# Table of Contents

## Overview
- Introduction
- Audience

## Deploying Unified Access Gateway with High Availability
- Introduction
- Architecture
- Prerequisites
- Logging In to the vSphere HTML5 Client
- Preparing the INI Files for Deployment
- Deploying the Unified Access Gateway Appliances
- Configuring High Availability
- Testing High Availability

## Summary and Additional Resources
- Conclusion
- Terminology Used in This Tutorial
- Additional Resources
- About the Author
- Feedback
Deploying VMware Unified Access Gateway with High-Availability : VMware Workspace ONE Operational Tutorial

Overview

Introduction
VMware provides this operational tutorial to help you with your VMware Workspace ONE® environment. In this tutorial, you deploy the VMware Unified Access Gateway and configure High Availability on Unified Access Gateway through the administration console.

Audience
This operational tutorial is intended for IT professionals and Workspace ONE administrators of existing production environments. Both current and new administrators can benefit from using this tutorial. Familiarity with networking and storage in a virtual environment is assumed, including Active Directory, identity management, and directory services. Knowledge of additional technologies such as VMware Workspace ONE® Access (formerly VMware Identity Manager) and VMware Workspace ONE® UEM is also helpful.

Deploying Unified Access Gateway with High Availability

Introduction
This tutorial guides you through the deployment of two Unified Access Gateway appliances and the setup of high availability in both. High availability for Unified Access Gateway simplifies your deployment by reducing the need for a third-party load balancer.

To watch a video demonstrating this procedure, click High Availability on VMware Unified Access Gateway, or click the video itself.

Unified Access Gateway high availability supports up to 10,000 concurrent connections in the cluster using a combination of traffic distribution methods:

- **Source IP Affinity** — Maintains the affinity between the client connection and Unified Access Gateway node. All connections with the same source IP address are sent to the same Unified Access Gateway node.
- **Round Robin Mode with High Availability** — Distributes incoming connection requests across the group of Unified Access Gateway nodes sequentially. When the Unified Access Gateway holding the virtual IP address fails, the virtual IP address is reassigned automatically to one of the nodes available in the cluster. The high availability and load distribution occurs among the nodes in the cluster configured with the same Group ID.
- **Least Connection Mode with High Availability** — Sends a new connection request to the Unified Access Gateway node with the fewest number of current connections from the clients.

The following table shows how the session affinity and distribution algorithms differ for each Unified Access Gateway service.

<table>
<thead>
<tr>
<th>Service</th>
<th>Session Affinity</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware Horizon 7</td>
<td>Source IP affinity</td>
<td>Round Robin mode with high availability</td>
</tr>
<tr>
<td>VMware Web Reverse Proxy</td>
<td>Source IP affinity</td>
<td>Round Robin mode with high availability</td>
</tr>
<tr>
<td>VMware Tunnel (Per-App VPN)</td>
<td>None</td>
<td>Least Connection mode with high availability</td>
</tr>
<tr>
<td>VMware Content Gateway</td>
<td>None</td>
<td>Least Connection mode with high availability</td>
</tr>
</tbody>
</table>
Architecture
In this tutorial, you learn how to setup and test High Availability on Unified Access Gateway. Before getting started, review the setup used for this tutorial.

Network Interfaces
The Unified Access Gateway server can be partitioned to receive traffic on a single interface or to route traffic to different interfaces. Although Unified Access Gateway can support up to three NICs, this tutorial implements a two NIC deployment. One NIC faces the internet, and the other one is dedicated to management and backend access.

Architecture Diagram
The following architectural diagram shows the setup of the test environment used for this tutorial. This test environment emulates a typical environment, and includes DMZ and internal networks.

At the top of the diagram is vCenter Networking. In this environment, external requests to the vApp are sent to the vPod Router, which directs those requests to the appropriate resource, based on the incoming port. Ports 4000-6500 are reserved for the environment components so all traffic coming in on these ports is forwarded to the appropriate Edge Service for the Unified Access Gateway server. In addition, ports 443 and 9443 are forwarded to the Unified Access Gateway server over the respective ports.

Note: In this example, the vCenter setup is hosted in a nested template. This is not usually the case when working with users in a live environment.

At the bottom of the diagram is the vApp network required to support the environment. The vApp networks (internal, DMZ, and transit) are created within the vApp. The internal and transit networks are NATed to the SE-UCS-Network for outbound internet connectivity while the DMZ network routes through the vPod Router for inbound and outbound access. Note that the vPodRouter does not have a NIC on the internal network and thus cannot route external traffic to resources on the internal network.

vPod Router | ESXi01 6.5.0 U1 | Control Center | vCenter Server 6.5 U1 hosted on ESXi01
For these exercises, the focus is on the network hosted on the ESXi, and represented by the following three networks:

- **VM Network & Management:** Represents the dedicated network to access the Management Console
- **Internal Network:** Represents the internal network on 172.16.0.x range. The Control Center, ESXi, and vCenter are part of the internal network.
- **DMZ Network:** Represents the DMZ network on 192.168.110.x which is where the Unified Access Gateway appliance is to be deployed. The Unified Access Gateway Internet-facing NIC is associated to this network.

**Note:** Keep in mind that the Unified Access Gateway requires a netmask, default gateway, and subnet to be defined for each network enabled during deployment.

**Prerequisites**

Before you can perform the exercises to deploy Unified Access Gateway using vSphere HTML5 Client, you must satisfy the following requirements:

- VMware vSphere 6.5 U1
- VMware Unified Access Gateway 3.4
- Set up a VMware vSphere ESXi host with a vCenter Server
- Windows 8.1 or Windows Server 2008 R2 or later machine with VMware OVF Tool 4.3 or later installed
- Obtain a Unified Access Gateway virtual appliance image OVA file, such as .euc-access-point-3.4.X.X-XXXXXXXXXXX.ova (see VMware Product Interoperability Matrixes to determine which version to download)
Access Gateway > uagdeploy-VERSION.ZIP.

Logging In to the vSphere HTML5 Client
To perform most of these exercises, you need to log in to the vSphere Web Client.

1. Launch Chrome Browser

Double-click the Chrome browser on the desktop.

2. Authenticate to the vSphere HTML5 Client

1. Launch the Chrome browser from your desktop and enter the following vSphere URL https://vc.corp.local/ui

2. Enter the username: administrator@vsphere.local

3. Enter the password: VMware11!
2. Enter the username, for example, administrator@vsphere.local.
3. Enter the password, for example, VMware1!.
4. Click Login.

After completing the login, you are presented with the vSphere HTML5 Client.

Preparing the INI Files for Deployment

A INI file containing all the configuration settings is required to deploy the Unified Access Gateway appliance using PowerShell deployment.

In this exercise, you configure two INI files; this example uses uag-HA1.ini and uag-HA2.ini.

uag-HA1.ini contains all the settings to deploy an instance named UAG-H1, and uag-HA2.ini will deploy an instance named UAG-H2.

Ensure you are logged in to the machine where you will install Unified Access Gateway. Extract the contents of the Unified Access Gateway ZIP file on this machine. The INI file is located in the Unified Access Gateway installer ZIP package.

1. Edit the INI Files

In this exercise, you use the uag-HA1.ini and uag-HA2.ini files to deploy two Unified Access Gateways, one named UAG-HA1 and the other named UAG-HA2. Each Unified Access Gateway will have two NICs, where NIC one is Internet-facing and NIC two for backend and management.
Navigate to your Unified Access Gateway INI file. In this example, the INI files are located in UAG Resources.

1. Click the File Explorer icon on the task bar.
2. Click Desktop.
3. Click UAG Resources.
4. Select both the uag-HA1.ini and uag-HA2.ini files, then right-click.
5. Click Edit with Notepad++ to open both files.

2. Review the IP address Assigned to Each Appliance
Note that distinct ip0 and ip1 addresses are used in each configuration file. The IP addresses are the only difference between the two appliances, all other values should be identical.

It is important to review and ensure that all the settings are configured identically, including the edge services on all appliances that will be part of the cluster.
Deploying the Unified Access Gateway Appliances

After you have reviewed the INI files for both Unified Access Gateway deployments, run the `uagdeploy.ps1` Powershell script to deploy each appliance.

Because you are deploying two appliances, the script will be executed twice, passing the correspondent INI file for each deployment.

1. Open PowerShell

Click the PowerShell icon located on the Windows task bar.

2. Navigate to the Unified Access Gateway Resources Directory

Navigate to the folder containing your INI file. For example, enter `cd '\Desktop\UAG Resources'` then press Enter.

3. Deploy the UAG-HA1 Appliance
After you run the script, it prompts for input. Enter the information requested, such as in the following example.

1. Enter ".\uagdeploy.ps1 \uag-HA1.ini VMware1! VMware1! false false no
2. The first VMware1! is the root password for the Unified Access Gateway appliance. The second VMware1! is the admin password for the REST API management access. The first false is to NOT skip the validation of signature and certificate. The second false is to NOT skip SSL verification for the vSphere connection. The no is to not join the VMware CEIP program.
3. Enter YOUR CERTIFICATE PASSWORD for the SSLcert and SSLcertAdmin fields when prompted.

To avoid a password request for the certificate, remove the pfxCert values and provide a PEM certificate in the INI file. Set the pemCerts and pemPrivKey for the SSLCert and SSLCertAdmin sections in the INI file.

The deployment starts and you can follow the progress in the same window or on your vSphere Web Client.

4. Confirm that the PowerShell Script Deployment Completes for UAG-HA1

After successfully finalizing the deployment, the script automatically powers on the UAG-HA1 VM.

The Received IP address presented by the script log is a temporary IP. The final IPs for NIC 1 and NIC2 are assigned to the Unified Access Gateway appliance during the first boot. Return to the vSphere Web Client to Validate the Deployment.

5. Deploying UAG-2 Appliance
Now, deploy the second appliance, called UAG-HA2, passing the `uag-HA2.ini` file as parameter.

1. Enter `.\uagdeploy.ps1 \uag-HA2.ini VMware1! VMware1! false false no

   The first `VMware1!` is the root password for the Unified Access Gateway appliance.
   The second `VMware1!` is the admin password for the REST API management access.
   The `false` is to NOT skip the validation of signature and certificate.
   The second `false` is to NOT skip SSL verification for the vSphere connection.
   The `no` is to not join the VMware CEIP program.

2. Enter your CERTIFICATE PASSWORD or the `SSLcert` and `SSLcertAdmin` fields when prompted.

To avoid a password request for the certificate, remove the pfxCert values and provide a PEM certificate in the INI file. Set the `pemCerts` and `pemPrivKey` for the SSLCert and SSLCertAdmin sections in the INI file.

The deployment starts and you can follow the progress in the same window or on your vSphere Web Client.

### 6. Validate the Deployment

1. Click VM and Templates.
2. Click UAG-HA1.
3. Click View all 2 IP addresses. Note the IP Addresses displayed for the VM.

Repeat steps #2 and #3 for UAG-HA2. The IP addresses for this appliance should differ from UAG-HA1.

**Note:** If the Unified Access Gateway appliance does not finalize the configuration during the first startup, you receive an error.
message from vSphere Web Client. If that happens, wait for the appliance to finalize, and refresh the entire Google Chrome browser.

7. Log In to the Unified Access Gateway Administration Console

1. Click the New Tab button to open a new tab.
2. Navigate to the first appliance, for example, https://uagha-1.airwlab.com:9443/admin or click the UAG Internal Admin Console bookmark.
3. Enter the username, for example, admin.
4. Enter the password, for example, **VMware1!** (created for the Admin API in the Deploy OVF Wizard).
5. Click **Login**.
6. Repeat steps 1-5, opening a new tab and log in to the second appliance, for example, using the following URL: https://uagha-2.airwlab.com:9443/admin

8. **Confirm the Unified Access Gateway Administration Console Login to the Internal Network**

A successful login redirects you to the following screen on both appliances, where you can import settings or manually configure the Unified Access Gateway appliance individually.

1. Click **Select** under Configure Manually in the **UAG-HA1** administration console.
2. Select the tab to return to the **UAG-HA2** administration console.
3. Click **Select** under Configure Manually in the **UAG-HA2** administration console.

**Configuring High Availability**

At this point, the Unified Access Gateway has been deployed and you can access the Unified Access Gateway administration console and update the appliance configuration.

In this exercise, you learn how to enable high availability on both deployed appliances, create a cluster, test the high availability component when accessing an internal website through the web reverse proxy edge service, and identify how Unified Access Gateway sets appliances in the cluster as **master** and **backup**.
1. Validate the Reverse Proxy Settings

Validate the web reverse proxy settings to access the intranet on both appliances, using the administration consoles for UAG-HA1 and UAG-HA2 that you previously logged in to.

Remember to perform the following steps on both UAG-HA1 and UAG-HA2, switching between the two browser tabs as needed to validate the settings on each Unified Access Gateway.

Perform the following steps on each appliance using the administration console.

1. Click **SHOW** next to **Edge Service Settings**, after you click **SHOW**, it changes to **HIDE**.
2. Click the **Gear icon** next to **Reverse Proxy Settings**.

1.1. Select the Reverse Proxy Instance Settings

Click the **Gear icon** for the intranet instance.
1.2. Validate Intranet Reverse Proxy Settings

Reverse Proxy Settings

- Enable Reverse Proxy Settings: Yes
- Instance Id: intranet
- Proxy Destination URL: https://intranet.corp.local
- Proxy Destination URL Thumbprints: sha1=1a bd c3 3d be dd 1e 4a 57 ae 54 9b d7 8a 81
- Auth Method: Select
- Health Check URI Path: /
- SAML SP
- External URL
- Proxy Pattern: ([/intranet.*)]
- UnSecure Pattern
- Auth Cookie
- Login Redirect URL
- Proxy Host Pattern: uagvip.airwlab.com
- Trusted Certificates: No trusted certificate is added for this edge service

Perform the following steps on both appliances.

Click the More hyperlink to expand the Settings. Note the Proxy Host Pattern value in this example is set to uagvip.airwlab.com — this address resolves the virtual IP address that is assigned to the master Unified Access Gateway Appliance, which then forwards the requested traffic to the respective appliance.

No changes are required. Click the Cancel button at the bottom after confirming the Proxy Host Pattern on both Unified Access
Gateway appliances.

1.3. Close the Reverse Proxy Settings

Close Reverse Proxy Settings

1.4. Validate Reverse Proxy Configuration

Validate Reverse Proxy Configuration

- Click the arrow down for the Reverse Proxy Settings.
- Click the refresh icon for the Edge Service Settings.
- Confirm the intranet proxy status is GREEN.

The reverse proxy settings for the intranet website, must be GREEN, which confirms that the appliance can communicate with the intranet website, otherwise it shows RED.

Note: It can take a few minutes for the intranet proxy to show as GREEN. If you do not see it, click the refresh icon in Step #2 until you see the status change to either GREEN or RED.

2. Configure High Availability on UAG-HA1
In the administration console, the High Availability Settings is currently **Not Configured** on UAG-HA1 appliance at this point.

Click the **High Availability Gear** icon to configure.

**2.1. Add Virtual IP Address and Group ID**
1. Enter a Virtual IP Address, for example, 192.168.110.50.
2. Enter the Group ID, for example, 50.
3. Click Save.

In this configuration, all the incoming traffic on 192.168.110.50 will be balanced by the cluster of Unified Access Gateway appliances on Group ID 50.

2.2. Monitor High Availability State

As you save the configuration, Unified Access Gateway broadcasts a signal on the VIP subnet looking for other appliances on the same Group ID. During that time, the High Availability state shows as Processing.
In the case where no other appliances are found, UAG-HA1 becomes the *master* and the High Availability state on the administration console switches to *Master* as shown in the screenshot.

**Note:** You may need to refresh the Unified Access Gateway administrator console after a few minutes to see the *Processing* status update to *Master*.

### 3. Configure High Availability on UAG-HA2

Now repeat the same steps to configure the High Availability settings on UAG-HA2.

From your Chrome Browser, return to the tab where you logged into the the administration console for UAG-HA2. The URL is [https://uagha-2.airwlab.com:9443/admin](https://uagha-2.airwlab.com:9443/admin).

The same Virtual IP Address (192.168.110.50) and Group ID (50) must be used on UAG-HA2 to make this appliance part of the same cluster where UAG-HA1 resides.

#### 3.1. Monitoring High Availability on UAG-HA2
After you complete the High Availability configuration on UAG-HA2, the high availability status changes to Backup.

Note: You may need to refresh the Unified Access Gateway administrator console after a few minutes to see the Processing status update to Backup.

4. Validate Virtual IP Address on the UAG-HA1 Virtual Machine

Return to the vSphere Web Client to validate the assignment of the additional virtual IP address to the master appliance.

1. Click VM and Templates.
2. Select the UAG-HA1 VM.
3. Click View all 3 IP addresses.
4. The virtual IP address 192.168.110.50 was assigned to the UAG-HA1 VM, the master appliance.
Note: You may need to refresh the page to see the IP addresses update properly.

Perform the same steps to view the IP addresses of the UAG-HA2 VM. Notice that it still has two IP addresses, as this appliance is set as the backup appliance on the high availability stack.

Testing High Availability
After you have completed the Unified Access Gateway High Availability component configuration, you can now test this feature.

In this exercise, you access the intranet website through Unified Access Gateway first, shut down the master appliance and test the access to the intranet website again, which should go through the backup appliance in the cluster.

1. Access the Intranet Website

1. In Google Chrome, click the New Tab button to open a new tab.
2. Enter the floating virtual IP address (VIP) that you configured on the master Unified Access Gateway when setting up high availability, for example, https://uagvip.airlab.com/intranet in the address bar and press Enter.
The result is a sample intranet page hosted on an internal IIS server.

2. Power Off UAG-HA1 Appliance

Return to the vSphere Web Client and Power Off the UAG-HA1 VM.

1. Click VM and Templates.
2. Click UAG-HA1 VM.
3. Click ACTIONS.
4. Hover over the Power option.
5. Click Power Off.
6. Click Yes to confirm Power Off action for UAG-HA1.

Wait for the UAG-HA1 complete shutdown. This triggers the backup Unified Access Gateway appliance in the cluster to become the master appliance.

3. Access the Intranet Website after UAG-HA1 Power Off
1. Click on the **New Tab button** to open a new tab.

2. Navigate to your intranet address, for example, [https://uagvip.airwlab.com/intranet/](https://uagvip.airwlab.com/intranet/).

The same intranet webpage should show up, without any disruption for the user, however the traffic now is going through the UAG-HA2.

**4. Validate UAG-HA2 High Availability Status**
Return to the UAG-HA2 console administration tab (for example, https://uagha-2.airwlab.com:9443/admin), in Google Chrome.

UAG-HA2 is now set as the master appliance and the virtual IP address is assigned to it.

**Note**: If the **High Availability Settings** do not show UAG-HA2 as the **Master** appliance, refresh the page.

### 5. Validate Virtual IP Address on the UAG-HA2 Virtual Machine
Return to the vSphere Web Client to validate the assignment of the additional virtual IP address to the master appliance.

1. Click VM and Templates.
2. Select UAG-HA2 VM.
3. Click View all 3 IP addresses.
4. The Virtual IP address 192.168.110.50 is now assigned to the UAG-HA2, the Master appliance.

**Note:** You may need to refresh the page to see the IP addresses update properly.

This confirms that when the master Unified Access Gateway appliance was taken offline, the backup Unified Access Gateway appliance was promoted to master and assigned the 192.168.110.50 virtual IP (uagvip.airwlab.com), and access to the intranet resource was uninterrupted.

### Summary and Additional Resources

**Conclusion**

In these exercises, you have learned how to:

- Deploy the VMware Unified Access Gateway on a two NIC configuration using PowerShell script for a high availability scenario
- Configure High Availability on Unified Access Gateway through the administration console
- Validate the web reverse proxy instance configuration to work in a high availability scenario
- Perform tests on a cluster of Unified Access Gateway appliances and confirm their high availability status

For additional documentation, be sure to check:

- VMware Unified Access Gateway on TechZone
- VMware Workspace ONE on TechZone
- VMware Unified Access Gateway documentation
- High Availability on VMware Unified Access Gateway feature walk-through video.

### Terminology Used in This Tutorial

The following terms are used in this tutorial:
application store
A user interface (UI) framework that provides access to a self-service catalog, public examples of which include the Apple App Store, the Google Play Store, and the Microsoft Store.

auto-enrollment
Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience.

catalog
A user interface (UI) that displays a personalized set of virtual desktops and applications to users and administrators. These resources are available to be launched upon selection.

cloud
Asset of securely accessed, network-based services and applications. A cloud can also host data storage. Clouds can be private or public, as well as hybrid, which is both private and public.

device enrollment
The process of installing the mobile device management agent on an authorized device. This allows access to VMware products with application stores, such as Workspace ONE Access (formerly VMware Identity Manager).

identity provider (IdP)
A mechanism used in a single-sign-on (SSO) framework to automatically give a user access to a resource based on their authentication to a different resource.

mobile device management (MDM) agent
Software installed on an authorized device to monitor, manage, and secure end-user access to enterprise resources.

one-touch login
A mechanism that provides single sign-on (SSO) from an authorized device to enterprise resources.

service provider (SP)
A host that offers resources, tools, and applications to users and devices.

virtual desktop
The user interface of a virtual machine that is made available to an end user.

virtual machine
A software-based computer, running an operating system or application environment, that is located in the data center and backed by the resources of a physical computer.

For more information, see the VMware Glossary.

Additional Resources
For more information about Workspace ONE, explore the VMware Workspace ONE Activity Path. The activity path provides step-by-step guidance to help you level-up in your Workspace ONE knowledge. You will find everything from beginner to advanced curated assets in the form of articles, videos, and labs.

Additionally, you can check out the VMware Workspace ONE and VMware Horizon Reference Architecture which provides a framework and guidance for architecting an integrated digital workspace using VMware Workspace ONE and VMware Horizon.

About the Author
This tutorial was written by:


Feedback
The purpose of this tutorial is to assist you. Your feedback is valuable. To comment on this tutorial, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.