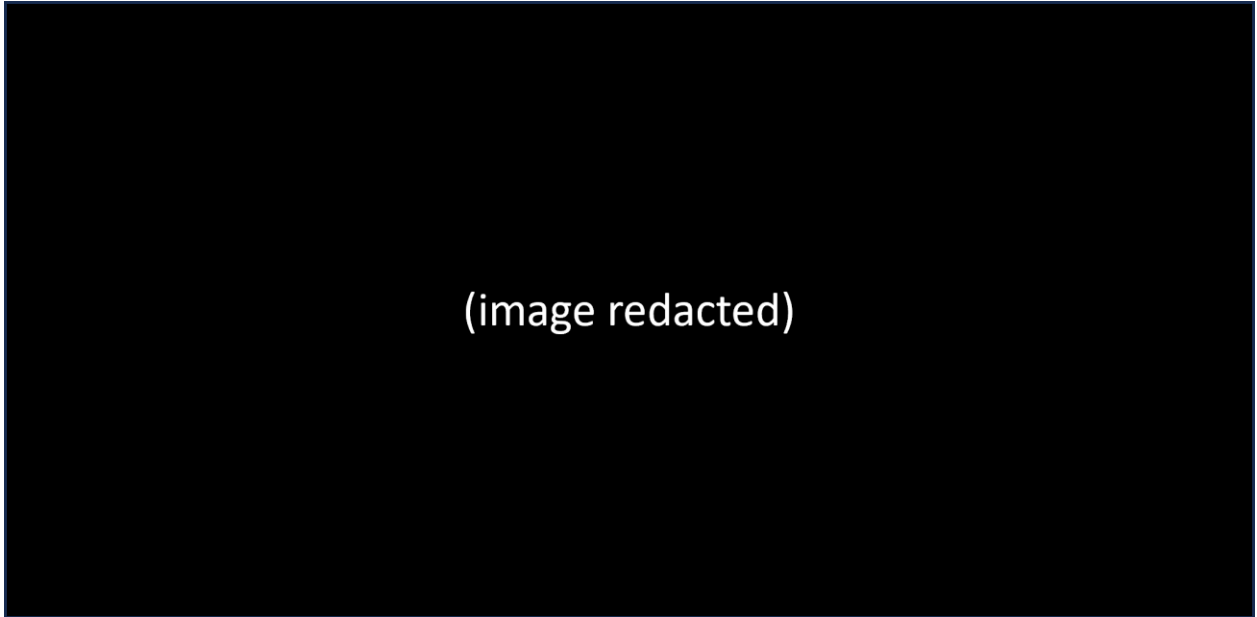
2. Select the *Edit* option. (Figure 69)

Figure 69



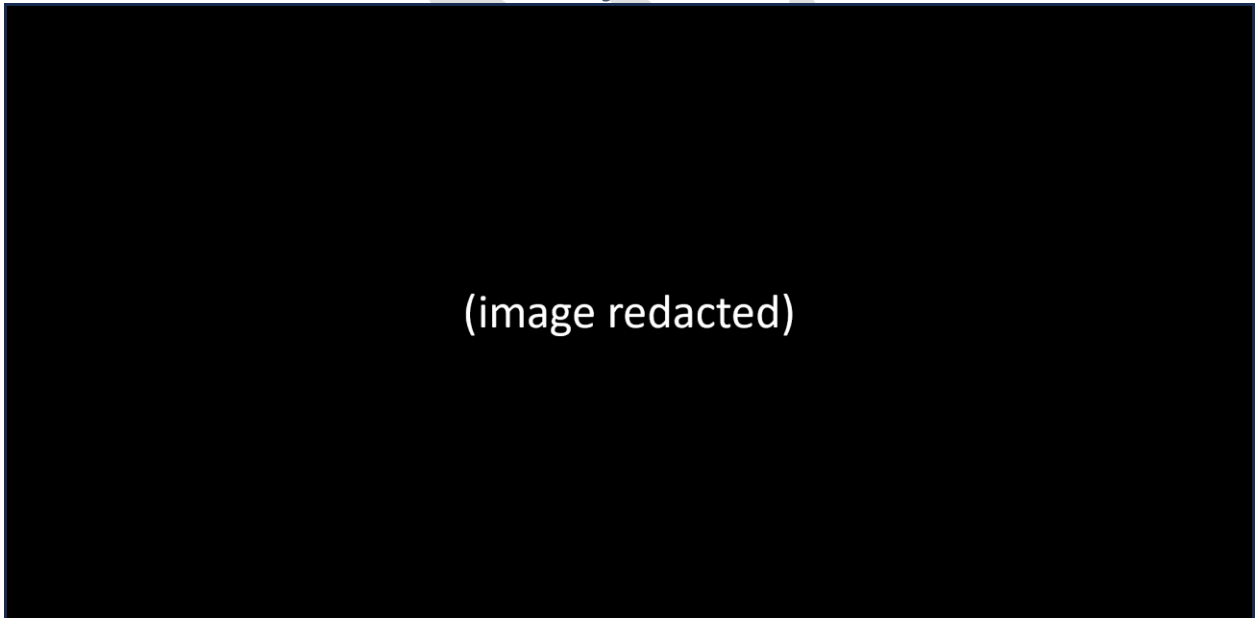
3. Edit the admin user information as desired. (Figure 70)

Figure 70



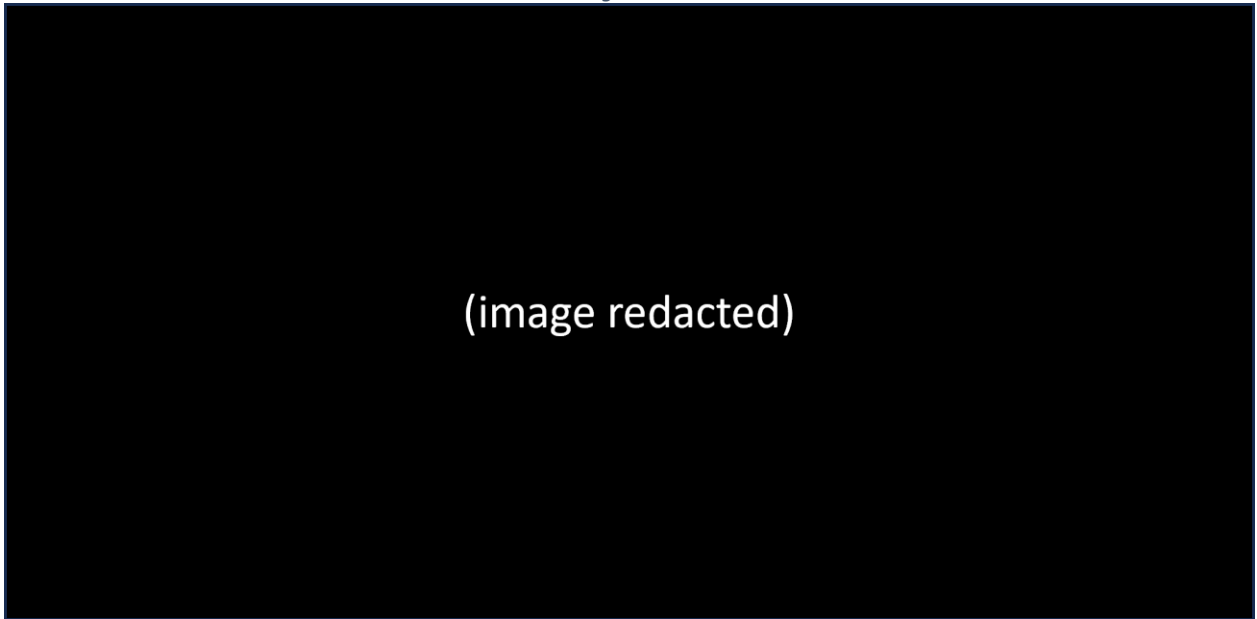
4. Click the *Save* button when finished editing the account. (Figure 71)

Figure 71



5. Notice the account has been successfully updated. (Figure 72)

Figure 72

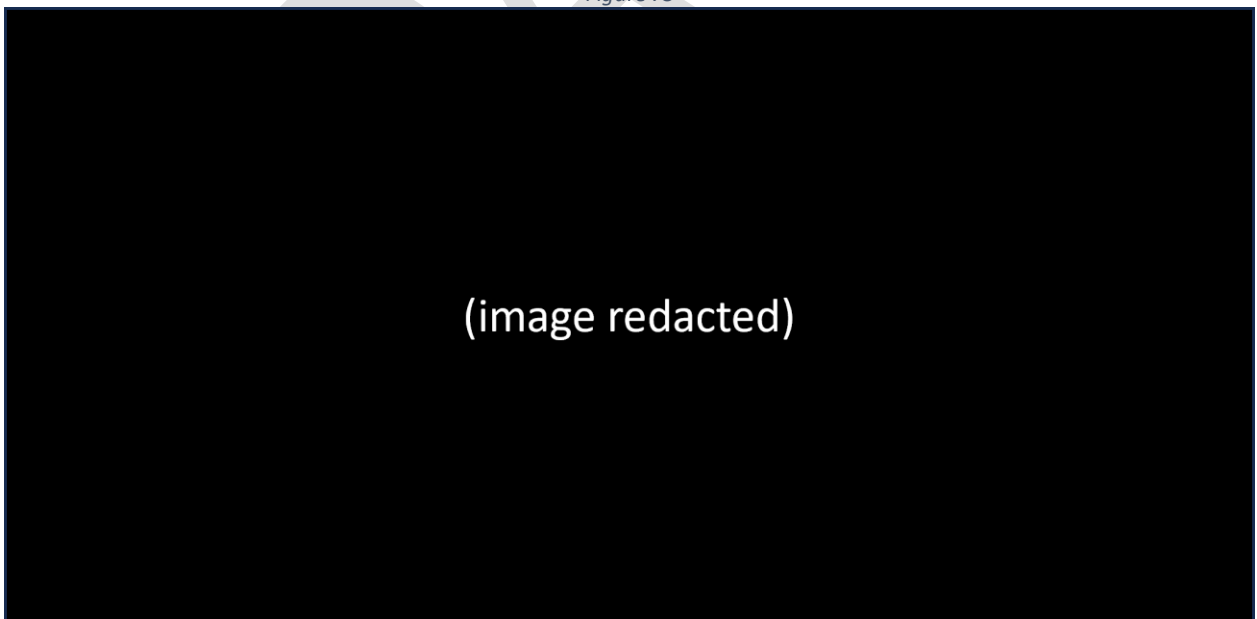


Delete an admin user

To delete an admin user, perform the following:

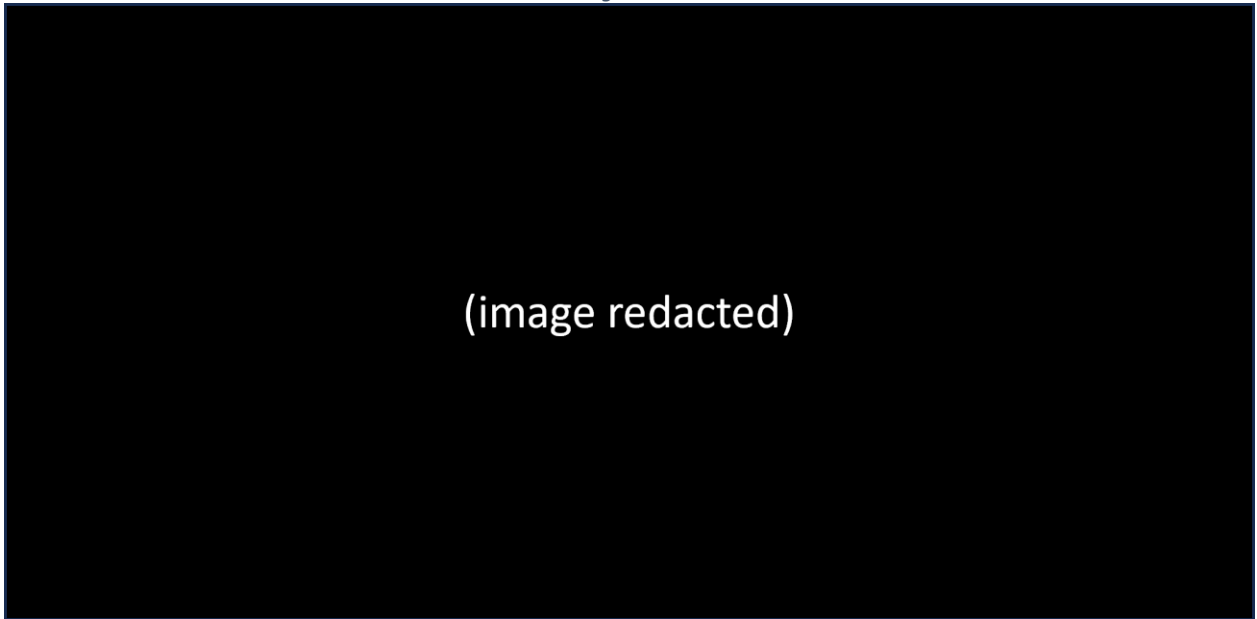
1. Click the action icon (located to the left of the User Name) you wish to delete. (Figure 73)

Figure 73



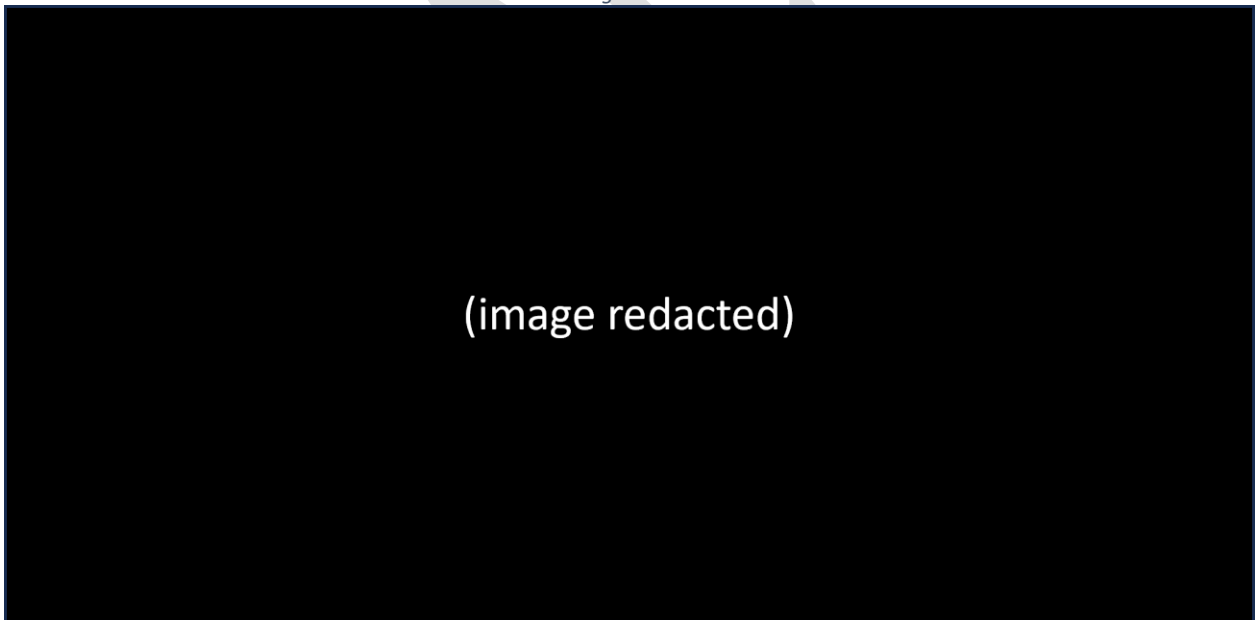
2. Select the *Delete* option. (Figure 74)

Figure 74



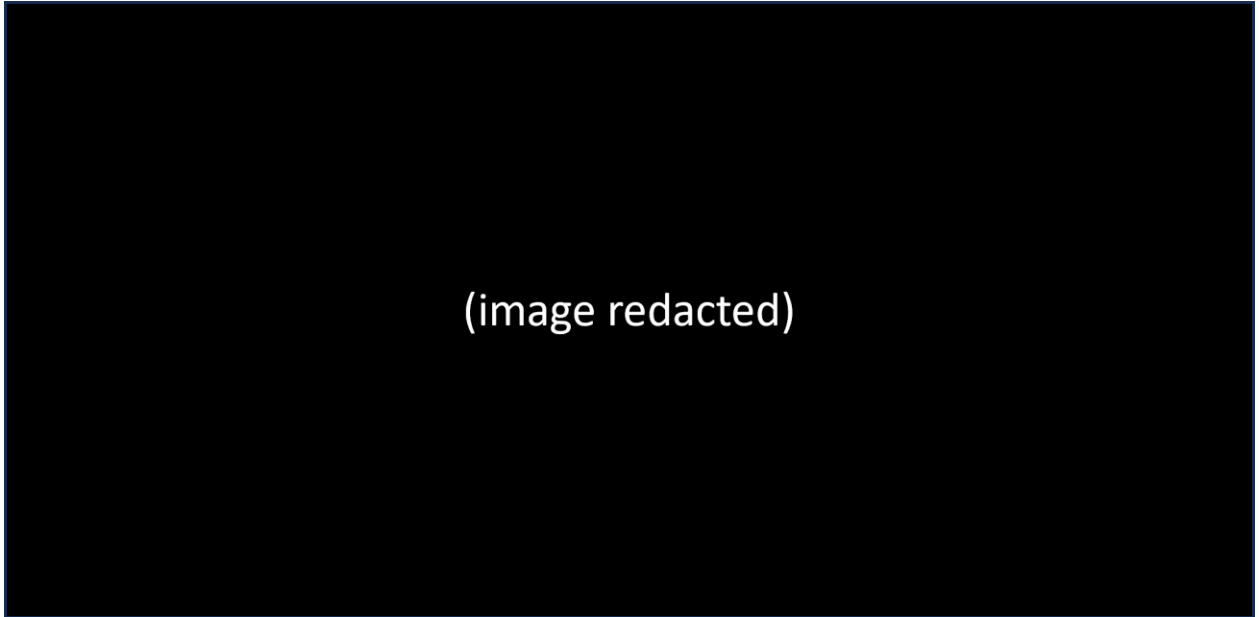
3. Click the *Confirm* button. (Figure 75)

Figure 75



4. Notice that the user has been deleted. (Figure 76)

Figure 76



REDACTED

Web users

Web users are the accounts that can access *GoAnywhere MFT* for exchanging files using standard protocols. web users can be external (for example, external vendors) or internal to [REDACTED] (for example, employees or custom applications). Web user accounts are created to provide users with the ability to connect to the services they need for secure file transfers.

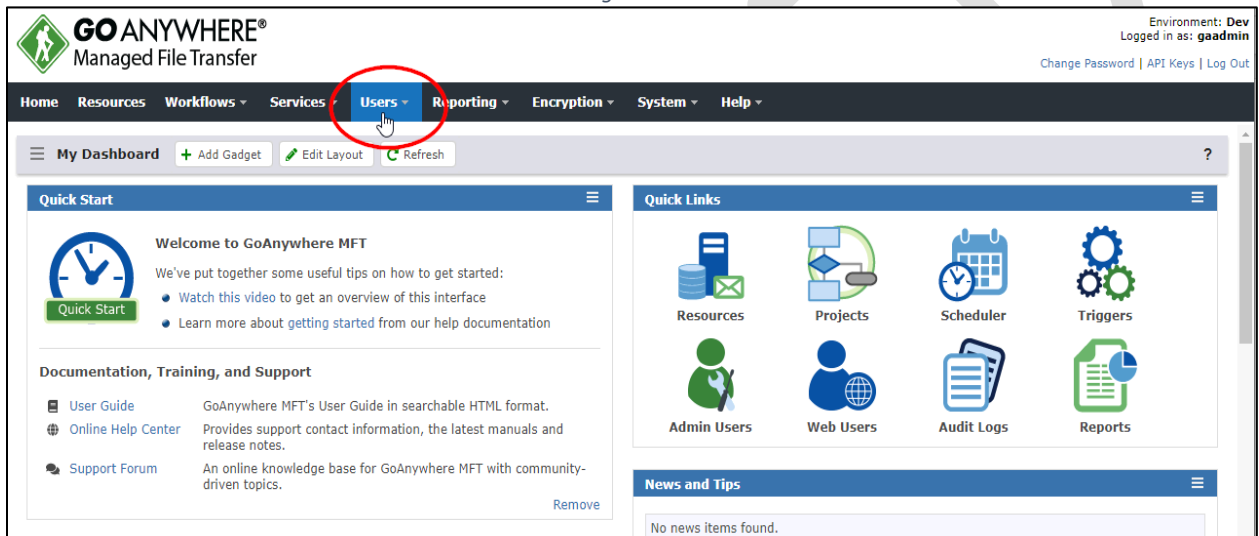
To manage web user accounts, you must be logged in as an admin user with the Web User Manager role.

Add a web user

To add a web user, perform the following:

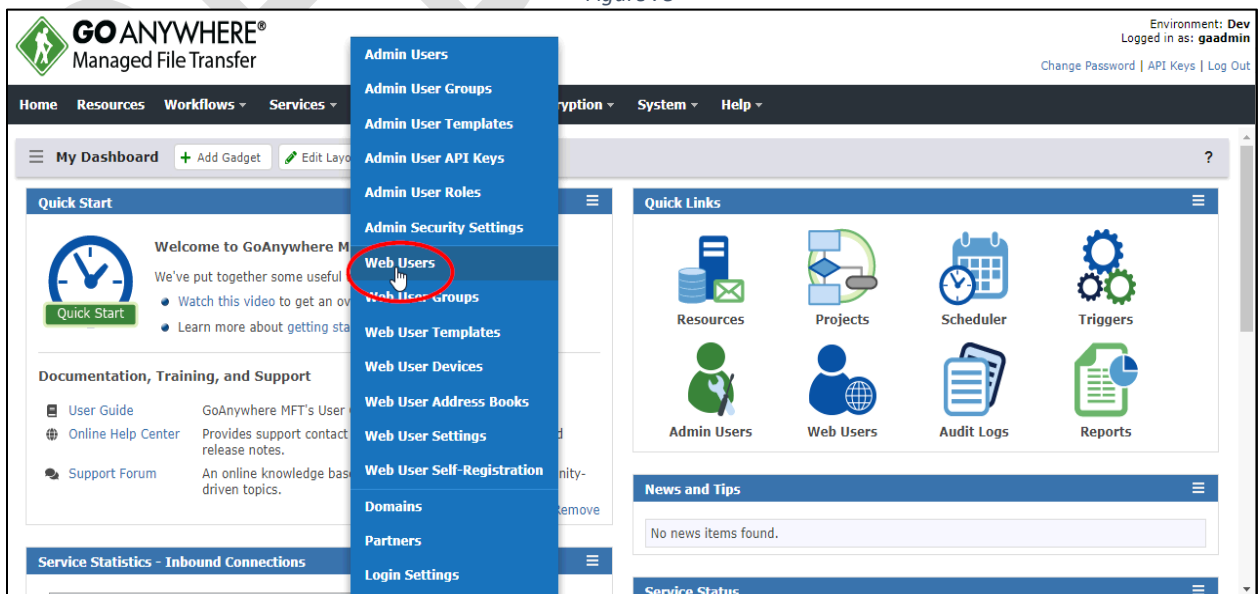
1. From the main menu bar, select *Users*. (Figure 77)

Figure 77



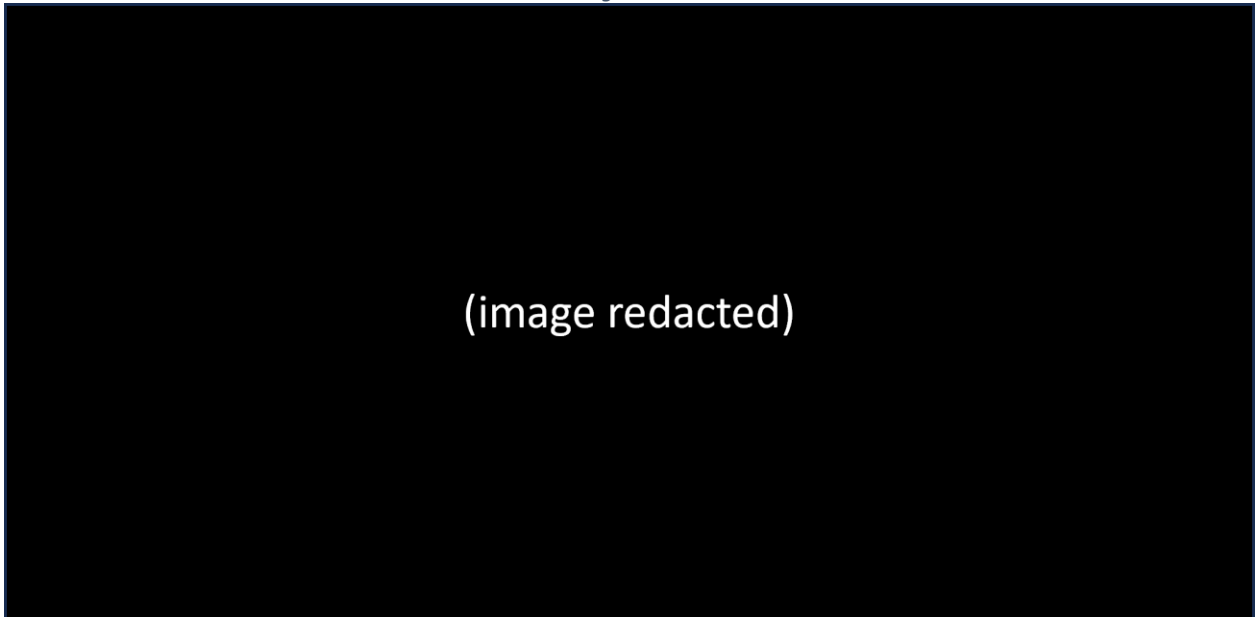
2. Select *Web Users*. (Figure 78)

Figure 78



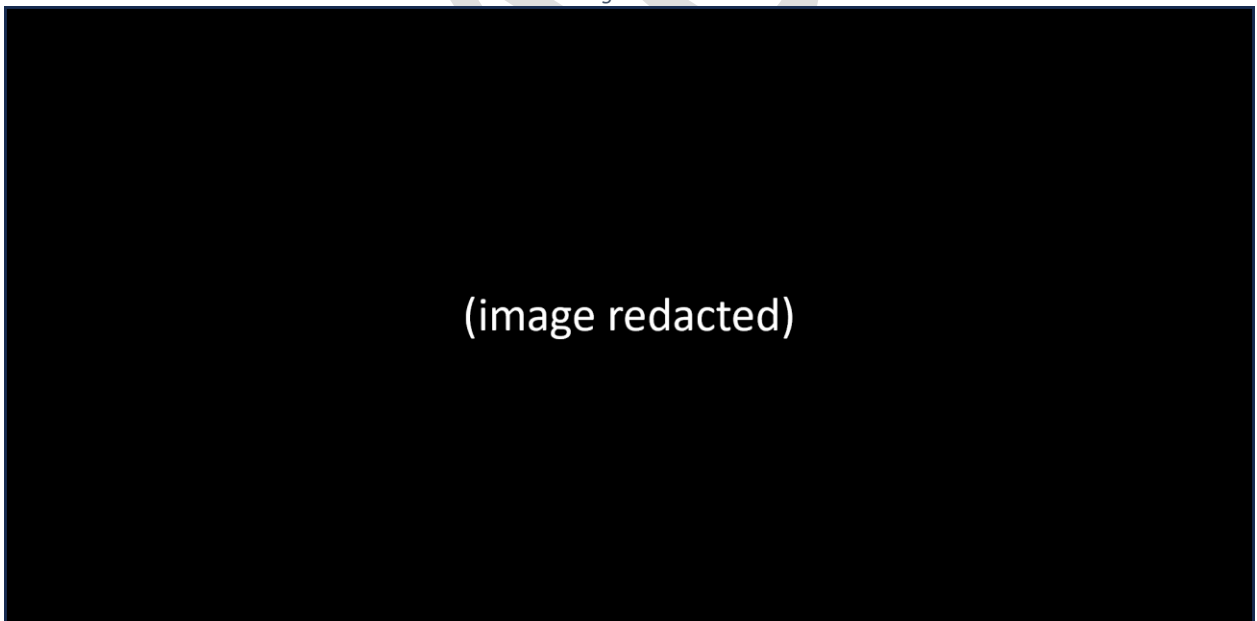
3. Click the *Add Web User* button. (Figure 79)

Figure 79



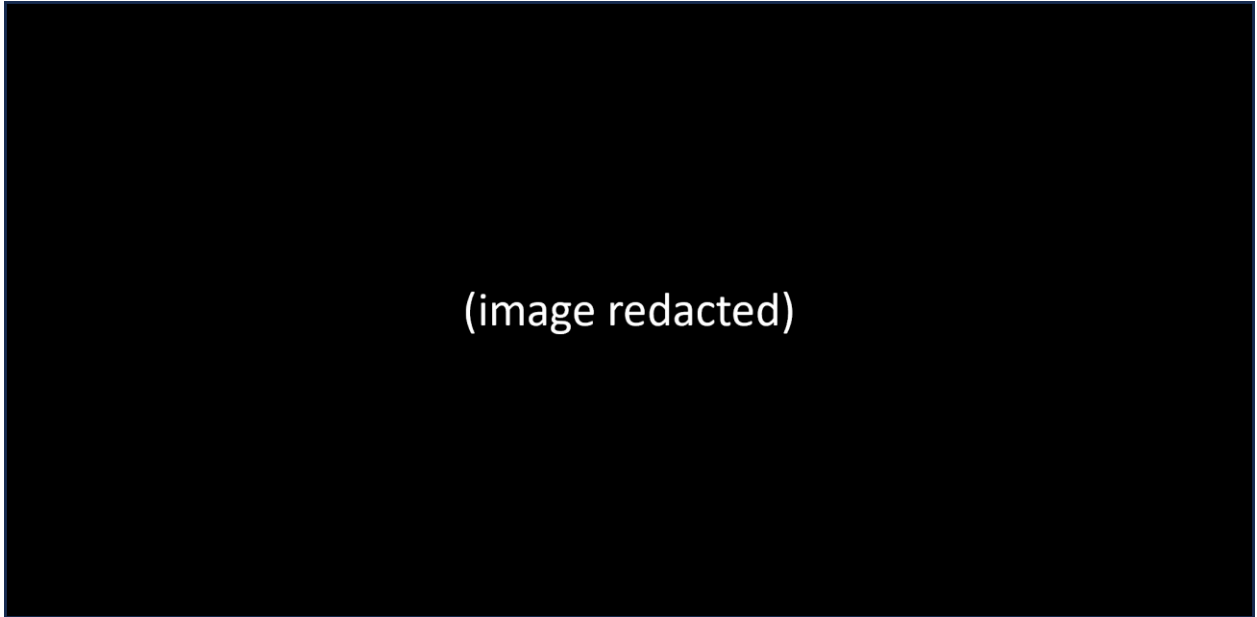
4. Select the *Web User Template* that will apply default security settings for the web user. (Figure 80)

Figure 80



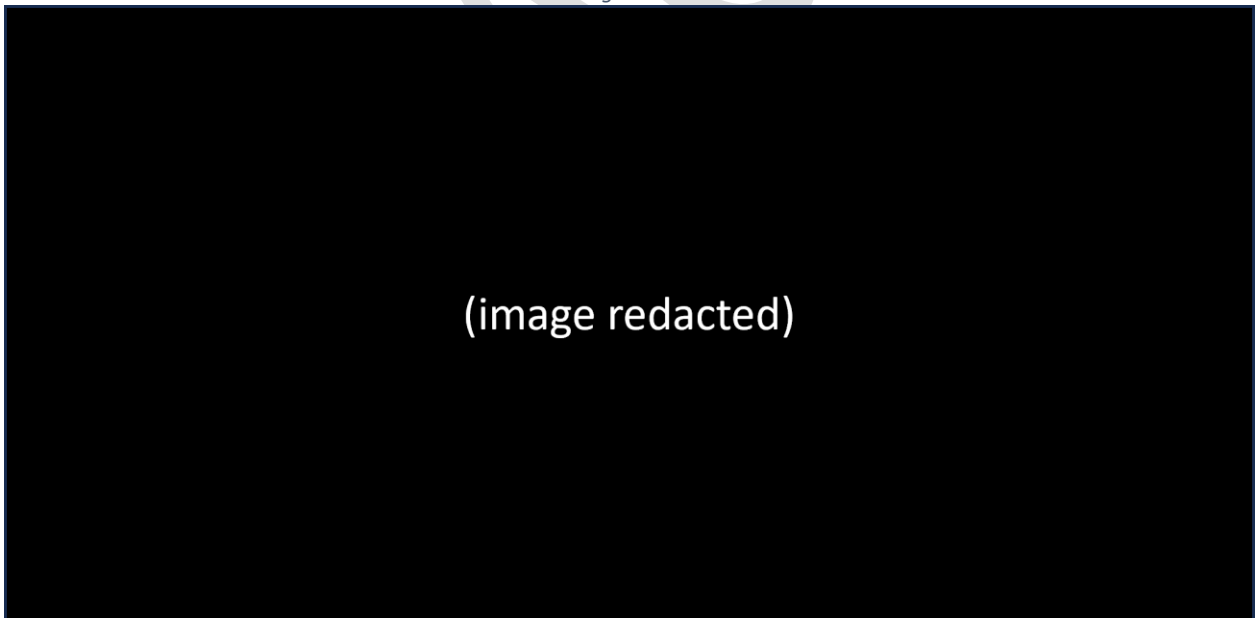
5. Click the *Continue* button. (Figure 81)

Figure 81



6. Enter the requested information in the *Add Web User* form^(a). (Figure 82)
7. Click the *Save* button^(b). (Figure 82)

Figure 82



8. Notice the new web user was added. (Figure 83 & Figure 84)

Figure 83

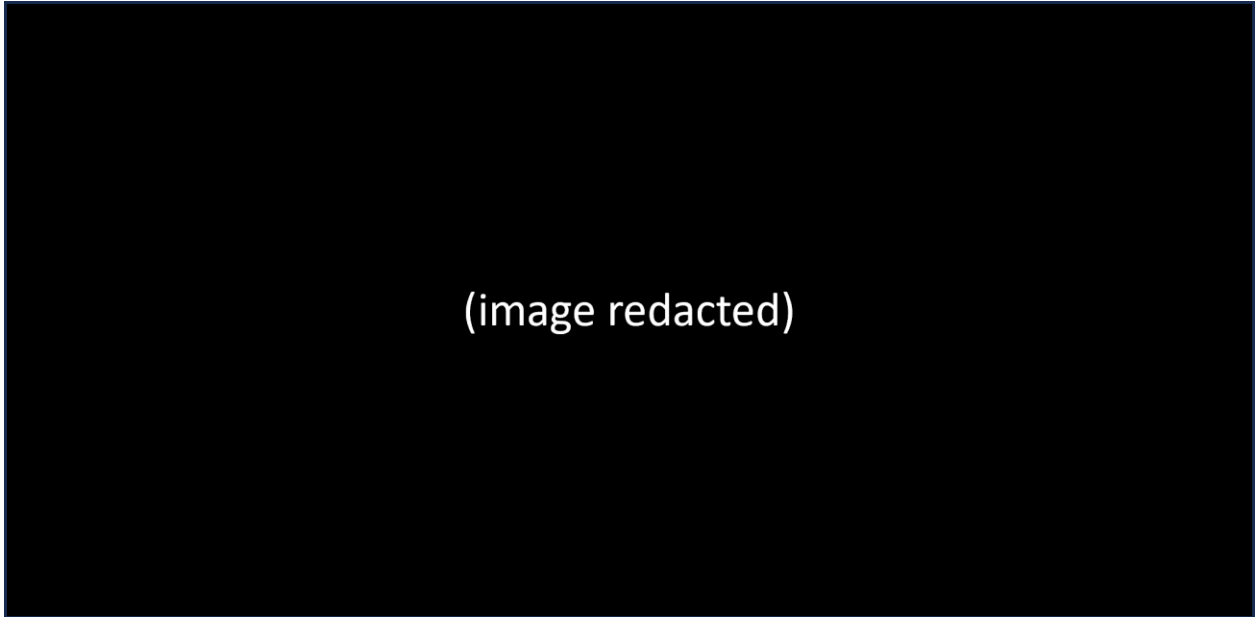
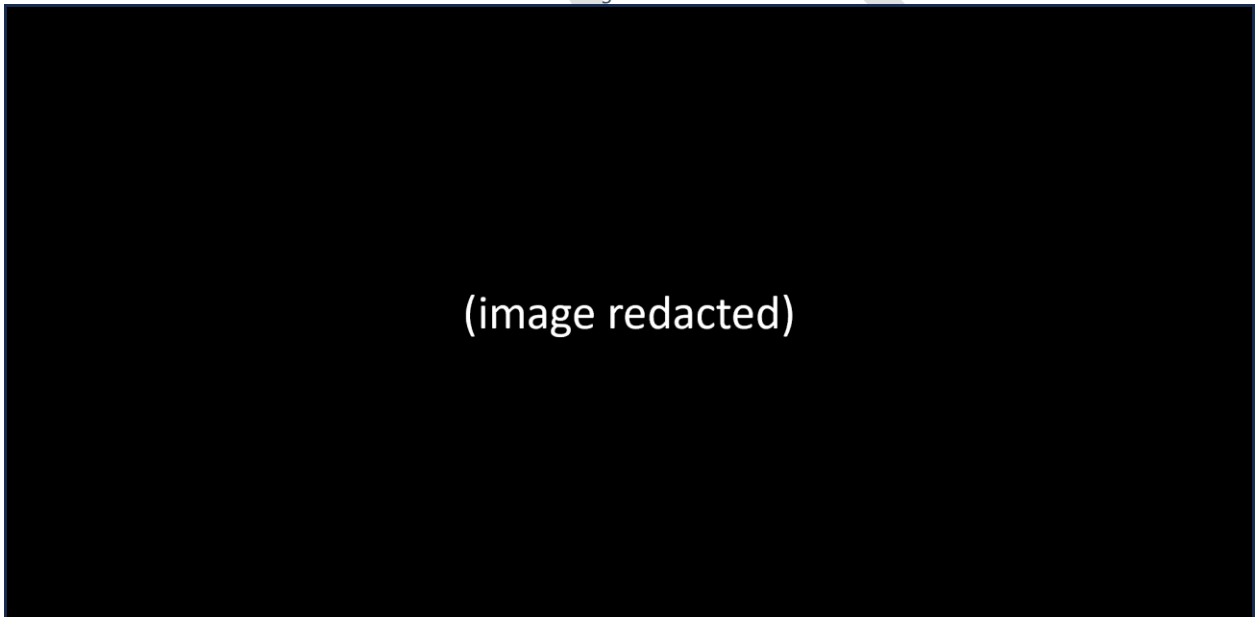


Figure 84

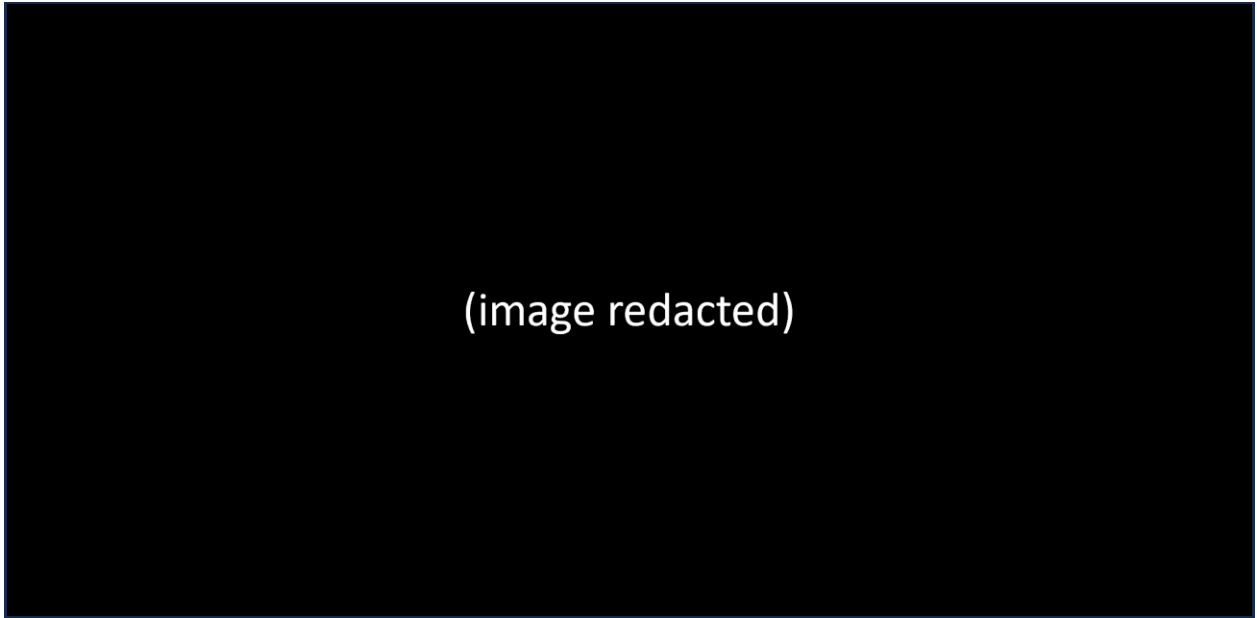


Edit a web user

To edit a web user, perform the following:

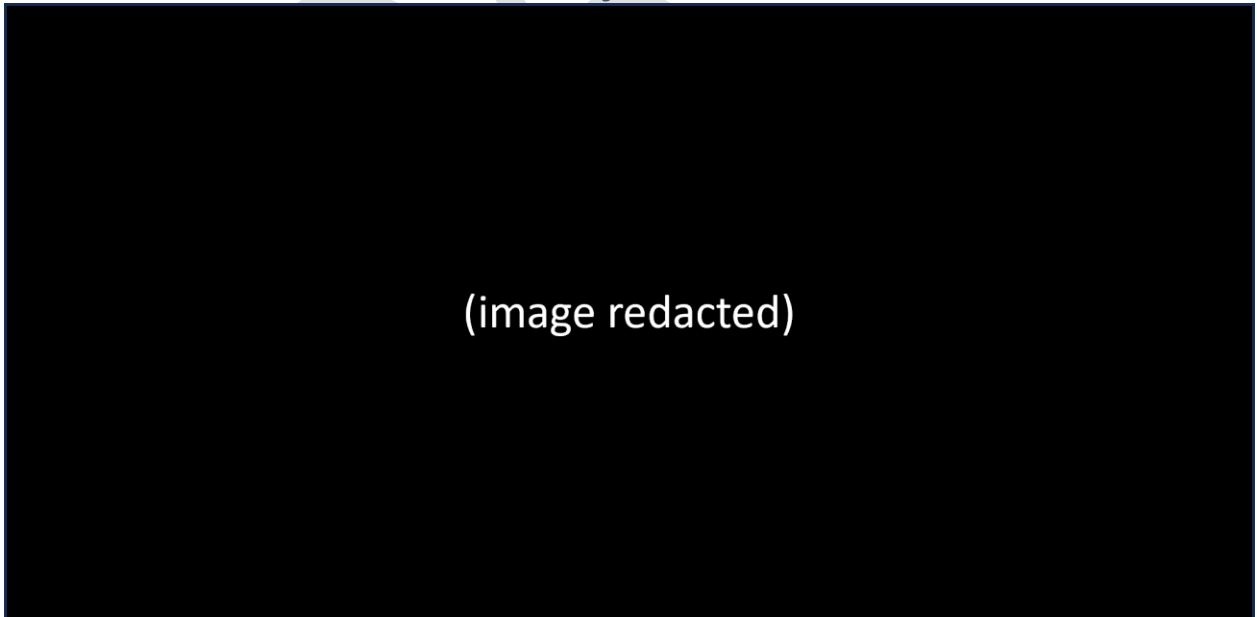
1. Click the action icon (located to the left of the User Name) you wish to edit. (Figure 85)

Figure 85



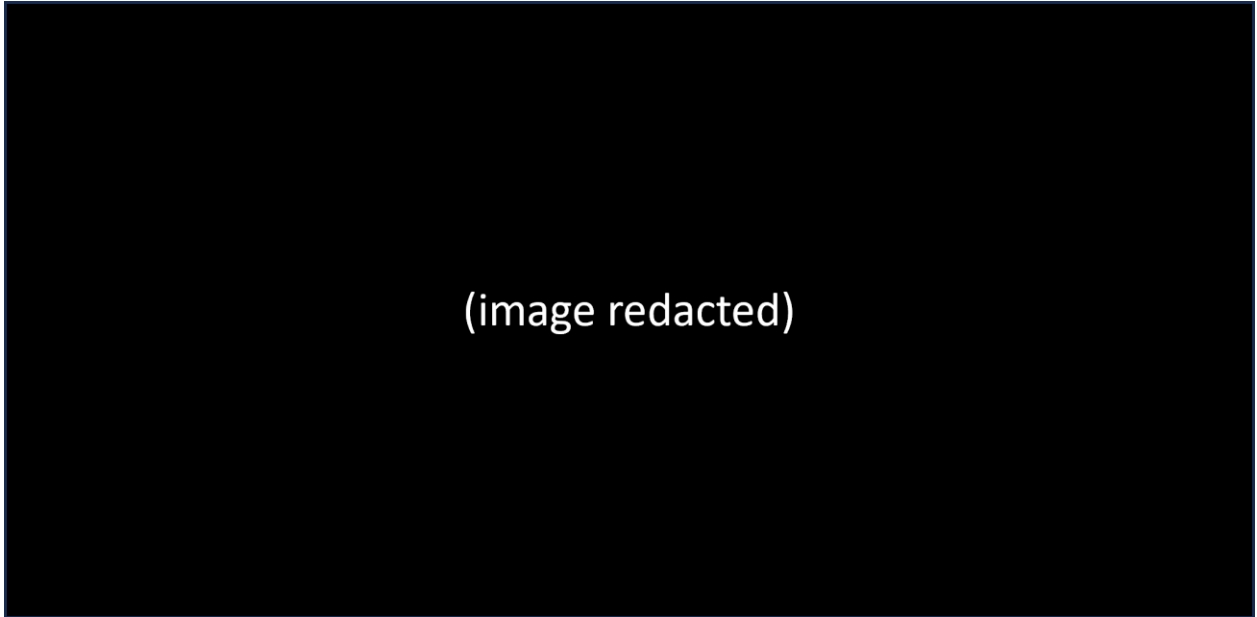
2. Select the *Edit* option. (Figure 86)

Figure 86



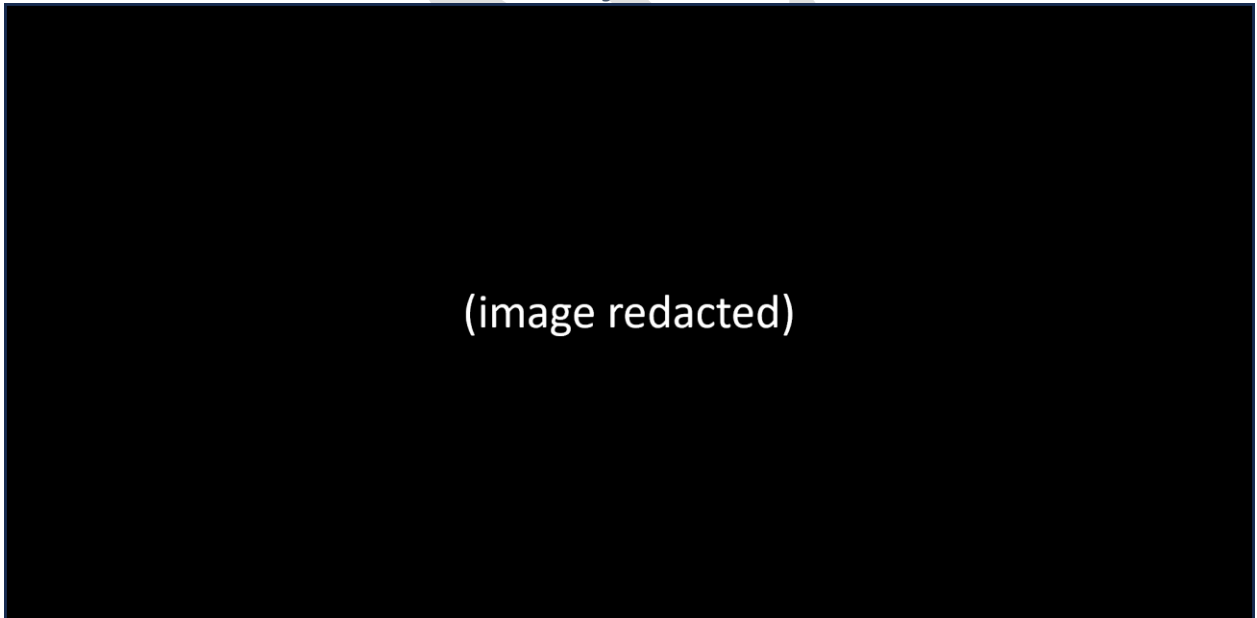
3. Edit the web user information as desired. (Figure 87)

Figure 87



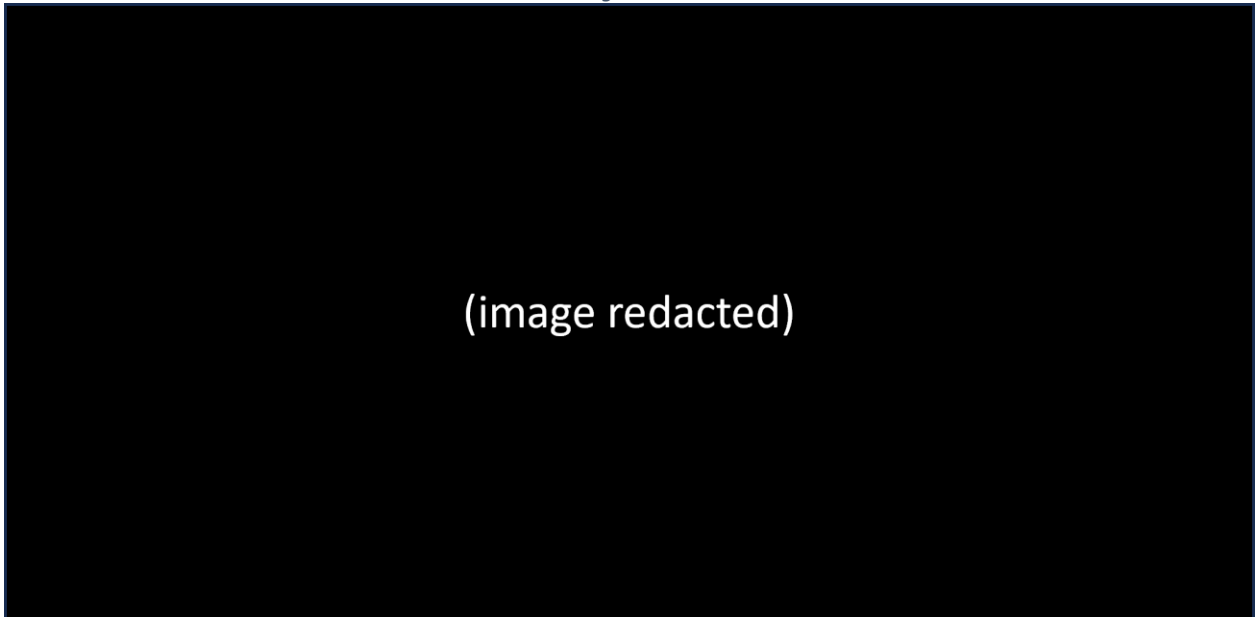
4. Click the *Save* button when finished editing the account. (Figure 88)

Figure 88



5. Notice the account has been successfully updated. (Figure 89)

Figure 89

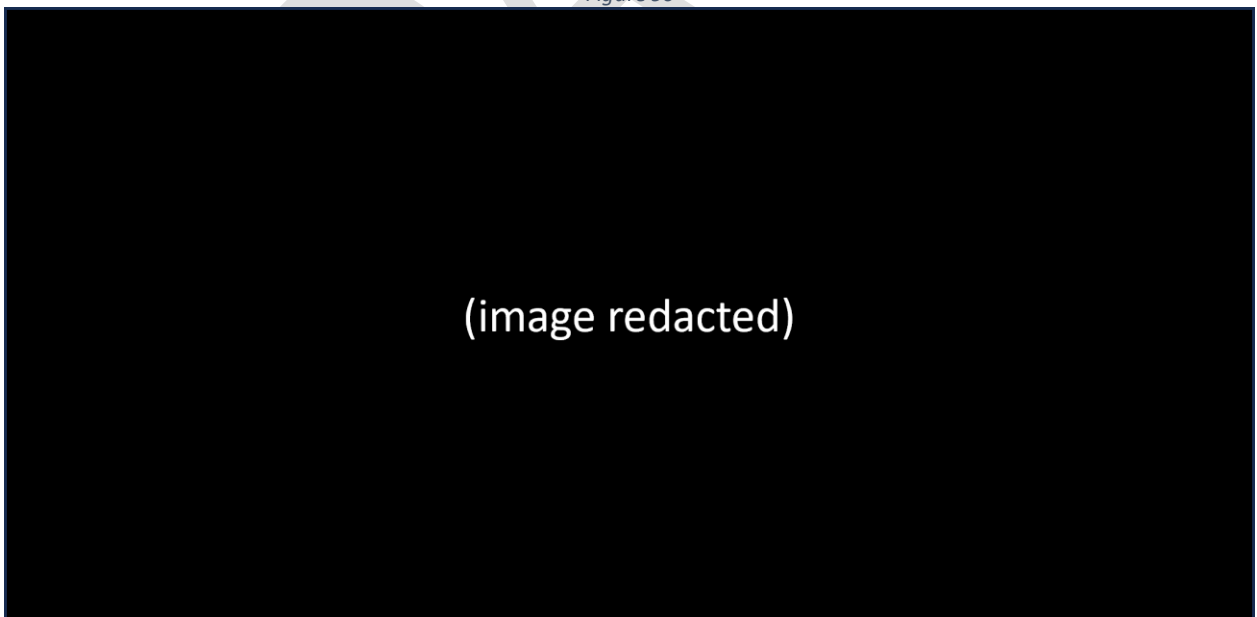


Delete a web user

To delete a web user, perform the following:

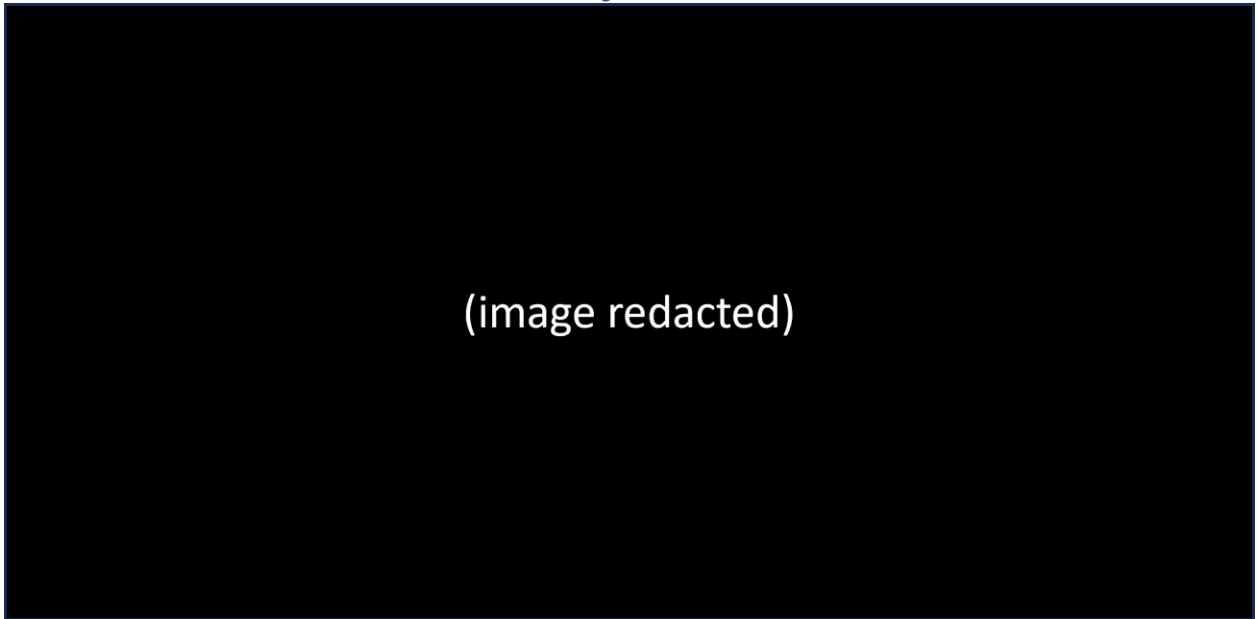
1. Click the action icon (located to the left of the User Name) you wish to delete. (Figure 90)

Figure 90



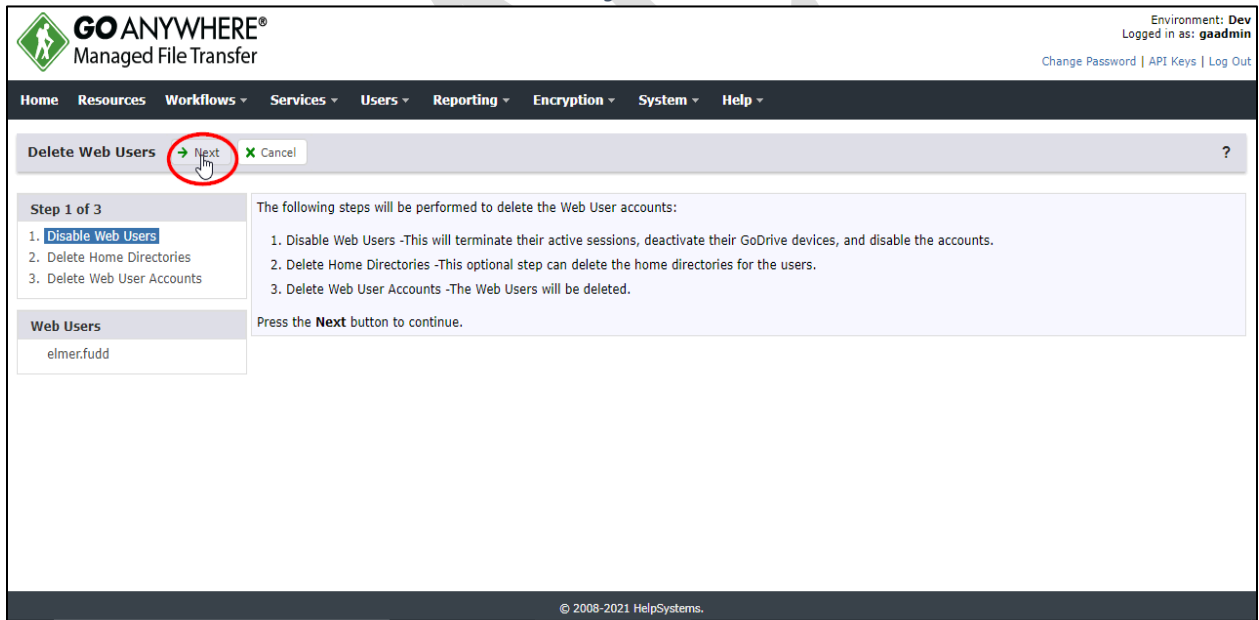
2. Select the *Delete* option. (Figure 91)

Figure 91



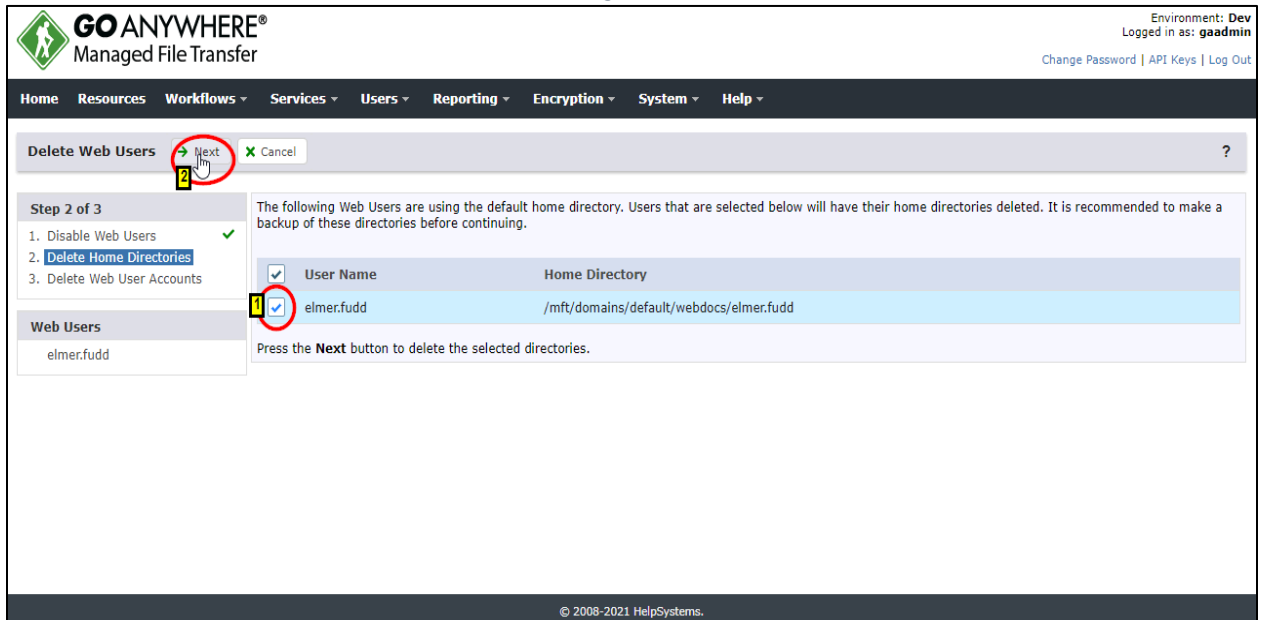
3. Click the *Next* button. (Figure 92)

Figure 92



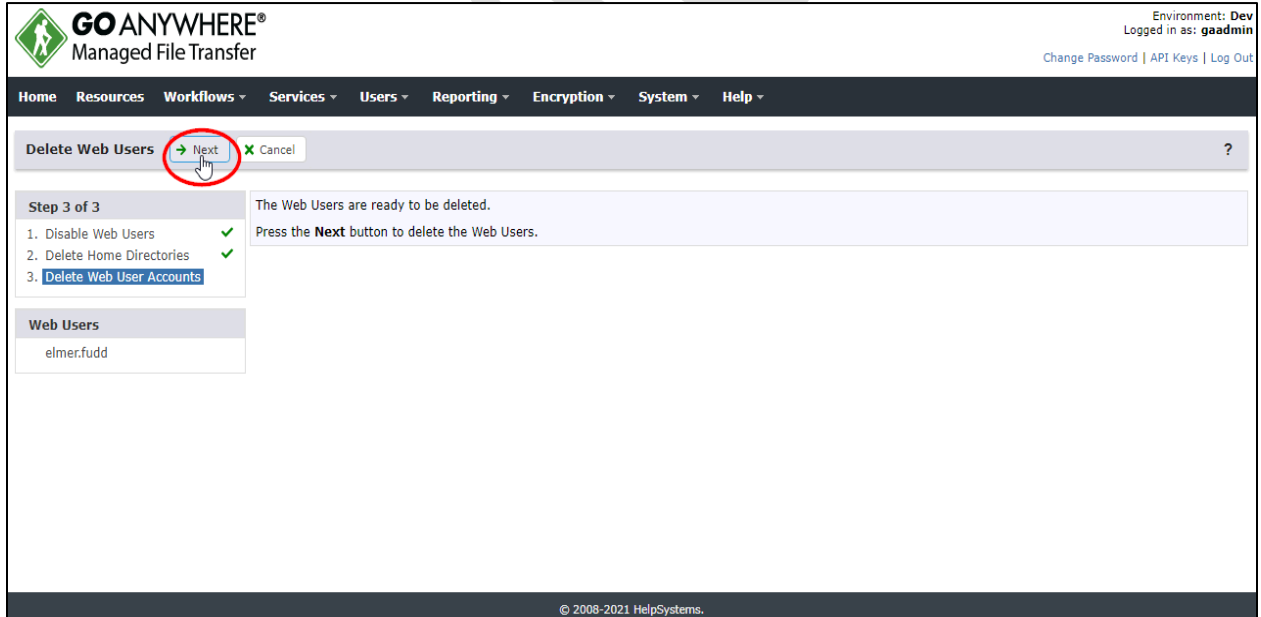
4. Check the box⁽¹⁾ associated with the user(s) you want deleted. (Figure 93)
5. Click the *Next* button⁽²⁾. (Figure 93)

Figure 93



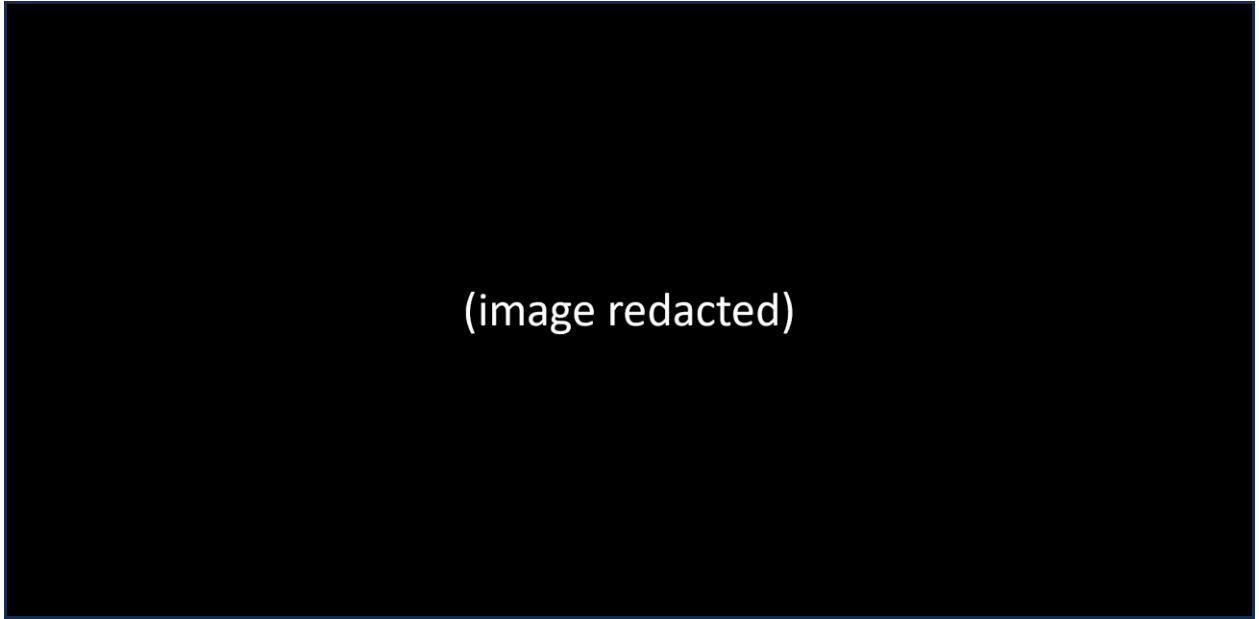
6. Click the *Next* button. (Figure 94)

Figure 94



7. Notice that the user has been deleted. (Figure 95)

Figure 95



REDACTED

Issue Resolution

Starting and stopping the GoAnywhere MFT application

To **Start** a GoAnywhere MFT application that is residing on a Linux or Unix server, perform the following:

1. Open a terminal window and navigate to the directory where GoAnywhere MFT is installed (i.e., /opt/HelpSystems/GoAnywhere.) (Figure 96)

Figure 96

```
[svc_goanywhere@vg1goappls01 HelpSystems]$ ls
GoAnywhere
[svc_goanywhere@vg1goappls01 HelpSystems]$ cd GoAnywhere/
[svc_goanywhere@vg1goappls01 GoAnywhere]$ ls
adminroot  dbscripts      jre             proddata        uninstall
as2root    gamft.lic      lib             release_notes.txt upgrader
as4root    ghttpsroot    license.html    swidtag         userdata
backups    goanywhere.sh license.txt     third_party_licenses
config     jce_policy_files messages        tomcat
[svc_goanywhere@vg1goappls01 GoAnywhere]$ pwd
/opt/HelpSystems/GoAnywhere
```

2. **Start** the GoAnywhere MFT application server by executing the following shell script (without the quotes): `./goanywhere.sh start`. (Figure 97)

Figure 97

```
un/user/935408456 PATH=/home/svc_goanywhere/.local/bin:/home/svc_goanywhere/bin
:/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin HISTSIZE=1500 LESSOPEN=||/usr
r/bin/lesspipe.sh %s _=/usr/bin/grep OLDPWD=/opt/HelpSystems
[svc_goanywhere@vg1goappls01 GoAnywhere]$ ./goanywhere.sh start
Using CATALINA_BASE:   /opt/HelpSystems/GoAnywhere/tomcat
Using CATALINA_HOME:   /opt/HelpSystems/GoAnywhere/tomcat
Using CATALINA_TMPDIR: /opt/HelpSystems/GoAnywhere/tomcat/temp
Using JRE_HOME:        ./tomcat/bin/../../jre
Using CLASSPATH:       /opt/HelpSystems/GoAnywhere/tomcat/bin/goanywhere_bootst
rap.jar:/opt/HelpSystems/GoAnywhere/tomcat/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Using GA_HOME:         /opt/HelpSystems/GoAnywhere
Tomcat started.
```

To **Stop** a *GoAnywhere MFT* application that is residing on a Linux or Unix server, perform the following:

1. Open a terminal window and navigate to the directory where *GoAnywhere MFT* is installed (i.e., `/opt/HelpSystems/GoAnywhere.`) (Figure 98)

Figure 98

```
[svc_goanywhere@vg1goappls01 HelpSystems]$ ls
GoAnywhere
[svc_goanywhere@vg1goappls01 HelpSystems]$ cd GoAnywhere/
[svc_goanywhere@vg1goappls01 GoAnywhere]$ ls
adminroot  dbscripts      jre             proddata        uninstall
as2root    gamft.lic      lib             release_notes.txt upgrader
as4root    ghttpsroot    license.html    swidtag         userdata
backups    goanywhere.sh license.txt     third_party_licenses
config     jce_policy_files messages        tomcat
[svc_goanywhere@vg1goappls01 GoAnywhere]$ pwd
/opt/HelpSystems/GoAnywhere
```

2. **Stop** the *GoAnywhere MFT* application server by executing the following shell script (without the quotes: `./goanywhere.sh stop`). (Figure 99)

Figure 99

```
[svc_goanywhere@vg1goappls01 GoAnywhere]$ ls
adminroot  dbscripts      jre             proddata        uninstall
as2root    gamft.lic      lib             release_notes.txt upgrader
as4root    ghttpsroot    license.html    swidtag         userdata
backups    goanywhere.sh license.txt     third_party_licenses
config     jce_policy_files messages        tomcat
[svc_goanywhere@vg1goappls01 GoAnywhere]$ pwd
/opt/HelpSystems/GoAnywhere
[svc_goanywhere@vg1goappls01 GoAnywhere]$ pwd
/opt/HelpSystems/GoAnywhere
[svc_goanywhere@vg1goappls01 GoAnywhere]$ ./goanywhere.sh stop
```

3. The example below shows the results. (Figure 100)

Figure 100

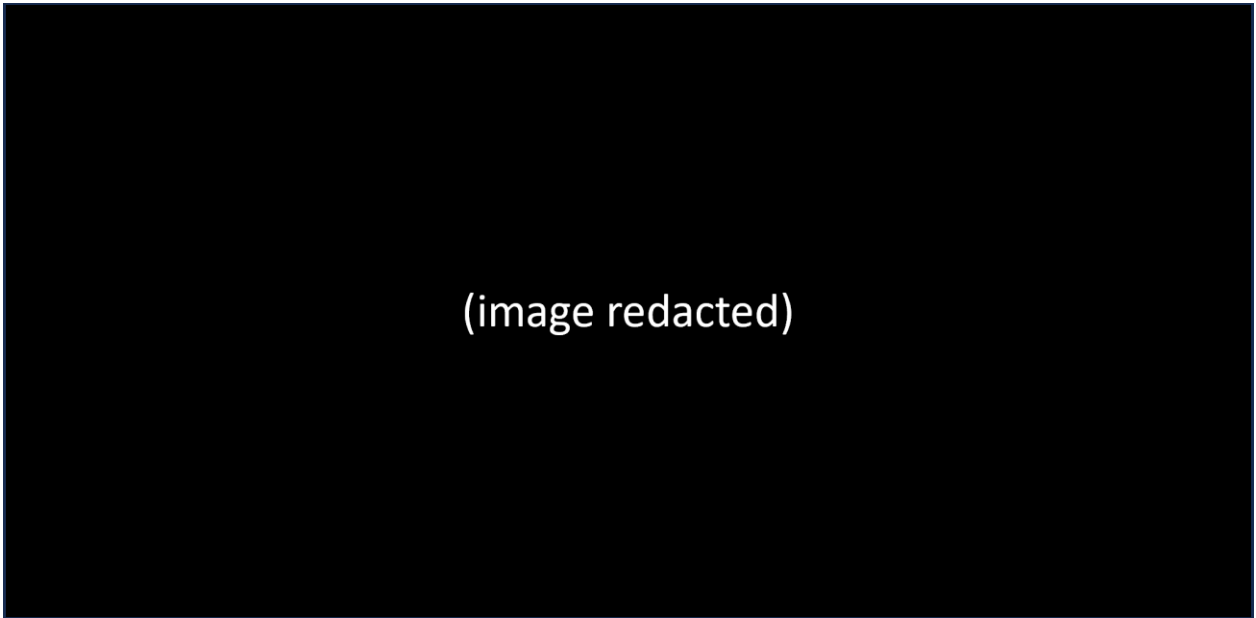
```
[svc_goanywhere@vg1goapplds01 GoAnywhere]$ ./goanywhere.sh stop
Using CATALINA_BASE: /opt/HelpSystems/GoAnywhere/tomcat
Using CATALINA_HOME: /opt/HelpSystems/GoAnywhere/tomcat
Using CATALINA_TMPDIR: /opt/HelpSystems/GoAnywhere/tomcat/temp
Using JRE_HOME: ./tomcat/bin/../../jre
Using CLASSPATH: /opt/HelpSystems/GoAnywhere/tomcat/bin/goanywhere_bootstrap.jar:/opt/HelpSystems/GoAnywhere/tomcat/bin/tomcat-juli.jar
Using CATALINA_OPTS:
Using GA_HOME: /opt/HelpSystems/GoAnywhere
Loading config directory property from: /opt/HelpSystems/GoAnywhere/config/system.properties
Loading config directory property from: config/system.properties
```

Server post-outage checklist

Whenever a *Go Anywhere MFT* server is brought online, whether as the result of a planned or unplanned outage, the following steps should be performed to ensure its proper operation going forward:

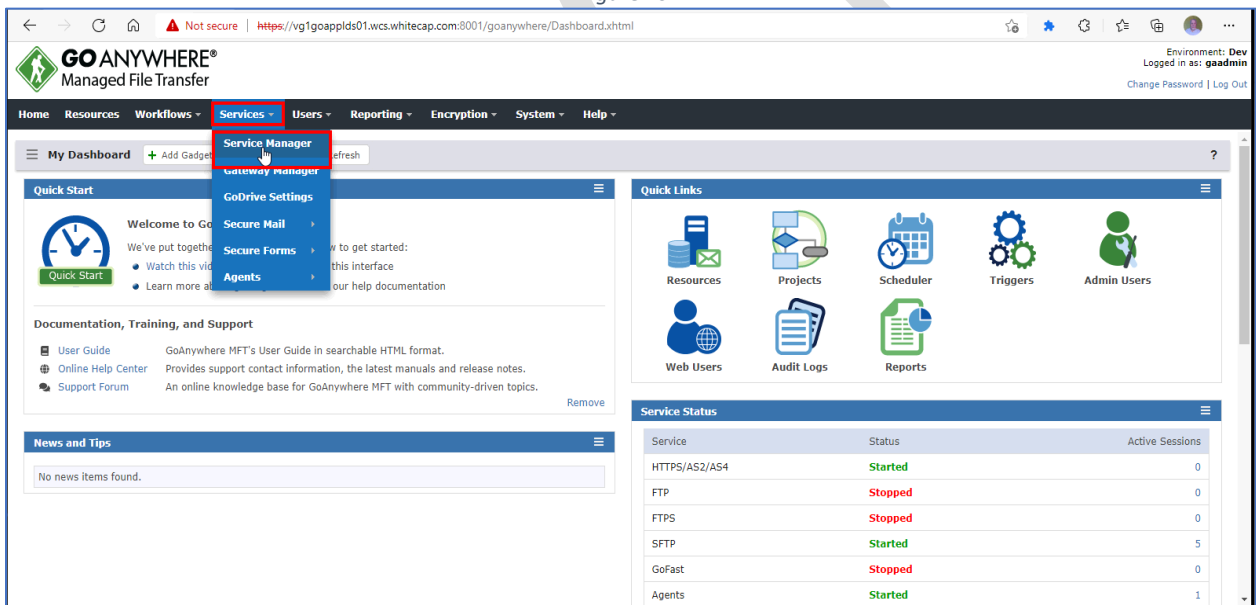
1. Verify the server is online.
 - If it is, continue to step 2.
 - If it is not, gather the following data and then engage the Linux team for help with resolution:
 - **What is the server name (SFTP connection)?**
 - **Is the file transport Inbound or Outbound?**
 - **What is the directory structure?**
 - **What is the current amount of available space on the server?**
2. Log in to the [REDACTED] *GoAnywhere MFT* dashboard at [https://\[REDACTED\]:8001/goanywhere/Dashboard.xhtml](https://[REDACTED]:8001/goanywhere/Dashboard.xhtml). (Figure 101)
 - If you are not able to access this URL, engage the Linux team for help with resolution.

Figure 101



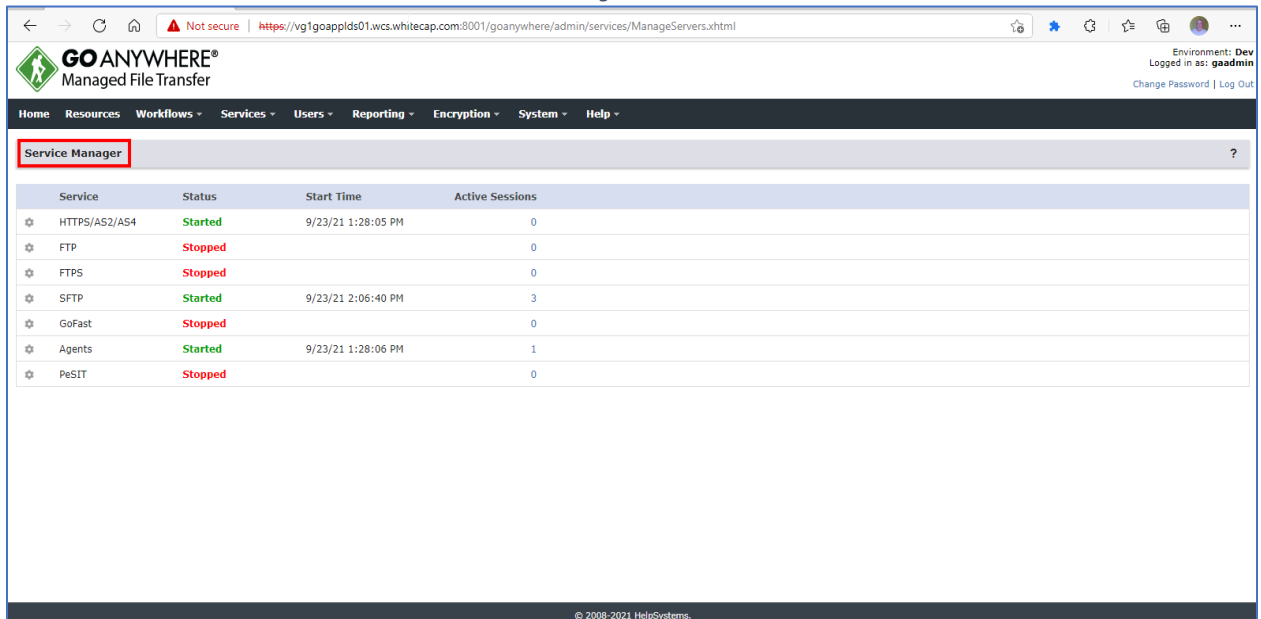
3. Select *Services > Service Manager*. (Figure 102)

Figure 102



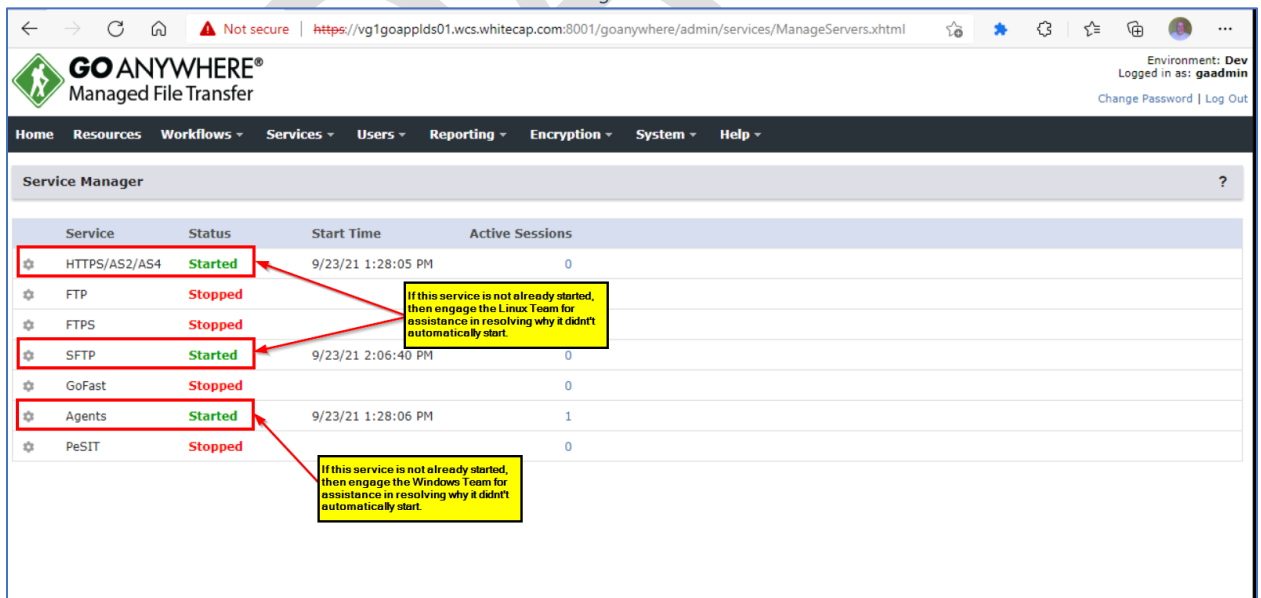
4. Does that take you to the *Service Manager*? (Figure 103)
 - If not, engage the Linux team for help with resolution.

Figure 103



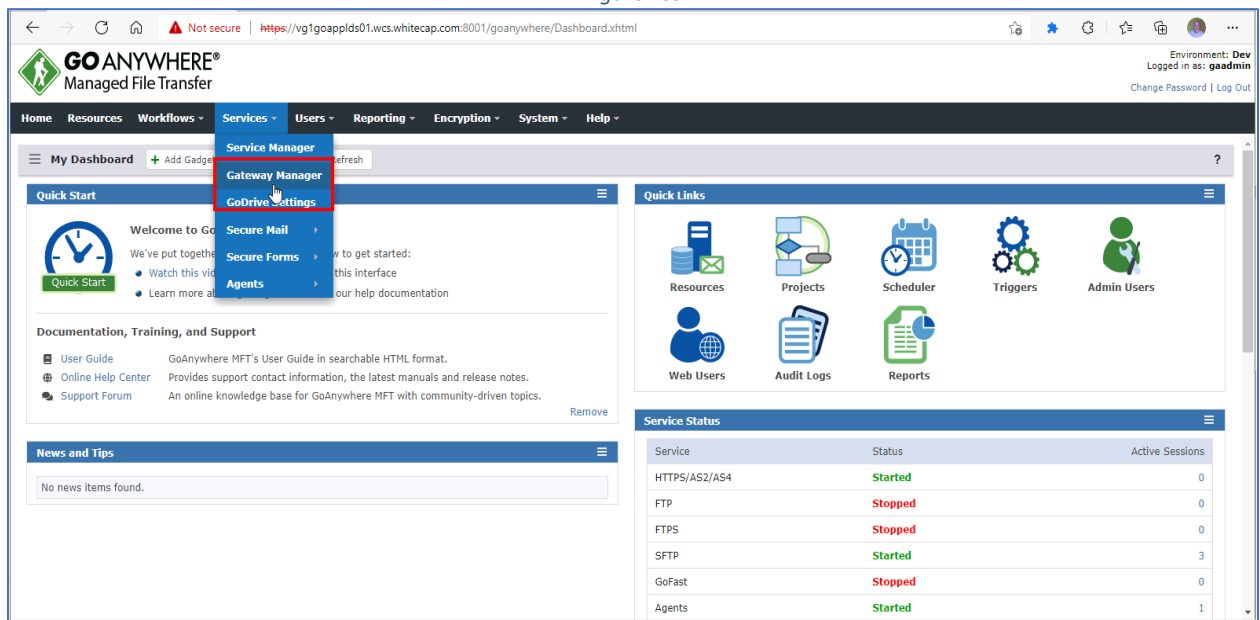
5. Are *HTTPS*, *SFTP*, and *Agents* started? (Figure 104)
 - If *HTTPS* or *SFTP* are not started, engage the Linux team for help with resolution.
 - If *Agents* is not started, engage the Windows team for help with resolution.

Figure 104



6. Select *Services > Gateway Manager* (Figure 105)

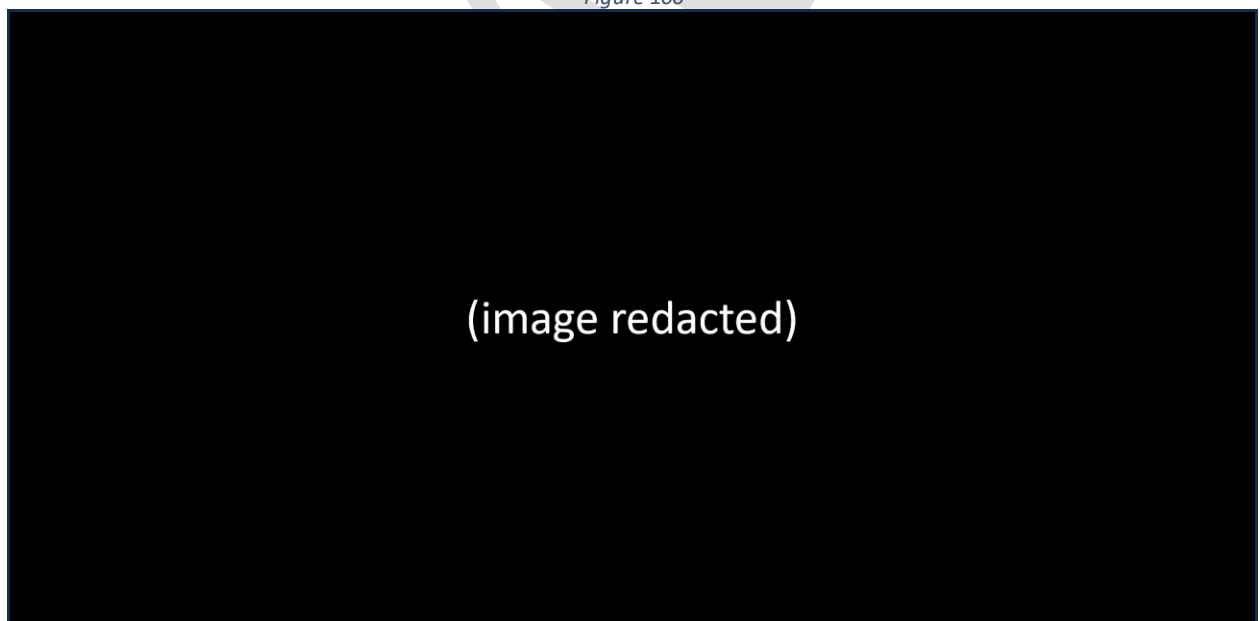
Figure 105



7. Does that take you to the *Gateway Manager*? (Figure 106)

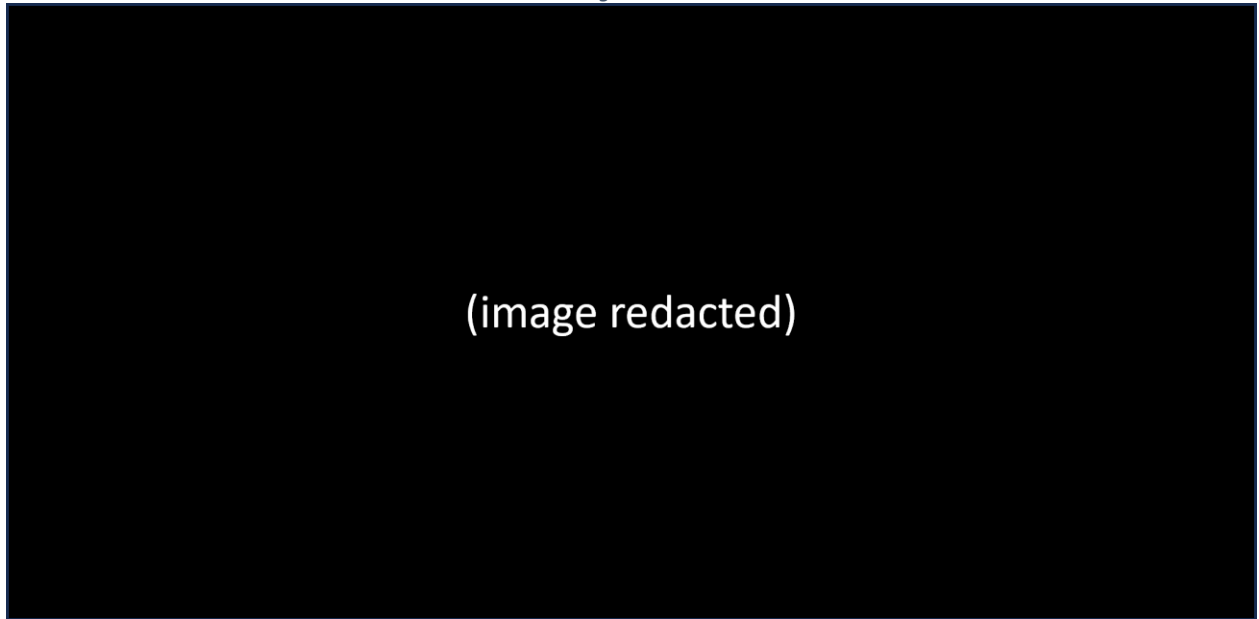
- If not, engage the Linux team (or other applicable team) for help with resolution

Figure 106



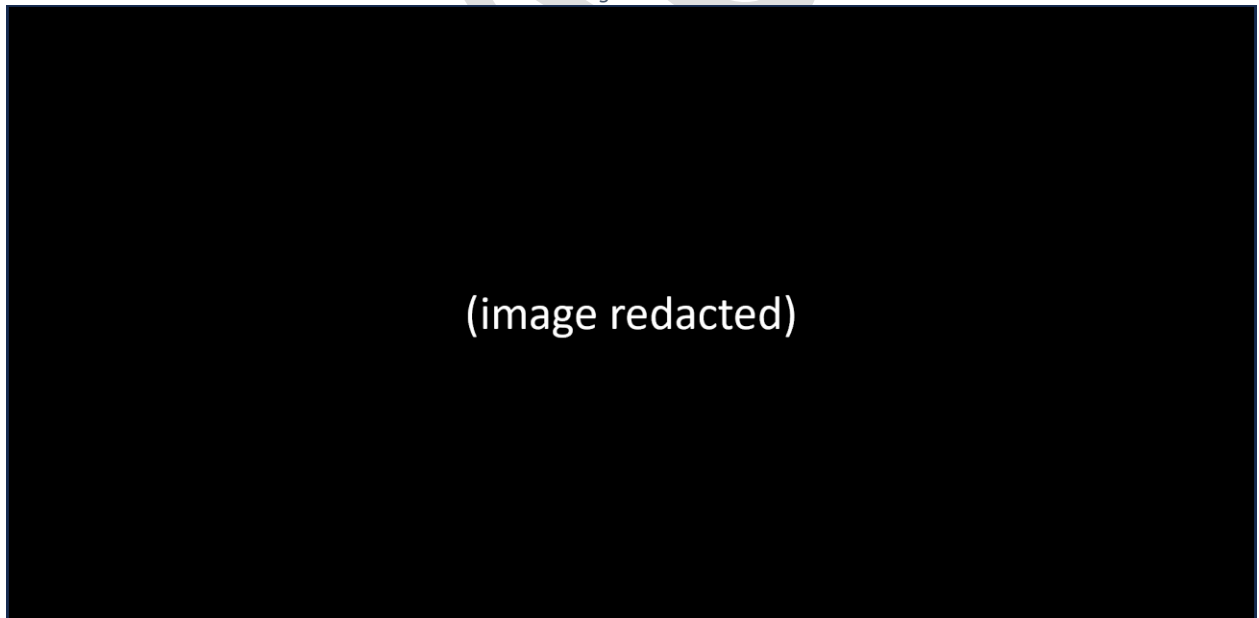
8. Select *Resources* and review the displayed connections for any issues (Figure 107)
 - If issue(s) are found, engage the Linux team (or other applicable team) for help with resolution.

Figure 107



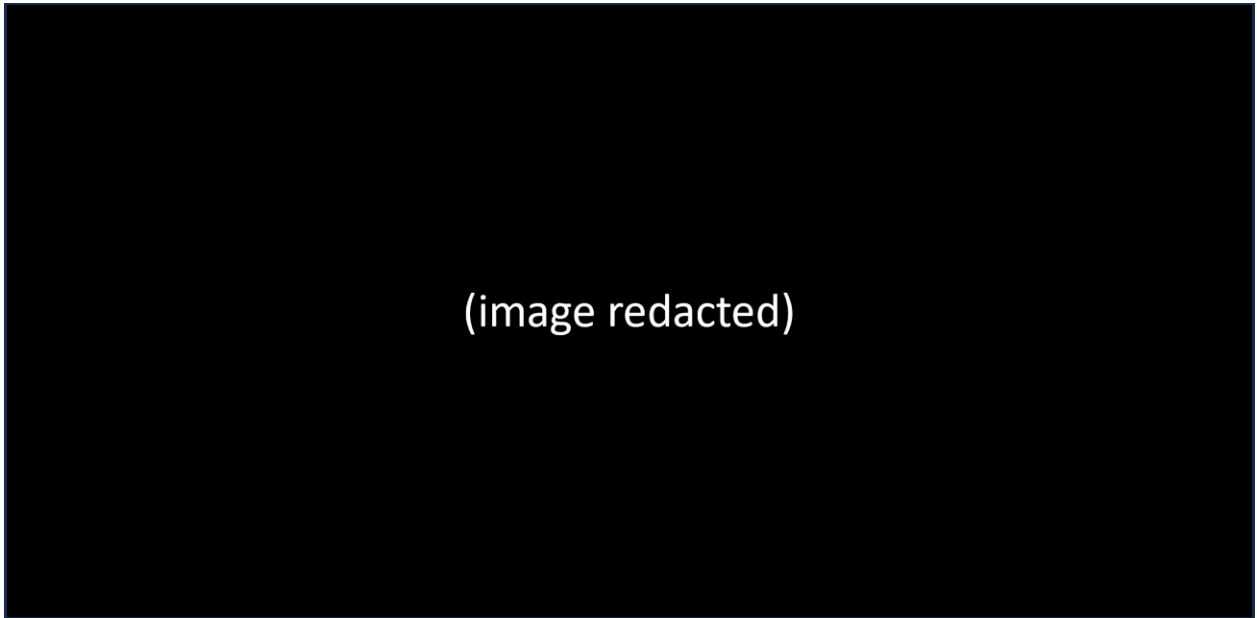
9. Select *Reporting > Audit Logs* (Figure 108)

Figure 108



10. Select *System* and review the displayed system log for any issues (Figure 109)
 - If issue(s) are found, engage the Linux team (or other applicable team) for help with resolution.

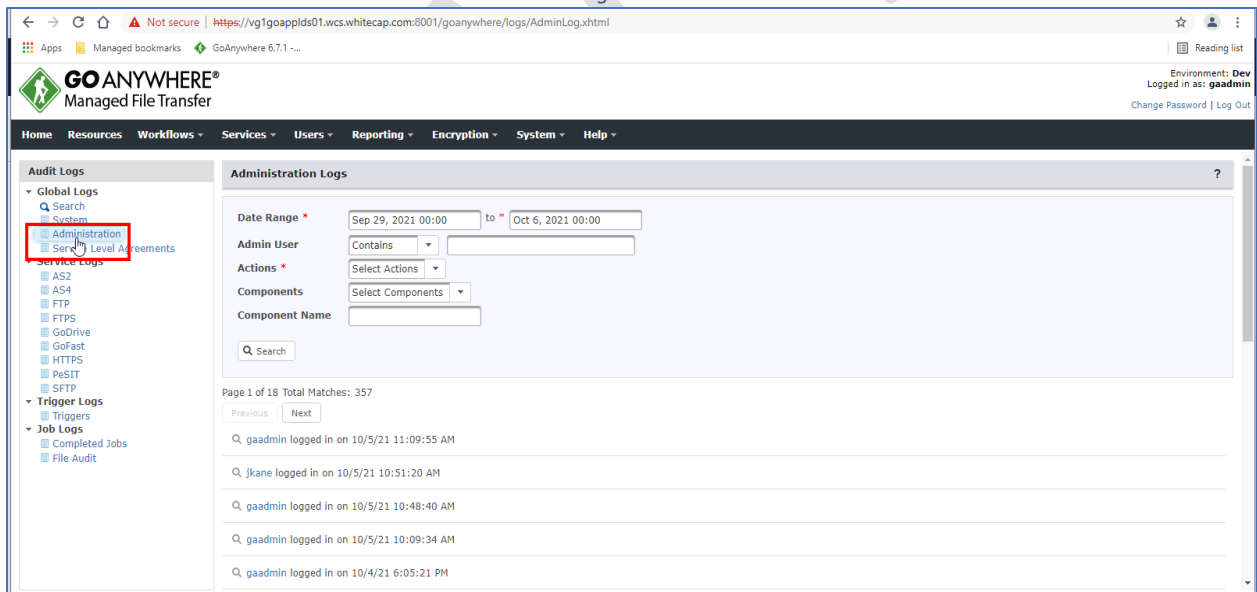
Figure 109



11. Select *Administration* and review the displayed log for any issues (Figure 110)

- If issue(s) are found, engage the Linux team (or other applicable team) for help with resolution.

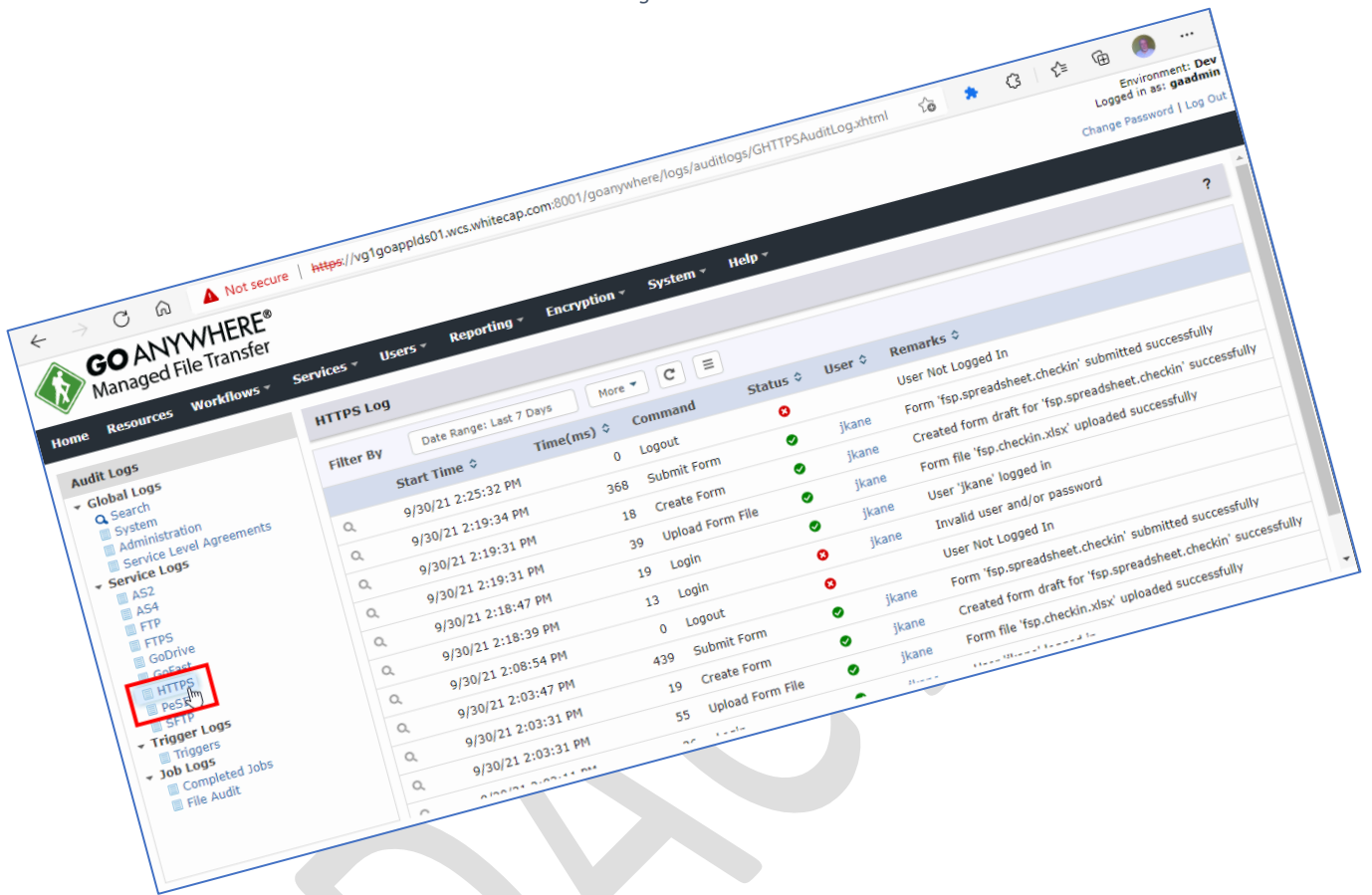
Figure 110



12. Under *Service Logs*, select *HTTPS* and review the displayed information (Figure 111)

- If issue(s) are found, engage the Linux team (or other applicable team) help with resolution.

Figure 111



13. Under *Service Logs*, select *SFTP* and review the displayed information (Figure 112)

- If issue(s) are found, engage the Linux team (or other applicable team) for help with resolution.
- If no issues are found at this point, the server is online successfully.

Figure 112

The screenshot displays the GoAnywhere Managed File Transfer web interface. The top navigation bar includes links for Home, Resources, Workflows, Services, Users, Reporting, Encryption, System, and Help. The left sidebar shows a tree view of logs, with 'SFTP' highlighted under 'Service Logs'. The main area shows the 'SFTP Log' with a table of events. The table has columns for Event ID, System Name, Start Time, End Time, Time(ms), Command, Event Type, and Status. The events listed are a sequence of connect and disconnect actions for various event IDs on 10/6/21.

Event ID	System Name	Start Time	End Time	Time(ms)	Command	Event Type	Status
Default_7583839	Default	10/6/21 2:15:36 PM	10/6/21 2:15:36 PM	0	Disconnect	Disconnect	✓
Default_7583838	Default	10/6/21 2:15:36 PM	10/6/21 2:15:36 PM	0	Connect	Connection Successful	✓
Default_7583837	Default	10/6/21 2:15:36 PM	10/6/21 2:15:36 PM	0	Disconnect	Disconnect	✓
Default_7583836	Default	10/6/21 2:15:36 PM	10/6/21 2:15:36 PM	0	Connect	Connection Successful	✓
Default_7583835	Default	10/6/21 2:15:31 PM	10/6/21 2:15:31 PM	0	Disconnect	Disconnect	✓
Default_7583834	Default	10/6/21 2:15:31 PM	10/6/21 2:15:31 PM	0	Connect	Connection Successful	✓
Default_7583832	Default	10/6/21 2:15:31 PM	10/6/21 2:15:31 PM	0	Connect	Connection Successful	✓
Default_7583833	Default	10/6/21 2:15:31 PM	10/6/21 2:15:31 PM	0	Disconnect	Disconnect	✓
Default_7583831	Default	10/6/21 2:15:26 PM	10/6/21 2:15:26 PM	0	Disconnect	Disconnect	✓
Default_7583830	Default	10/6/21 2:15:26 PM	10/6/21 2:15:26 PM	0	Connect	Connection Successful	✓

REDACTED

Appendix

Glossary of terms

The following terms are used within this document.

Term	Description
Agent	<i>Agents</i> provide real-time remote workflow and file transfer capabilities that are controlled from a central server. <i>Agents</i> can run on systems inside an organization's network to move files throughout the data center. Additionally, you can deploy <i>Agents</i> to remote sites. At [REDACTED], when an <i>Agent</i> starts up, it will connect to <i>GoAnywhere MFT</i> which will then take over management of that <i>Agent</i> .
Certificate	Certificates are digital identification documents that allow both servers and clients to authenticate each other. A certificate contains information about a company and the organization that signed the certificate. Certificates are used within SSL connections.
Gateway	A <i>Gateway</i> is a network node equipped for interfacing with another network that uses different communication protocols. The <i>GoAnywhere Gateway</i> integrates with the <i>GoAnywhere MFT</i> file server to provide a secure and managed solution for hosting and exchanging files.
GoAnywhere MFT	The collection of software components used by [REDACTED] for the SFTP transfer of its inbound and outbound files. The application is located at: https://[REDACTED]:8001/goanywhere/Dashboard.xhtml
Key pair	A key pair is a combination of a public key that is used to encrypt data and a private key that is used to decrypt data.
Key Vault	<i>GoAnywhere MFT's</i> integrated Key Management Systems allows administrators to create Key Vaults that are used to create and store certificates, SSH keys, and PGP keys. By default, <i>GoAnywhere MFT</i> includes two Key Vaults, the System and Default vaults.
Linux Team	The [REDACTED] team responsible for providing support of the Linux operating system at [REDACTED]. NOTE: As of this writing (10/05/2021), the Linux team can be reached at LinuxTeam@[REDACTED]. A list of the current team members can be found by viewing the members of the MS-Outlook distribution list [REDACTED] IT Linux Team.
MFT	M anaged F ile T ransfer
Private key	In cryptography, a private key is a large, randomly-generated number with hundreds of digits. If you encode a message using a person's public key, they can only decode it using their matching private key.
Public key	In cryptography, a public key is a large numerical value that is used to encrypt data. The public key is used for encrypting plain text to convert it into cipher text.
SFTP	S SH (or S ecure) F ile T ransfer P rotocol. A network protocol that provides file access, file transfer, and file management over any reliable data stream.
SSH	The S ecure S hell Protocol (SSH) is a cryptographic network protocol for operating network services securely over an unsecured network. Its most notable applications are remote login and command-line execution.
SSL	S SL is an abbreviation for S ecure S ockets L ayer. SSL is a security protocol for encrypting communications between two hosts over a network. SSL utilizes certificates to establish trust

Term	Description
	between the two hosts.
VDI	<u>V</u> irtual <u>D</u> esktop <u>I</u> nfrastructure is a <i>Citrix/Microsoft</i> desktop virtualization engine.
Windows Team	The [REDACTED] team responsible for providing support of the Windows operating system at [REDACTED]. NOTE: As of this writing, the Windows team can be reached at [REDACTED]@[REDACTED]_or [REDACTED]@[REDACTED].

Admin user roles

The following table describes the roles and privileges that can be assigned to “administrative level” (aka admin user) users.

Admin role	Privileges
Agent Manager	<ul style="list-style-type: none"> • Create, configure, deploy, and monitor Agents.
Auditor	<ul style="list-style-type: none"> • View Resources, Projects, and Project categories, Monitors, Triggers, Schedules, Secure Forms, and Secure Mail Packages. • View Logs and Reports for GoDrive, GoFast, FTP, FTPS, SFTP, HTTPS, AS2, AS4, PeSIT, Completed Jobs, and Triggers. • View Admin Users, Groups, Templates, Active Sessions, and Roles. • View Partners. • View Web Users, Groups, Templates, Active Sessions, Active Transfers, and Devices. • View all configurations including Database, Domains, Gateway, Holiday Calendars, IP Filters, Licenses, Log Exemptions, Login Methods, Master Encryption Keys, Job Queues, and SLAs. • View defined objects including Add-Ons, Address Books, Agent Templates, Custom Tasks, Encrypted Folders, and Key Vaults.
Dashboard Manager	<ul style="list-style-type: none"> • Manage Shared Dashboards.
File Manager	<ul style="list-style-type: none"> • Manage files (for example, download, copy, delete, upload) on the server on which GoAnywhere is installed.
Job Manager	<ul style="list-style-type: none"> • Add, change, and delete Scheduled Jobs and Monitors. • Disable Monitors or Scheduled Jobs. • View any jobs in the job queue. • Cancel any jobs from the job queue. • View, hold, release, and cancel any active jobs. • View any completed job logs for Projects. • View change history for Monitors and Scheduled Jobs.
Key Manager	<ul style="list-style-type: none"> • Manage PGP keys. • Manage SSH keys. • Manage SSL certificates.

Admin role	Privileges
Log Viewer	<ul style="list-style-type: none"> • View Audit Logs for GoDrive, FTP, FTPS, SFTP, HTTPS, AS2, AS4, and PeSIT services. • View statistics of total uploads, downloads, and errors. • View the Server Log. • View Trigger Logs. • View Completed Job Logs for Projects.
Partner Manager	<ul style="list-style-type: none"> • Create, configure, and delete Partners.
Product Administrator	<ul style="list-style-type: none"> • View and change global preferences. • Download product updates. • View, install and uninstall the product license. • View the Server Log. • Manage Partners. • Manage Services Configuration and Preferences. • Manage GoAnywhere Gateway. • Configure, tune, and migrate the GoAnywhere database. • View and change settings for the Log Settings and Audit Log Rules. • Manage GoDrive Settings. • Manage AS4 Message Channels. • Manage PeSIT File Templates.
Project Designer	<ul style="list-style-type: none"> • Create new Project folders. • Rename and delete Project folders*. • Create, change, copy and delete Projects*. • Restore Projects to previous versions*. • Import Project definitions from external sources*. • Promote Projects into other installations of GoAnywhere*.
Project Executor	<ul style="list-style-type: none"> • Run Projects*. • Monitor jobs on the job queue (which the Project Executor submitted). • Monitor active jobs (which the Project Executor submitted). • View completed jobs and job logs (which the Project Executor submitted).
Resource Manager	<ul style="list-style-type: none"> • Add new Resources (FTP server connections, database connections, HTTP connections, etc.). • Change and Delete Resources (if they have WRITE permission on the Resource). • View existing Resources (if they have READ permission on the Resource). • Promote Resources into other installations of GoAnywhere.

Admin role	Privileges
Secure Forms Manager	<ul style="list-style-type: none"> • View and edit Secure Forms settings. • Create and manage Secure Forms. • View Secure Forms submissions.
Secure Mail Manager	<ul style="list-style-type: none"> • View and edit Secure Mail settings. • Manage Packages.
Security Officer	<ul style="list-style-type: none"> • Manage Domains. • Configure how User and Web User passwords are authenticated. • Manage Admin User API Keys. • Manage Users and their assigned Roles. • Manage Groups and their assigned Roles. • Manage IP Filters. • Manage Web User Password Policy. • Manage Web User Self-Registration Settings. • Reset User passwords.
Trigger Manager	<ul style="list-style-type: none"> • Manage Triggers. • View Trigger Logs. • View Trigger change history.
Web User Device Manager	<ul style="list-style-type: none"> • Manage Web User devices.
Web User Manager	<ul style="list-style-type: none"> • Manage Web Users and their assigned permissions. • Manage Web User Groups and their assigned permissions. • Assign Web Users to Web User Groups. • Manage Web User Templates. • View change history for Web Users and Web User Groups. • View Audit Logs for GoDrive, FTP, FTPS, SFTP, HTTPS, AS2, AS4, and PeSIT services.

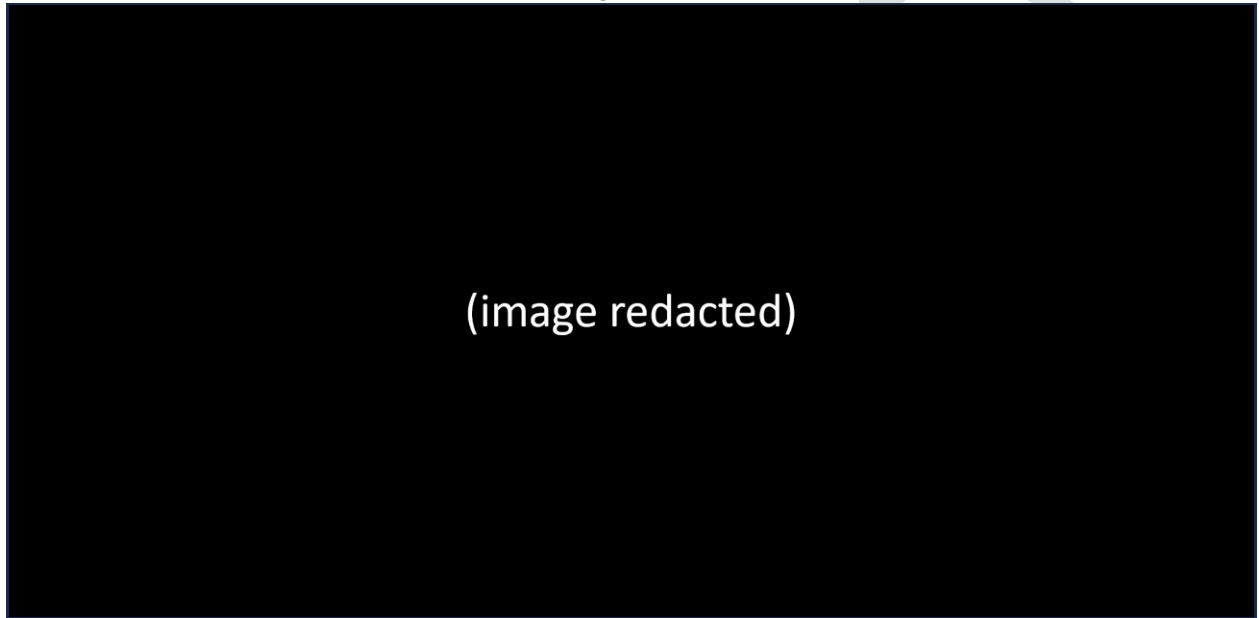
** The Admin User must also have appropriate permissions to the Project folder.*

Accessing the [REDACTED] Citrix VDI desktop

To launch certain applications, such as *GoAnywhere MFT*, the user must first be logged into the *Citrix VDI* platform. To access the [REDACTED] Citrix VDI desktop, perform the following:

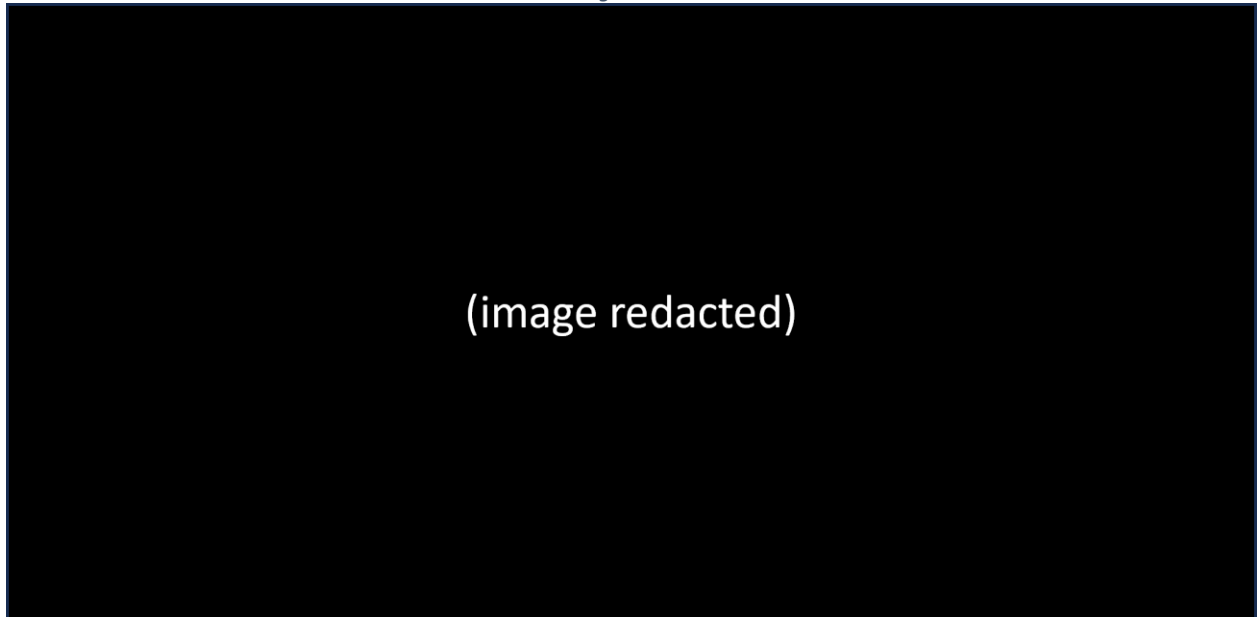
1. Navigate to VDI at [https://apps. \[REDACTED\]/Citrix/\[REDACTED\]/](https://apps.[REDACTED]/Citrix/[REDACTED]/). (Figure 113)
2. Select a desktop⁽¹⁾. (Figure 113)
3. Click the *Open* icon⁽²⁾. (Figure 113)

Figure 113



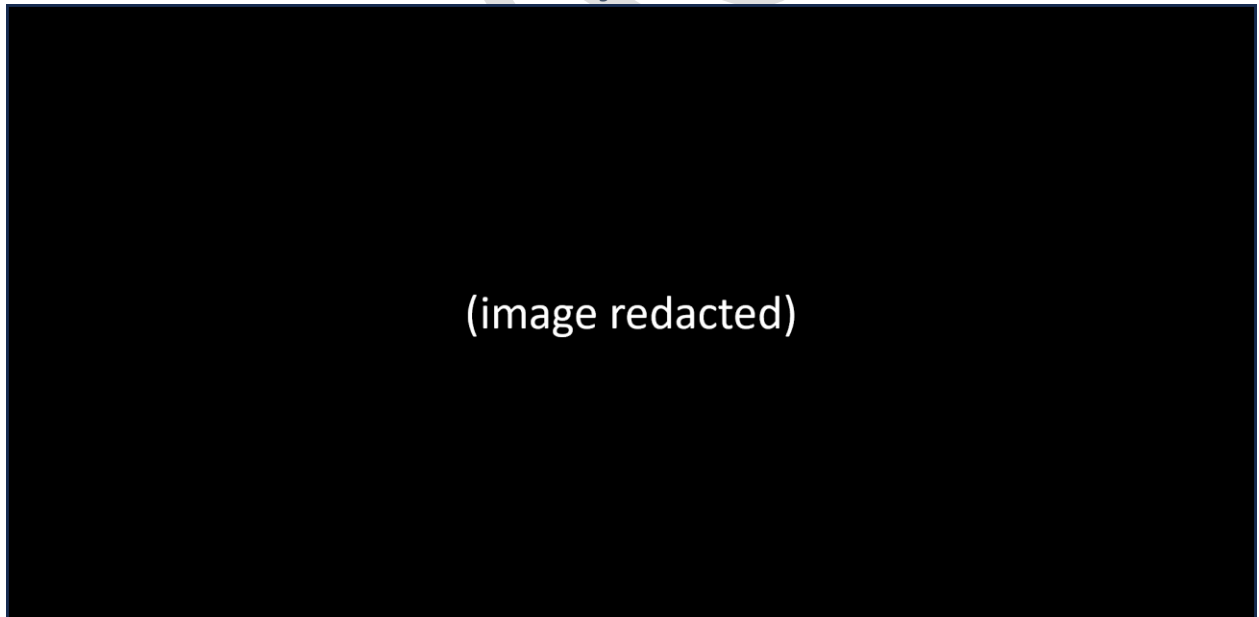
4. Click the *OK* button. (Figure 114)

Figure 114



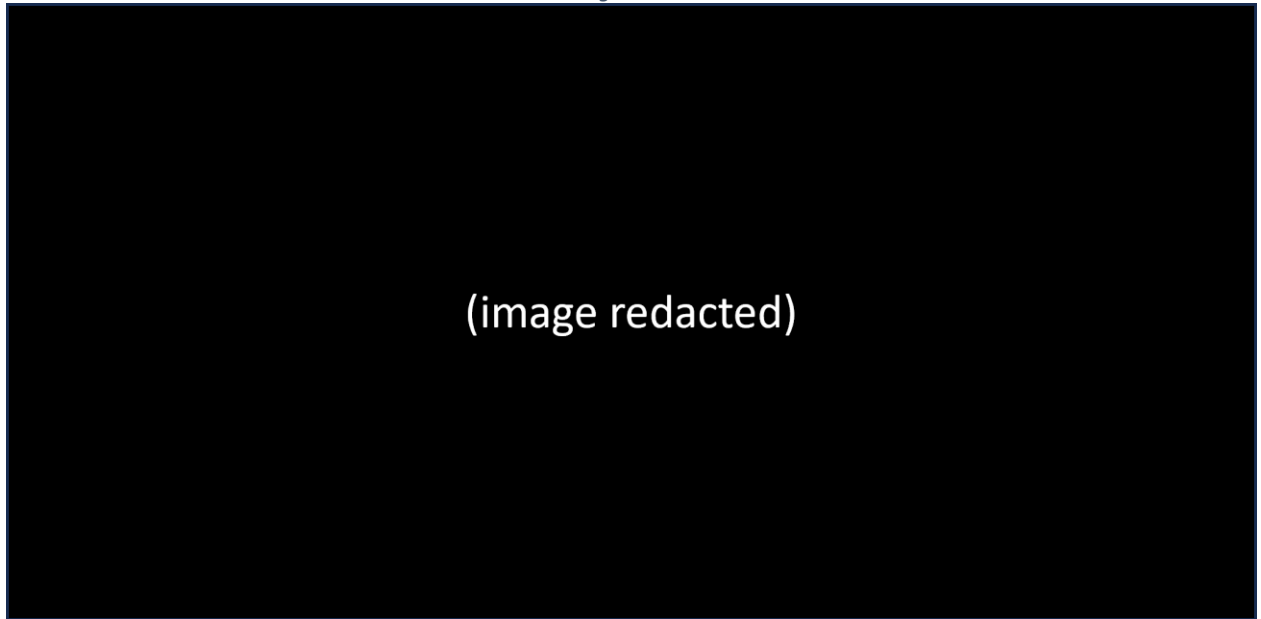
5. Enter your VDI credentials⁽¹⁾. (Figure 115)
6. Click the arrow button⁽²⁾. (Figure 115)

Figure 115



7. You have now arrived at your VDI desktop. (Figure 116)

Figure 116



REDACTED