
Installing and Upgrading Actifio Global Manager on a VMware Server

Copyright, Trademarks, and other Legal Matter

Copyright © 2009 - 2020 Actifio, Inc. All rights reserved.

Actifio®, AnyIT®, Dedup Async®, OnVault®, Enterprise Data-as-a-Service®, FlashScan®, AppFlash DEVOPS Platform®, Copy Data Cloud®, and VDP® are registered trademarks of Actifio, Inc.

Actifio Sky™, Actifio One™, and Virtual Data Pipeline™ are trademarks of Actifio, Inc.

All other brands, product names, goods and/or services mentioned herein are trademarks or property of their respective owners.

Actifio, Inc., is a provider of data protection and availability products. Actifio's technology is used in products sold by the company and products and services sold and offered by its commercial partners. The current list of Actifio patents is available online at: <http://www.actifio.com/patents/>

Actifio believes the information in this publication is accurate as of its publication date. Actifio reserves the right to make changes to information published in this document, including without limitation specifications and product descriptions, at any time and without notice. This document supersedes and replaces all information supplied prior to the publication hereof.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." ACTIFIO, INC. MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

This software and the associated documentation are proprietary and confidential to Actifio. Use, copying, and distribution of any Actifio software described in this publication requires an applicable software license. Any unauthorized use or reproduction of this software and the documentation may be subject to civil and/or criminal liability.

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

Published March 19, 2020

Contents

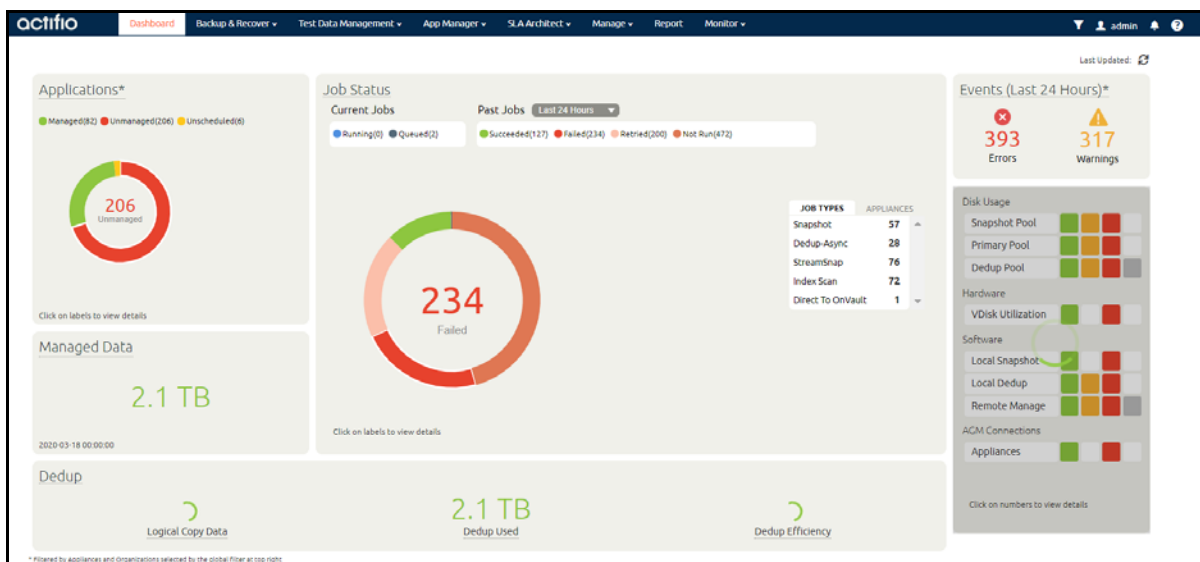
Chapter 1 – Introduction	1
Report Manager (RM) Integration with AGM.....	1
Chapter 2 – Actifio Global Manager Requirements	3
Software Requirements.....	3
AGM VM Requirements	3
Supported AGM Configurations.....	4
vSphere NTP	5
Port Requirements.....	5
Web Browser Requirements.....	5
Chapter 3 – Best Practices for AGM High Availability	7
Distributed Resource Scheduler (DRS) and Distributed Power Management (DPM).....	7
Affinity Rules.....	8
Resource Pools	8
Configuring VMware for AGM HA Failover.....	8
Protecting the AGM VM.....	9
Chapter 4 – Installing Actifio Global Manager	11
The AGM OVA File.....	11
Verifying the Integrity of the AGM.OVA File.....	11
Deploying and Installing the AGM OVA	13
Deploying and Installing the AGM OVA Using VMware vSphere 6.7 Web Client.....	13
Deploying and Installing the AGM OVA Using VMware vSphere 6.5 Web Client	17
Deploying and Installing the AGM OVA Using VMware vSphere 5.5 Web Client	21
Replacing a Previously Installed AGM OVA	23
Chapter 5 – Configuring Resources	25
Adding Resources to Enable Catalog	25
Removing Resources to Disable Catalog.....	27
Adding Resources to Enable Report Manager.....	28
Chapter 6 – Accessing Actifio Global Manager	29
Chapter 7 – Accessing Report Manager	31

Chapter 8 - Adding Appliances to an AGM Deployment	33
Selecting the First Actifio Appliance to Import.....	34
Sharing Mode Options.....	34
Managing SLA Templates Prior to Importing.....	35
Managing Roles.....	35
Managing Organizations	35
Resource Conflict Resolution Tool.....	36
Chapter 9 - Upgrading Actifio Global Manager	39
Before You Begin.....	39
Upgrading AGM.....	39

1 Introduction

Actifio Global Manager (AGM) is a virtual appliance. AGM provides centralized management capabilities that can be deployed on standard VMware ESX servers and Hyper-V hypervisors as well as in most cloud platforms. From one centralized AGM management system, you use the AGM web-based UI to manage multiple VDP appliances and perform various day-to-day copy data operations. VDP appliances are the highly scalable copy data platforms that virtualize application data to improve the resiliency, agility, and cloud mobility of your business.

With AGM you can manage many VDP appliances. AGM communicates with each appliance using the IP address or fully qualified domain name (FQDN) of the appliance. When you add an appliance to AGM, all SLA templates, organizations, users, and roles are imported into the AGM database and become AGM-level objects. You can then use these objects across all managed appliances. As of AGM 8.0.4, you can install AGM with or without the Catalog feature. For more information on Catalog, see the AGM Online Help.



Report Manager (RM) Integration with AGM

Report Manager (RM) can now be installed as part of AGM and run in the same virtual machine (additional memory and CPU are required). This integration simplifies deployment and streamlines ongoing management. When deployed in this integrated configuration:

- User authentication to RM is done via AGM, instead of one of the appliances. This means that any AGM user can log in to RM.
- Organization membership information is pulled from AGM.

- All appliances managed by AGM are automatically added to RM. Additional appliances can be manually added to RM.
- All upgrades are done through the AGM UI and include upgrades to both AGM and Report Manager components.
- The AGM version is always listed, even from the **RM Help > About** dialog.

2 Actifio Global Manager Requirements

This chapter details the system requirements for Actifio Global Manager (with or without Catalog) and also the requirements for AGM and RM installation. These requirements include:

- [Software Requirements](#) on page 3
- [AGM VM Requirements](#) on page 3
- [Supported AGM Configurations](#) on page 4
- [vSphere NTP](#) on page 5
- [Port Requirements](#) on page 5
- [Web Browser Requirements](#) on page 5

Software Requirements

AGM and RM support VDP appliances running 8.1 and higher.

AGM VM Requirements

During deployment, AGM will optionally come up with additional services of catalog and Report Manager according to the resources allocated to the VM.

AGM Only (Without Catalog or RM)

- Reserved 4 virtual CPUs*
- Reserved 8 GB of memory*
- 50 GB free datastore space
- One (1) virtual network interface card (vNIC)
- A static (and unique) IPv4 address

*Both the virtual CPU as well as virtual RAM allocation should be reserved.

AGM With Catalog

- Reserved 8 virtual CPUs*
- Reserved 20 GB of memory*
- Three (3) separate virtual disks for storage:
 - o One 50 GB disk for the operating system and AGM repository
 - o One 250 GB disk for the catalog index

- o One 400 GB disk to store backups of the catalog data
- One (1) virtual network interface card (vNIC)
- A static (and unique) IPv4 address

*Both the virtual CPU as well as virtual RAM allocation should be reserved.

AGM With RM

- Reserved 6 virtual CPUs*
- Reserved 16 GB of memory*
- 50 GB free datastore space
- 250 GB free datastore space for Report Manager data
- One (1) virtual network interface card (vNIC)
- A static (and unique) IPv4 address

*Both the virtual CPU as well as virtual RAM allocation should be reserved.

AGM With Catalog and RM

- Reserved 10 virtual CPUs*
- Reserved 28 GB of memory*
- Four (4) separate virtual disks for storage:
 - o One 50 GB disk for the operating system and AGM repository
 - o One 250 GB disk for the catalog index
 - o One 400 GB disk to store backups of the catalog data
 - o One 250 GB disk for Report Manager
- One (1) virtual network interface card (vNIC)
- A static (and unique) IPv4 address

*Both the virtual CPU as well as virtual RAM allocation should be reserved.

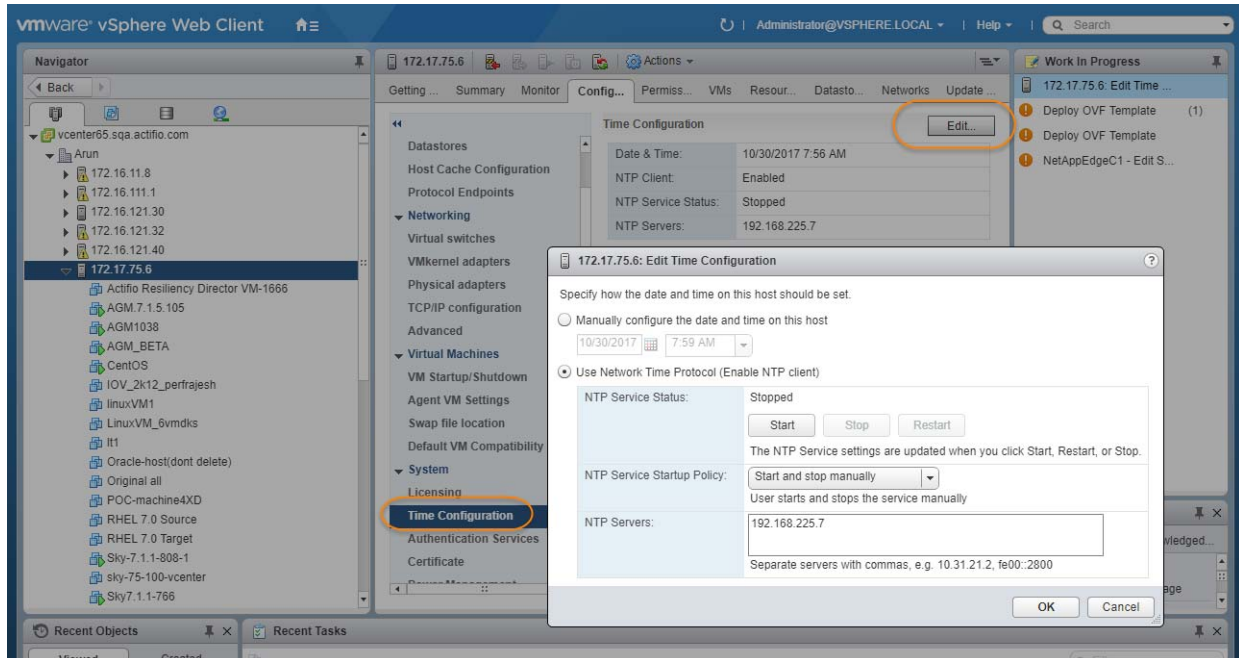
Supported AGM Configurations

The following table lists the supported AGM configurations.

Configuration	Cores (Virtual CPUs)	RAM (GB)	Base Partition Size (GB)	Additional Partitions (Minimum Size)
AGM (without Catalog or RM)	4	8	50	-
AGM with Catalog (no RM)	8	20	50	One 250 GB partition + One 400 GB partition
AGM with RM (no Catalog)	6	16	50	One 250 GB partition
AGM with Catalog and RM	10	28	50	Two 250 GB partitions + One 400 GB partition

vSphere NTP

Do not use VMware Tools periodic time synchronization for the AGM VM. You must use NTP.



Port Requirements

The following table details the required AGM port settings:*

Description	Port	Initial Connection Request*
Management of VDP appliances by AGM	TCP-5103 and TCP-443 if there is a firewall in the network	Outbound
Web browser access to AGM	TCP-443	Inbound
Remote CLI access to AGM	TCP-26 and, optionally, port TCP-22	Inbound
LDAP server authentication/authorization	Plain text LDAP: TCP-389 LDAP over SSL: TCP-636	Outbound

*Once the connection is established, data flow is bidirectional.

Web Browser Requirements

The AGM UI supports the following minimum web browsers:

- Google Chrome version 46.0 and higher
- Microsoft Internet Explorer version 11.0 and higher
- Mozilla Firefox version 41 and higher

The recommended minimum display screen resolution is 1280 x 1024 to run the AGM UI in a web browser.

3 Best Practices for AGM High Availability

VMware HA provides high availability for virtual machines by pooling them and the hosts they reside on into a cluster. Hosts in the cluster are monitored and in the event of a failure, the virtual machines on a failed host are restarted on alternate hosts.

There are two primary failover use cases with an Actifio Global Manager VM that require VMware's HA capabilities:

- **Planned Failover:** This includes DRS, DPM, and vMotion migrations of the AGM VM to other clusters due to operational requirements, maintenance windows, and so on. These operations should be expected to succeed and running jobs will continue and complete during the AGM VM migration. AGM will continue to operate normally during this operation. During failover you may encounter some performance issues.
- **Host Failure:** For any scenario where the host was not cleanly shut down, including host failure. VMware HA can perform a restart of the AGM VM on another host in the HA cluster.

This chapter details

- [Distributed Resource Scheduler \(DRS\) and Distributed Power Management \(DPM\)](#) on page 7
- [Affinity Rules](#) on page 8
- [Resource Pools](#) on page 8
- [Configuring VMware for AGM HA Failover](#) on page 8
- [Protecting the AGM VM](#) on page 9

Distributed Resource Scheduler (DRS) and Distributed Power Management (DPM)

Using VMware HA with DRS combines automatic failover with load balancing. This combination can result in faster rebalancing of virtual machines after VMware HA has moved virtual machines to different hosts.

In some scenarios, VMware HA might not be able to fail over virtual machines because of resource constraints. This can occur if HA admission control is disabled and DPM is enabled. This can result in DPM consolidating virtual machines onto fewer hosts and placing the empty hosts in standby mode leaving insufficient powered-on capacity to perform a failover.

In such cases, VMware HA will use DRS to try to adjust the cluster (for example, by bringing hosts out of standby mode or migrating virtual machines to defragment the cluster resources) so that HA can perform the failovers.

If DPM is in manual mode, you might need to confirm host power-on recommendations. Similarly, if DRS is in manual mode, you might need to confirm migration recommendations.

Affinity Rules

An affinity rule is a setting that establishes a relationship between two or more VMware virtual machines (VMs) and hosts. Affinity rules and anti-affinity rules tell the vSphere hypervisor platform to keep virtual entities together or separated.

If you are using VM-Host affinity rules, VMware HA will not perform a failover if doing so violates one of those rules.

Resource Pools

One of the benefits of resource pools is that they allow you to separate memory and CPU allocations from hardware. For example, if you are using clusters enabled for DRS, the resources of all hosts are always assigned to the cluster. That means administrators can perform resource management independently of the actual hosts that contribute to the resources. If a VM uses resource pools, the resources in its pools follow the VM, regardless of where in the cluster the VM is moved.

For more information on VMware and HA, consult your VMware documentation.

Configuring VMware for AGM HA Failover

AGM supports VMware HA and DRS/DPM. To use these features to use VMware HA to failover AGM you must consider the following:

Note: *As to be expected, there will be some performance degradation after the VM has failed over and restarted. Once an AGM VM has failed over and is running on a new ESX host in the cluster, performance will return to normal levels.*

- **Storage Accessibility:** Movement of an AGM VM from one ESX host or storage system to another using vMotion and/or DRS/DPM is supported. For this reason, Actifio recommends that the AGM VM disk devices reside on storage that is accessible to all hosts in the ESX cluster.
- **Host vMotion:** Host vMotion is supported provided you meet all of VMware's requirements for host vMotion. There is no need to shut down the AGM VM for a host vMotion operation. Host vMotion has minimal impact on performance.
- **Storage vMotion:** Storage vMotion is supported provided you meet all of VMware's requirements for Storage vMotion. Keep in mind that CPU utilization can trigger CPU alarms when running multiple Storage vMotion jobs in parallel. Actifio recommends not performing a Storage vMotion while the AGM VM is powered on.

Note: *The AGM user interface does not allow you to shut down AGM. To shut down AGM you must power down the AGM VM from the vSphere interface.*

- **VMware Fault Tolerance Configurations:** AGM does not support the VMware Fault Tolerance feature.
- **Use of Resource Pools with AGM VMs:** Manage AGM VM's resources with reserved resource pools. This ensures that the allocated (reserved) memory and CPUs for the AGM VM follow the AGM VM regardless of where VMware moves the VM. See [AGM VM Requirements](#) on page 3 for memory and CPU requirements.
- **Networking Considerations:** Network implementation and capacity for the HA cluster must allow for seamless failover of the AGM VMs and the entire Actifio appliance-managed network infrastructure must be accessible to the AGM VMs during failover (for example, DNS and NTP).
- **Resource Pools:** When adding an AGM VM to a Resource Pool, do not over-commit the pool resources. Configure a dedicated resource pool for the AGM VM. Ensure that the VMware HA cluster nodes have sufficient resources to handle all moved or recovered AGM VMs.

- VMware Slot Calculations: Ensure VMware HA slot calculations for the AGM's HA cluster is running.
- Frequency of Planned Failovers: Keep the frequency of planned failovers to a minimum. Only move AGM VMs between cluster hosts when necessary for maintenance operations or long term migrations. Ensure DRS and DPM only move the AGM VM when it is absolutely necessary and performed during periods the AGM VM is least busy.

Protecting the AGM VM

The AGM VM can be protected like any other VM. As a best practice, always protect your AGM VM before upgrading its software.

The AGM Online Help provides step-by-step instructions that walk you through:

- Adding the server on which the VM resides.
- Discovering VMs. In this case the AGM VM.
- Protecting VMs. You will need to select one of the Actifio appliances that the AGM VM manages to perform the actual protection.
- Restoring VMs.

When protecting the AGM VM you have several options for where the protected image(s) will reside:

- Local to the data center in which the AGM VM resides.
- Local to the data center in which the AGM VM resides and another data center where the AGM VM manages a VDP appliance.
- Local to the data center in which the AGM VM resides and in a cloud object store (OnVault).
- In a cloud object store only (Direct to OnVault).

Where captured images reside depends on your business needs and the risks you are willing to assume. For example:

- AGM VM images that reside in your local data center ensure that your AGM VM is recoverable as quickly as possible if you encounter issues with your VMware environment.
- AGM VM images kept at a remote site or in the cloud ensure that your AGM VM is recoverable if your data center experiences a catastrophic event.

4 Installing Actifio Global Manager

This chapter details:

- [The AGM OVA File](#) on page 11
- [Deploying and Installing the AGM OVA](#) on page 13
- [Replacing a Previously Installed AGM OVA](#) on page 23

If you want to upgrade an existing AGM VM, see [Upgrading Actifio Global Manager](#) on page 39.

To enable the AGM Catalog feature, see [Adding Resources to Enable Catalog](#) on page 25 for more information. To add RM resources, see [Adding Resources to Enable Report Manager](#) on page 28.

The AGM OVA File

The AGM deployment and installation process can take approximately 30 minutes. Your Actifio representative will help you deploy the OVA in your environment. The representative will provide you with access to the latest AGM release OVA and MD5 files. Be sure to place these two files in a location that is easily accessible by the VMware vSphere that will host AGM.

The two AGM installation files are named using the following naming convention:

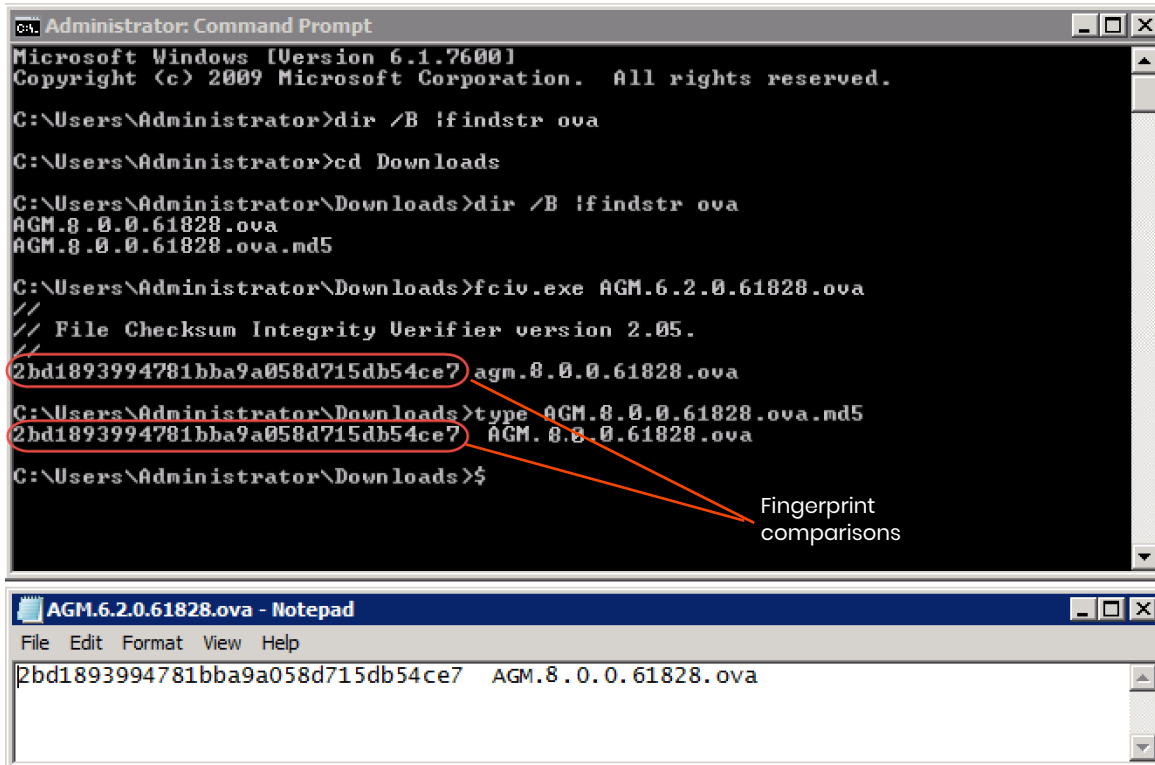
- `AGM.x.x.x.xxxxx.ova`
- `AGM.x.x.x.xxxxx.ova.md5`

The `AGM.x.x.x.xxxxx.ova.md5` file is the digital fingerprint of the installation file and is used to verify the integrity of the `AGM.x.x.x.xxxxx.ova` file.

Verifying the Integrity of the AGM.OVA File

Before you deploy the AGM.ova file, we recommend that as a best practice you first verify that its MD5 digital fingerprint matches the fingerprint file that Actifio provides in the separate *.ova.md5 file along with the *.ova file. Verifying the integrity of the AGM.OVA file will help to minimize downtime and ensure that the AGM deployment and installation process goes smoothly and without a failure. You can use a checksum utility such as File Checksum Integrity Verifier (FCIV) or md5sum to perform the verification.

The example show below uses FCIV to perform the comparison. If the fingerprints are different, the AGM installation file is corrupted. Contact your Actifio representation if this occurs.



Deploying and Installing the AGM OVA

This section describes how to deploy and install the AGM OVA file in your VMware ESX server environment using the VMware vSphere Web Client. Deployment and installation of the AGM OVA is also supported with the VMware vSphere 5.1 and later versions. The deployment and installation of the AGM OVA using a standalone ESXi host is not supported.

Note: The deployment and installation of the AGM OVA using a standalone ESXi host is not supported.

Your Actifio field representative will help you in deploying the solution in your environment. They will provide you with the latest AGM release OVA file and will place it in a location that is easily accessible by the vSphere Web Client that will host AGM. You will deploy the Actifio OVA like any other VMware OVA.

Based on your supported version of the VMware vSphere Web Client, refer to:

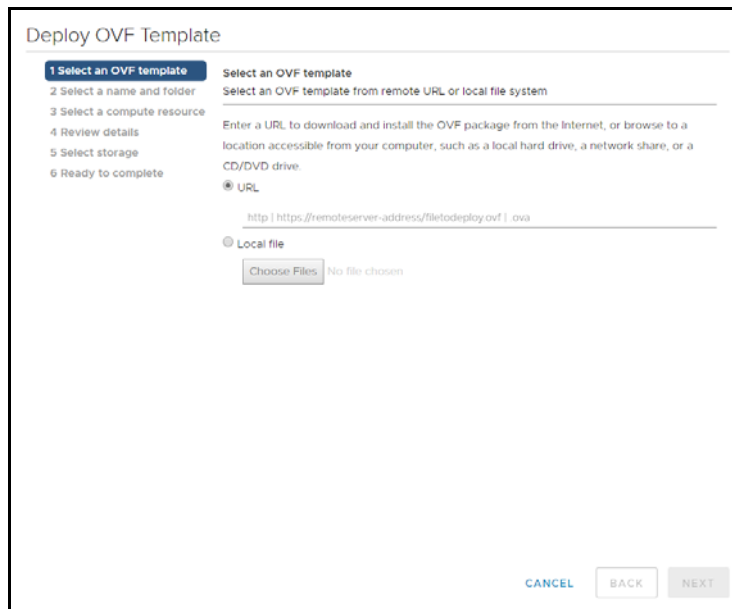
- [Deploying and Installing the AGM OVA Using VMware vSphere 6.7 Web Client](#) on page 13
- [Deploying and Installing the AGM OVA Using VMware vSphere 6.5 Web Client](#) on page 17

Deploying and Installing the AGM OVA Using VMware vSphere 6.7 Web Client

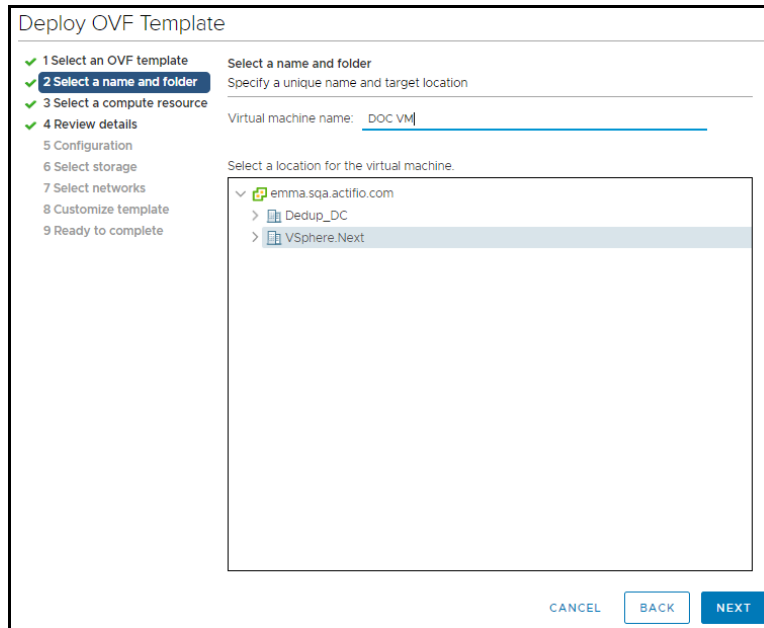
This procedure describes how to deploy and install the AGM OVA file using the VMware vSphere 6.7 Web Client using HTML5. You can also deploy AGM using Flash deployment.

To deploy and install AGM OVA using VMware vSphere 6.7 Web Client:

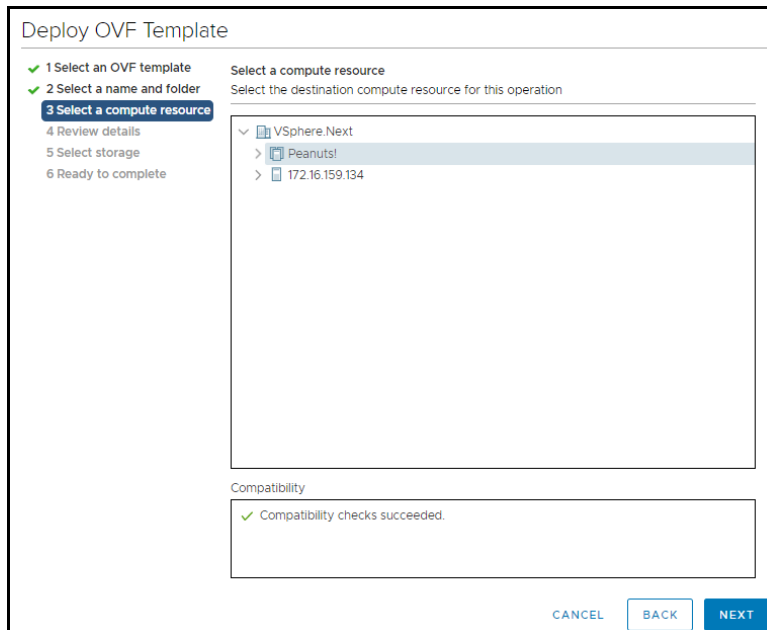
1. Open the vSphere 6.7 Web Client. Select Actions > Deploy OVF Template. The Deploy Template wizard opens showing the Select Template option.
2. In the Select Template window, browse to or enter the path to the AGM OVA file, then click **Next** to continue.



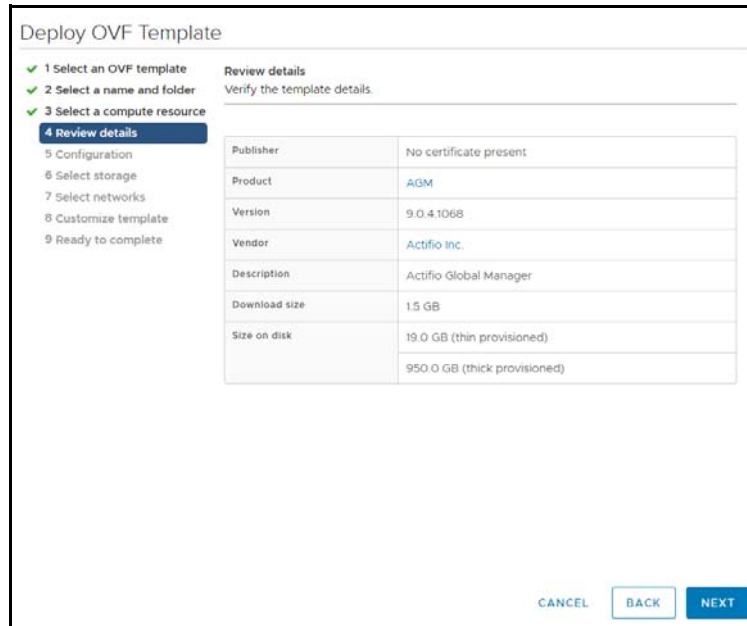
3. Select a name for the installation instance as well as its location, then click **Next** to continue.



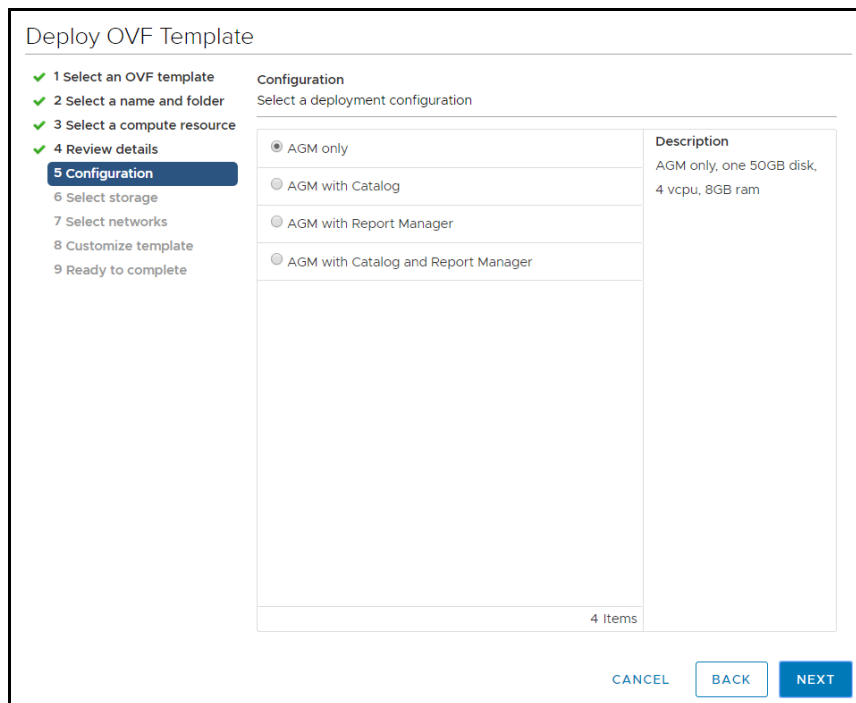
4. Select the resource pool where the deployment should be run, then click **Next** to continue.



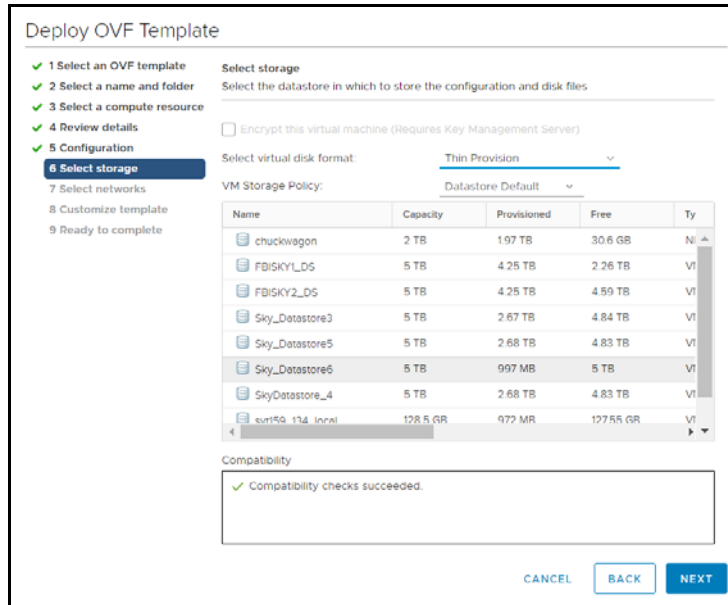
5. In the Review Details window, review the details of the AGM OVF template, then click **Next**.



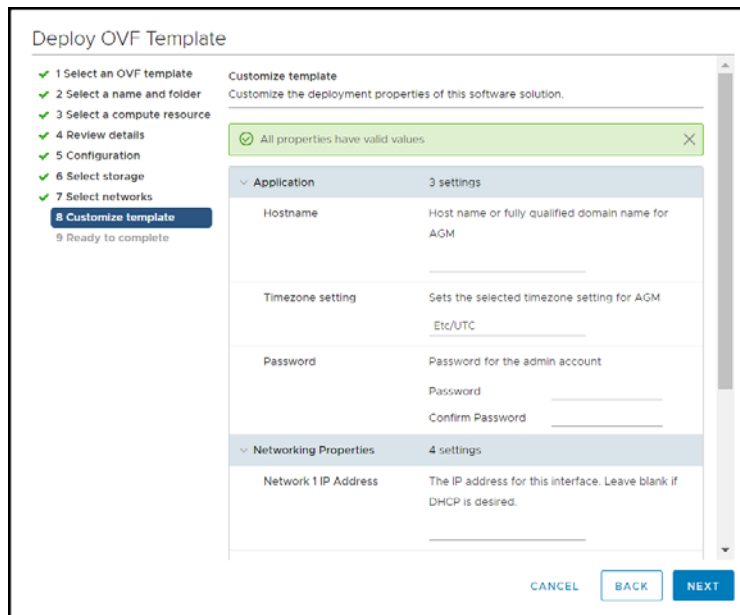
6. Select the deployment option. To install AGM only, keep the default selection, otherwise select from AGM with Catalog, AGM with Report Manager, or AGM Catalog and Report Manager, then click **Next**.



7. In the Select Storage page, select a datastore with sufficient free space to meet the minimum storage requirements for the AGM VM. From the Select virtual disk format option, choose **Thick Provision**, then click **Next**.
8. In the Setup Networks page, make any required network changes for the AGM VM, then click **Next**.



9. In the Customize Template page, customize the deployment using the information below:



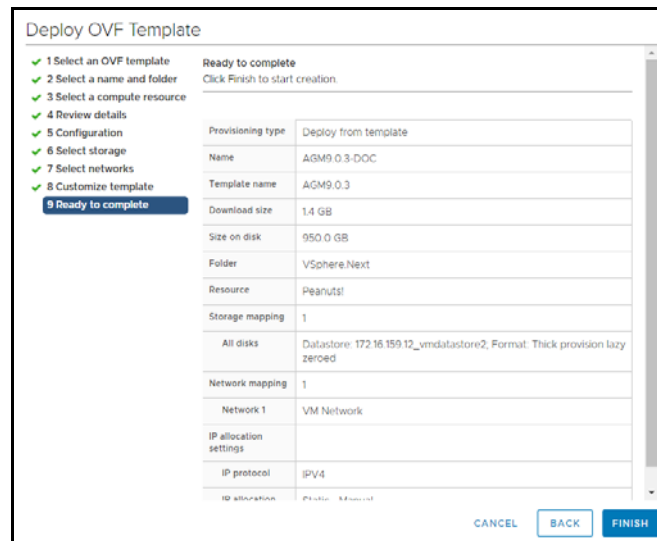
Application

- o Hostname - Enter the name or fully qualified domain name of the host. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
- o Timezone Setting - Enter the timezone of where the AGM is located.
- o Password - The password for the admin account. It can be any alphanumeric string to a maximum of 128 characters.

Networking Properties

Note: AGM deployment supports DHCP in addition to static IP support.

- o Network 1 IP Address - The IP address for this virtual machine. Copy the IP address for use when accessing the AGM (see [Accessing Actifio Global Manager](#) on page 29).
 - o Network 1 Netmask - The subnet mask or prefix for this virtual machine.
 - o Default Gateway - The default gateway for this virtual machine.
 - o DNS - The domain name server for this virtual machine.
10. Click **Next**. In the Ready to Complete window, review the deployment settings for the AGM OVF template.



11. If you need to make any changes, click **Back** and modify the settings. Click **Finish**.
12. The Deploying OVF Template message box opens listing the AGM deployment status. The AGM will reboot one additional time after deployment is completed to complete the configuration. You may need to manually power on AGM. Copy the IP address for use when accessing the AGM (see [Accessing Actifio Global Manager](#) on page 29).

Once deployment is complete, you can manually change the configuration to run AGM with or without the Catalog feature. See [Configuring Resources](#) on page 25 for more information.

Deploying and Installing the AGM OVA Using VMware vSphere 6.5 Web Client

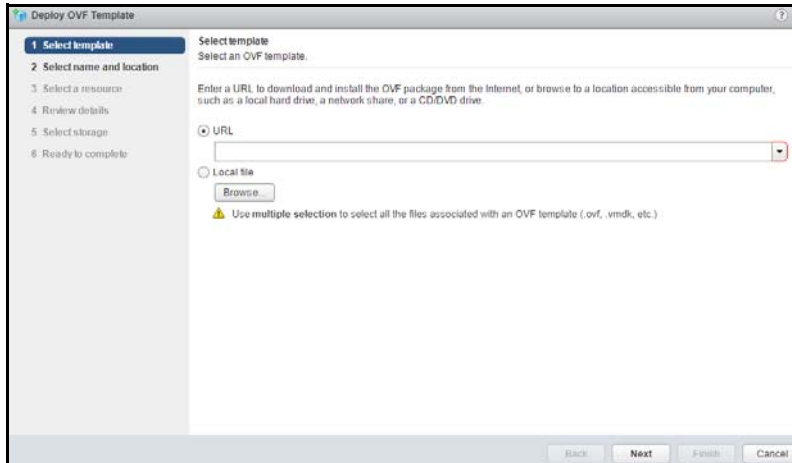
This procedure describes how to deploy and install the AGM OVA file using the VMware vSphere 6.5 Web Client. AGM 8.0.4 and later versions can be installed with or without Catalog. You will see the AGM installation options for Flash deployment and only if you are using VMware vSphere 6.5 Web Client (HTML5) updated or later.

For earlier version of Web Client (HTML5), AGM will get deployed and installed without Catalog. You will have to manually add the system resources required for a Catalog configuration. For more information, see

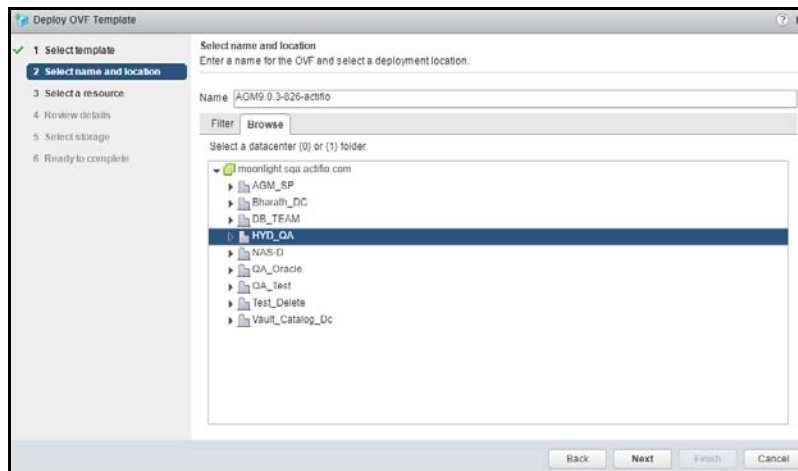
Note: For VMware vSphere 6.5 Flash deployment, you will not have the option to deploy and power up the VM. You will have to manually power it up. For more information, see <https://kb.vmware.com/s/article/2148007>.

To deploy and install AGM OVA using VMware vSphere 6.5 Web Client:

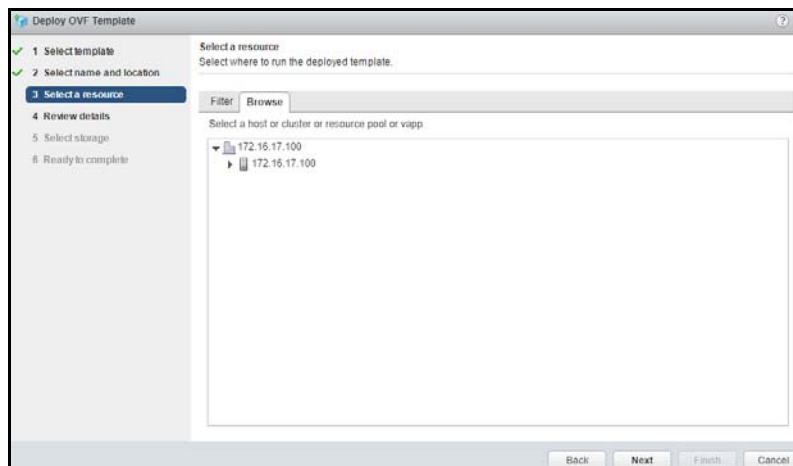
1. Open the vSphere 6.5 Web Client. Select Actions > Deploy OVF Template. The Deploy Template wizard opens showing the Select Template option.
2. In the Select Template window, browse to or enter the path to the AGM OVA file.



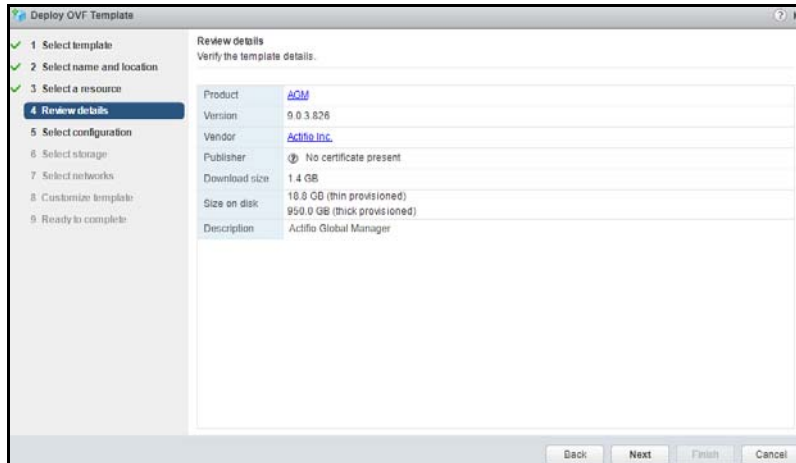
3. Click **Next** to open the select name and location dialog.
4. Select a name for the installation instance as well as its location.



5. Click **Next** to open the Select resource dialog.
6. Select the resource pool where the deployment should be run.

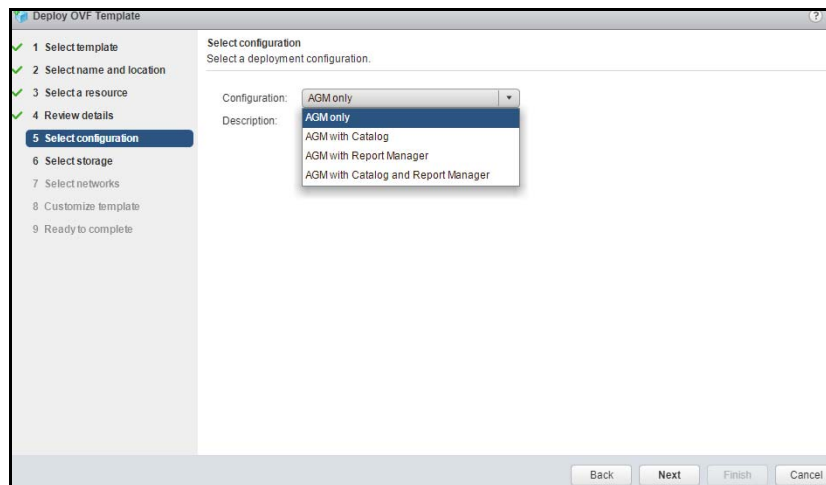


7. Click **Next** to open the Review Details dialog.
8. Review the details of the AGM OVF template.

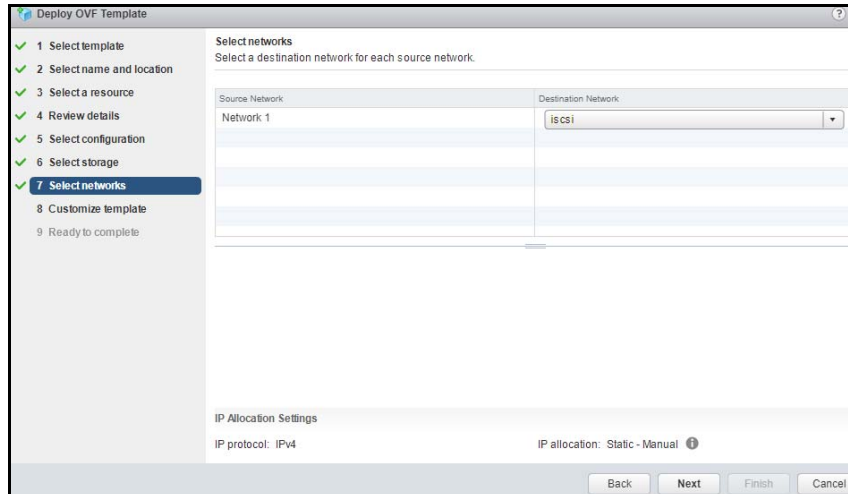


9. Click **Next**.
10. Select the deployment option. To install AGM only, keep the default selection. Otherwise, select from AGM with Catalog, AGM with Report Manager, or AGM Catalog and Report Manager.

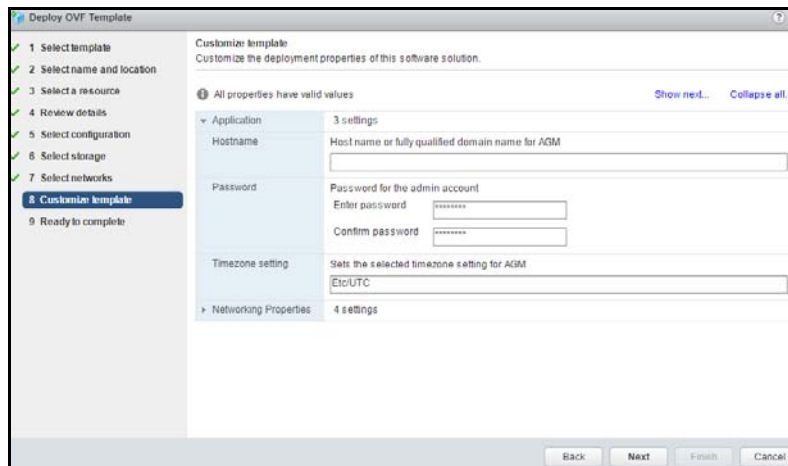
Note: You will see the deployment options only when using VMware vSphere 6.5 Web Client (HTML5) updateId or later.



11. Click **Next**.
12. In the Select Storage page, select a datastore with sufficient free space to meet the minimum storage requirements for the AGM VM.
13. From the Select virtual disk format option, choose **Thick Provision**, then click **Next**.
14. In the Setup Networks page, make any required network changes for the AGM VM, then click **Next**.



15. In the Customize Template page, customize the deployment as follows and click **Next**.



Application

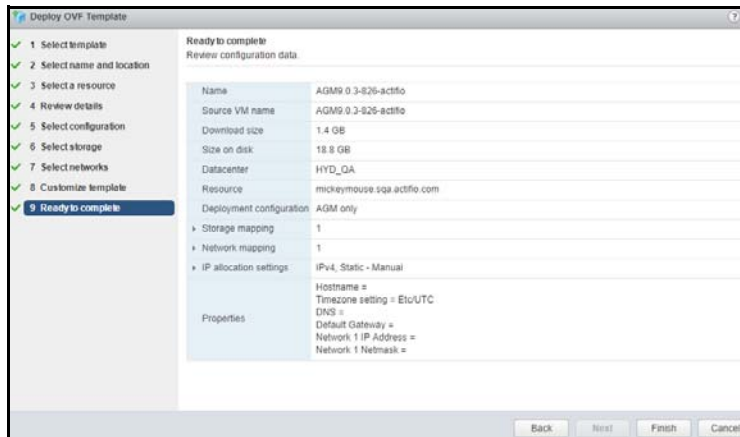
- o Hostname - Enter the name or fully qualified domain name of the host. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
- o Timezone Setting - Enter the timezone of where the AGM is located.
- o Password - The password for the admin account. It can be any alphanumeric string to a maximum of 128 characters.

Networking Properties

Note: AGM deployment supports DHCP in addition to static IP support.

- o Network 1 IP Address - The IP address for this virtual machine. Copy the IP address for use when accessing the AGM (see [Accessing Actifio Global Manager](#) on page 29).
- o Network 1 Netmask - The subnet mask or prefix for this virtual machine.
- o Default Gateway - The default gateway for this virtual machine.
- o DNS - The domain name server for this virtual machine.

16. Click **Next**. In the Ready to Complete window, review the deployment settings for the AGM OVF template.
-



17. If you need to make any changes, click **Back** and modify the settings. Then click **Finish**.
18. The Deploying OVF Template message box opens listing the AGM deployment status. The AGM will reboot one additional time after deployment is completed to complete the configuration. If you had selected **Power on after deployment**, AGM is fully powered on and ready for use. Otherwise manually power on AGM. Copy the IP address for use when accessing the AGM (see [Accessing Actifio Global Manager](#) on page 29).

Once deployment is complete, you can manually change the configuration to run AGM with or without the Catalog feature. See [Configuring Resources](#) on page 25 for more information.

Deploying and Installing the AGM OVA Using VMware vSphere 5.5 Web Client

This procedure describes how to deploy and install the AGM OVA file using the VMware vSphere 5.5 Web Client.

To deploy and install AGM OVA using VMware vSphere 5.5 Web Client:

1. Open the vSphere 5.5 Web Client and select **Deploy OVF Template**. The **Deploy OVF Template** wizard opens.
2. In the **Select Source** window, browse to or enter the path to the AGM OVA file, then click **Next** to continue.
3. In the **Review Details** page, review the details of the AGM OVF template, then click **Next**.
4. In the **Select Name and Folder** page:
 - o For **Name**, enter the name of the AGM you are to install. The name can contain up to 80 characters.
 - o In the **Select a Folder or Datacenter** pane, select the data center and cluster/ESX host for the deployment of the AGM VM, then click **Next**.
5. In the **Select Configuration** page, select the AGM configuration you want to install. You can change the system resources after installation is complete if necessary. See [Configuring Resources](#) on page 25 for more information. Click **Next**.
6. In the **Select resource** page, select the cluster, host or resource pool in which you want to run the deployed template, then click **Next**.
7. In the **Storage** page, select a datastore with sufficient free space to meet the minimum storage requirements for the AGM VM.
8. For the **Select virtual disk format** option, select **Thin Provision**, then click **Next**.

9. In the Setup Networks page, make the required network changes for the AGM VM, then click **Next**.

10. In the Customize Template page, customize the deployment properties as follows:

Application

- o Hostname - Enter the name or fully qualified domain name of the host. The name of a host should start with a letter, and can contain letters, digits (0-9), and an underscore ('_').
- o Timezone Setting - Enter the timezone where the AGM is located
- o Password - Enter the password for the admin account. The password can be any alphanumeric string to a maximum of 128 characters.

Networking Properties

Note: AGM deployment supports DHCP in addition to static IP support.

- o Network 1 IP Address - Enter the IP address for this virtual machine. Copy the IP address for use when accessing the AGM (see [Accessing Actifio Global Manager](#) on page 29).
- o Network 1 Netmask - Enter the subnet mask or prefix for this virtual machine.
- o Default Gateway - Enter the default gateway for this virtual machine.
- o DNS - Enter the domain name server for this virtual machine.

Click **Next**.

11. In the Ready to Complete window, review the deployment settings for the AGM OVF template. If you need to make any changes, click Back and modify the settings. Optionally, click the Power on after deployment check box if you want to start the AGM immediately after deployment completes. Once you are satisfied with the configuration, click Finish to begin the install.

12. The Deploying OVF Template message box opens listing the AGM deployment status. The AGM will reboot one additional time after deployment is completed to complete the configuration. If you had selected Power on after deployment, AGM is fully powered on and ready for use. Otherwise manually power on AGM. Copy the IP address for use when accessing the AGM (see [Accessing Actifio Global Manager](#) on page 29).

Once deployment is complete, you can manually change the configuration to run AGM with or without the Catalog feature. See [Configuring Resources](#) on page 25 for more information.

13. Click **OK** to close the Virtual Machine Properties page.

14. Power on AGM with Catalog. Continue to launching AGM in a web browser. See [Accessing Actifio Global Manager](#) on page 29 for more information.

Replacing a Previously Installed AGM OVA

In case you need to replace a previously installed AGM VM, follow the sequence outlined below prior to deploying and installing the new AGM OVA. This procedure will help ensure a smooth installation and operational transition to the new AGM VM:

1. Remove all managed VDP appliances from the existing AGM through the Domain Manager service (see “Removing an Appliance from AGM” in the AGM Online Help System). Removing each VDP appliance from the AGM server completely removes the management of the VDP appliance by AGM. All resources associated with the managed VDP appliance will be removed from AGM.
2. Power down and remove the existing AGM VM from the VMware ESX server.
3. Deploy the new AGM OVA file (see [Deploying and Installing the AGM OVA](#) on page 13).

Note: *If you encounter issues during the deployment and installation of the new AGM OVA, please contact your Support representative.*

4. After you successfully complete deploying the AGM OVA file and launch AGM, your next step will be to add all managed VDP appliances to AGM through the Domain Manager service (see “Adding a VDP Appliance to AGM” in the AGM Online Help System).

As a deployment best practice, we recommend that you first import a baseline VDP appliance before adding the other VDP appliances to be managed by the new AGM (see [Adding Appliances to an AGM Deployment](#) on page 33). This AGM and VDP appliance deployment best practice will import all SLA templates (and policies) and security objects (organizations, roles, users) from the VDP appliances to become AGM-level objects. This object importing sequence includes SLA templates created in your original AGM and had been pushed to the managed VDP appliances. These are SLA templates that were used to manage applications on the appliance.

5 Configuring Resources

This chapter details:

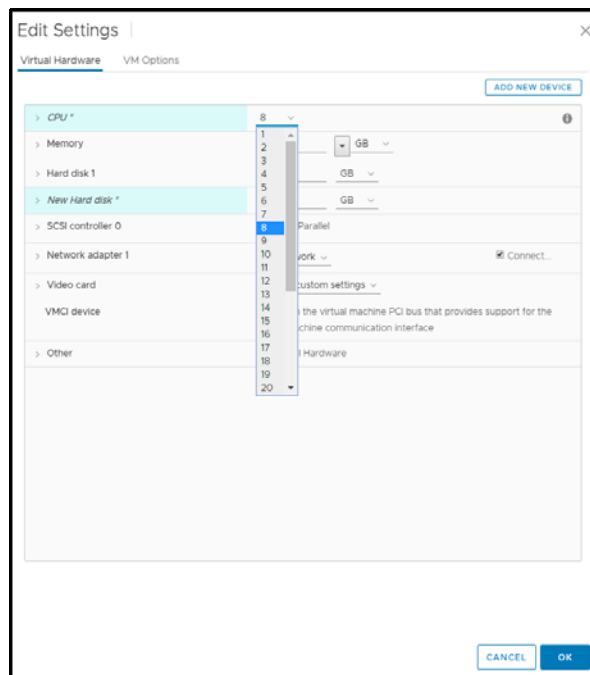
- [Adding Resources to Enable Catalog on page 25](#)
- [Removing Resources to Disable Catalog on page 27](#)
- [Adding Resources to Enable Report Manager on page 28](#)

Adding Resources to Enable Catalog

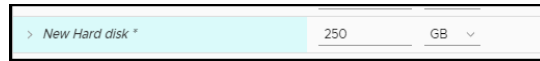
This procedure is helpful if you want the AGM Catalog feature but during AGM deployment the Catalog resources were not enabled. (The images in this section are from vSphere Client 6.7. The options you see may be slightly different depending on the version on vSphere Client you are using.)

After AGM deployment is complete, but before it is powered up:

1. Select the AGM VM and click **Edit Virtual Machine Settings**. The Virtual Machine Properties page opens.
2. Increase Memory size from 8GB to 20GB and then increase virtual CPUs from 4 to 8.



3. From the **Add New Device** drop-down, select **Hard Disk** and click **Add**.
4. Configure the new hard disk for 250 GB of storage for the index store and click **OK**. The new disk is added.



The new disk gets added as Hard Disk 2.

5. Add Hard Disk 3 with 400 GB of storage space for backup catalog data.
6. Click **OK** to close the Virtual Machine Properties page.
7. Power on AGM with Catalog. Continue to launching AGM in a web browser. See [Accessing Actifio Global Manager](#) on page 29 for more information.

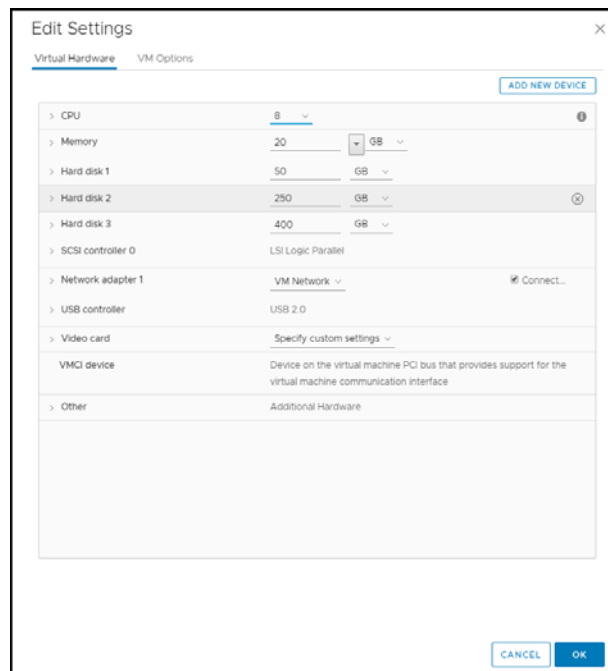
Note: You must have an Administrator account or an account in the Administrators group when accessing cataloged data, otherwise scanning for indexed data may fail.

Removing Resources to Disable Catalog

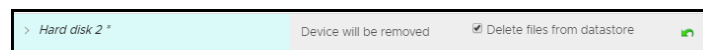
This procedure is helpful if you do not want the AGM Catalog feature but during AGM deployment the Catalog resources were enabled.

After AGM deployment is complete and before it is powered up:

1. Select the AGM VM and click **Edit Virtual Machine Settings**. The Virtual Machine Properties page opens.
2. Reduce Memory size from 20GB to 8GB.
3. Reduce virtual CPUs from 8 to 4.



4. Select Hard disk 2 and click Remove as shown in the image.
5. From removal options, select **Delete files from disk**.



6. Remove Hard disk 3.
7. Click **OK** to close the Virtual Machine Properties page.
8. Power on AGM. Continue to launching AGM in a web browser. See [Accessing Actifio Global Manager](#) on page 29 for more information.

Adding Resources to Enable Report Manager

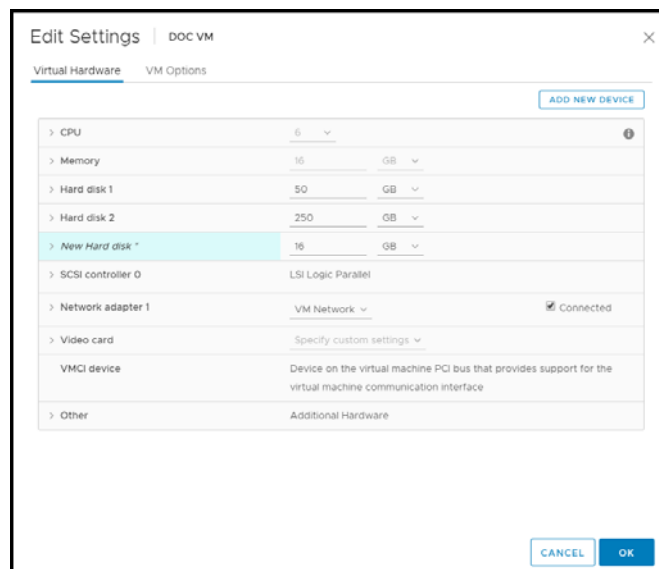
This section explains how to manually add resources to the AGM VM to enable RM. Adding the resources may take a long time (over an hour). While the resources are getting added, AGM will not be available for use.

Note: Do not remove the disk you will be adding for RM (step 6) under any circumstances. This will corrupt your AGM database.

1. Verify that the AGM VM is powered off.
2. Select the AGM VM and click **Edit Settings**. The Edit Settings page opens.
3. Increase virtual CPUs:
 - o For AGM Without Catalog, increase virtual CPUs from 4 to 6.
 - o For AGM with Catalog, increase virtual CPUs from 8 to 10.
4. Increase Memory size:
 - o For AGM Without Catalog, increase the Memory size from 8 GB to 16 GB.
 - o For AGM With Catalog, increase the memory size from 20 GB to 28 GB.
5. From the **Add New Device** drop-down, select **Hard Disk** and click **Add**.
6. Configure the new hard disk for 250 GB and click **OK**. The new disk is added.

Note: Do not remove the disk; it will corrupt AGM.

The following image shows an AGM VM (without Catalog) and with RM resources added.



7. Click **OK** to close the Virtual Machines Properties page.
8. Power on AGM with RM.
9. Continue launching AGM and RM in a web browser. See [Accessing Actifio Global Manager](#) on page 29. After you launch AGM, continue to launch RM in a web browser. For more information, see [Accessing Report Manager](#) on page 31.

6 Accessing Actifio Global Manager

After the AGM is configured and powered up, you can launch AGM in a web browser:

Note: You can find the IP address of the AGM on the AGM VM's Summary tab.

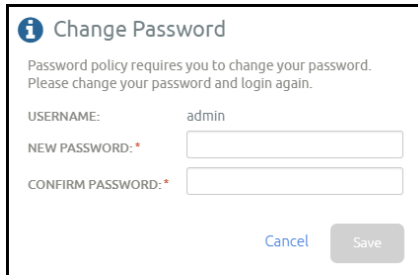
1. Open a browser and in the address space, enter the IP address of the AGM VM:
`https://<AGM IP address>/`



2. In the AGM Login window, enter the login credentials you specified during deployment. If you did not specify anything, enter the default login credentials: USERNAME admin and PASSWORD password
3. Click Login.

Note: If you are using a Microsoft Internet Explorer browser to log in to AGM and the Username and Password fields are disabled in the Login window, access the Compatibility View Settings dialog box (select **Tools > Compatibility View settings**) and ensure that the **Display intranet site in Compatibility View** check box is checked.

The AGM application opens and prompts you to change your password as part of security enhancement.



Change Password

Password policy requires you to change your password.
Please change your password and login again.

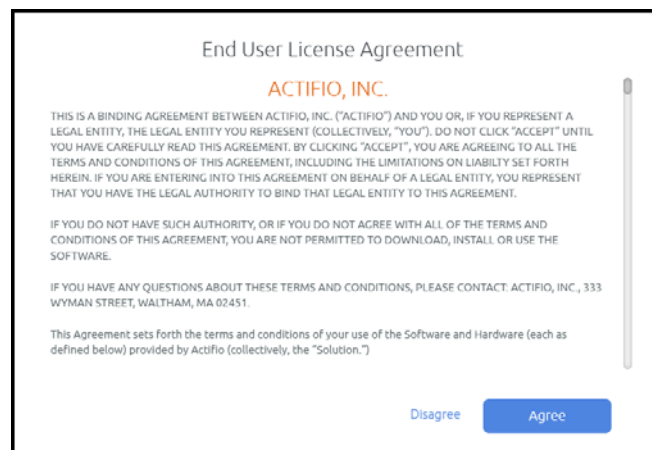
USERNAME: admin

NEW PASSWORD: *

CONFIRM PASSWORD: *

Cancel Save

4. Enter a new password of at least six (6) characters (it can be the same as your old password).
5. Click Save to save the new password. You are taken back to the login screen.
6. Enter your user name and new password.
7. Click Login. The AGM application opens and shows the EULA.



End User License Agreement

ACTIFIO, INC.

THIS IS A BINDING AGREEMENT BETWEEN ACTIFIO, INC. ("ACTIFIO") AND YOU OR, IF YOU REPRESENT A LEGAL ENTITY, THE LEGAL ENTITY YOU REPRESENT (COLLECTIVELY, "YOU"). DO NOT CLICK "ACCEPT" UNTIL YOU HAVE CAREFULLY READ THIS AGREEMENT. BY CLICKING "ACCEPT", YOU ARE AGREEING TO ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT, INCLUDING THE LIMITATIONS ON LIABILITY SET FORTH HEREIN. IF YOU ARE ENTERING INTO THIS AGREEMENT ON BEHALF OF A LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE LEGAL AUTHORITY TO BIND THAT LEGAL ENTITY TO THIS AGREEMENT.

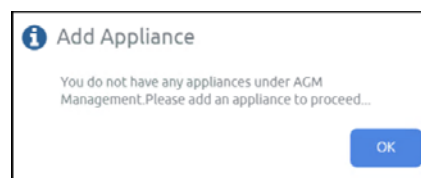
IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT AGREE WITH ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, YOU ARE NOT PERMITTED TO DOWNLOAD, INSTALL OR USE THE SOFTWARE.

IF YOU HAVE ANY QUESTIONS ABOUT THESE TERMS AND CONDITIONS, PLEASE CONTACT: ACTIFIO, INC., 333 WYMAN STREET, WALTHAM, MA 02451.

This Agreement sets forth the terms and conditions of your use of the Software and Hardware (each as defined below) provided by Actifio (collectively, the "Solution.")

Disagree Agree

8. Read the license agreement in its entirety, and click Agree.
You are prompted to add an appliance.



Add Appliance

You do not have any appliances under AGM Management. Please add an appliance to proceed...

OK

9. Click OK to open the Add Appliance page. Add the first appliance and subsequently add more appliances following guidelines [Adding Appliances to an AGM Deployment](#) on page 33.
10. Click the ? in the upper right corner of the AGM browser to launch the AGM Online Help system. You can read up about the Dashboard, Domain Manager, SLA Architect, Application Manager, Catalog, System Monitor, and Upgrade services in the Help.
11. To logout of AGM or to change users, click the active user listed at the top of AGM and select Logout.

7 Accessing Report Manager

After you have launched AGM in a web browser, launch RM.

Note: RM uses the same IP address as AGM.

To access RM:

1. Open a browser and in the address space enter the IP address of the RM.
https://<AGM IP address>/rm or **https://<AGM IP address>/report**
2. Enter your AGM user name and password.

Note: AGM users with Administrator role can perform administrative tasks in RM.

3. Click **Login**.

8 Adding Appliances to an AGM Deployment

Before you add appliances to AGM, perform a business requirements analysis of the SLA templates (and policies), roles, organizations, and users created on each of the Actifio appliances to be imported into AGM. Consistency is critical to ensuring a centralized and consolidated set of imported policy and security objects from your Actifio appliances into AGM. This is especially important for SLA templates and policies, as well as for user roles, that have been defined in your individual appliances.

Ideally, the SLA templates and policies used by the appliances in your operating environment follow a consistent governance for SLA template and policy naming conventions along with the definition of policy attributes across each appliance. However, SLA templates in multiple Actifio appliances may use the same name, but are configured differently. For example:

Two or more appliances can each have an SLA template named Tier 1. Upon closer inspection, there can be differences in the policies in each template. These inconsistencies will result in conflicts when you attempt to add those templates to the appliances into AGM. You must resolve those differences before importing the Actifio appliances.

Object conflicts during the import process typically occur under the following conditions:

- o SLA templates of the same name have a different number of policies and/or defined attributes between the appliance and AGM.
- o Roles of the same name have differences in services and/or Access Control Level (ACL) rights between the appliance and AGM.

Note: During Actifio appliance importing, the mapping of LDAP groups will not be brought into AGM. For example, if there is an LDAP group named “DNSUpdateProxy” on Appliance 1, after importing Appliance 1 to AGM “DNSUpdateProxy” will not appear in AGM.

After you import your Actifio appliance(s) into AGM, configure the LDAP server on AGM and then recreate the missing mapped LDAP groups in AGM. Be sure to assign the proper organizations and roles to them. For more information, go to the **AGM Online Help System**, and read the “Configuring LDAP Settings” and “Mapping LDAP Groups to Roles and Organizations” topics.

Review the following planning topics to help you pro-actively address potential conflicts and ensure a smooth import of your Actifio appliances and its associated policy and security objects:

- [Selecting the First Actifio Appliance to Import](#) on page 34
- [Managing SLA Templates Prior to Importing](#) on page 35
- [Managing Roles](#) on page 35
- [Resource Conflict Resolution Tool](#) on page 36
- [Managing Organizations](#) on page 35

Selecting the First Actifio Appliance to Import

Choose an appliance that is used in a production environment as the first appliance to add into AGM. This will help establish a baseline for the templates, organizations, roles, and users imported into the AGM database for addressing potential conflicts with subsequent appliances you add into AGM.

The first Actifio appliance that you plan to import into AGM should contain policy and security objects (Templates, Organizations, Roles, and Users) with names and configurations that are most representative of the typical operating environment of your organization. The first appliance that you add into AGM serves as the baseline appliance used by AGM as the standard for comparison with all subsequent imported appliances for object consolidation.

For example, if you import an appliance that is used in a Test/Dev environment, the templates, organizations, roles, and users that are imported in AGM may contain actual object names but may contain atypical configuration settings. When you attempt to import additional appliances that contain Templates, Organizations, Roles, or Users with the same names, this can result in object conflicts between AGM and that appliance at the point of import.

Sharing Mode Options

When two Actifio appliances are joined with Sharing Mode enabled and you are adding them to AGM, you can:

Add Just the Primary Appliance

In this case, AGM pushes templates only to the Primary appliance. The Primary appliance will then push templates to the Secondary appliance. AGM will be able to manage applications on the Primary appliance, but not on the Secondary appliance. You must log on to the Secondary appliance to manage its applications. Sharing Mode maintains the Organizations and users defined between the Primary and Secondary appliances.

Add Both the Primary and Secondary Appliances

In this case, you MUST add the Primary appliance first.

After both appliances are added, updated templates can be pushed to both appliances. When the Primary receives an updated template it will push the updated template to the Secondary.

AGM will be able to manage applications on both the Primary and Secondary appliances. Sharing Mode maintains the Organizations and users defined between the Primary and Secondary appliances.

Disable Sharing Mode Then Add Both Appliances

In this case, un-join the appliances, then join them again in non-sharing mode. Add the primary appliance first and then the secondary appliance of the pair.

After both appliances are added, templates can be pushed to both appliances. AGM will be able to manage applications on both appliances. You may have to log in to what was the Secondary appliance and configure/reconfigure Organizations and users. Organizations and users on what was the Primary will remain intact.

Managing SLA Templates Prior to Importing

Check the SLA template naming conventions used on two or more appliances that you plan to import into AGM. If multiple appliances contain SLA templates of the same name, but those templates contain either a different number of policies or different policy attributes, this will result in a conflict when you go to import those appliances.

Excluding the first appliance that you plan to import as the baseline appliance, you can attempt an initial clean-up of the other appliances in the following areas:

- Rename conflicting SLA templates.
- Modify a conflicting SLA template to either add the missing policies or remove the extra policies.
- Modify the attributes in the differing policy (or policies) in the conflicting SLA template to make them the same.

The Dry Run tool in AGM identifies conflicts between the incoming appliance and what currently exists in AGM during the import process (see [Resource Conflict Resolution Tool](#) on page 36).

Managing Roles

Check the roles (names and attributes) used on the appliances that you plan to import into AGM. If you have multiple roles of the same name but those roles have differences in services and/or Access Control Level (ACL) rights, this will result in a conflict when you go to import those appliances.

Excluding the first Actifio appliance that you plan to import as the baseline appliance, on the other appliances you can attempt a clean-up of the services and/or rights associated with the conflicting role(s) to make them the same.

You may encounter an instance when AGM detects a conflict because of a missing role-right assignment on the appliance to be added yet the role-right assignments appear to be identical. In this case, if differences are detected in role-right assignments between the appliance and AGM, delete the problematic role from AGM and then retry adding the appliance to AGM.

The Dry Run tool in AGM identifies security conflicts between the in-coming appliance and what currently exists in AGM during the import process (see [Resource Conflict Resolution Tool](#) on page 36).

Managing Organizations

When you add an Actifio appliance to AGM, the organizations from each appliance are imported to AGM. Keep in mind that:

- An appliance's organizations are imported to AGM when the appliance is added to AGM.
- Existing organizations, new organizations, or changes to organizations in AGM are not exported to appliances.
- When two or more appliances use the same name for an organization, then upon import to AGM, a single organization is created that has all of the resources specified in the imported organizations.

For example, before appliances are added to AGM:

Appliance1 has three organizations. Only the Public organization contains resources:

```
Organization: Private1
Organization: Private2
Organization: Public
  User Ken
  Host 172.10.111.11
```

Appliance2 has three organizations. Only the Public organization contains resources:

```
Organization: Administrators
Organization: Public
  User Bob
```

Host 172.10.131.98
Organization: Test
AGM has two organizations:

Organization: Finance
Organization: Marketing

After the two appliances are added to AGM, both appliances keep their respective organizations. AGM will import copies of each appliance's organizations as follows:

Organization: Administrators (From Appliance2)
Organization: Finance (Original to AGM)
Organization: Marketing (Original to AGM)
Organization: Private1 (From Appliance1)
Organization: Private2 (From Appliance1)
Organization: Public (From Appliance1 and Appliance2)
User Ken (From Appliance1)
User Bob (From Appliance2)
Host 172.10.111.11 (From Appliance1)
Host 172.10.131.98 (From Appliance2)
Organization: Test (From Appliance2)

The organization Public from both appliances is imported in to a single organization named Public. AGM's Public organization contains the resources from the Public organizations from both appliances

Resource Conflict Resolution Tool

When you add a new VDP appliance, AGM automatically runs the Dry Run Tool and performs a conflict analysis. This tool identifies conflicts between appliances currently managed by AGM and an Actifio appliance being imported.

The Dry Run tool resolves resource conflicts as follows:

- SLA Templates—Templates go through a conflict-resolution process by AGM.
- Organizations—Imported appliance-level organizations with the same name are merged with the AGM-level organizations, and their AGM-level objects (users and SLA templates) are associated with their respective AGM objects.
- Users—Users that already exist in AGM are ignored and are not imported from the appliance.
- Roles—Roles go through a conflict-resolution process by AGM.

During the dry-run phase of the appliance import process a log is displayed that details all import actions and decisions. For example, in the following screen capture of a log:

- Policies are missing from the Standard and Enterprise templates found in the incoming appliance and AGM.
- Specific rights are missing from the Basic role found in the incoming appliance and AGM.

If you encounter a conflict during Dry Run, resolve each conflict on the appliance that is experiencing the issue.

The screenshot shows the 'Add New Appliance' page in the Actifio interface. The page title is 'Add New Appliance'. Below the title, there is a sub-header: 'Once you add to AGM, we'll import the users, organizations, hosts and apps.' The 'IMPORT STATUS' is 'Failure', indicated by a red 'x' icon. A red error message box contains the text: '172.15.9.132 is not reachable, or it is not a supported appliance, or the credential provided is wrong(10040)'. Below the error message is a link: 'Open Troubleshooting Guide'. The form fields are: 'IP ADDRESS OR FQDN*' with the value '172.15.9.132', 'ADMIN USERNAME*' with the value 'admin', and 'ADMIN PASSWORD*' with masked characters '*****'. At the bottom right of the form are two buttons: 'Cancel' and 'Add Appliance'.

For example, based on the identified conflict flagged during Dry Run for the appliance you wish to import into AGM, you can:

- Rename conflicting SLA templates on the appliance.
- Modify a conflicting SLA template on the appliance to add the missing policies or remove the extra policies.
- Modify the attributes in the differing policy (or policies) in the conflicting SLA template on the appliance to make the attributes the same.
- Modify the services and/or rights associated with the conflicting role identified on the appliance to make the services and/or rights the same.

For details on the appliance import process, including import guidelines, recommendations, the step-by-step import process, and conflict troubleshooting, see the following AGM Online Help System topics:

- [Importing Overview](#)
- [Adding an Appliance to AGM](#)

“Troubleshooting Conflicts” For the best practices associated with creating and modifying SLA policy templates for use by an Actifio appliance, see Best Practices for the Actifio SLA Architect’s Policy Templates located in the Actifio Documentation Library included with each Actifio appliance and also available on the [ActifioNow customer portal](#).

9 Upgrading Actifio Global Manager

This chapter details the upgrade instructions for the Actifio Global Manager. It includes the following topics:

- [Before You Begin](#) on page 39
- [Upgrading AGM](#) on page 39

Note: During an upgrade there will be a period of time when AGM synchronizes new data with the appliances. This may lead to incorrect values being shown on the AGM Dashboard. We recommend that you wait for a period of one to two hours for the inconsistencies to resolve. If they persist even after that time, contact Support for help.

Before You Begin

Before you begin you must:

Take a Snapshot of the current AGM VM

In the unlikely event that you encounter an issue while upgrading, a snap shot will allow you to revert back to the previous state of your AGM VM.

Obtain the AGM.gpg upgrade file

Your Actifio representative will provide you with the latest AGM upgrade file. Place a copy of that file in a location that is easily accessible from the AGM browser-based UI.

Upgrading AGM

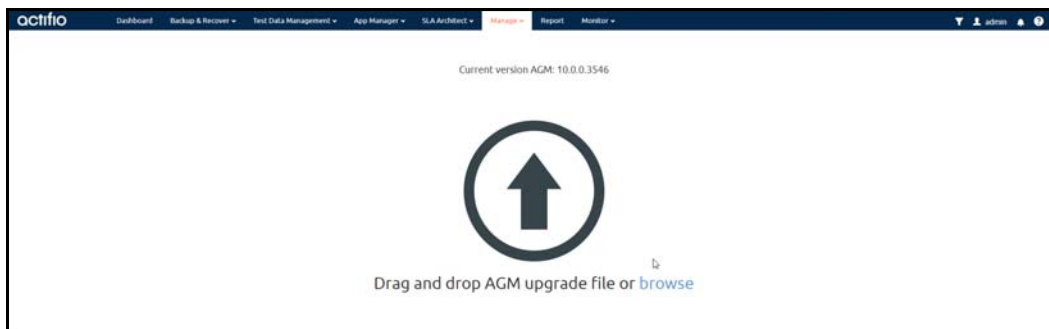
Note: AGM version 9.0.5 and higher can update to AGM 10.0 directly.
AGM version 9.0.4 or older must upgrade first to AGM 9.0.5 and then upgrade to AGM 10.0.
AGM version 10.0 can manage appliances that are running 8.1 and higher.

After reviewing the information outlined in [Before You Begin](#) on page 39, perform the AGM software upgrade as follows:

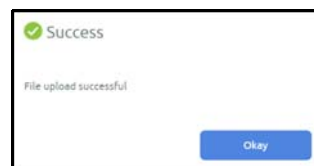
1. Open a browser, and in the address space enter the IP address of the AGM VM:
`https://<VM IP address>/`
2. In the AGM Login page, enter the username and password, then click **Log In**.



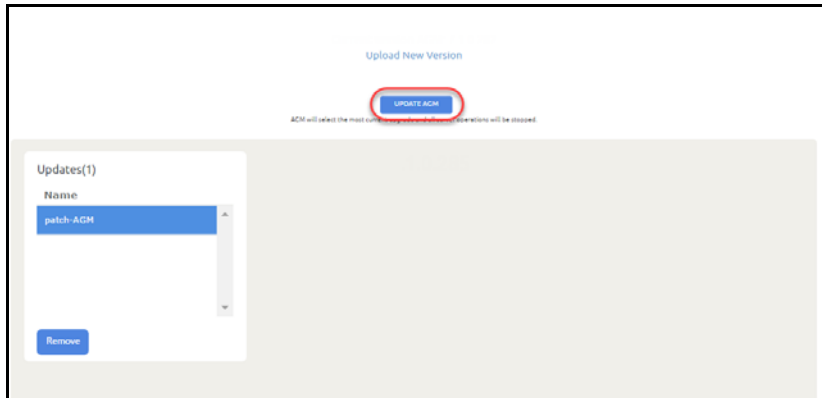
3. From the AGM Dashboard, click the **Manage** tab. Select **Upgrade** from the drop-down menu. The Upgrade page opens.



4. From the Upgrade page, you can either:
 - o Browse to the location of the AGM.gpg upgrade file and upload it into this window.
 - o Drag and drop the AGM.gpg upgrade file into this window.
5. AGM begins the upload process. A Progress bar shows the status of the upload. The file upload sequence undergoes three phases: file upload, file unpack, and file extraction.



6. When the file upload is complete and the upgrade image has been extracted, a Success dialog opens.
7. Click **Okay** and the Upgrade page opens.



8. From the Upgrade page, click Update AGM to initiate the software upgrade sequence. AGM will always select and install the latest upgrade software even if there are multiple upgrade versions listed in the Upgrade window.

Note: If required, you can remove an older software upgrade version from AGM. AGM will automatically select the first item in the Updates listing on the left side of the window. Select the version you want to delete and then click **Remove**. You cannot select multiple upgrades for deletion.

The Update confirmation dialog opens.

9. Click Update AGM again to confirm that you want to upgrade the AGM software.
10. The software upgrade process begins and the AGM Upgrade page displays its progress.

Note: If you encounter issues during the upgrade, contact your Support representative for assistance.

11. After the software upgrade is completed, log back into the AGM UI and confirm that the upgrade was successful. Click **Okay** to resume operation of all AGM activities.

Note: If you encounter issues when attempting to log in, contact your Support representative.

