

**PROVIDING SECURE ACCESS
TO VMWARE HORIZON 7 AND
VMWARE IDENTITY
MANAGER WITH THE
VMWARE UNIFIED ACCESS
GATEWAY**

Table of Contents

[Introduction](#)

[Deployment Options](#)

[Preparation](#)

[Configuration](#)

[Deployment](#)

[Horizon HTML Access](#)

[Summary](#)

[About the Author](#)

Providing Secure Access to VMware Horizon 7 and VMware Identity Manager with the VMware Unified Access Gateway

Introduction

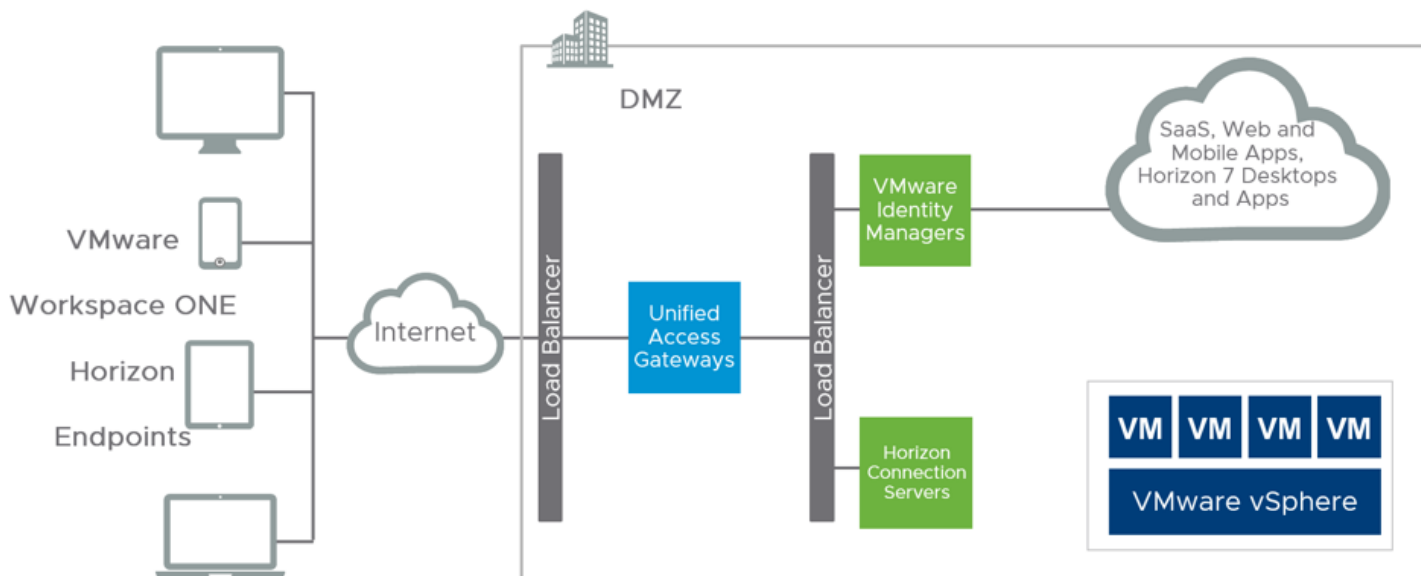
The [VMware Unified Access Gateway](#) is a platform that provides secure edge services and access to defined resources that reside in the internal network. This allows authorized, external users to access internally located resources in a secure manner.

The VMware Unified Access Gateway can be used for multiple use cases including

- Remote access to [VMware Horizon 7](#) desktops and applications
- Reverse proxying of web servers such as [VMware Identity Manager](#)
- Access to on-premises legacy applications that use Kerberos or header-based authentication with identity bridging from SAML or certificates
- Provision of [VMware AirWatch](#) or [VMware Workspace ONE](#) Per-App Tunnels and Tunnel Proxy to allow mobile applications secure access to internal services
- Allowing [VMware Content Locker](#) access to internal files shares or SharePoint repositories by running the [VMware Content Gateway service](#)

A Unified Access Gateway appliance typically resides within a network demilitarized zone (DMZ) and acts as a proxy host for connections inside your organization's trusted network. This design provides an additional layer of security by shielding the internal resources such as VMware Identity Manager, virtual desktops, application hosts, and servers from the public-facing Internet.

This article describes how to deploy a single Unified Access Gateway to proxy VMware Horizon 7 traffic *and* to also reverse-proxy VMware Identity Manager web traffic.



For Horizon 7, Unified Access Gateway provides very similar functionality to the [View security server](#) but does not need one-to-one pairing with a View Connection Server. Unified Access Gateway is also capable of proxying sessions to other VMware products and providing more advanced security options, including authentication in DMZ. If you are running View security servers, take the time to look at replacing them with Unified Access Gateway appliances.

In larger-scale environments, you may still want to have separate Unified Access Gateway appliances for certain edge use cases, to provide scale and operational separation. But in mid-sized to smaller environments, where the load on Unified Access Gateway is not

substantial, combining workloads on one set of Unified Access Gateway appliances is convenient.

Deployment Options

Following are two ways to deploy and configure a Unified Access Gateway:

<div style="background-color: #76b82a; color: white; padding: 5px; text-align: center; font-weight: bold;">vSphere OVF and Admin UI</div> <p>GUI driven.</p> <p>Separates Install & Configuration steps.</p> <ul style="list-style-type: none"> • Deploy of OVF template in vSphere • Log in to Admin UI to configure Edge Services <p>Admin UI provides management & monitoring tools</p> <p>Export Settings in JSON & INI formats to save config for rollback or leverage in additional installations</p>	<div style="background-color: #0070c0; color: white; padding: 5px; text-align: center; font-weight: bold;">PowerShell</div> <p>Simple to use PowerShell script.</p> <p>All settings configured in a single INI file provided</p> <p>Ready on first boot.</p> <ul style="list-style-type: none"> • Deploys appliance and configures services. <p>Repeatable installation / upgrade / configuration changes.</p> <p>Expedites large deployments</p>
---	--

This section walks through using the PowerShell method with the script and the sample INI settings files provided in [Using PowerShell to Deploy VMware Unified Access Gateway](#). Do not be put off by the fact that this method uses PowerShell. You will be running a single command that calls an INI file that contains all of your settings. You do not need to know PowerShell.

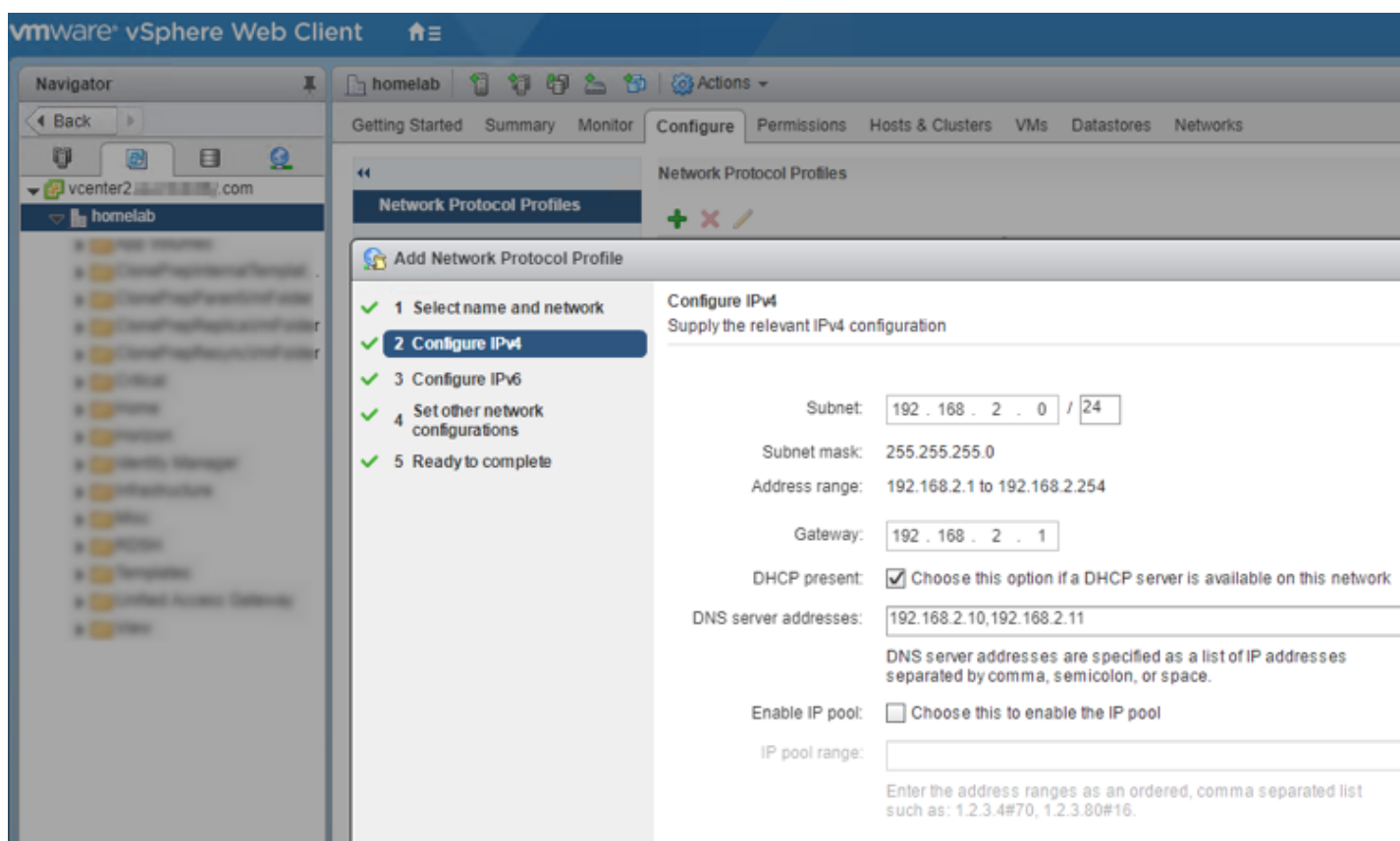
Preparation

First, download the latest version of the PowerShell script and the sample INI settings files.

1. Visit the community page [Using PowerShell to Deploy VMware Unified Access Gateway](#).
2. Download the latest version of the ZIP file and extract the contents. (At time of writing, this is `uagdeploy-320-v5.zip`).

Before you can deploy a Unified Access Gateway appliance to VMware vSphere, you must define vSphere Network Protocol Profiles for any network that you intend to connect an appliance to. This prerequisite will be removed in a future release of Unified Access Gateway.

See *Configuring Protocol Profiles for Virtual Machine Networking* in the [vSphere Networking documentation](#) for more details on how to do this.



Configuration

From the downloaded ZIP file, use the sample INI settings files to create your own settings file.

1. Make a copy of the `uag10-vidm.ini` file and edit it.
2. As with any deployment, go through and enter your information as required for the `General` and `SSLCert` sections.

Leave all other lines as they are. In the following example, spaces and comment lines have been removed to conserve space.

```
[General]
```

```
name=uag1
```

```
source=S:\euc-unified-access-gateway-3.2.0.0-7395815_OVF10.ova
```

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.3.12/Datacenter/host/Cluster/
```

```
ds=vsanDatastore

netInternet=DMZ

netManagementNetwork=DMZ

netBackendNetwork=DMZ

deploymentOption=onenic

ip0=192.168.2.36

dns=192.168.3.10
```

```
[SSLCert]
```

```
pfxCerts=sslcertificate.pfx
```

Depending on your network topology, you may need to use a `twonic` or `threenic` deployment. Uncomment the lines for your choice and add the required networking information as necessary.

SSL Certificates can also be provided in PEM format. Comment out the `pfxcerts` line and uncomment the following two `pemCerts` lines and complete if using PEM format.

```
pemCerts=sslcertificate.pem
```

```
pemPrivKey=private.key
```

3. Complete the `WebReverseProxy` section to configure access to VMware Identity Manager.

The only line you need to change here is the `proxyDestinationURL` line. Do not change the `proxyPattern` lines.

```
[WebReverseProxy]
```

```
proxyDestinationURL= https://workspace.domain.com
```

In the example above, `workspace.domain.com` is the internal address of the VMware Identity Manager appliance (or the internal load balancer address if you have more than one VMware Identity Manager appliance).

4. Next, add in a `Horizon` section by copying that section from the `uag2-advanced.ini` file and paste it into your first file (your copy of `uag10-vidm.ini`) at the end, on a new line after the `authCookie` line.
5. Complete the `Horizon` section and enter the following relevant values for your environment.

```
[Horizon]
```

```
proxyDestinationUrl=https://view.domain.com
```

```
tunnelExternalUrl=https://horizon.domain.com:443
```

```
blastExternalUrl=https://horizon.domain.com:443
```

```
pcoipExternalUrl=88.100.100.100:4172
```

In the example above:

- `view.domain.com` is the internal address of the Connection Server (or the internal load balancer address if you have more than one Connection Server).
- `horizon.domain.com` is the external address used for Horizon 7 connections.
- `88.100.100.100` is the external IP address for `horizon.domain.com`.

Deployment

Now you are ready to deploy the Unified Access Gateway appliance.

1. Open a PowerShell prompt and change to the directory where the scripts are located.
2. Run `./uagdeploy.ps1 ./<filename>.ini`, follow the prompts, and enter the passwords.
3. After the process is complete, wait a few minutes for the Unified Access Gateway appliance to boot completely.

You can monitor this process in VMware vCenter Server to see when the assigned IP address is reported on the Summary page for the VM.

If you have all the settings in the `INI` file completed correctly, and your certificates are in order, you will have a fully operational Unified Access Gateway that will proxy connections to both your Horizon Connection Server and the VMware Identity Manager appliance.

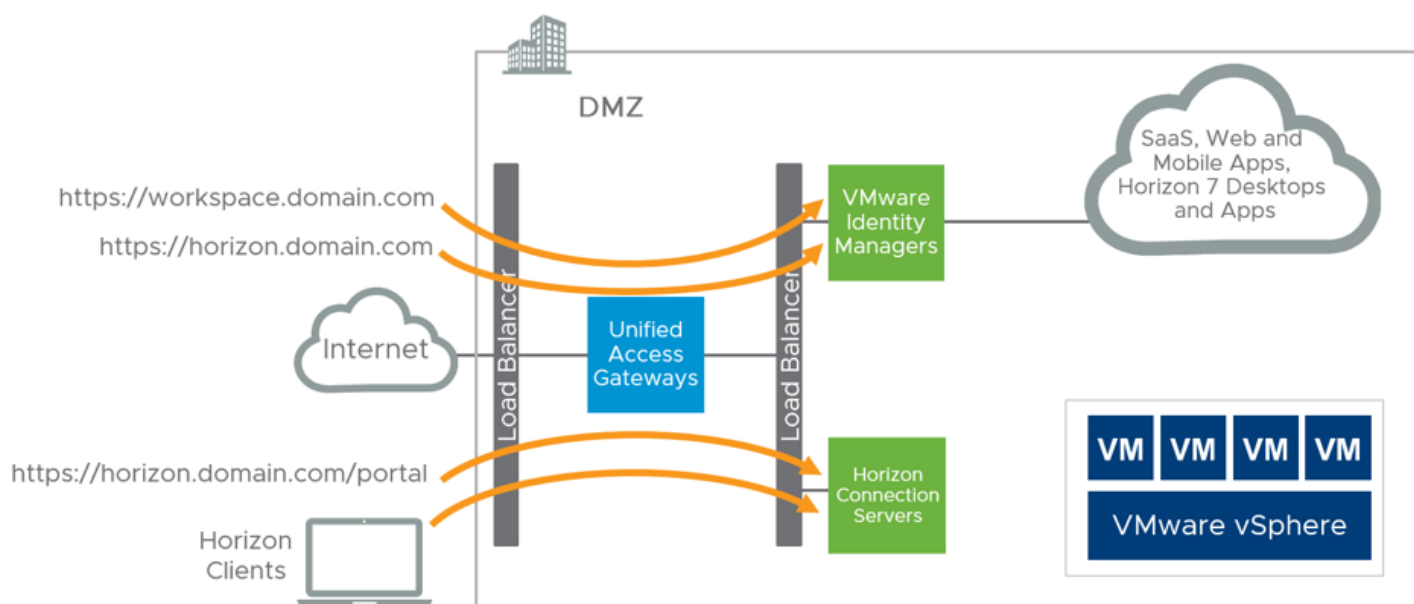
Horizon HTML Access

One slight nuance of this combined deployment model is where a Unified Access Gateway appliance is used for both VMware Identity Manager and Horizon 7. Direct, *external Web* access to the Horizon 7 HTML login page is not possible using the root URL.

In this example, you have two FQDNs:

- `horizon.domain.com` for your Connection Servers
- `workspace.domain.com` for your VMware Identity Manager appliances

If the user enters either `https://horizon.domain.com` or `https://workspace.domain.com`, the user always gets directed to the VMware Identity Manager login page.



This should not be a concern, as you want your primary *external Web* entry point for users to be through VMware Identity Manager. From there, a user can always connect to a Horizon 7 desktop or application using HTML Access or the Horizon Client. Users can also access the Horizon 7 HTML login page by appending `/portal` to the URL, for example:

`https://horizon.domain.com/portal`

External access using the Horizon Client is unaffected by this behavior and routes as normal to the Connection Server and the Horizon Agent in the virtual desktop or published application.

Summary

Of course, this configuration of Unified Access Gateway works with multiple components (Unified Access Gateway appliances, Connection Servers, VMware Identity Manager appliances) and load balancers. To understand how to deploy multiple components with load balancers, see the [Horizon 7 Enterprise Edition Reference Architecture](#).

You can create PowerShell scripts that quickly deploy the appliance and provide secure edge services to multiple use cases, including Horizon Connection Server, VMware Identity Manager, VMware AirWatch components such as the Content Gateway, and VMware Tunnel, and to provide identity bridging. Try the deployment instructions in this article and use this as an opportunity to make the move to Unified Access Gateway. You can also mix and match the deployment approaches and use the administrative UI on a running Unified Gateway appliance to modify or add new edge services.

Learn more about deploying Unified Access Gateway in the blog post [VMware Unified Access Gateway Technical Deep Dive](#) and the accompanying videos that cover overview, use cases, deployment requirements, deployment options, deploying with vSphere OVF and administrative console, deploying with PowerShell, scaling, upgrades, authentication, and troubleshooting.

About the Author

This article was written by Graeme Gordon, Senior Staff End-User-Computing Architect, EUC Technical Marketing, VMware.



vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.