Setting Up Users and Roles with the Domain Manager

Copyright, Trademarks, and other Legal Matter

Actifio strives to produce quality documentation and welcomes your feedback. Please send comments and suggestions to **docs@actifio.com**.

Contents

Preface

This guide provides step-by-step instructions on how to use the Actifio Domain Manager to create users and assign them to roles and organizations. It assumes you have read ***Getting Started with Actifio Copy Data Management***, are familiar with the components of the Actifio Desktop, and have a grasp of the basic concepts associated with an Actifio appliance.

Your Actifio appliance's Documentation Library contains detailed, step-by-step, application-specific instructions on how to protect and access your data. Each guide is in PDF format and may be viewed online, downloaded, or printed on demand. The following guides will be of particular interest:

- ***Configuring Resources and Settings With the Domain Manager***
- ***Connecting Hosts to Actifio Appliances***
- ***Planning and Developing Service Level Agreements***
- ***Virtualizing and Protecting Copy Data with the Application Manager***
- ***Accessing and Recovering Copy Data with the Application Manager***
- ***Replicating Data Using Actifio Appliances***

Actifio Appliances

Unless otherwise specified, all features and functions described in this document apply to all Actifio appliances.

The ActifioNOW Customer Portal

During the configuration and initialization of your Actifio appliance your Actifio representative provided you with a user name and password for the ActifioNOW customer portal.

From the ActifioNOW customer portal you can obtain detailed reports about your Actifio appliance, access the Actifio product documentation, including release notes, and search the knowledge base for answers to specific questions.

To log into the ActifioNOW customer portal:

1. Go to: **https://now.actifio.com**.
2. When prompted, enter the user name and password provided by your Actifio representative.

Actifio Support Centers

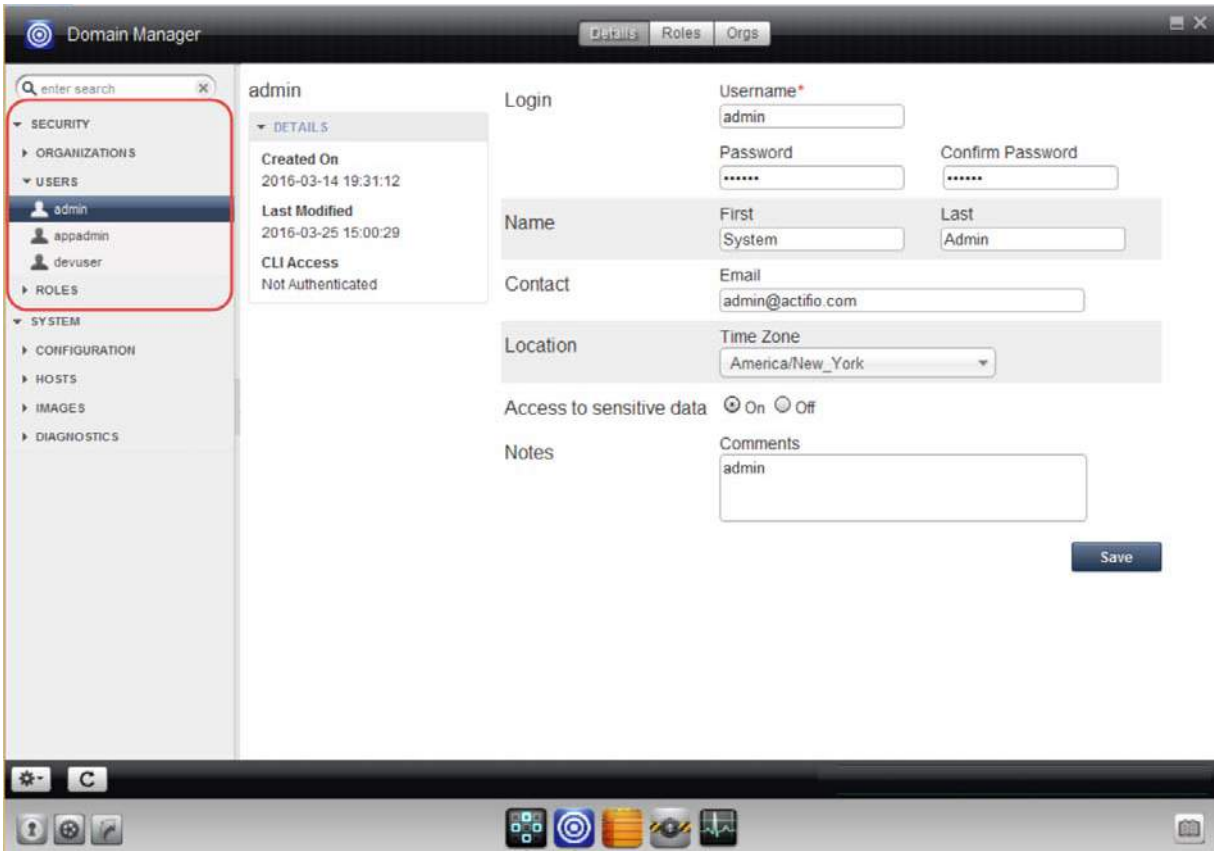
To contact an Actifio support representative, you can:

- Send email to: support@actifio.com
- Call:
  From anywhere: +1.315.261.7501
  US Toll-Free: +1.855.392.6810
  Australia: 0011 800-16165656
  Germany: 00 800-16165656
  New Zealand: 00 800-16165656
  UK: 0 800-0155019

1 Introduction to the Security Functions of the Domain Manager

The Actifio Desktop Domain Manager service is your primary tool for configuring and managing relationships among all resources protected by an Actifio appliance. The **Security** function is where you manage organizations and users that have access to an Actifio appliance, and the roles that you create and assign to them. This document provides an overview on organizations, users, and roles in the Actifio appliance, and includes the procedures for you to follow to create and manage those security resources.

This introduction discusses:



The Security Functions of the Actifio Desktop Domain Manager

The Domain Manager also includes a System section for managing hosts and appliances on which your data resides. These functions are detailed in ***Configuring Resources and Settings With the Domain Manager***, ***Configuring Actifio Event Alerting***, and ***Connecting Hosts to Actifio Appliances***.

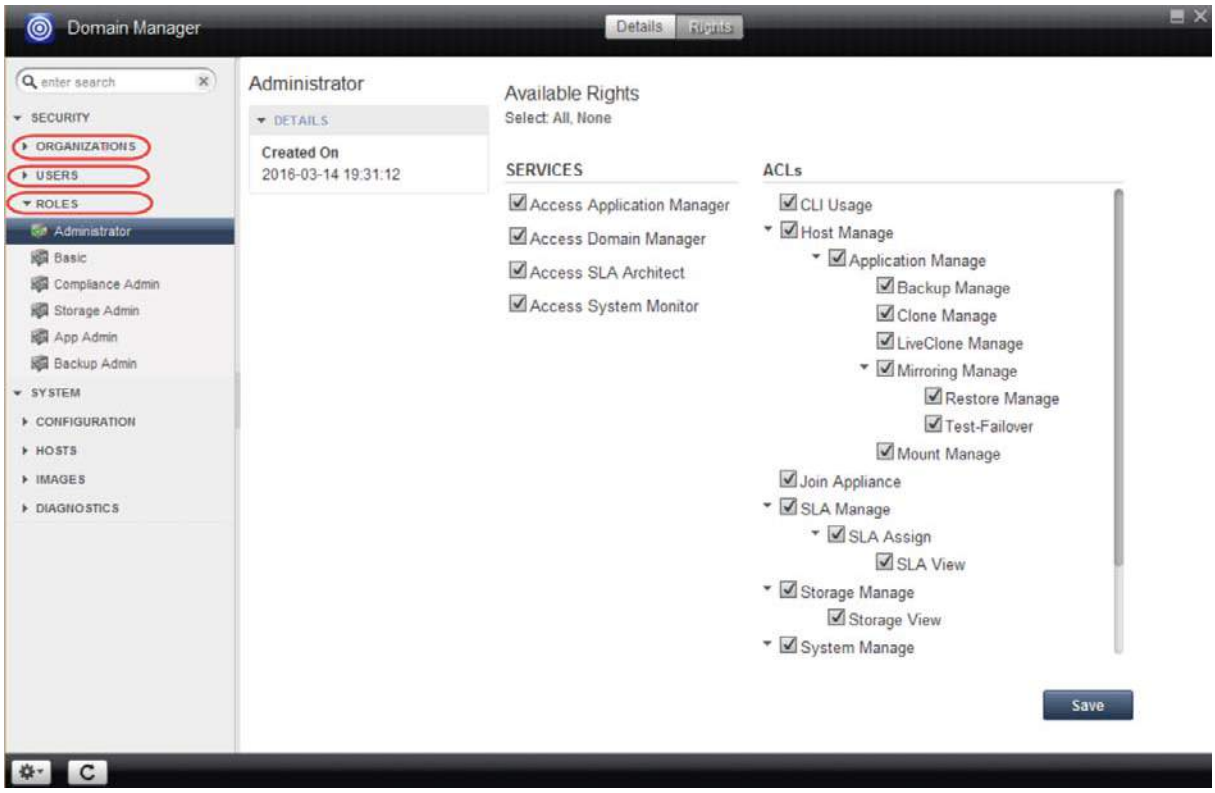
Functions of the Domain Manager Security Service

The Security function of the Domain Manager provides the following security services:

Organizations: Govern which users can access and manage which resources within an Actifio appliance. Tools for creating and managing organization resources are described in introduced in Chapter 2, Creating and Managing Organizations.

Users: Govern who is able to use Actifio Desktop and Actifio appliances. Users can have varying levels of access rights. Tools for creating users and assigning roles are described in Chapter 3, Creating and Managing Users.

Roles: Govern what actions users can take on the resources under their control. Tools for creating roles and assigning rights are described in Chapter 4, Creating and Managing Roles.



The Three Security Services of the Domain Manager's Security Section

The Domain Manager Service Menu

The Domain Manager's service menu includes functions for Security functions and System functions.

Domain Manager Service Menu Items

Command Name	Task
Security Functions Service Menus (This Book)	
New Organization...	Create a new organization and assign resources. See Chapter 2, Creating and Managing Organizations.
New User...	Create a new user and assign roles to the user. See Chapter 3, Creating and Managing Users.
New Role...	Create a new role. See Chapter 4, Creating and Managing Roles.
System Functions Service Menus (see *Configuring Resources and Settings With the Domain Manager*)	
New Host...	Configure a new host.
Add New NAS Server	Add a NAS Server to an Actifio CDS appliance and specify its ports and virtual disks. ***Note:*** *See* ***Configuring Actifio Big Data Director (BDD)*** *for instructions on how to configure and use the Actifio Big Data Director (BDD).*
Join Appliance	Joins two Actifio appliances for copy data replication.
Certificate Exchange	Exchange security certificates between two Actifio appliances. This allows you to replicate data to and from the appliances.
Upload Certificate...	Upload the security certificate of a remote Actifio appliance to the Actifio appliance that you are logged into.
Download Certificate...	Download the security certificate of the Actifio appliance that Actifio Desktop is connected to a local folder.
Archive Job History...	Archive a record of jobs executed using Actifio Desktop.
Add CLI Access	Add an SSH public key to enable Command Line Interface (CLI) access for a user.
Remove CLI Access	Disable CLI access to a user.
Upload System Update	Upload patches and hotfixes to Actifio appliance (visible only to admin role).
Delete	Delete a user, role, organization, or host.

2 Creating and Managing Organizations

This chapter introduces features related to managing organizations:

Managing Organizations

This section describes:

Actifio Appliance Organizations

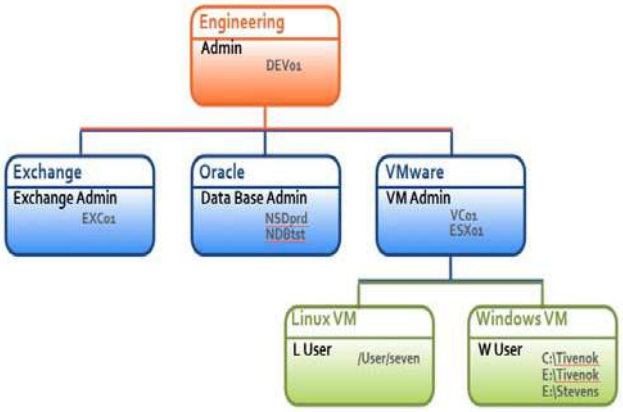
An Actifio appliance provides two predefined organizations: ALL and PUBLIC. You can create other organizations as needed.

ALL: All Actifio appliance resources of types other than user are resources of this organization. A user added to the organization "ALL" has access to every Actifio appliance resource (this is usually reserved for administrators).

PUBLIC: Every Actifio appliance user is a member of this organization. Every Actifio appliance user has access to an Actifio appliance resource (of type other than user) added to organization "PUBLIC".

Hierarchy of Organization Resources

Organizations and Roles work together to enforce rules set up by Actifio appliance administrators for users. Organization membership governs which users can access/manage which resources within an Actifio appliance. Roles govern what actions users can take on the resources under their control. Organizations can be defined in a hierarchical fashion to match your organizational structure.



Organizations and Their Access Relationships

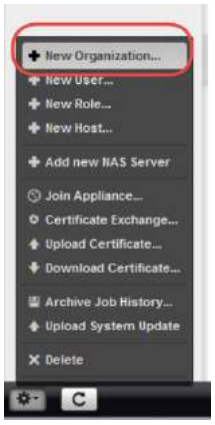
Example: Organization Resources

Organization	Resources			
	Child Organizations	Child Organizations	Users	Hosts
Engineering	-	-	Admin	DEV01
	Exchange	-	ExchangeAdmin	EXC01
	Oracle	-	DataBaseAdmin	NSDprd NDBtst
	VMware	-	VMAdmin	VC01 ESX01
		LinuxVM	LUser	/User/seven
		WindowsVM	WUser	C:/Tivenok E:/Tivenok E:/Stevens

Creating an Organization

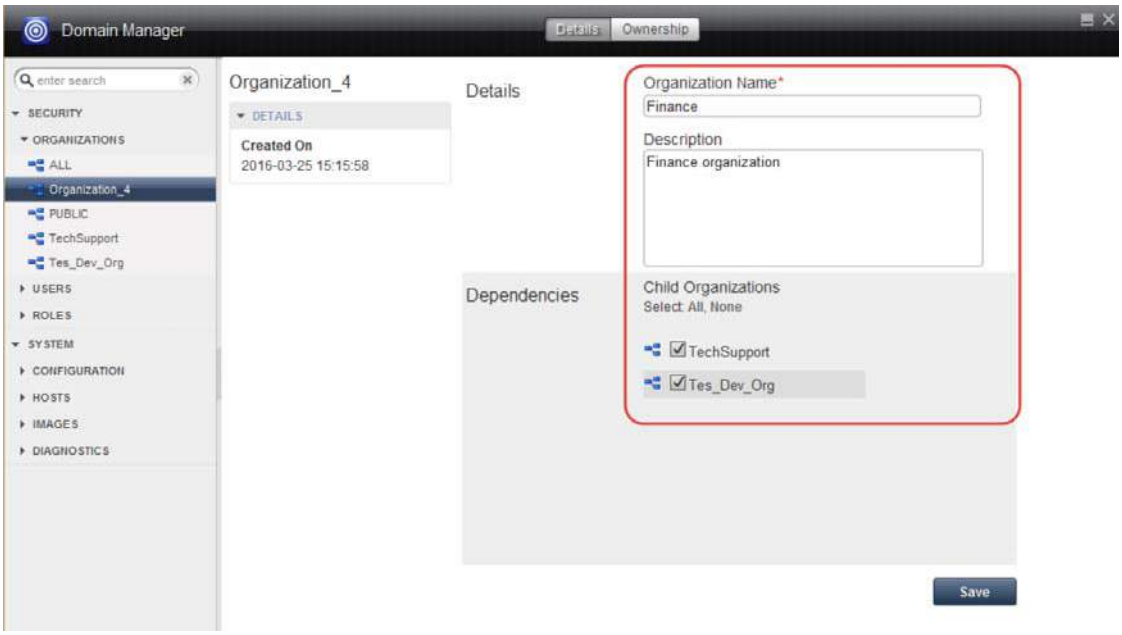
To create a new organization:

1. Open the Actifio Desktop to the **Domain Manager**.
2. From the Domain Manager service menu, select **New Organization**.



Creating a New Organization

The organization details page opens:



Choosing Organization Dependencies

3. Enter a name for the organization, and a brief description. Check the check-boxes for any existing organizations that should be dependents of the new organization.

Note: *The name can be up to 64 alphanumeric characters, with no spaces or special characters. Hyphens (-) and underscores (_) are permitted.*

---

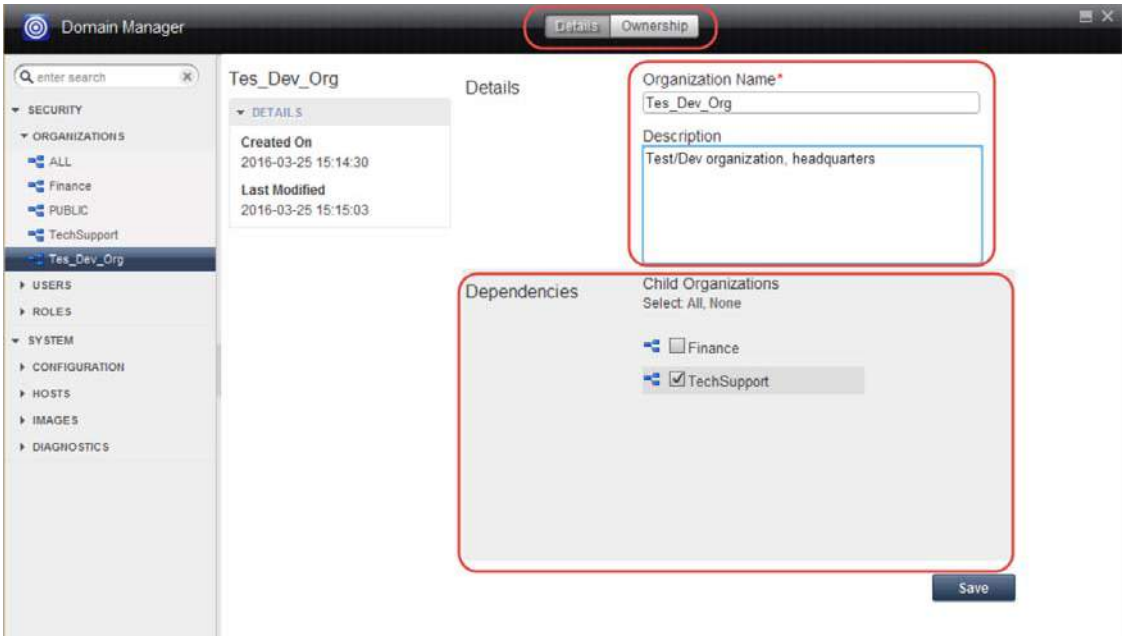
4. Click **Save**.

Viewing and Editing an Organization

The organization details page provides information about organizations, such as the name of the organization, creation date, and the dependent organization resources.

To view or edit an organization:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Click **Organizations** from the navigation pane.
3. Select the **Organization**.
4. Click the **Details** tab. The Details pane displays the organization information.
5. To view the organization resources, click the **Ownership** tab.
6. Modify the name and description as needed and click **Save** to update the changes.



Editing Organization Details

Deleting an Organization

You can delete an organization that is no longer needed. To remove an organization:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Under **Organizations** from the navigation pane, select the Organization.
3. Right-click the organization name and select **Delete**.
4. Click **Yes** in the confirmation dialog.

Note: *The organizations ALL and PUBLIC cannot be deleted.*

About Organization Resources

Organizations can be assigned resources. Resources are listed under the Ownership tab. Resources can be assigned to multiple organizations, and organizations can be assigned as dependents to other organizations. The following resource types can be owned by an organization:

Policy Templates are collections of policies. Each policy defines how the backup data is managed. Policy comprises of the type of the backup operation (snapshot, deduplication, replication etc.), frequency of the backup operation and life-time of the backed up data.

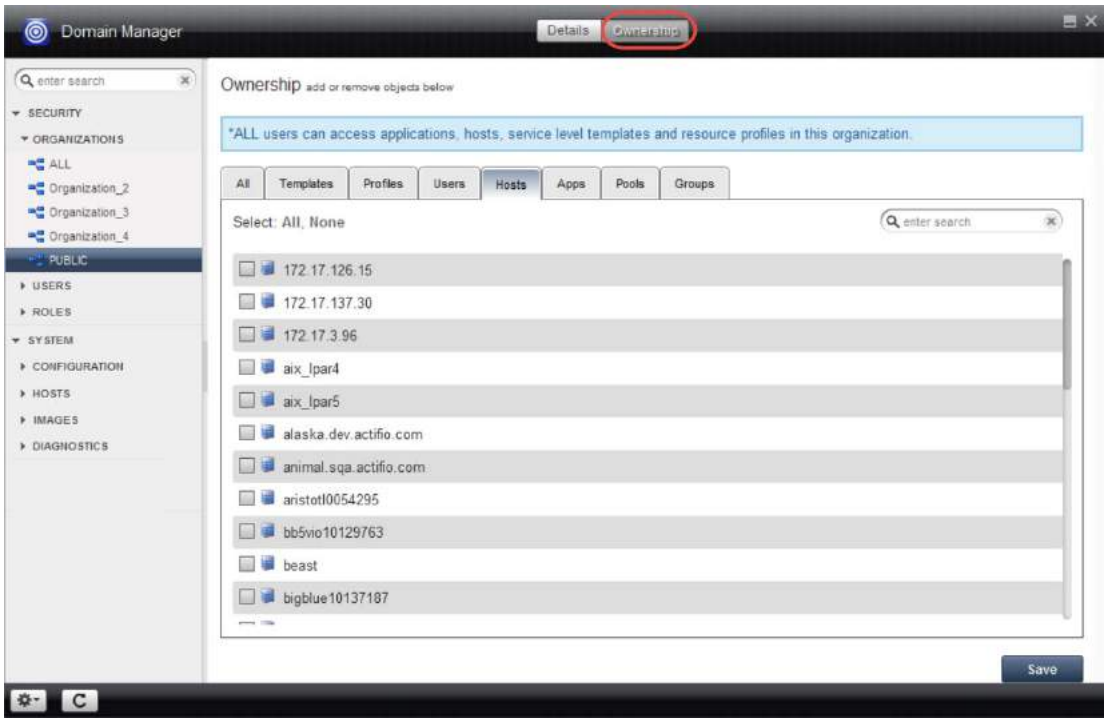
Profiles also known as Resource Profiles, specify the storage media for the backed up data.

Users are Actifio Desktop users of any level.

Hosts are data resources that will be protected by Actifio. Hosts can be physical servers or hypervisors.

Apps are applications. This is a generic term for data resources to be protected by an Actifio appliance.

Pools are storage resources.



Organizations May Be Assigned Templates, Profiles, Users, Hosts, Applications, and Pools

Hosts, Apps, and Groups

- There is no need to add an application to an organization if you are already placing its host into the organization. Placing a host into an organization automatically adds its apps. When new apps appear on that host over time (like new SQL databases), that host's new apps will automatically be in the organization.

Note: *If you have a host with multiple apps that belong exclusively to different organizations, then do not add the host to either organization. Add the apps and leave the host with no organization.*

- There is no need to add applications to an organization if the organization contains a Group that contains those apps. Placing a Group (not a Consistency Group) into an organization automatically adds that Group's apps to the organization. When new apps are added to the Group over time, the new apps in that Group are automatically added to the organization as well.

Managing Organization Resources

This section describes:

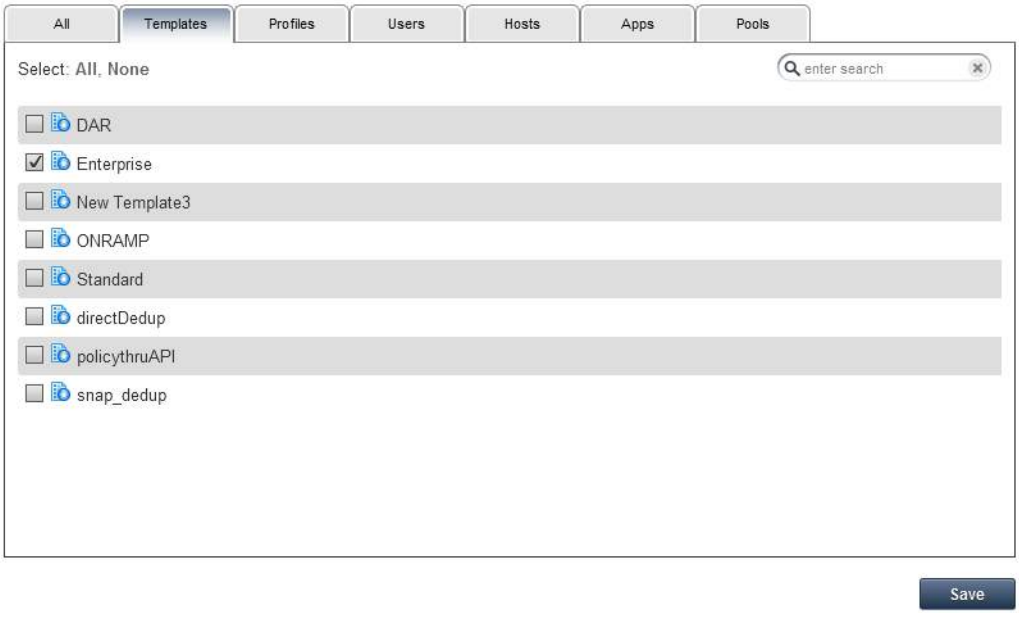
Adding Resources to an Organization

To create a relationship between resources and an organization, you must add resources to the organization. The procedure for adding templates, profiles, users, hosts, apps, and pools is the same. The procedure for adding a dependent organization is a little different; it is detailed in Adding a Dependent Organization on page 11.

To add a resource:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Click **Organizations** from the navigation pane.
3. Select the Organization.
4. Click the **Ownership** tab.
5. Click the sub-tab for the type of resource you want to add. The tab lists the current resources of that class.
6. Select the resource(s) by checking the appropriate check-box.
   - Use the All option to select all the resources at once.
   - Use the Search option to find a specific resource.
7. Click **Save** to update the changes.

Note: *When you create a resource of any kind, you add it to one of your organizations.*

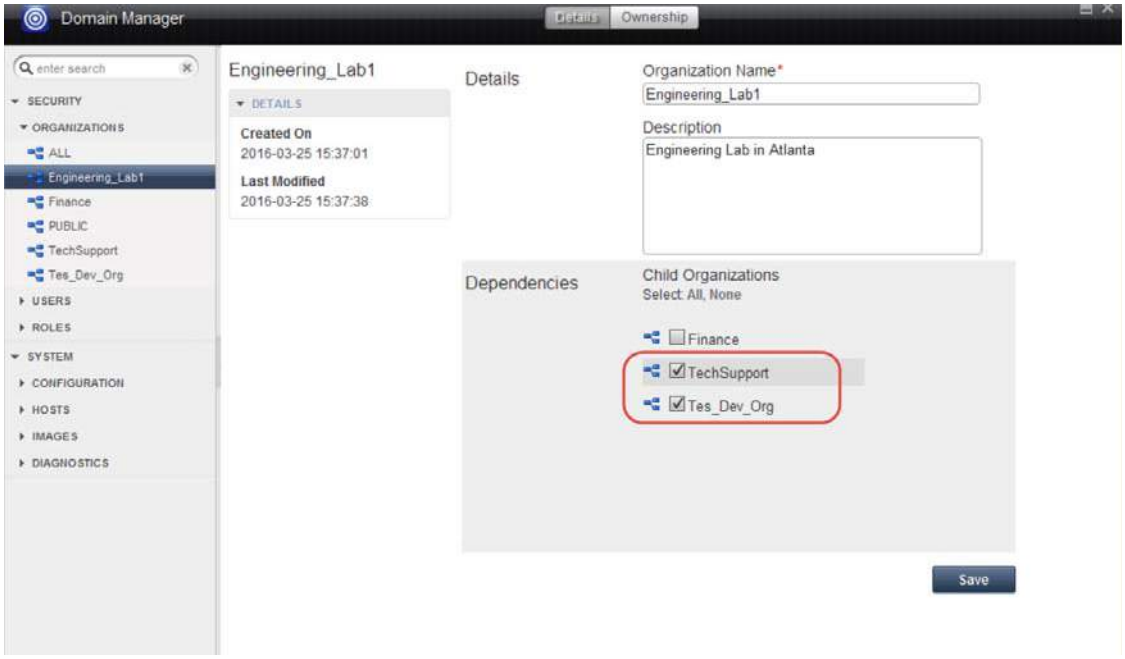


Adding a Template

Adding a Dependent Organization

To add an organization as a dependent to an existing organization:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Click **Organizations** from the navigation pane.
3. Select the Organization that will be parent to the dependent organization.
4. Click the **Details** tab.
5. Select the check-box corresponding to the dependent organization in **Dependencies**.
6. Click **Save** to update the changes.



Adding an Organization as a Dependent of Another Organization

Viewing Resources

You can view an organization's resources and any dependent organizations:

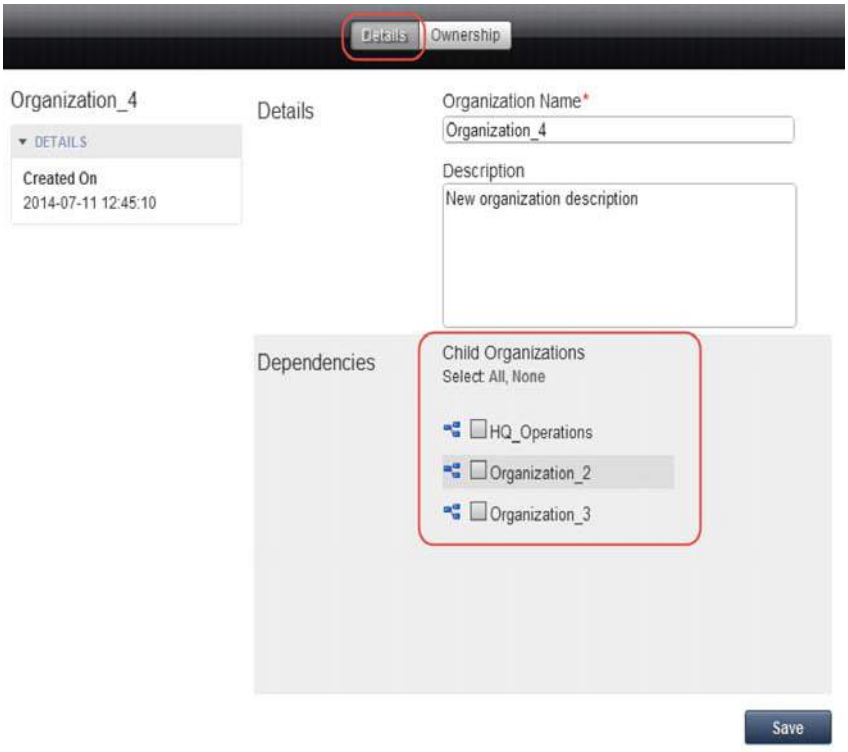
Viewing Dependent Organizations on page 12

Viewing Other Organization Resources on page 13

Viewing Dependent Organizations

To view an organization's dependent organizations:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Click **Organizations** from the navigation pane.
3. Select the Organization.
4. Click the **Details** tab. Checkbox(es) corresponding to dependent organization(s) are checked in the Dependencies:

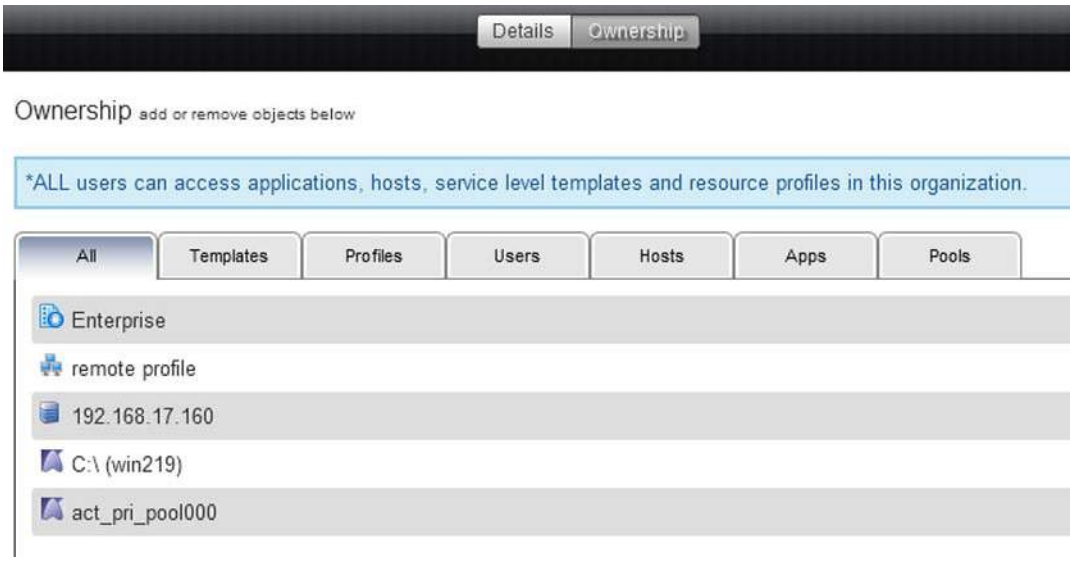


Viewing Dependent Organizations

Viewing Other Organization Resources

To view other (non-dependent organization) resources of an organization:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Click **Organizations** from the navigation pane.
3. Select the Organization.
4. Click the **Ownership** tab and the **All** sub-tab. The page displays existing resources of selected organization; this includes templates, resource profiles, users, hosts, applications, and storage pools:



Viewing Resources of an Organization

Removing Resources from an Organization

To remove a resource from an organization:

Dependent Organizations

To remove a dependent organization of an organization:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Click **Organizations** from the navigation pane.
3. Select the Organization.
4. Click the **Details** tab.
5. Uncheck the organization(s) in **Dependencies**.
6. Click **Save** to update the changes.

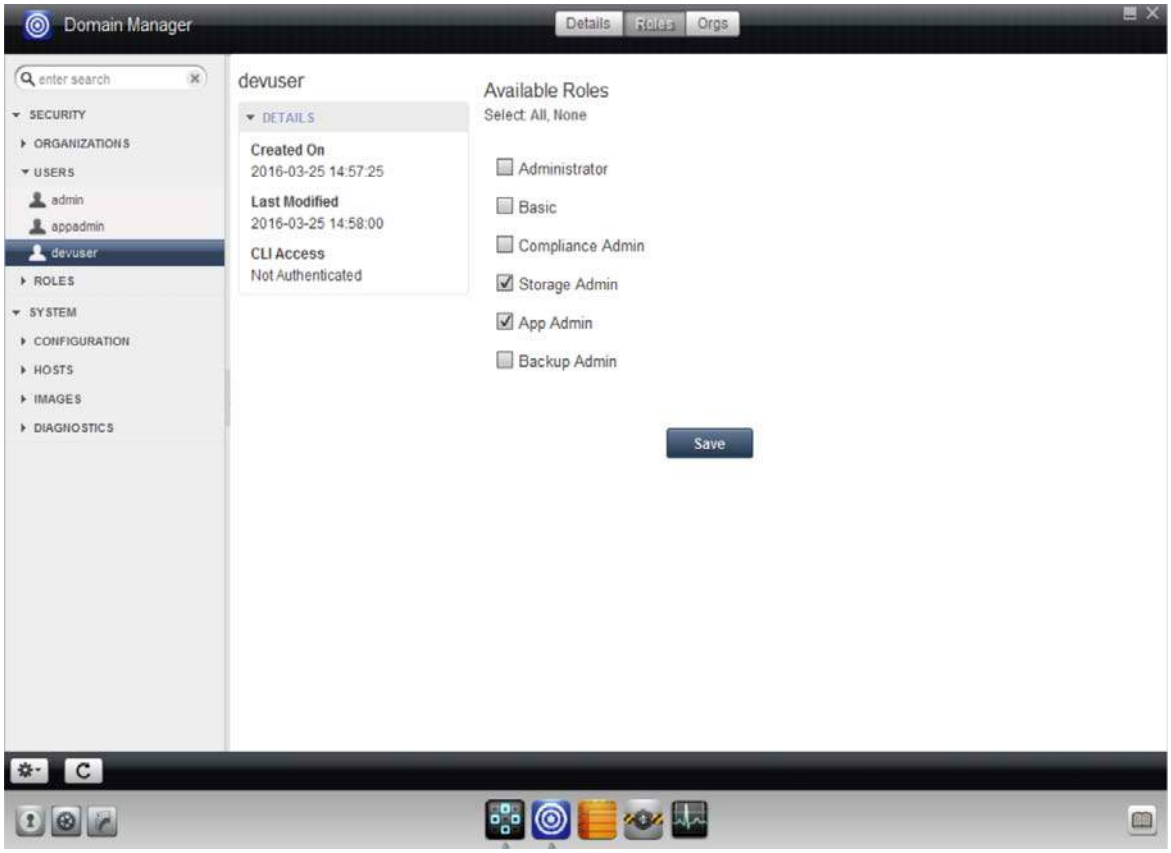
Other Resources

To remove other resources of an organization

1. Open the Actifio Desktop to the **Domain Manager**.
2. Click **Organizations** from the navigation pane.
3. Select the Organization.
4. Click the **Ownership** tab.
5. Select the desired resource subtab. The page displays all the existing resources.
6. Uncheck the appropriate resource(s).
7. Click **Save** to update the changes.

3 Creating and Managing Users

An Actifio appliance allows you to create and manage multiple Actifio Desktop users. This chapter describes:



Users And Roles

Note: *You can use a single existing LDAP (Lightweight Directory Access Protocol) server for Actifio Desktop user authentication and to map LDAP groups to Actifio appliance roles. See* ***Configuring Resources and Settings With the Domain Manager*** *in the Actifio Documentation Library for details on how to configure your Actifio appliance to use LDAP server authentication.*

Creating a User

You can create users with varying levels of access rights. These users use Actifio Desktop and the Actifio appliances.

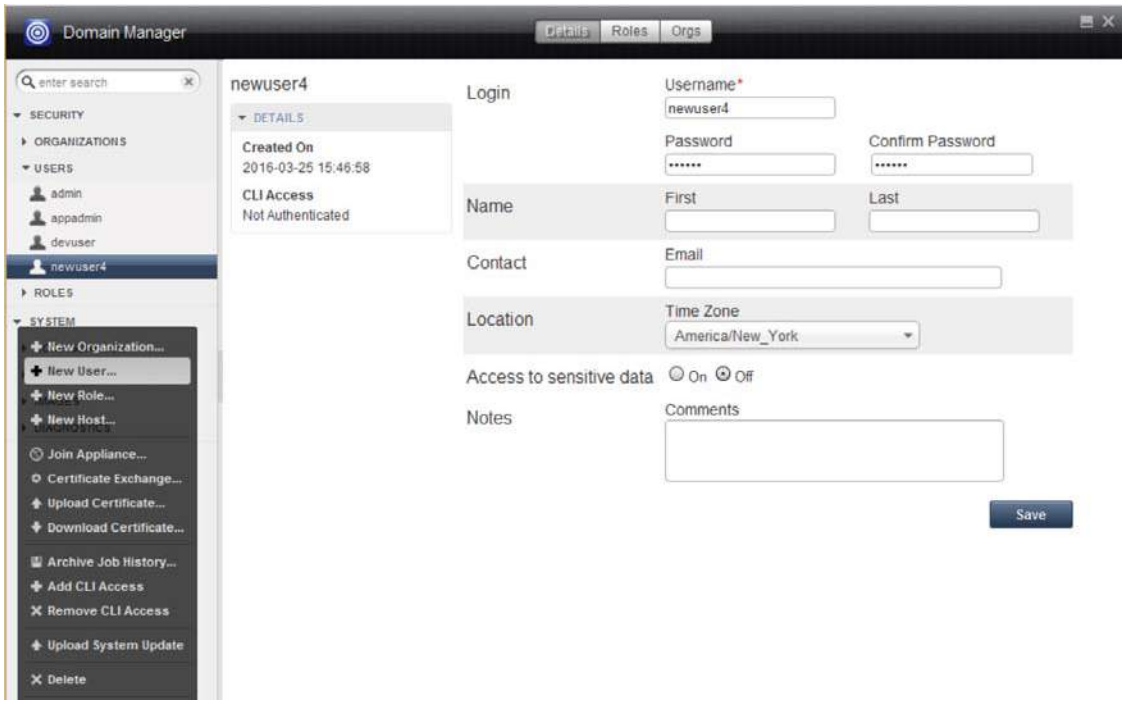
To create a new user:

1. Open the Actifio Desktop to the **Domain Manager**.
2. From the Service Menu, select **New User**....
3. Enter the desired user name in **Username**. The username field is case sensitive.
4. Enter the password in **Password** and **Confirm Password** fields.
5. Enter the name of the user in **First** and **Last**.
6. Enter the email address of the user in **Email**.
7. Select the user's time zone from **Timezone**.
8. Specify in **Access to sensitive data** if this user should have the necessary rights to see image data that is flagged as being "sensitive." An image can be marked sensitive explicitly by an administrator. It also inherits the application's sensitivity attribute. Its intent is to restrict access to data that has been marked as sensitive. You mark data as sensitive in the Restore window of the Application Manager. You can use LiveClone workflows to scrub sensitive information and then mount the scrubbed data.

   When **On**, this user is able to see sensitive backup image data. When **Off,** this user can see only nonsensitive image data.

   Note: *See* Summary of Rights Required to Perform Operations in an Actifio Appliance *on page 26 for additional information.*

9. Optionally, you can enter some notes in **Comments**.
10. Click **Save**.



Creating a New User

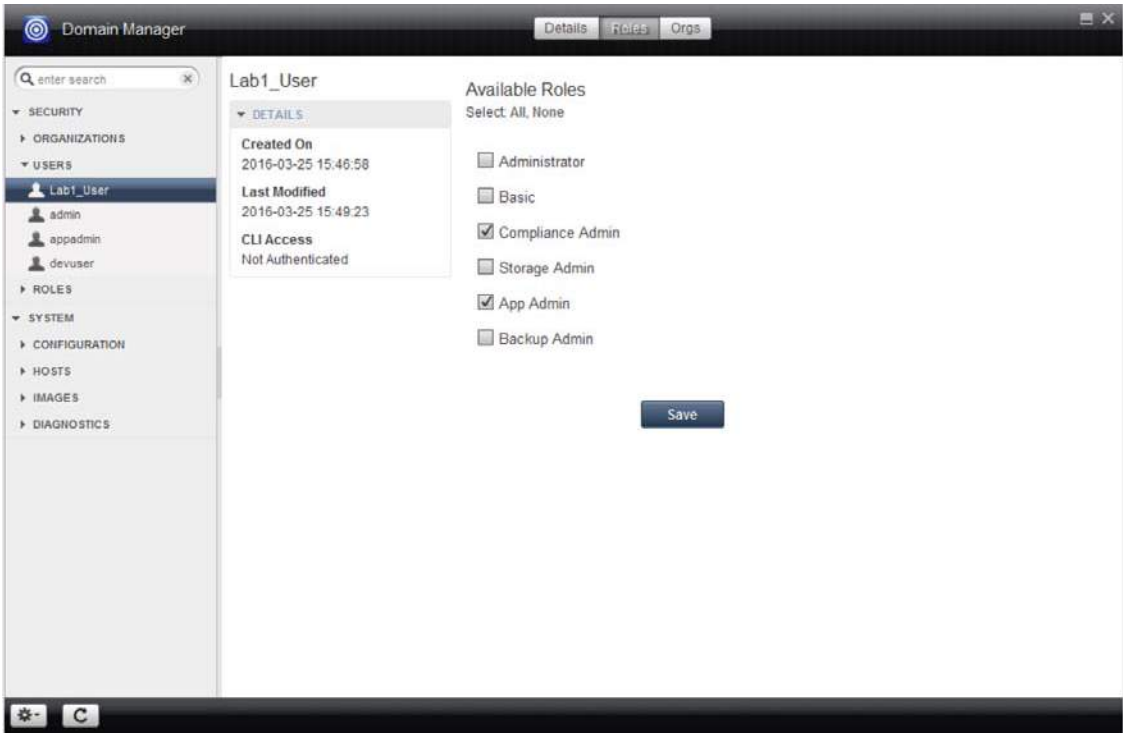
Assigning Roles to a User

Assign roles to the users in an Actifio appliance so that they have authorization to execute certain functions.

> ***Note:*** *To create a role, see* Creating and Managing Roles *on page 21.*

To assign one or more roles to a user:

1. Open the Actifio Desktop to the **Domain Manager**.
2. In the navigation pane, under Users, select the user.
3. Select the **Roles** tab. The available roles are listed in the display pane.
4. Check the roles that you would like to assign to the user.
5. Click **Save**.



Assigning Roles to a User

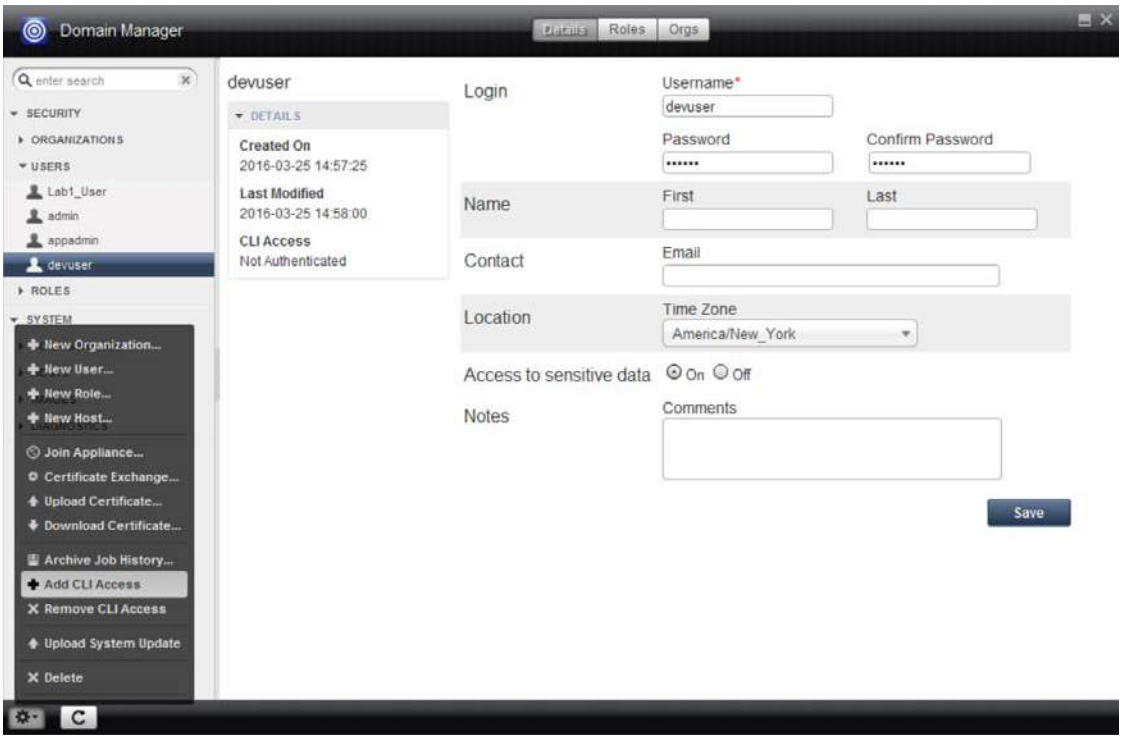
Adding CLI Access for a User

The Actifio appliance command line interface (CLI) is a set of commands for performing the same functions from a command-line that you can perform from the Actifio Desktop. It is detailed in the ***Actifio CLI Reference*** included in the Actifio Documentation Library.

To grant CLI access to a user via the Actifio Desktop, you must upload the SSH public key of the user of the Actifio appliance who requires CLI access. The public/private key pair identifies a single user uniquely. The Actifio Desktop administrator should enter one public key for each user with CLI access.For more information about generating the SSH public/private key pair, configuring a host to run an SSH client, and starting an SSH session, refer to the ***Actifio CLI Reference***.

To add CLI access for a user:

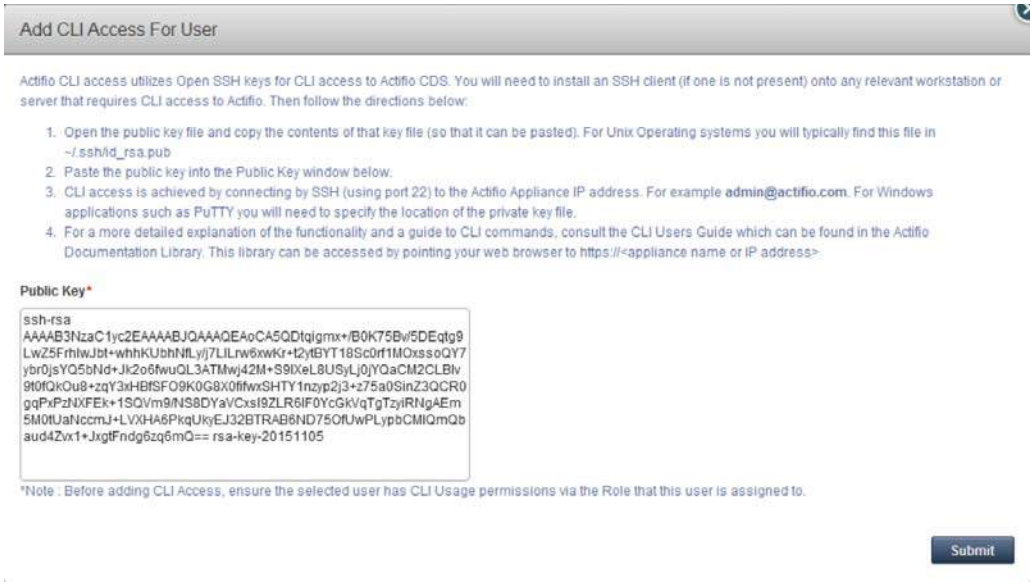
1. Open the saved public key file in a text editor.
2. Open the Actifio Desktop to the **Domain Manager**.
3. Select the user to whom you want to grant access from **Security** > **Users**.
4. From the service menu, click **Add CLI Access**.



5. Copy the public key content from the text editor and paste it into the **Public Key** field.

Note: *Be sure to copy the entire public key from the text editor. Do not include additional spaces.*

6. Click **Submit**.



Note: *For CLI user login, ensure that the role associated with the user has the CLI Usage right. Refer to* Creating a Role and its Rights *on page 22.*

Deleting a User

You need System Manage rights to delete a user.

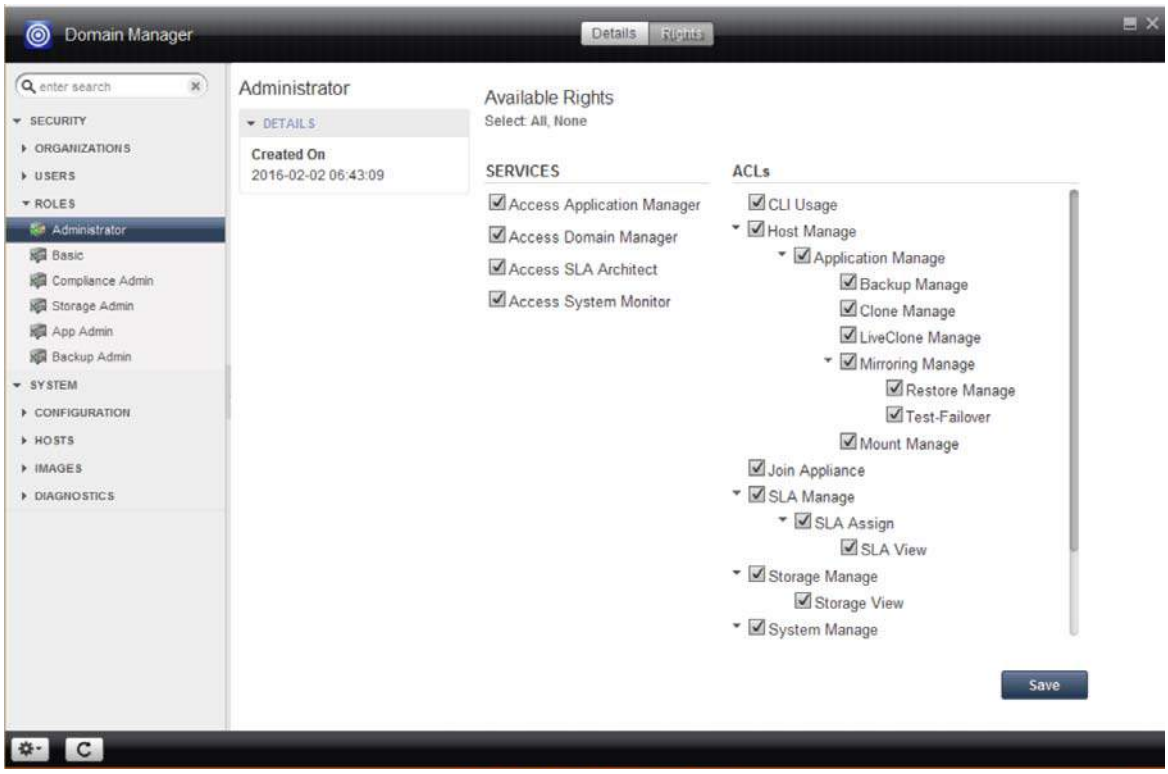
To delete a user:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Select and right-click on the user that you want to remove from **Security** > **Users**.
3. Click **Delete**.
4. Click **OK** in the confirmation dialog.

4 Creating and Managing Roles

An Actifio appliance allows you to create and manage multiple users, roles, and organizations. This chapter describes how to create and manage various types of roles. Roles correlate with groups of users that share similar responsibilities and have similar requirements when using the Actifio Desktop. Permissions are assigned to roles to grant or deny access to various features.

This chapter contains:



The Rights That Can Be Included in a Role

Assigning a Role to a User

To assign one or more roles to a user, see Assigning Roles to a User on page 17.

Creating a Role and its Rights

You can create a role and assign rights to the role. Based on the rights assigned to a user's role, the user is constrained from using or viewing the various components of Actifio Desktop.

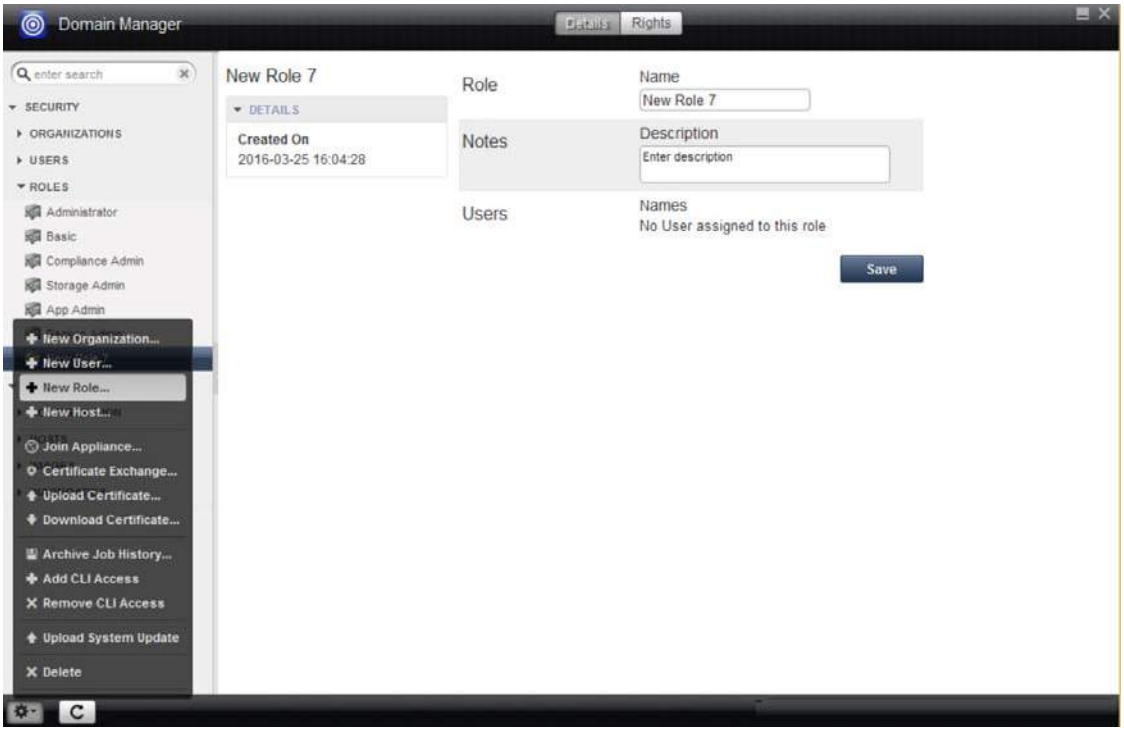
This section describes:

See Summary of Rights Required to Perform Operations in an Actifio Appliance on page 26 for rights that can be assigned to a role.

Creating a Role

To create a role:

1. Open the Actifio Desktop to the **Domain Manager**.
2. From the Service Menu, click **New Role**....
3. Enter a name for the role in **Name**.
4. Enter a description in **Description**.
5. Click **Save**.



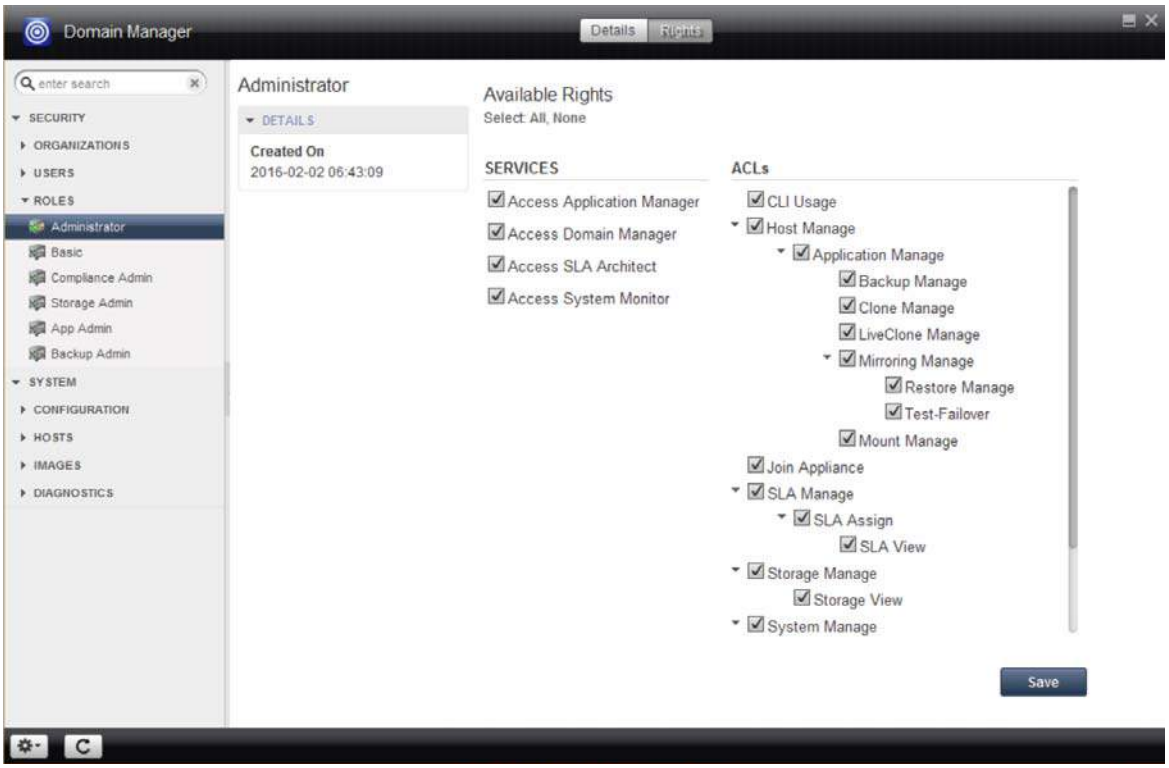
Creating a New Role

About Administrative Rights

There are two classes of rights:

- Access to an entire Actifio Desktop service. You can uncheck a service, or select it and then restrict it to some degree through the Access Control Levels (ACLs).
- ACLs provide additional rights and permit you to restrict some of the rights available within the Actifio Desktop services. ACLs are detailed in Actifio Desktop Access Control Levels (ACLs) on page 24.

> ***Note:*** *Assigning a right automatically assigns all subordinate rights. You can uncheck specific subordinate rights associated with a role.*



The Rights That Can Be Included in a Role

Actifio Desktop Access Control Levels (ACLs)

Rights	Description
CLI Usage	To use the Actifio Command-Line Interface.
Host Manage	To create/modify/delete hosts, to add virtual machines, to restore, clone, mount, unmount, and delete backup images.
Application Manage	To create/modify/delete/view groups and consistency groups, to restore, clone, mount, unmount, and delete backup images, to run an on-demand backup, and to export templates.
Backup Manage	To perform backup operations: Backup Now, Expire, and Modify Expiration.
Clone Manage	To create a cloned image.
LiveClone Manage	To manage LiveClone images.
Mirroring Manage	To perform Failover, Syncback, Cleanup, Failback, and Delete operations for a Dedup-Async or StreamSnap replication image.
Restore Manage	To restore an image.
Test-Failover	To perform Test Failover and Delete Test Failover for a Dedup-Async or StreamSnap image.
Mount Manage	To Mount Image, Unmount Image, Re-Mount Image, and Delete Image.
Join Appliance	To join two Actifio appliances for copy data replication.
SLA Manage	To create/modify/delete/view and assign policy templates and resource profiles.
SLA Assign	To assign pre-configured policy templates and resource profiles to applications.
SLA View	To view policy templates and resource profiles.
Storage Manage	To add/remove/view storage and to add/remove/ view disk-pools. The Storage Manage ACL is not applicable to Actifio Sky appliances.
Storage View	To view the storage and disk pool configuration.
System Manage	To manage all Actifio appliance configurations, including users, roles, and organizations.
System View	To view Actifio appliance configuration information.
Workflow Manage	To add/remove/view Workflows. A Workflow can be scheduled or initiated on-demand.
Workflow Run	To allow a user to run a Workflow. This ACL right does **not** include the right for that user to also manage a Workflow. This level of permission is required in a Test/Dev environment.
Workflow View	To view scheduled Workflows.

Assigning Rights to a Role

For a list of rights that can be assigned to a role, see Summary of Rights Required to Perform Operations in an Actifio Appliance on page 26.

To assign rights to a role:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Select the Role from the navigation pane.
3. Click **Rights** from the Service Menu.
4. Select the rights using the check boxes.
5. Click **Save**.

Assigning Rights to a Role

Deleting a Role

You need System Manage rights to delete a role.

To delete a role:

1. Open the Actifio Desktop to the **Domain Manager**.
2. Select and right-click on the role that you want to remove from **Security** > **Roles**.
3. Click **Delete**.
4. Click **OK** in the confirmation dialog.

Summary of Rights Required to Perform Operations in an Actifio Appliance

By default, each Actifio appliance user can view all applications in their associated organization(s) irrespective of the specified sensitivity defined for this user through the **Access to Sensitive Data** option (see Creating a User on page 16). However, the user will be restricted from performing certain operations on applications if their ACL right does not match the sensitivity level of the application.

An Actifio appliance user requires a specified privilege to see the backup images that match their specific data access levels as defined through the **Access to Sensitive Data** option and their specified ACL rights.

- Users with a data access level set to sensitive (**Access to Sensitive Data** set to **On**) are able to see sensitive and nonsensitive backup images.
- Users with a data access level set to nonsensitive (**Access to Sensitive Data** set to **Off**) can see only nonsensitive backup images.

The following table summarizes the different operations that a user can perform in the Actifio appliance and the necessary rights required in a role to be able to perform those operations.

Note: *Any change to sensitive applications is only allowed by a user with the Access to Sensitive Data option turned On (Creating a User on page 16), for operations such as Delete Application, Mark Application Ignored, Set/Unset Application Class.*

Rights Required to Perform Actifio Appliance Operations

Operation	Required ACL Right	Comments
Create User	System Manage	----------
Create Role	System Manage	----------
Create Organization	System Manage	----------
Add Host	Host Manage	----------
Discover App	Host Manage	----------
Discover VMs	Host Manage	----------
New Application	Application Manage	----------
New NAS Dataset	Application Manage	----------
New Consistency Group	Application Manage	----------
New Group	Application Manage or System Manage	----------
Delete Application	Application Manage	----------

Operation	Required ACL Right	Comments
Mark Application as Sensitive or Nonsensitive	Application Manage	Only users with **Access to Sensitive Data** set to **On** can mark application sensitivity in the Application Manager.
Mark Application Ignored	Application Manage	Only users with **Access to Sensitive Data** set to **On** can mark application as ignored in the Application Manager.
Set/Unset Application Class	Application Manage	Only users with **Access to Sensitive Data** set to **On** can set or unset an application class in the Application Manager.
Join Actifio Appliances	Join Appliance	----------
Protect/Unprotect Application	SLA Assign	----------
Run Now Backup Image	Backup Manage	For sensitive applications, a user's ACL right must match the application sensitivity.
Mount Backup Image	Mount Manage	A user's ACL rights must match the image sensitivity.
Clone Backup Image	Clone Manage	A user's ACL rights must match the image sensitivity.
LiveClone Backup Image	LiveClone Manage	A user's ACL rights must match the image sensitivity.
Expire Backup Image	Backup Manage	A user's ACL rights must match the image sensitivity.
Restore Backup Image	Mirroring Manage or Restore Manage	A user's ACL rights must match the image sensitivity.
Mark Backup Image as Sensitive or Nonsensitive	Application Manage	Only users with **Access to Sensitive Data** set to **On** can mark image sensitivity in the Application Manager.
Unmount Backup Image	Mount Manage	----------
Unmount & Delete Backup Image	Mount Manage	----------
Prep-mount Backup Image	LiveClone Manage	A user's ACL rights must match the image sensitivity.
Prep-unmount Backup Image	LiveClone Manage	----------
LiveClone Refresh	LiveClone Manage	----------

Operation	Required ACL Right	Comments
LiveClone Delete	LiveClone Manage	----------
Workflow Create	Workflow Manage	----------
Workflow Edit	Workflow Manage	----------
Workflow Delete	Workflow Manage	----------
Workflow Disable	Workflow Manage	----------
Workflow Run Now (Scrub)	Workflow Run and LiveClone Manage	A user can view only the images that their ACL rights allow them to see.
Workflow Run Now (Mount)	Workflow Run and Mount Manage	A user can view only the images that their ACL rights allow them to see.

Some Notes about Role-Based Access Control

Actifio implements RBAC (Role Based Access Control) using the two concepts of Roles (what a user can do) and Orgs (what a user can see). A user should be assigned both a Role and an Org. This can be done through LDAP group mapping or manually per user.

Here are some tips to help you use this powerful tool effectively:

The Administrator Role is truly all powerful

The Administrator Role is akin to 'root' in Unix. The Administrator Role gives the user not only full Rights to perform all actions and access all panels in the GUI, it also allows the user to see all resources, regardless of what other Orgs the user is in. This means that once you apply the Administrator Role to a user you don't need to worry about Orgs for that User. Equally, don't give the Administrator Role to any user that you don't want to have access to every resource.

You cannot make an Administrator Role

If you create a new Role and tick every single box, this does not make a user with this role the same as one who has the Administrator Role. This is because while any user with your new role can perform any action and access any panel in the GUI, they can only access resources in their Assigned orgs (or PUBLIC).

The PUBLIC Org is truly Public

Take care when placing resources in the PUBLIC Org, as they are now truly public. All Users are placed into the PUBLIC Org by default and cannot be removed. By default the PUBLIC Org contains no resources. However any resource (template, profile, application or disk pool) that is placed into the PUBLIC org is visible to all users regardless of what other Orgs that user is in. This is helpful if you have a common template and profile that all Orgs use, or to give access to the default snapshot pool.

Children follow their Parents into Orgs

There are three common scenarios where resources can be visible to a User even though you did not assign them access through their Org:

Groups are parents of Applications: If you add a Group to an Org, any application in that Group is implicitly in the same Org. New applications added to the Group are visible to users in that Org.

Hosts are parents of Applications: If you add a host to an Org, any application discovered on that host is implicitly in the same Org. New applications discovered on that host are visible to users in that Org.

Orgs can be parents of Orgs: If you add an Org to an Org, then any resource in the child Org is visible to any User with access to the Parent Org.

Actifio does not support Nested Active Directory Groups

In Active Directory, administrators can create nested groups, so you can have a structure like this in Active Directory:

Example Nested Group Structure in Active Directory

Parent DBA Group (not mapped to any Actifio Org or Role)		
	DBA Team 1 (not mapped to any Actifio Org or Role)	
	DBA Team 2 (not mapped to any Actifio Org or Role)	
		DBA Team 2b (Mapped to Actifio Org1 and Actifio Role1)
	DBA Team 3 (not mapped to any Actifio Org or Role)	
		DBA Team 3a (Mapped to Actifio Org2 and Actifio Role2)

In the Actifio LDAP Group Mapping panel each of these Groups is examined separately. The parent relationship is not examined. So we have mapped DBA Team 2b to Actifio Org1 and Actifio Role1. But if an AD User in DBA Team2 logs into an Actifio Desktop or AGM, they will not be placed into a role or a group, because that AD Group is not discretely mapped to any Actifio Role or Org.

The same would apply to a user in the Parent DBA Group. Even though from an AD Group perspective, all DBA Teams are nested under Parent DBA, as an Actifio user they would not get a role or an Org as DBA Group is not mapped to any Actifio Role or Org.

Index