# Table of Contents

Lab Overview - HOL-1957-08-UEM - Workspace ONE UEM - Unified Access Gateway ............ 3  
Lab Guidance .................................................................................................................. 4  

Module 1 - Unified Access Gateway Deployment with vSphere ..................................... 9  
Introduction ................................................................................................................... 10  
Logging In to the vSphere Web Client ........................................................................... 11  
Deploying Unified Access Gateway with vSphere ......................................................... 13  
Updating network settings ......................................................................................... 38  
Remove Virtual Machines ....................................................................................... 46  
Conclusion ............................................................................................................... 49  

Module 2 - Unified Access Gateway Deployment with PowerShell .......................... 50  
Introduction ............................................................................................................... 51  
Logging In to the vSphere Web Client ....................................................................... 52  
Power ON Virtual Machines .................................................................................... 54  
Starting Windows PowerShell .................................................................................... 56  
Preparing the INI File for Deployment ................................................................. 57  
Deploying Unified Access Gateway Appliance ......................................................... 61  
Configuring Web Reverse Proxy ............................................................................. 66  
Power OFF and Remove Virtual Machines .............................................................. 72  
Conclusion ............................................................................................................. 75  

Module 3 - Web Reverse Proxy secure access to Internal Websites ....................... 76  
Introduction ............................................................................................................... 77  
Logging In to the vSphere Web Client ....................................................................... 78  
Power ON Virtual Machines .................................................................................... 80  
Deploying Unified Access Gateway Appliance ......................................................... 82  
Configuring Web Reverse Proxy to access non-SSL website (HTTP/Port 80) ........ 87  
Configuring Web Reverse Proxy to access SSL website (HTTPS/Port 443) .......... 92  
Add Certificate Authentication to the Intranet website ......................................... 97  
Power OFF Virtual Machines ............................................................................... 118  
Conclusion ............................................................................................................. 122  

Module 4 - Identity Bridging and Single Sign-On access to Legacy Web Applications ... 123  
Introduction ............................................................................................................... 124  
Kerberos Delegation Overview ............................................................................... 126  
Logging In to the vSphere Web Client ....................................................................... 128  
Power ON Virtual Machines .................................................................................... 130  
Deploying Unified Access Gateway Appliance ......................................................... 132  
Configuring Kerberos Authentication on IIS Website ........................................... 135  
Configuring Kerberos Delegation ......................................................................... 151  
Log In to the Unified Access Gateway Admin Console ........................................... 166  
Confirm the itbudget Reverse Proxy Settings were Configured ............................... 168  
Configuring Identity Bridging on Unified Access Gateway .................................... 169  
Configure a Web App in VMware Identity Manager ............................................. 183  
Testing Web Application and SSO through Identity Bridging .................................... 191
Conclusion
Lab Overview - HOL-1957-08-UEM - Workspace ONE UEM - Unified Access Gateway
Lab Guidance

Note: It may take more than 90 minutes to complete this lab. You should expect to only finish 2-3 of the modules during your time. The modules are independent of each other so you can start at the beginning of any module and proceed from there. You can use the Table of Contents to access any module of your choosing.

The Table of Contents can be accessed in the upper right-hand corner of the Lab Manual.

The Unified Access Gateway can empower your digital workforce by allowing authorized users and devices to securely access internal resources from anywhere. Learn how to deploy the Unified Access Gateway and understand best practices and deployment configurations for enterprise-level security. Explore how the Unified Access Gateway can also provide secure access to internal web applications through certificate authentication and Identity Bridging configurations to cover a variety of use cases.

Lab Module List:

• **Module 1 - Unified Access Gateway Deployment with vSphere** (30 minutes) (Beginner) Learn how to deploy Unified Access Gateway using vSphere Web Client and the different aspects of network and certificate configuration when deployment the Unified Access Gateway.

• **Module 2 - Unified Access Gateway Deployment with PowerShell** (30 minutes) (Intermediate) Install and configure the Unified Access Gateway using PowerShell. Explore additional deployment and management use cases for recommended security design strategies.

• **Module 3 - Web Reverse Proxy secure access to Internal Websites** (60 minutes) (Intermediate) The Unified Access Gateway is the Security Gateway for Workspace ONE that provide secure access to internal resources for external users. Learn how to configure Web Reverse Proxy using Device Certificate for authentication to legacy Web applications to restrict access to specific devices.

• **Module 4 - Identity Bridging and Single Sign-On access to Legacy Web Applications** (60 Minutes) (Intermediate) Learn how to setup Identity Bridging to provide Single Sign On to legacy Web Applications using Kerberos Constrained Delegation (KCD), allowing VMware Identity Manager to act as identity provider integrated with Unified Access Gateway to handle user authentication by acting as a service provider by converting the incoming SAML assertion to Kerberos.

Lab Captains:

• Roger Deane, Sr. Manager, Technical Marketing, USA
• Andreano Lanusse, EUC Staff Architect, USA
• Chris Halstead, EUC Staff Architect, USA
• Justin Sheets, Sr. Technical Marketing Architect, USA
This lab manual can be downloaded from the Hands-on Labs Document site found here:

http://docs.hol.vmware.com

This lab may be available in other languages. To set your language preference and have a localized manual deployed with your lab, you may utilize this document to help guide you through the process:


**Location of the Main Console**

1. The area in the RED box contains the Main Console. The Lab Manual is on the tab to the Right of the Main Console.
2. A particular lab may have additional consoles found on separate tabs in the upper left. You will be directed to open another specific console if needed.
3. Your lab starts with 90 minutes on the timer. The lab can not be saved. All your work must be done during the lab session. But you can click the **EXTEND** to increase your time. If you are at a VMware event, you can extend your lab time twice, for up to 30 minutes. Each click gives you an additional 15 minutes. Outside of VMware events, you can extend your lab time up to 9 hours and 30 minutes. Each click gives you an additional hour.
Alternate Methods of Keyboard Data Entry

During this module, you will input text into the Main Console. Besides directly typing it in, there are two very helpful methods of entering data which make it easier to enter complex data.

Click and Drag Lab Manual Content Into Console Active Window

You can also click and drag text and Command Line Interface (CLI) commands directly from the Lab Manual into the active window in the Main Console.

Accessing the Online International Keyboard

You can also use the Online International Keyboard found in the Main Console.

1. Click on the Keyboard Icon found on the Windows Quick Launch Task Bar.

Click once in active console window

In this example, you will use the Online Keyboard to enter the "@" sign used in email addresses. The "@" sign is Shift-2 on US keyboard layouts.

1. Click once in the active console window.
2. Click on the Shift key.
Click on the @ key

1. Click on the "@ key".

Notice the @ sign entered in the active console window.

**Activation Prompt or Watermark**

When you first start your lab, you may notice a watermark on the desktop indicating that Windows is not activated.

One of the major benefits of virtualization is that virtual machines can be moved and run on any platform. The Hands-on Labs utilizes this benefit and we are able to run the labs out of multiple datacenters. However, these datacenters may not have identical processors, which triggers a Microsoft activation check through the Internet.

Rest assured, VMware and the Hands-on Labs are in full compliance with Microsoft licensing requirements. The lab that you are using is a self-contained pod and does not have full access to the Internet, which is required for Windows to verify the activation. Without full access to the Internet, this automated process fails and you see this watermark.

This cosmetic issue has no effect on your lab.
Look at the lower right portion of the screen

Please check to see that your lab is finished all the startup routines and is ready for you to start. If you see anything other than "Ready", please wait a few minutes. If after 5 minutes you lab has not changed to "Ready", please ask for assistance.
Module 1 - Unified Access Gateway Deployment with vSphere
Introduction

This module will guide you through the GUI based deployment and configuration of the Unified Access Gateway OVF in the vSphere Web Client.

The manual provides steps for deploying one Unified Access Gateway Appliance in vSphere using ONE NIC deployment, make use of Administration Console to configure certificate and change network settings.

This manual covers Unified Access Gateway 3.3 deployment in vSphere 6.5 U1.

Prerequisites

All of the following pre-requisites are already installed for this Module, the following information is just for your reference.

To deploy Unified Access Gateway using vSphere Web Client, you must use specific versions of VMware products.

- vSphere ESXi host and vCenter Appliance.
- Download a version of Unified Access Gateway virtual appliance image from VMWare. This is an OVA file e.g., .euc-unified-access-gateway-3.X.X.X-XXXXXXXXXXXXXX.ova. Refer to VMware Product Interoperability Matrices to determine the version to download.
- You must select the vSphere data store and the network to use.

Starting with version 3.3, you can deploy Unified Access Gateway without specifying the netmask and default gateway settings in Network Protocol Profiles(NPP). You can specify this networking information directly during deployment of your Unified Access Gateway appliance.
Logging In to the vSphere Web Client

To perform most of this exercise, you need to log in to the vSphere Web Client.

Launch Chrome Browser

Double-click the Chrome Browser on the lab Desktop
Authenticate to the vSphere Web Client

1. Click the **New Tab** button.
2. Click the **vSphere Web Client** bookmark. The URL for this bookmark is https://vcsa-01a.corp.local/vsphere-client/?csp.
3. Enable the **Use Windows session authentication** option.
4. Click **Login**.

After completing the Login, you will be presented with the vSphere Web Client.

**NOTE:** You can also login without using Windows session authentication by using **CORP\Administrator** for the username and **VMware1!** for the password.
Deploying Unified Access Gateway with vSphere

In this section, you explore the vSphere Admin UI and learn how to deploy an OVF Template by configuring the necessary fields for the Unified Access Gateway. You deploy the Unified Access Gateway in a one-NIC configuration, meaning that the Internet-facing, internal-facing, and management networks all reside on a single NIC.

Deploying the OVF Template

1. Click the **VMs and Templates** tab.
2. Right-click the Region named **RegionA01**.
3. Click **Deploy OVF Template**.

1. **VMs and Templates** tab
2. **RegionA01**
3. **Deploy OVF Template**
Uploading OVF Template

1. Select **Local File**.
2. Click **Browse**.
Select the OVF File

1. Click **Documents**.
2. Click **HOL**.
3. Click **Unified Access Gateway**.
4. Select the **euc-unified-access-gateway-3.3.0.0-#####.ova** file.
5. Click **Open**.
Continue after OVF File Selected

Click Next.
Select Name and Location

1. Enter **UAG-1NIC** for the Name.
2. Select **RegionA01**.
3. Click **Next**
1. Select **RegionA01-COMP01**.
2. Click **Next**.
Review the details here, these items will be updated as you complete the OVF Template wizard.

Click **Next**
1. Select **Single NIC**.
2. Click **Next**.

Note: The Dropdown menu provides a short description of each configuration and sizing of the UAG VM. In this module, the **Single NIC** configuration means all traffic to the UAG will be received on the same interface regardless of the source and the Admin UI will run on the same NIC over port 9443.

Selecting **Two NICs** will direct traffic from external networks to the public interface and traffic from within the network to an internal interface. The Admin UI will run on the same internal interface.

Selecting **Three NICs** will direct traffic from external networks to the public interface and traffic from within the network to an internal interface. In this configuration, the Admin UI will run on a separate, dedicated Network Interface. When selecting multiple NICs, you must then configure the corresponding network values for each NIC in the Setup Networks and Customize Template sections later in the wizard.
Customers who require multiple NICs typically follow this same protocol for other web application servers within their organization. For more information on deploying the UAG with multiple NICs, please see the UAG Guide located [here](#).

**Select Storage**

1. Select **Thin provision** for the virtual disk format.
2. Select the **RegionA01-ISCSI01-COMP01** datastore.
3. Select **Next**.
Select Networks

1. Select the **VM-DMZ-RegionA01-vDS-COMP** destination network for ManagementNetwork source.
2. Select the **VM-DMZ-RegionA01-vDS-COMP** destination network for BackendNetwork source.
3. Select the **VM-DMZ-RegionA01-vDS-COMP** destination network for Internet source.
4. Click **Next**

**NOTE:** We already selected a Single NIC configuration, meaning the Internet, Management and Backend traffic all goes through a Single NIC, however this step of the wizard asks for three destination networks which can lead to some confusion when you are configuring the UAG for the first time. Since this is a single NIC deployment, you just need to select the same Network for all the Source Networks.
Configure CIEP Settings

1. Uncheck the **Join CEIP** option.
2. Click the **Networking Properties** dropdown to expand these options.
3. Scroll down.
Configure Networking Settings

1. Enter **192.168.110.10** for the DNS server addresses.
2. Enter **STATICV4** for the IPMode for NIC 1.
3. Enter **192.168.110.1** for the IPv4 Default Gateway.
4. Enter **192.168.110.150** for the NIC 1 (eth0) IPv4 Address.
5. Scroll down to configure additional settings.
Configure Additional Networking Settings

1. Enter **255.255.255.0** for the **NIC1 (eth0) IPv4 netmask**.
2. Enter **UAG-1NIC** for the **Unified Gateway Appliance Name**.
3. Click the **Password Options** dropdown to expand these settings.
4. Scroll down to find the Password Options section.
Configure Password Settings

1. Enter **VMware1!** for the admin user, which enabled REST API access.
2. Reenter **VMware1!** to confirm the password.
3. Enter **VMware1!** for the root user password of the Unified Access Gateway Virtual Machine.
4. Reenter **VMware1!** to confirm the password.
5. Click **Next**.
Ready to Complete

Review all the settings entered in the Network Mapping and Properties to ensure there are no errors.

Click **Finish**
Accessing the Task Console

You can follow the status of the OVF deployment through the Task Console.

1. Click the **Home icon**
2. Click **Tasks**

Monitoring OVF Import and Deployment

1. Wait until the **Deploy OVF package** and **Deploy OVF Template** tasks

   *NOTE - Due to Hands on Labs limitations, this installation will run for several minutes before completing. Please allow the tasks to complete before continuing.*
2. Click **Back** once the tasks have completed.

### Handling a Failed OVF Deploy (IF NEEDED)

If your Import OVF package task fails with the error "Failed to deploy OVF package" on the Tasks Console, you should restart the deployment by returning to step **Deploying the OVF Template**.

### Power on UAG Appliance

1. Expand **RegionA01-COMP01**
2. Select the **UAG-1NIC** virtual machine.
3. Click the **Summary** tab.
4. Click the **Power On** icon. Wait for the virtual machine to power on.

   **NOTE:** If the **Power On** icon is not clickable, you may need to refresh the page first!
5. Click the **Refresh** icon to check the status of the virtual machine. The IP Addresses field will populate once it is powered on.
6. The screen will appear as the blue login page as soon the initialization completes.
7. The IP address **192.168.110.150** will be assigned to this virtual machine.

**NOTE - Do NOT continue to the next step until the VM receives the associated IP address! This may take 1-2 minutes.**
Navigate to the UAG Admin UI Login

NOTE: The page may say it is unavailable when you try attempting to connecting. This is because the Unified Access Gateway appliance service is still starting up and may take a minute or two before it is available.

1. Click the New Tab button.
2. Enter \texttt{https://uag.corp.local:9443/admin} for the URL and press \texttt{ENTER}.
3. Click the Advanced link.

\textbf{NOTE:} The page may say it is unavailable when you try attempting to connecting. This is because the Unified Access Gateway appliance service is still starting up and may take a minute or two before it is available.
4. Accept the security exception and click the **Proceed to uag.corp.local (unsafe)** link.

**NOTE:** The connection is not private because no SSL Certificate has been supplied for our Unified Access Gateway. We will access the Admin Console to supply a SSL certificate now. Other Hands on Labs Modules will cover how to deploy Unified Access Gateway with a SSL Certificate in order to skip this step.

**Login to the UAG Admin UI**

1. Enter **admin** for the username.
2. Enter **VMware1!** the password created for the Admin API in the Deploy OVF Wizard.
3. Click **Login**.
**UAG Import and Configuration Settings**

Unified Access Gateway Appliance v3.3

**Import Settings**
Jumpstart your Gateway configuration by importing your settings (JSON)

**Configure Manually**
Configure settings manually

A successful login will redirect you to the following screen, where you can import settings or manually configure the UAG appliance.

Click **Select** for Configure Manually.
Configuring TLS/SSL Certificates for Unified Access Gateway Appliances

Click the Gear icon for TLS Server Certificate Settings under Advanced Settings.


TLS/SSL server certificates are signed by a Certificate Authority (CA). A CA is a trusted entity that guarantees the identity of the certificate and its creator. When a certificate is signed by a trusted CA, users no longer receive messages asking them to verify the certificate, and thin client devices can connect without requiring additional configuration. A default TLS/SSL server certificate is generated when you deploy a Unified Access Gateway appliance.

Up to this point the UAG Appliance is using the default certificate, which is not signed by a trusted CA.
Configuring Type of Certificate

1. Enable the **Admin Interface** option.
2. Enable the **Internet Interface** option.
3. Select **PFX** for the Certificate Type.
4. Click the **Select** link to upload a PFX.
Select PFX Certificate

1. Click **Documents**.
2. Click **HOL**.
3. Click **Unified Access Gateway**.
4. Click **wildcard_corp_local.pfx**.
5. Click **Open**.
Enter Certificate Password and Save

1. Enter VMware1! for the certificate password.
2. Click Save

UAG Certificate Changed

You will receive a message stating that the Internet facing interface certificate was changed. You will need to reload the Admin UI to see the changes you have made.

1. Click the Close button on the UAG Admin UI browser tab.
2. Click the New Tab button.
Validating Certificate installation

Enter [https://uag.corp.local:9443/admin](https://uag.corp.local:9443/admin) for the URL and press **ENTER** to return to the Unified Access Gateway Admin Console.

You should no longer see a certificate error on the Browser navigation bar, confirming that the certificate upload was successful.
Updating network settings

You can now log in to the Unified Access Gateway administration console and update the network settings so that the Unified Access Gateway is deployed on a different IP than originally.

Log In to the Unified Access Gateway Administration Console

Log in to the Unified Access Gateway administration console (such as https://uag.airwlab.com:9443/admin).

1. Enter admin for the username.
2. Enter VMware1! for the password.
3. Click Login.
Select Configure Manually

**Import Settings**

Jumpstart your Gateway configuration by importing your settings (JSON)

- [Select]

**Configure Manually**

Configure settings manually

- [Select]

Under Configure Manually, click **Select**.
Access Network Settings

Under Advanced Settings, click the gear icon for **Network Settings**.
View and Edit the Network Settings

1. Click the dropdown arrow for NIC 1: Internet facing interface.
2. This section shows all of the configurations associated with NIC 1.
3. Click the Gear icon after NIC 1: Internet facing interface to update the IP address.
Change Network Settings

NIC 1: Internet facing interface

UAG admin interface may become inaccessible if this NIC’s IP address is changed

IPv4 Address * 192.168.110.151
IP Allocation Mode DYNAMIC STATIC
Static Routes Not Available
Netmask 255.255.255.0

The Unified Access Gateway administration console allows you to update the IPv4 address and IP allocation mode associated to NIC 1.

1. Enter **192.168.110.151** in the IPv4 Address to update this from 192.168.110.150.
2. Click **Save**.

Wait for Network Settings to Complete

Network Settings

NIC 1 configuration in progress

Default Gateway 192.168.110.1
NIC 1: Internet facing interface

Close
After saving, a message appears: **NIC1 configuration in progress**. This means that the Unified Access Gateway is updating the NIC with the new IP address, and restarting the NIC. Users lose connectivity with the administration console and this message disappears when the configuration is finished.

After the configuration completes, click **Close**.

**Validate the Network Changes**

![Image of validation process]

1. **Not secure**
2. **Advanced**
3. **Proceed to 192.168.110.161 (unsafe)**

---

**HOL-1957-08-UEM**

Page 43
The page should automatically reload to [https://192.168.110.151:9443/admin](https://192.168.110.151:9443/admin) after the appliance configuration updates, which is the IP address you configured. You may also enter the address manually.

**NOTE:** The appliance may take several minutes to be reachable at 192.168.110.151 after the change. You may need to wait several minutes before the below page will load.

1. Enter [https://192.168.110.151:9443/admin](https://192.168.110.151:9443/admin) and press **ENTER**, or wait for the page to reload.
2. Click **Advanced**.
3. Click **Proceed to 192.168.110.151 (unsafe)**.

**NOTE:** Notice that the connection is not private again, since we are browsing to an IP instead of our previous hostname. This is just to demonstrate the IP address change, so continue to the page for now.

**Log in to the Unified Access Gateway Administration Console**

1. Enter **admin** for the username.
2. Enter **VMware1!** for the password.
3. Click **Login**.

Confirm that you are able to login successfully and access the Unified Access Gateway Administration Console over the new IP address that you configured.
Remove Virtual Machines

You are about to move to the next Module. Before continuing, you will power down and remove the deployed virtual machines you utilized for this exercise. This will release the storage and resources allocated to this virtual machine, allowing these resources to be utilized by other virtual machines that you will deploy in other modules.

Power OFF UAG VM Appliance

Return to Google Chrome. In the vSphere Web Client,

1. Click on UAG-1NIC.
2. Click on the Power OFF button.

Confirm Guest Shut Down

Click Yes.
Delete the Unified Access Gateway Appliance

1. Click the **Refresh** button to check if the Unified Access Gateway virtual machine has powered off.
2. Right-Click the UAG-1NIC virtual machine.
3. Click **Delete from Disk**.
   
   **NOTE:** If Delete from Disk is not available, the virtual machine is still powering off. Click the Refresh button until the virtual machine is powered off.
Confirm the Delete

Click **Yes** to confirm the delete.
Conclusion

In this module, you've learned:

- Deploy the VMware Unified Access Gateway on one NIC using the vSphere Web Client.
- Access the VMware Unified Access Gateway Admin UI.
- Configure a TLS Certificate for the UAG Admin and Internet interfaces.

If you are interested in learning more about the Unified Access Gateway, the remaining lab modules will guide you through more advanced topics and will build upon the knowledge you have learned here. Be sure to check them out for additional learning.

For additional UAG documentation, be sure to check out the VMware Unified Access Gateway Reference page at https://docs.vmware.com/en/Unified-Access-Gateway/.
Module 2 - Unified Access Gateway Deployment with PowerShell
Introduction

This module will guide you through the configuration and deployment of the Unified Access Gateway Appliance using the PowerShell script and how to setup a Reverse Proxy to access internal web sites through the Unified Access Gateway Administration Console.

The Unified Access Gateway Appliance will be deployed with two NICs. One NIC will be facing the internet and the second NIC will be dedicated to the Management and Backend networks.

This manual covers Unified Access Gateway 3.3 deployment in vSphere 6.5 U1.

Prerequisites

All of the following pre-requisites are already installed for this Module, the following information is just for your reference.

To deploy Unified Access Gateway using PowerShell script, you must use specific versions of VMware products.

- vSphere ESX host and vCenter Appliance.
- PowerShell script runs on Windows 8.1 or later machines or Windows Server 2008 R2 or later.
- The Windows machine running the script must have VMware OVF Tool command installed.
- You must install OVF Tool 4.3 or later from https://www.vmware.com/support/developer/ovf/
- Download a version of Unified Access Gateway virtual appliance image from VMWare. This is an OVA file e.g. .euc-access-point-3.3.X.X-XXXXXXXXXXX.ova. Refer to VMware Product Interoperability Matrixes to determine the version to download.
- Download the correct UAG PowerShell script, it's name uagdeploy-VERSION.ZIP file and extract the files into a folder on your Windows machine. The scripts are host here https://my.vmware.com
- You must select the vSphere data store and the network to use.

Starting with version 3.3, you can deploy Unified Access Gateway without specifying the netmask and default gateway settings in Network Protocol Profiles(NPP). You can specify this networking information directly during deployment of your Unified Access Gateway instance.
Logging In to the vSphere Web Client

To perform most of this exercise, you need to log in to the vSphere Web Client.

Launch Chrome Browser

Double-click the Chrome Browser on the lab Desktop
Authenticate to the vSphere Web Client

1. Click the New Tab button.
3. Enable the Use Windows session authentication option.
4. Click Login.

After completing the Login, you will be presented with the vSphere Web Client.

NOTE: You can also login without using Windows session authentication by using **CORP\Administrator** for the username and **VMware1!** for the password.
Power ON Virtual Machines

You will be utilizing other virtual machines that have already been deployed for you as part of this exercise. To ensure these virtual machines are powered on and ready for use during later steps, you will power them on now.

Navigate to VMs and Templates

1. Click the Home icon.
2. Click VMs and Templates.
Power ON Intranet VM

1. Click the arrow by RegionA01 to expand it.
2. Click the Intranet virtual machine.
3. Click the Power ON button.

The Intranet virtual machine will act as our web server, and it's named INTRANET.CORP.LOCAL.

This server host two websites on IIS:

1. **INTRANET** - This website is available through port 80 and 443. The hostname INTRANET.CORP.LOCAL and will be used for this module.
2. **IT** - This website can be ignored, as it will not be used in this exercise.
Starting Windows PowerShell

Click on the **PowerShell** icon located on the Windows Task Bar.

Navigate to the Unified Access Gateway Resources Directory

Navigate to the UAG Resources Directory under the Desktop user folder by entering `cd 'C:\Users\Administrator\Documents\HOL\Unified Access Gateway'` and then press **ENTER**.
Preparing the INI File for Deployment

You will now learn how the Ini file is used to deploy and configure a UAG using Powershell and how to edit the contents of the Ini file for your UAG deployments.

Configuring the General deployment settings

An Initialization (INI) file containing all the configuration settings is required to deploy the Unified Access Gateway Appliance.

In this lab you will use the uag-2NIC.ini file and fill out the respective parameters for your deployment.

You will be deploying a new Unified Access Gateway appliance called UAG-2NIC that has two NICs. NIC1 will be set to the internet facing network and NIC2 for the backend and management networks.
Open the UAG-2NIC.ini File for Editing

1. Click the **File Explorer** icon from the task bar.
2. Click **Documents**.
3. Click **HOL**.
4. Click **Unified Access Gateway**.
5. Right-click the **uag-2NIC.ini** file.
6. Click **Edit with Notepad++**.

1. Click the **File Explorer** icon from the task bar.
2. Click **Documents**.
3. Click **HOL**.
4. Click **Unified Access Gateway**.
5. Right-click the **uag-2NIC.ini** file.
6. Click **Edit with Notepad++**.
Configure General Settings (1/2)

On the General section provide the following settings on the INI file:

1. Enter **UAG-2NIC** for the name field.
2. Enter `C:\Users\Administrator\Documents\HOL\Unified Access Gateway\euc-unified-access-gateway-3.3.0.0-8539135_OVF10.ova` for the source field.
3. Enter `vi://administrator@vsphere.local:VMware1!@vcsa-01a.corp.local/RegionA01/host/RegionA01-COMP01` for the target field.
   NOTE: You can replace `VMware1!` with `PASSWORD` and the script will prompt for the password during the PowerShell execution.
4. Enter **thin** for the diskmode field.
5. Enter **RegionA01-ISCSI01-COMP01** for the ds field (ds referring to Data Store).
6. Enter **twonic** for the deploymentOption field.

Configure General Settings (2/2)
Continuing the General section configuration, set the following values for the parameters on the INI file:

1. Enter `STATICV4` for the `ipMode` field.
2. Enter `192.168.110.1` for the `defaultGateway` field.
3. Enter `192.168.110.10/32 192.168.120.1` for the `routes1` field.
4. Enter `192.168.110.10` for the `dns` field.
5. Enter `192.168.110.160` for the `ip0` field. **NOTE:** ip0 will be the Internet facing NIC.
6. Enter `192.168.120.160` for the `ip1` field. **NOTE:** ip1 will be the Management and Backend facing NIC.
7. Enter `255.255.255.0` for the `netmask0` and `netmask1` fields.
8. Enter `VM-DMZ-RegionA01-vDS-COMP` for the `netInternet` field.

### Configuring TLS/SSL Certificates for Unified Access Gateway Appliance

The `SSLCert` and `SSLCertAdmin` contain the information regarding the SSL Certificates for the Admin and Internet interfaces

1. Enter `C:\Users\Administrator\Documents\HOL\Unified Access Gateway\wildcard_corp_local.pfx` for the `pfxCerts` field under `SSLCert`. **NOTE:** This certificate is for the Internet interface.
2. Enter `C:\Users\Administrator\Documents\HOL\Unified Access Gateway\wildcard_corp_local.pfx` for the `pfxCerts` field under `SSLCertAdmin`. **NOTE:** This certificate is for the Admin and Backend interface.

The certificate password will be requested during the deployment.

### Save the configuration file

Click the icon from the Tool Bar to save `uag-2NIC.ini` file
Deploying Unified Access Gateway Appliance

Now that you have configured the ini file for your Unified Access Gateway deployment, we will run the `uagdeploy.ps1` PowerShell script and provide this ini file as the configuration to automate the deployment.

Executing the Deployment Script

As the scripts starts a couple questions will be asked, follow the steps below in order to provide the correct information.

1. Click the **PowerShell** icon from the taskbar to return to the PowerShell terminal you opened previously.
2. Enter `.\uagdeploy.ps1 .\uag-2NIC.ini VMware! VMware! false false no` as the password for both the `SSLcert` and `SSLcertAdmin` fields when prompted.
3. The **first VMware!** is to set the **root password** for the Unified Access Gateway appliance. The **second VMware!** is to set 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 in response to joining the VMware CEIP (Customer Experience Improvement Program).
4. Enter **VMware!** as the password for both the `SSLcert` and `SSLcertAdmin` fields when prompted.
To avoid password request for the certificate, remove the pfxCerts values and provide a PEM certificate, set the pemCerts and pemPrivKey for the SSLCert and SSLCertAdmin sections of the INI file.

The deployment starts and you can follow the progress on the same window or on your vSphere Web Client, which we leaved open at the beginning of this module.

Confirm the PowerShell Script Deployment Completes

After the deployment script completes, the UAG-2NIC virtual machine will be automatically powered on. The script will output **Completed successfully** once the process has completed.

The **Received IP address** presented by the script log is a temporary IP, the final IPs for NIC 1 and NIC2 will be assigned to the Unified Access Gateway appliance during the first start. You can return to the vSphere Web Client to validate that as described on the next step.
Validating the deployment

Return to the VMware vSphere Web Client in Google Chrome.

1. Click on the **VM and Templates** tab.
2. Click on **UAG-2NIC**.
3. Click the **Summary** tab.
4. Click on **View all 2 IP addresses**.
5. Confirm the IP Addresses listed are **192.168.110.160** and **192.168.120.160**. These are the IPs you specified in the INI file used by the PowerShell script.
6. If the IP Addresses have not populated, you may need to click the **Refresh** button and check again.

**NOTE:** In case the Unified Access Gateway appliance has not finalized the configuration during the first startup, you will receive an error message from vSphere Web Client. If this happens, wait for the Appliance to finish deploying and refresh the whole Chrome Browser.
Log In to the Unified Access Gateway Administration Console

1. Click the **New Tab** button.
2. Enter `https://uag-intranet.corp.local:9443/admin` and then press **ENTER**.
3. Enter `admin` for the username.
4. Enter `VMware1!` for the password. **NOTE:** This password was created for the Admin API during the PowerShell script deployment.
5. Click **Login**.
Choose Manual Configuration

A successful login redirects you to the window where you can import settings or manually configure the Unified Access Gateway appliance.

Under Configure Manually, click **Select**.

You will be returning to the Unified Access Gateway administration console and modifying the configuration manually in upcoming steps, so leave this page open.
Configuring Web Reverse Proxy

At this point, the Unified Access Gateway has been deployed and you have accessed the Unified Access Gateway Admin Console. This exercise will teach you how the Unified Access Gateway can be used as a Web Reverse Proxy.

Access Reverse Proxy Settings

1. Click the **Show toggle** by Edge Service Settings. After you click it, it will switch to Hide.
2. Click the **Gear icon** next to Reverse Proxy Settings.
Add Reverse Proxy Settings

Reverse Proxy Settings

Add

No reverse proxy settings has been added.

Close

Click Add to create a new reverse proxy settings that will be use to access the Intranet.

Define Features Used by Reverse Proxy

Reverse Proxy Settings

Enable Reverse Proxy Settings

Enable Identity Bridging

In this step, click Enable Reverse Proxy Settings only. The toggle will switch to YES.

The Unified Access Gateway identity bridging feature can be configured to provide single sign-on (SSO) to legacy Web applications that use Kerberos Constrained Delegation (KCD) or header-based authentication. You will NOT enable that feature for this lab, but other modules will review this feature if you are interested in learning more.
Config Intranet Reverse Proxy Settings

Reverse Proxy Settings

1. Enter **intranet** for the Instance Id, which is a unique name to identify and differentiate a web reverse proxy instance from all other web reverse proxy instances.
2. Enter **http://intranet.corp.local** for the Proxy Destination URL, which represents the address of the web application.
3. Enter **([/intranet(.*)])** for the Proxy Pattern, which specifies that the matching URI paths will forward to the destination URL.
4. Click **Save**.

Additional parameters can be configured for this type of reverse proxy, more information available [here](#).
Close the Reverse Proxy Settings

Click Close.

Validating Reverse Proxy Configuration

1. Click on the arrow down for the Reverse Proxy Settings.
2. Click on the refresh icon for the Edge Service Settings.
3. Confirm the intranet proxy status is GREEN.

After you added the reverse proxy settings for intranet, the Unified Access Gateway appliance tests the communication between the appliance and the intranet endpoint. The status turns GREEN if a connection is possible, otherwise it will show RED.
NOTE - It may 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.

Accessing Intranet through Reverse Proxy

1. Click the New Tab button to open a new tab.
2. Enter https://uag-internet.corp.local/intranet/ in the address bar and press ENTER.
   NOTE: uag-internet.corp.local resolves to 192.168.110.160, which is the IP address associated with the Unified Access Gateway internet-facing NIC that you configured as part of the deployment through the PowerShell script.
3. Confirm that the sample Intranet site is displayed.

For further clarification about the traffic routing to the Unified Access Gateway:
• Access to the Intranet is going to the Unified Access Gateway over port 443 as a result of the TLS port sharing configuration enabled by default during deployment.
• Access to the Admin Console is going to the Unified Access Gateway port 9443 and IP 192.168.120.160, which is the IP associated with the intranet-facing NIC that you configured as part of the deployment through the PowerShell script.
Power OFF and Remove Virtual Machines

You are about to move to the next Module. Before continuing, you will power down and remove the deployed virtual machines you utilized for this exercise. This will release the storage and resources allocated to these virtual machine, allowing these resources to be utilized by other virtual machines that you will deploy in other modules.

**NOTE: ONLY** delete the virtual machines explicitly instructed in the following steps! Some virtual machines are intended to be used across multiple exercises (the Intranet virtual machine, for example) that you DO NOT want to remove!

### Power OFF UAG VM Appliance

1. Click the **VMs and Templates** tab if you are not already there.
2. Click the **UAG-2NIC** virtual machine.
3. Click the **Power OFF** button.

#### Confirm Guest Shut Down

![Confirm Guest Shut Down](image)

Return to Google Chrome. In the vSphere Web Client,

1. Click the **VMs and Templates** tab if you are not already there.
2. Click the **UAG-2NIC** virtual machine.
3. Click the **Power OFF** button.
Click **Yes**.

**Delete the Unified Access Gateway Appliance**

1. Click the **Refresh** button to check if the Unified Access Gateway virtual machine has powered off.
2. Right-click the **UAG-2NIC** virtual machine.
3. Click **Delete from Disk**.

**NOTE:** If Delete from Disk is not available, the virtual machine is still powering off. Click the Refresh button until the virtual machine is powered off, which is indicated by no longer having the Green Power On icon next to the UAG-2NIC virtual machine icon.
Confirm the Delete

Click **Yes** to confirm the delete.
Conclusion

In this module, you've learned:

- Deploy the VMware Unified Acces Gateway on two NIC configuration using PowerShell script.
- Configure TLS Certificate for the UAG Appliance using PowerShell script.
- Access the VMware Unified Acces Gateway Administration Console.
- Configure a Web Reverse Proxy to access an internal website.

For additional UAG documentation, be sure to check out the VMware Unified Access Gateway Reference page at [https://docs.vmware.com/en/Unified-Access-Gateway/](https://docs.vmware.com/en/Unified-Access-Gateway/)
Module 3 - Web Reverse Proxy secure access to Internal Websites
Introduction

This module will guide you through the configuration of a Web Reverse Proxy instance to access an intranet website using device certificate as authentication method on the Unified Access Gateway.

This exercise provides steps to deploy the Unified Access Gateway Appliance with two NICs, configure multiple Web Reverse Proxy instance using HTTP and HTTPS, and securing with Device Certificate Authentication. All the configuration will be done through the Unified Access Gateway administration console.

This manual covers Unified Access Gateway 3.3 deployment and configuration in vSphere 6.5 U1.

Prerequisites

All of the following pre-requisites are already installed for this Module, the following information is just for your reference.

To deploy Unified Access Gateway using PowerShell script, you must use specific versions of VMware products.

- vSphere ESX host and vCenter Appliance.
- PowerShell script runs on Windows 8.1 or later machines or Windows Server 2008 R2 or later.
- The Windows machine running the script must have VMware OVF Tool command installed.
- You must install OVF Tool 4.3 or later from https://www.vmware.com/support/developer/ovf/
- Download a version of Unified Access Gateway virtual appliance image from VMWare. This is an OVA file e.g. .euc-access-point-3.3.X.X-XXXXXXXXXXX.ova. Refer to VMware Product Interoperability Matrixes to determine the version to download.
- Download the correct Unified Access Gateway PowerShell script, it's name uagdeploy-VERSION.ZIP file and extract the files into a folder on your Windows machine. The scripts are host here https://my.vmware.com
- You must select the vSphere data store and the network to use.
- CA Root and Intermediate certificate, and user certificate to configure Device Certificate Authentication
Logging In to the vSphere Web Client

To perform most of this exercise, you need to log in to the vSphere Web Client.

Launch Chrome Browser

Double-click the Chrome Browser on the lab Desktop
Authenticate to the vSphere Web Client

1. Click the New Tab button.
3. Enable the Use Windows session authentication option.
4. Click Login.

After completing the Login, you will be presented with the vSphere Web Client.

**NOTE:** You can also login without using Windows session authentication by using CORP\Administrator for the username and VMware1! for the password.
Power ON Virtual Machines

1. Click the **Home icon**
2. Click **VMs and Templates**

Power ON Intranet VM
1. Click the arrow by Nested_Datacenter to expand it.
2. Select Intranet VM
3. Click the Power ON button

The Intranet VM will act as our Web Server, and it's named INTRANET.CORP.LOCAL

This server host two web sites on IIS:

1. **INTRANET website** - website available through port 80 and 443, DNS name INTRANET.CORP.LOCAL and will be used for this module.
2. **IT website** - this one won't be used on this module.
Deploying Unified Access Gateway Appliance

The Unified Access Gateway ini file is already configured and contain all the required information to automate this deployment.

Launch PowerShell

Launch PowerShell by clicking the **PowerShell icon** from the Taskbar

Executing the Deployment Script

As the scripts starts a couple questions will be asked, follow the steps below in order to provide the correct information.

1. Enter `cd 'C:\Users\Administrator\Documents\HOL\Unified Access Gateway'` to navigate to the directory with the Unified Access Gateway deployment scripts. Press **ENTER**.
2. Enter `.\uagdeploy.ps1 .\uag-appliance.ini VMware1! VMware1! false false no`. Press **ENTER**.
   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 `VMware1!` as the password for the **SSLCert** and **SSLCertAdmin** fields when prompted.

The deployment starts and you can follow the progress on the same window or on your vSphere Web Client, which we leaved open at the beginning of this module.
**NOTE:** To avoid password request for the certificate, remove the pfxCerts values and provide a PEM certificate, set the pemCerts and pemPrivKey for the SSLCert and SSLCertAdmin sections of the INI file.

## Confirm the PowerShell Script Deployment Completes

1. Confirm the Unified Access Gateway deployed successfully. The **Completed successfully** text will be shown in the output.
2. Click **Close**.

After successfully finalized the deployment the script will automatic Power on the VM UAG-2NIC.

The **Received IP address** presented by the script log is a temporary IP, the final IPs for NIC one and NIC two will be assigned to the Unified Access Gateway appliance during the first start. You can return to the vSphere Web Client to validate that as described on the next step.

**NOTE:** Deploying the Unified Access Gateway may take a several minutes to complete. Please be patient while the task is fully completed.
Validating the deployment

1. Ensure that you are in the menu **VMs and Templates**
2. If you do not see the UAG-2NIC VM under RegionA01, you may need to click **Refresh** first.
3. Click on **UAG-2NIC**.
4. Click the **Summary** tab.
5. Click on **View all 2 IP addresses**.
6. The IP Addresses should show:
   - 192.168.110.160
   - 192.168.120.160

**NOTE:** If the Unified Access Gateway appliance has not finalized the configuration during the initial start-up, you will receive an error message from the vSphere Web Client. If this happens, refresh the Google Chrome browser.
Log In to the Unified Access Gateway Administration Console

1. Click the **New Tab** button to open a new tab.
   **NOTE:** This is the hostname for the intranet facing NIC that the Unified Access Gateway was deployed on (192.168.120.110).
3. Enter **admin** for the username.
4. Enter `VMware1!` for the password.

   **NOTE:** This password was created for the admin account as part of the PowerShell script deployment.

5. Click **Login**.

**Confirm the Unified Access Gateway Administration Console Login on the Internal Network**

A successful login will redirect you to the following screen, where you can import settings or manually configure the Unified Access Gateway Appliance.

Click **Select** under Configure Manually.
Configuring Web Reverse Proxy to access non-SSL website (HTTP/Port 80)

At this point, the Unified Access Gateway has been deployed and you are able to access the Unified Access Gateway administration console to add and change configurations of your Unified Access Gateway appliance.

This exercise shows you how Unified Access Gateway can be used as a Web reverse proxy, and can act as either a plain reverse proxy or an authenticating reverse proxy in the DMZ. In this exercise, you learn how to set up a plain reverse proxy.

Access to the Reverse Proxy Settings

1. Click the Show toggle by Edge Service Settings, clicking on it will cause it to switch to Hide.
2. Click the Gear icon next to Reverse Proxy Settings.
Our goal on this chapter is to enable external access to the Intranet website through the Unified Access Gateway Appliance, using the Reverse Proxy feature.

Click Add to create a new reverse proxy instance in to the reverse proxy settings, that instance will contain the configuration required to access the intranet.

### Define Features Used by Reverse Proxy

In this step, click Enable Reverse Proxy Settings only. The toggle will switch to YES. The Unified Access Gateway identity bridging feature can be configured to provide single sign-on (SSO) to legacy Web applications that use Kerberos Constrained Delegation (KCD) or header-based authentication. You will not enable this feature in this exercise, but will be covered in the following module.
Configuring Intranet Reverse Proxy Settings

Reverse Proxy Settings

1. Enter `intranet` for the Instance Id, which is a unique name to identify and differentiate a Web reverse proxy instance from all other Web reverse proxy instances.

2. Enter `http://intranet.corp.local` for Proxy Destination URL, which represent the address of the Web Application.

3. Enter `(/intranet.*)` for Proxy Pattern, which specifies that the matching URI paths will forward to the destination URL.

4. Click **Save**

Additional parameters can be configured for this type of reverse proxy, more information available [here](#).
Close the Reverse Proxy Settings

Reverse Proxy Settings

<table>
<thead>
<tr>
<th>Instance Id</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>intranet</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Click Close.

Validating Reverse Proxy Configuration

1. Click on the arrow down for the Reverse Proxy Settings
2. Click on the refresh icon for the Edge Service Settings
3. Confirm the intranet proxy status is GREEN

After you added the reverse proxy settings for intranet, the Unified Access Gateway appliance tests the communication between appliance and intranet and the status turn GREEN if a connection is possible, otherwise it will show RED.
NOTE - It may 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.

Access Intranet through Reverse Proxy

1. Click the New Tab button to open a new tab.
2. Enter https://uag-internet.corp.local/intranet/ in the address bar and press ENTER.

NOTE: The uag-internet.corp.local hostname resolves to the Internet facing NIC that you deployed the Unified Access Gateway on (192.168.110.160).

The result is a sample intranet page hosted on an internal IIS Server.

- Access to the intranet site is going through UAG over port 443 as result of the TLS port sharing configuration enabled by default during deployment.
- Access to the Admin UI is going through UAG port 9443 to uag-intranet.corp.local (192.168.120.160).
Configuring Web Reverse Proxy to access SSL website (HTTPS/Port 443)

In order to access an internal website over HTTPS, an additional configuration is required to establish trust between Unified Access Gateway and the internal website. This exercise will explain how configure this trust using the current Intranet Reverse Proxy instance.

Access to the Reverse Proxy Settings

1. Click Close for the Intranet site tab that you opened for https://uag-internet.corp.local/intranet/.
2. Click the Unified Access Gateway Admin UI tab.
3. Click the Gear icon next to Reverse Proxy Settings.
Your goal for this exercise is to enable external access to the Intranet website over HTTPS through the Unified Access Gateway appliance by using the Reverse Proxy feature.

Click the Gear icon to change the configuration settings for the Intranet instance.
Configuring Intranet Reverse Proxy Settings

2. Enter sha1=f3 b6 e8 35 36 ef c9 04 16 45 da 3b 86 0a f7 1b af 7d f3 c7 for Proxy Destination URL Thumbprints, which represents the list of acceptable SSL server certificates.

   **NOTE:** This is the Thumbprint of the SSL certificate issued to our intranet.corp.local server that the IIS web server is using to establish connections over 443 to the intranet application.

   **NOTE:** If you wish to view and validate the certificate, you can do so by finding the certificate at C:\Users\Administrator\Documents\HOL\Unified Access Gateway\intranet_corp_local.crt.

3. Click **Save**.

**NOTE:** A thumbprint is in the format `{alg=}xx:xx`, where `{alg}` can be sha1, the default, or md5 and the `{xx}` represents hexadecimal digits of the value. The `:` separator can also be a space or removed entirely. The casing of the letters in a thumbprint is ignored. If you do not configure the thumbprints, the server certificates must be issued by a trusted CA.

Additional parameters can be configured for this type of reverse proxy, more information available [here](#).
Close the Reverse Proxy Settings

Reverse Proxy Settings

<table>
<thead>
<tr>
<th>Instance Id</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>intranet</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Click Close.

Validating Reverse Proxy Configuration

1. Click on the arrow down for the Reverse Proxy Settings
2. Click on the refresh icon for the Edge Service Settings
3. Confirm the intranet proxy status is GREEN

After you added the reverse proxy settings for intranet, the Unified Access Gateway appliance tests the communication between appliance and intranet and the status turn GREEN if a connection is possible, otherwise it will show RED.
NOTE - It may 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.

Accessing Intranet through Reverse Proxy

1. Click the New Tab button to open a new tab
2. Enter `https://uag-internet.corp.local/intranet/` in the address bar and press **ENTER**.

   **NOTE:** The uag-internet.corp.local hostname resolves to the Internet facing NIC that you deployed the Unified Access Gateway on (192.168.110.160).

The result is the same intranet page hosted on an internal IIS Server. However, the Unified Access Gateway is now accessing the Intranet site on port 443 via HTTPS instead of port 80 via HTTP.

- Access to the intranet site is going through Unified Access Gateway over port 443 as result of the TLS port sharing configuration enabled by default during deployment.
- Access to the Admin UI is going through Unified Access Gateway port 9443 to uag-intranet.corp.local (192.168.120.160).
Add Certificate Authentication to the Intranet website

The current intranet website configuration through Reverse Proxy on the Unified Access Gateway is open to anyone to access. You can restrict access to the intranet website to certain users by configuring a device certificate as the authentication method on the Unified Access Gateway Appliance.

Adding certificate as authentication method will restrict access to the intranet site for only those users who have a certificate installed on their device. The user certificate must match the root certificate set on the Unified Access Gateway appliance.
Enabling the X.509 Certificate Settings

1. Click Close for the Intranet site tab that you opened for https://uag-internet.corp.local/intranet/.
2. Click the Unified Access Gateway Admin UI tab.
3. Click on Show for the Authentication Settings.
4. Click the Gear icon next to X.509 Certificate.
Uploading Certificate into Unified Access Gateway Appliance

1. Click **NO** to enable X.509 Certificate. This will reveal additional configuration options and switch to **YES**, indicating it is enabled.
2. Click **Select** to upload the Root and Intermediate CA Certificates.
Select the Root CA Certificate

1. Click **Documents**.
2. Click **HOL**.
3. Click **Unified Access Gateway**.
4. Click **CA-Certificate.cer**.
5. Click **Open**.

**NOTE:** Since this lab only implements a root CA and NOT a subordinate, we will be using only the ROOT certificate during the authentication process. In a real word scenario, you would have ROOT and INTERMEDIATE certificate available, and you must upload both to the Unified Access Gateway Appliance.
Save the X.509 Certificate Authentication Changes

Click **Save**.

After saving, you will see a message that says "Configuration is saved successfully". Once this displays, the certificate has been uploaded and added to the Unified Access Gateway Appliance certificate store.
Enabling Certificate Authentication for Intranet Web Site

Select the **Gear icon** for the **Reverse Proxy Settings**.

The next steps is to tell the Unified Access Gateway that certificate authentication will be required in order to access the Intranet website through the Reverse Proxy. This means that the client device must have a user certificate that matches to the root certificate upload to the Unified Access Gateway Appliance.
Edit the Intranet Reverse Proxy Settings

Reverse Proxy Settings

<table>
<thead>
<tr>
<th>Instance Id</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>intranet</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Select the **Gear icon** for the intranet Instance

**Configuring 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=f3 b6 e8 35 36 ef c9 04 16 45 da 3b 86 0a f7`

Proxy Pattern: ([/intranet(*)])

Click **More**.
Configure the Authentication Method

Select `certificate-auth` for the Authentication Method.

Save the Reverse Proxy Settings

1. Scroll down to the bottom of the Reverse Proxy Settings window.
2. Click **Save**.
Close the Reverse Proxy Settings

Reverse Proxy Settings

<table>
<thead>
<tr>
<th>Instance Id</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>intranet</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Click **Close**.

Importing the User Certificate to the local Windows Store

[Image of browser settings with highlighted steps: 1. Click the three dots, 2. Select Settings]
1. On Google Chrome Browser click the **Options** button.
2. Click on **Settings**.

**Access the Certificate Settings**

1. Enter **Manage Certificates** in the search bar.
2. Click on **Manage Certificates**.
Choose Import Certificate

1. Click the **Personal** tab.
2. Click **Import**.
Start the Certificate Import Wizard

Click **Next**.
Browse for the User Certificate

Click **Browse**.
Select the User Certificate

1. Click **Documents**.
2. Click **HOL**.
3. Click **Unified Access Gateway**.
4. Select **All Files (*.*)** for the filter.
5. Click **intranet_corp_local.pfx**.
6. Click **Open**.

**NOTE:** For the purposes of this exercise, any certificate that is trusted by the ROOT certificate you uploaded earlier will be sufficient.
Enter the User Certificate Password

1. Set the Password to VMware1!
2. Click Next
Select the Personal Certificate Store

1. The Personal Certificate Store will be pre-selected since you choose to upload a Personal certificate. Do not modify these settings.
2. Click **Next**.
Complete the Certificate Import Wizard

Click **Finish**.
1. Click OK to confirm the import was successful.
2. The list of certificates will be refreshed and the intranet.corp.local certificate will be listed as part of the Personal Store.

Normally, you would need to add both the Personal and the Trusted Root Certificate. However, the Trusted Root Certificate for this infrastructure has already been added, and you will not need to manually included it.

**NOTE:** Should you wish to view it, you can navigate to the Trusted Root Certification Authorities tab in the Certificates window to find the CONTROLCENTER-CA certificate.
Testing the Certificate Authentication

1. In Google Chrome, click **Options**.
2. Click **New incognito window**.
Navigate to the Intranet Site

2. Select the `intranet.corp.local` certificate.
3. Click OK.

You are seeing this prompt because Certificate Authentication is required to visit the intranet site now. Selecting the intranet.corp.local certificate is choosing to present this user certificate to access the intranet site.

Confirm Certificate Authentication was Successful

As result, you will see the intranet page which can now only be accessible from the external network for users that present the correct user certificate.
Click **Close**.
Power OFF Virtual Machines

You are about to move to the next Module, to complete the next Module successful it’s required to follow the next steps to power the current Unified Access Gateway Appliance and Intranet Server.

Return to the vSphere Web Client on your Google Chrome browser.

Power OFF Intranet VM

In the vSphere Web Client,

1. Click the VM and Templates tab.
2. Click the Intranet VM.
3. Click the Power OFF icon.
1. Click on **UAG-2NIC**.
2. Click the **Power OFF** icon.
Delete the UAG VM Appliance

You will remove the Unified Access Gateway Appliance since other Modules may require that you re-deploy the Unified Access Gateway Appliance with the same name but with other configurations.

1. Right-Click **UAG-2NIC**.
2. Click **Delete from Disk**.

![Diagram showing steps to delete the UAG VM Appliance]
Confirm the Delete

Click **Yes** to confirm the delete.
Conclusion

In this module, you've learned how to:

- Deploy the VMware Unified Access Gateway on a two NIC configuration using the PowerShell script.
- Configure the Web Reverse Proxy to access internal Web sites via HTTP and HTTPS protocols.
- Configure Device Certificate Authentication to secure and restrict access to internal websites through Web Reverse Proxy configuration.

For additional UAG documentation, be sure to check out the VMware Unified Access Gateway Reference page at https://docs.vmware.com/en/Unified-Access-Gateway/.
Module 4 - Identity
Bridging and Single Sign-On access to Legacy Web Applications
Introduction

This module will guide you through on how to setup Identity Bridging to provide Single Sign On (SSO) to legacy Web Application using Kerberos Constrained Delegation (KCD).

Unified Access Gateway in identity bridging mode acts as the service provider that passes user authentication to the configured legacy applications. VMware Identity Manager acts as an identity provider and provides SSO into SAML applications. When users access legacy applications that require KCD or header-based authentication, Identity Manager authenticates the user. A SAML assertion with the user’s information is sent to the Unified Access Gateway. Unified Access Gateway uses this authentication to allow users to access the application.

During the lab you will:

- Deploy an Unified Access Gateway Appliance with two NICs, one facing internet and the second one dedicated to Management and Backend access, in addition to that the Web Reverse Proxy configuration to access the Intranet will be automatically configured during deployment.
- Configure Internet Information Server (IIS) to support Kerberos Authentication
- Configure Kerberos Delegation on the Service Account
- Configure Identity Bridging on Unified Access Gateway
- Configuring WebApp (SAML) on VMware Identity Manager
- Test external access to an internal Web Application using SSO through Identity Bridging (SAML -> Kerberos)

This manual covers Unified Access Gateway 3.3 integrated with VMware Identity Manager 3.2.0, both hosted on vSphere 6.5 U1.

Prerequisites

All of the following pre-requisites are already installed for this Module, the following information is just for your reference.

To configure Identity Bridging in Unified Access Gateway, you must use specific versions of VMware products.

- vSphere ESX host with a vCenter Server.
- PowerShell script runs on Windows 8.1 or later machines or Windows Server 2008 R2 or later.
- The Windows machine running the script must have VMware OVF Tool command installed.
- You must install OVF Tool 4.3 or later from [https://www.vmware.com/support/developer/ovf/](https://www.vmware.com/support/developer/ovf/)
Download the following Virtual Appliance image from VMWare.
  ◦ VMware Unified Access Gateway (UAG) OVA file e.g. .euc-access-point-3.3.X.X-XXXXXXXXXXX.ova.
  ◦ VMware Identity Manager (vIDM) OVA file e.g. .euc-identity-manager-3.2.X.X-XXXXXXXXXXX.ova.

For both Appliance refer to VMware Product Interoperability Matrixes to determine the version to download.

Download the correct Unified Access Gateway PowerShell script, it's name uagdeploy-VERSION.ZIP file and extract the files into a folder on your Windows machine. The scripts are host here https://my.vmware.com.

Network access from the Unified Access Gateway Backend services NIC to the internal website used on the reverse proxy.
Kerberos Delegation Overview

Kerberos Delegation means a system and user is configured to request Kerberos tokens on behalf of another user.

Since Unified Access Gateway is not joined to the domain we need to add AD Domain Kerberos support to Unified Access Gateway. This is done with the help of generating a Keytab file. This file contains necessary security tokens/hashes for Unified Access Gateway to interact with AD. The Keytab file contains the information about the user delegated to request Kerberos tokens on another users’ behalf.

Microsoft recommends that each internal Web Application has its own delegated user and therefore different Keytab file, technically you can have one delegated user and Keytab file for many different internal apps, but you are taking the risk in case the Keytab file is compromised to give access to all internal apps. When you have one user / Keytab file per application this allows you to disable access to only one system at a time.

While creating the user and keytab file for each application requires more administration it has its clear security benefits.

REALM is often something you hear talking about Kerberos. A REALM is basically your trust boundaries. In AD Kerberos that is your clients, AD servers and application servers all joined to the domain. Each one trusts each other since they are all part of the same Kerberos REALM.

Environment configuration:

- AD Domain and Kerberos REALM: **CORP.LOCAL**
- Internal web server computer name: **INTRANET**
- Internal web server URL: **http://it.corp.local**
- Internal web application (Kerberos enabled): **http://it.corp.local/itbudget**
- URL to be used for external access to internal app: **https://uag.airwlab.com/itbudget**
- VMware Identity Manager FQDN: **https://vidm.airwlab.com**
- User to be used for Kerberos delegation: **iis_it@CORP.LOCAL**
Authentication Flow

The below diagram describe step by step the authentication flow that you will be configuring in this lab.

1. Client navigates to application URL **https://uag-internet.corp.local/itbudget**.
2. Client is redirected to the Identity Provider (IdP), which is Workspace ONE in this setup, for authentication (**https://vidm.corp.local**). The IdP issue a SAML assertion upon authentication.
3. Client passes the SAML assertion to the Unified Access Gateway (**http://uag-internet.corp.local**). The Unified Access Gateway validates the SAML assertion is from the trusted IdP by using the SAML certificate from the IdP Metadata uploaded.
4. The Unified Access Gateway extracts the client’s username from the SAML assertion and requests a Kerberos ticket from Active Directory (CORP.LOCAL) on behalf of that user.
5. Unified Access Gateway authenticates against the internal web server (**https://it.corp.local**) using the Kerberos ticket obtained from AD.
Logging In to the vSphere Web Client

To perform most of this exercise, you need to log in to the vSphere Web Client.

Launch Chrome Browser

Double-click the Chrome Browser on the lab Desktop
Authenticate to the vSphere Web Client

1. Click the **New Tab** button.
2. Click the **vSphere Web Client** bookmark. The URL for this bookmark is  
   ![URL](https://vcsa-01a.corp.local/vsphere-client/?csp).
3. Enable the **Use Windows session authentication** option.
4. Click **Login**.

After completing the Login, you will be presented with the vSphere Web Client.

**NOTE:** You can also login without using Windows session authentication by using **CORP\Administrator** for the username and **VMware1** for the password.
Power ON Virtual Machines

1. Click the **Home icon**
2. Click **VMs and Templates**

Power ON Intranet VM
1. Select **Intranet VM**
2. Click the **Power ON** button

The Intranet VM will act as our Web Server, and it's named INTRANET.CORP.LOCAL

This server host two WebSites on IIS:

1. **INTRANET website** - this one won't be used on this module
2. **IT website** - website available through port 443 only, DNS name IT.CORP.LOCAL and will be used for this module.

### Power ON Identity Manager Appliance

1. Select **vIDM-3.2.0 VM**
2. Click the **Power ON** button

VMware Identity Manager instance that will be used to integrated with Unified Access Gateway.
Deploying Unified Access Gateway Appliance

You will be using the PowerShell script to deploy the Unified Access Gateway using an .ini file that has already been configured with you to setup a similar configuration to what you configured in Module 3 as a starting point. You will use this starting point to configure Kerberos Delegation and Identity Bridging.

Open PowerShell window

![PowerShell icon]

Click on the PowerShell icon

Deploying Unified Access Gateway Appliance via PowerShell

![PowerShell window]

As the scripts starts a couple questions will be asked, follow the steps below in order to provide the correct information.

1. Enter `cd \Users\Administrator\Documents\HOL\Unified Access Gateway\` then press ENTER.
2. Enter `\uagdeploy.ps1 \uag-ReverseProxy.ini VMware1! VMware1! false false no` then press ENTER.

   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 VMware1! as the password for the SSLcert and SSLcertAdmin fields when prompted.

To avoid password request for the certificate, remove the pfxCerts values and provide a PEM certificate, set the pemCerts and pemPrivKey for the SSLCert and SSLCertAdmin sections of the INI file.

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

**Confirm the PowerShell Script Deployment Completes**

1. Confirm the Unified Access Gateway deployment completed successfully. The Completed successfully text will be shown in the output.
2. Click Close.

After successfully finalized the deployment the script will automatic Power on the VM UAG-2NIC.

The Received IP address presented by the script log is a temporary IP, the final IPs for NIC one and NIC two will be assigned to the Unified Access Gateway appliance during the first start. You can return to the vSphere Web Client to validate that as described on the next step.

**NOTE:** Deploying the Unified Access Gateway may take a several minutes to complete. Please be patient while the task is fully completed.
Validating the deployment

Return to the VMware vSphere Web Client in Google Chrome.

1. Click on the VM and Templates tab.
2. Click on UAG-2NIC.
3. Click the Summary tab.
4. Click on View all 2 IP addresses.
5. Confirm the IP Addresses listed are 192.168.110.160 and 192.168.120.160. These are the IPs you specified in the INI file used by the PowerShell script.
6. If the IP Addresses have not populated, you may need to click the Refresh button and check again.

**NOTE:** In case the Unified Access Gateway appliance has not finalized the configuration during the first startup, you will receive a error message from vSphere Web Client. If this happens, wait for the Appliance to finish deploying and refresh the whole Chrome Browser.

You will continue with configuring Kerberos and other tasks while you wait for the Unified Access Gateway appliance to finish deploying and enabling the various services that were configured as part of the PowerShell deployment.
Configuring Kerberos Authentication on IIS Website

Return to the vSphere Web Client,

1. Click the Intranet VM.
2. Click the Summary tab.
3. Click the Gear icon on the Intranet Screen.
4. Click Launch Remote Console.

NOTE: A new browser tab will open and the VMware Remote Console will load after a few seconds.
Login to the Intranet VM

The VMware Remote Console may take a few seconds to launch. Once the VMware Remote Console launches,

1. Press the **Ctrl+Atl+Delete** button to open the login page.
2. Enter **VMware1!** for the password
3. Click the **Login** button, or press **ENTER**.
Launch IIS

Click the **IIS Manager** icon from the toolbar
Open **IIS (Internat Information Server)** located on the Task Bar at the bottom

1. Click on **Arrow Down** to expand the INTRANET node
2. Click on **Arrow Down** to expand the Sites node
3. Click on **IT Site**
4. Double Click on **Authentication**
Enable Windows Authentication Method

2. Click on Enable.

NOTE: Make sure Anonymous Authentication, ASP.NET Impersonation and Basic Authentication are Disabled. When you install IIS for the first time, Anonymous Authentication is always enabled by default.

Configure Authentication Providers
After Enable Windows Authentication Method you will be able to setup the Authentication Providers.

Click **Providers** to open the list of Providers available for Windows Authentication.

**Configure Providers**

![Configure Providers](image)

Negotiate and NTLM have already been configured as the two enabled providers available. In a new IIS installation that won't be the case and you will need to install the providers as part of the IIS installation, and add those here. These tasks are beyond the focus of this lab and have been configured for you.

Negotiate is a container that uses Kerberos as the first authentication method, and if the authentication fails, NTLM, which means username and password will be used.

It is mandatory that Negotiate comes first in the list of providers, **check and confirm that Negotiate is first and NTLM second**.

Click **X** to close the Window.
Configure Kernel-mode Authentication

1. Click on **Windows Authentication**
2. Click on **Advanced Settings...**

Enable Kernel-mode Authentication

1. Check **Enable Kernel-mode authentication**
2. Click **OK**

Leave **Extended Protection Off** for this lab, however in a production environment you should configure this option, as it enhances the existing Windows Authentication.
functionality to mitigate authentication relay or "man in the middle" attacks. You can find more information about Extended Protection [here](#).

**Configure IIS Application Pool**

On this step you are configuring the Application Pool to launch from a specific account (corp\iis_it) that is already created.

**Configure Identity for an Application Pool**

1. Select **Application Pools**
2. Select **IT** on the list of Application Pools
3. Click **Advanced Settings**
Update the Application Pool Identity

In this step we will set `CORP\iis_it` as the account to be used to launch the Pool.
Select the "..." for **Identity** under Process Model
Select Custom Account

1. Select **Custom account**
2. Click **Set...**

Set Custom Account Credentials

1. Enter `corp\iis_it` for User name
2. Enter `VMware1!` for Password
3. Enter `VMware1!` for Confirm password
4. Click **OK**
Confirm Custom Account for Application Pool Identity

Click **OK** to confirm that **corp\iis_it** is the account to be used by this pool.
Confirm the Updated Application Pool Identity

1. `corp\iis_it` is now set as the account
2. Click **OK**
Configure Application Pool to use Identity Credentials

1. Click on the **IT Web Site**
2. Double click on **Configuration Editor**
Select Windows Authentication

1. Open the **Section list**.
Update Windows Authentication Configuration

1. Click the **dropdown arrow** for useAppPoolCredentials.
2. Select **True** for useAppPoolCredentials.
3. Click **Apply**.

When you set `useAppPoolCredentials` to true you are telling IIS that it needs to use its application pool identity (which you set for `CORP\iis_it`) to decrypt the Kerberos token/ticket which was obtained from AD and forwarded by the client to the server to authenticate the user.

**Reset IIS**

Open Command Prompt for the Intranet VM within the VMware Remote Console and type the command to Reset IIS
1. Open Command Prompt from the taskbar.
2. Enter `iisreset` and press `ENTER`.
3. Confirm IIS successfully stops and then starts again.

**Minimize Intranet VM**

Click on the icon to **minimize** Intranet VM
Configuring Kerberos Delegation

You will now configure Kerberos Delegation for the IIS IT service account that has been assigned to handle Kerberos Delegation for the IIS website.

Active Directory Setup

From the Main Console (NOT the Intranet VM opened in the VMware Remote Console!),

1. Click the Windows button.
2. Type `active directory` to search.
3. Click **Active Directory Users and Computers**.
Find IIS IT User

We already create a service account (IIS_IT) that will be used for Kerberos delegation on your web application.

You can see the account created through the Active Directory Users and Computers management console from the Main Console:

1. Click Users
2. Look for the Name IIS IT

Configure Service Principal Name (SPN) for Service Account

The next step includes the registration of Service Principal Name (SPN) entries for the name the website has to respond, in this case IT.CORP.LOCAL.
The SPN can be associated with the Web Server machine name or with the Service Account under which the Application Pool's web server will be running, it can be Local System, Network Service or a domain account.

In case the IIS website needs to be available only by the name of the server on which it is located (for this lab are https://it.corp.local) you would not need to create additional SPN entries as these already exist in the server account IIS_IT in Active Directory. Since the DNS name we are using is IT.CORP.LOCAL and the Web Server machine is INTRANET, you will create a SPN entry HTTP/IT.CORP.LOCAL for the user account CORP\IIS_IT.

**NOTE:** Another important point, for Kerberos authentication to succeed in a Load Balanced scenario, the Web servers must use an alternate credential that's shared by all members of the array. The credential must also be associated with the array-specific SPNs. This shared credential may be either a computer account or a service account and must be known by every Web server within the array.

Load Balance is not part of this exercise, however you can obtain more information about this scenario [here](#).

### Assign Service Principal Name to Service Account

1. Click the **Command Prompt** icon from the taskbar on the Main Console (do not return to the Intranet VM in the VMware Remote Console).
2. Enter the command `setspn /s HTTP/it.corp.local CORP\iis_it` and press **ENTER**.
3. Confirm the command ran successfully, noted by the **Updated object** output.
With this command, you are giving permission to CORP\IIS_IT to decrypt Kerberos tickets, when users accesses these addresses and authenticate sessions.

**Assign Delegation Rights to the Service Account**

1. Click on the **Active Directory Users and Computers icon** from the Main Console taskbar
2. Right-click on the **IIS IT** user.
3. Click on **Properties**.
Update Delegation Settings

1. Click on Delegation tab.
2. Select Trust this user for delegation to specified services only.
3. Select Use any authentication protocol.
4. Click on Add.
Launch Computer Search

Click on **Users or Computers**.

**Search for the Intranet Object Name**

1. Enter `intranet` on the Enter the object names to select.
2. Click **OK**.
Select the HTTP Service

1. Select **http** for the INTRANET computer on the list of Available Services.
2. Click **OK**.
Add HTTP Service for the Delegation

1. Confirm that **http for INTRANET computer** was added to the list of services to which the IIS_IT account can present delegated credentials. The computer value will be refreshed next time you come back to the Delegation tab, instead of INTRANET you will see INTRANET.CORP.LOCAL.

2. Click **OK**.

The CORP\IIS_IT account is now authorized to delegate the user logged in credentials to any HTTP service on the INTRANET machine. This setting varies on the type of SPN you have registered and might fall under any one of the below categories.
Create a Keytab file

Keytab is the token that will be used to connect to Active Directory and request an authentication ticket without a login password. Keytab files contain a pair of Kerberos principals and encrypted keys which allows authentication using Kerberos without the need to enter a password. Keytabs can only be generated through Windows Server OS.

To generate the Keytab file, access the Command Prompt from the Main Console again (do NOT return to the Intranet VM).

1. Click on the **Command Prompt** icon from the Main Console.
2. Enter the following command:
   ```
ktpass -princ HTTP/it.corp.local@CORP.LOCAL -mapuser iis_IT@CORP.LOCAL -mapOp set -pass VMware1! -crypto all -ptype KRB5_NT_PRINCIPAL -out C:\it.keytab
   ```

   After you execute this command a file named `it.keytab` will be created in `C:\`. This file will be used later during the configuration of the Identity Bridging on the Unified Access Gateway.
Each parameter we passed to the ktpass toll is explained below:

- **-princ** - Specifies the principal name in the form HTTP/it.corp.local@CORP.LOCAL that you created in the previous steps.
  **WARNING:** This parameter is case sensitive and there is no validation to see if the parameter matches the exact case of the userPrincipalName attribute value when generating the Keytab file.
- **-mapuser** - Maps the name of the Kerberos principal, which is specified by the princ parameter, to the specified domain account.
- **-map0p** - Specifies how the mapping attribute is set. In this case, `set` sets the value for Data Encryption Standard (DES) - only encryption for the specified local user name.
- **-crypto** - Specifies the keys that are generated in the keytab file.
- **-ptype** - Specified the principal type. `KRB5_NT_PRINCIPAL` is the general and recommended principal type.
- **-out** - Specifies the path and name of the Kerberos version 5 .keytab file to generate.
Download IdP Metadata from VMware Identity Manager

As part of this exercise, you will configure a VMware Identity Manager tenant and make a web application available to your users that allows them to access the https://it.corp.local intranet site with Kerberos and Identity Bridging through the Unified Access Gateway. Some setup of VMware Identity Manager has already been configured for you to focus the scope of this lab.

Return to Google Chrome on the Main Console,

1. Click the New tab button.
2. Enter [https://vidm.corp.local](https://vidm.corp.local) and press **ENTER**.
   **NOTE:** This is the hostname that points to the VMware Identity Manager appliance that is deployed within vSphere that you powered on earlier in this exercise.
3. Select **System Domain**.
4. Uncheck **Remember this setting**.
5. Click **Next**.

### Enter the Admin Credentials

1. Enter **admin** for the Username.
2. Enter **VMware1!** for the Password.
3. Click **Sign in**.

1. Enter **admin** for the Username.
2. Enter **VMware1!** for the Password.
3. Click **Sign in**.
**Access Catalog Settings**

1. Click **Catalog**.
2. Click **Settings**.

**Download the Identity Provider Metadata**

1. Click on **SAML Metadata**
2. Right Click on **Identity Provider (IdP) metadata**
3. Click on **Save link as...**
You will need this file during the Identity Bridging configuration in an upcoming step to establish trust between the VMware Identity Manager tenant and the it.corp.local intranet site.

**Save the Identity Provider Metadata**

1. Click the **Downloads** folder.
2. Check the file name for the metadata is set to **idp.xml**.
3. Click **Save**.
Close the Catalog Settings

Click the **Close** button to close the Catalog Settings screen.
Log In to the Unified Access Gateway Admin Console

NOTE: The Unified Access Gateway appliance may take 5 - 10 minutes to fully deploy and be accessible. If you are not able to connect using the below URL, please wait and try again in a few minutes.

1. Click the **New Tab** button to open a new tab.
3. **NOTE:** This is the hostname for the intranet facing NIC that the Unified Access Gateway was deployed on (192.168.120.110).
4. Enter `admin` for the username.
5. Enter `VMware1!` for the password.
6. **NOTE:** This password was created for the admin account as part of the PowerShell script deployment.
7. Click **Login**.

### Validate Configuration Settings

A successful login will redirect you to the following screen, where you can import settings or manually configure the Unified Access Gateway Appliance.

Click **Select** under **Configure Manually**.
Confirm the itbudget Reverse Proxy Settings were Configured

Following the steps below to see that a Web Reverse Proxy instance named itbudget has been automatically configured, later you will enable Identity Bridging feature for this Instance.

The Unified Access Gateway Appliance has been pre-configured with a Reverse Proxy named itbudget which was configured as part of the .ini file used during the PowerShell deployment. This has been done to limit the setup time required for this exercise and is similar to the setup seen in Module 3. You will later enable the Identity Bridging feature for this itbudget instance.

1. Click SHOW for the Edge Service Settings, after you click it will switch to HIDE.
2. Click the dropdown arrow for the Reverse Proxy Settings.
3. Confirm the itbudget Reverse Proxy instance exists.
Configuring Identity Bridging on Unified Access Gateway

You are now ready to configure the Identity Bridging feature on the Unified Access Gateway appliance. By providing the IdP Metadata XML from the VMware Identity Manager tenant and the Keytab file generated for the IIS_IT@corp.local user, you will be able to configure the Unified Access Gateway to authenticate users with SAML to your it.corp.local intranet website.

Configure Identity Provider

1. Scroll down until you see the option for **Identity Bridging Settings**
2. Click the **Gear** for **Upload Identity Provider Metadata** under Advanced Settings.

### Upload the Identity Provider Metadata

![Upload Identity Provider Metadata](image)

- **Entity ID**
- **IDP Metadata**

Click **Select** for the IDP Metadata field.

### Select the Identity Provider Metadata

![Select Identity Provider Metadata](image)

1. **Downloads**
2. **idp.xml**
3. **Open**
1. Click Downloads.
2. Click idp.xml.
   **NOTE:** This is the Identity Provider Metadata XML you downloaded from the VMware Identity Manager tenant in previous steps.
3. Click Open.

### Save the Uploaded Identity Provider Metadata

Click **Save**.

**NOTE:** It may take a moment to save the configuration after you click Save. Please do not click multiple times, the page should update after 5 - 10 seconds.

After hit Save, you should receive a pop-up message showing "**Configuration is saved successfully**".

**NOTE:** The Entity ID will be detected from the IDP metadata XML, so no need to enter this manually.
Configure Keytab

Click the Gear for Upload Keytab Settings under Advanced Settings

Update the Keytab Settings

1. Enter HTTP/it.corp.local@CORP.LOCAL for the Principal Name.
2. Click on **Select** for the Keytab File.

## Select the Keytab File

1. Click **Local Disk (C:)**.
2. Click **it.keytab**.
   
   **NOTE**: This is the keytab file you generated from a previous step by running the ktpass command from the Command Prompt.
3. Click **Open**.
Save the Uploaded Keytab File

Click **Save**.

**NOTE:** It may take a few seconds for the console to update after you click Save. Please do not click Save multiple times, the page will refresh automatically within a few seconds.

After hit Save, you should receive a pop-up message showing "**Keytab upload is successful**".

**NOTE:** The first Principal Name found on the Keytab file will be used when not provided, if your Keytab contain multiple Principal Names it's recommend that you inform the Principal Name to be used.
Configure REALM

Advanced Settings

- Advanced Settings
  - System Configuration
  - Network Settings
  - TLS Server Certificate Settings
  - SAML Settings
  - Endpoint Compliance Check Provider Settings
  - Account Settings

- Identity Bridging Settings
  - Upload Identity Provider Metadata
  - Upload Keytab Settings
  - Realm Settings
  - OCSP Settings

Click the Gear for **Realm Settings** under Advanced Settings.

Add a Realm Setting

Realm Settings

No realm setting has been added.
Click **Add**.

**Configure the Realm Settings**

1. Enter **CORP.LOCAL** for Name of the realm.
   **NOTE:** This entry MUST BE IN CAPITAL. It is advised to copy the value directly or drag-and-drop the text from the manual for accuracy.
2. Enter **corp.local** for Key Distribution Centers.
3. Enter **3** for KCD Timeout (in seconds).
4. Click **Save**.

After you click Save, you should receive a pop-up message showing "**Configuration saved successful**"
Close the Realm Settings

Click Close.

Configure Identity Bridging

1. Click the SHOW toggle for the Edge Service Settings. This will change to HIDE after you click it.
2. Select the Gear icon for Reverse Proxy Settings.

1. Click the SHOW toggle for the Edge Service Settings. This will change to HIDE after you click it.
2. Select the Gear icon for Reverse Proxy Settings.
Open the itbudget Reverse Proxy Settings

Reverse Proxy Settings

<table>
<thead>
<tr>
<th>Instance Id</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>itbudget</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

Select the **Gear** icon for the itbudget Reverse Proxy Instance.
Update the itbudget Reverse Proxy Settings

Reverse Proxy Settings

Enable Reverse Proxy Settings: YES

Instance Id: itbudget

Proxy Destination URL: https://it.corp.local

Proxy Destination URL Thumbprints: sha1=b2 56 a1 cf 8b 21 95 22 45 c2 c0 30 91 7c 1b

Proxy Pattern: (/itbudget(*))

Enable Identity Bridging: YES

Authentication Types: SAML

Identity Provider: https://vidm.airlab.com

Keytab: HTTP/it.corp.local@CORP.LOCAL

Target Service Principal Name: HTTP/it.corp.local@CORP.LOCAL

Service Landing Page: /

User Header Name: AccessPoint-User-ID

Download SAML service provider metadata

Save | Cancel
1. Click **NO** to show the Enable Identity Bridging, it will switch to **YES** after you enable it.
2. Select **SAML** for Authentication Types.
3. Select **https://vidm.airwiab.com** for Identity Provider. This Identity Provider was made available with the IdP Metadata XML you uploaded from the previous steps.
4. Select **HTTP/it.corp.local@CORP.LOCAL** for Keytab. This Keytab was made available with the Keytab file you uploaded from the previous steps.
5. Enter **HTTP/it.corp.local@CORP.LOCAL** for Target Service Principal Name.
7. Click **Download SAML service provider metadata**, this will open another screen.

**NOTE:** Do NOT click save yet! Continue to the next step.

**Download the SAML Service Provider Metadata**

1. Enter **uag-internet.corp.local** for External Host Name.
   **NOTE:** This is the internet facing NIC that was configured for the Unified Access Gateway appliance during deployment using the .ini file with PowerShell.
2. Click **Download**.

**NOTE:** It may take a moment for the download to start after clicking Download. Please wait a moment and do not click Download multiple times!

A file named **uag-internal.corp.local.xml** will be download into the Downloads folder, this file will be used during the Web App setup in VMware Identity Manager.

**Keep the SAML Service Provider Metadata (IF NEEDED)**
If you are prompted to keep or discard the uag-internet.corp.local.XML download, click **Keep**.

**Save the Reverse Proxy Settings**

1. Scroll down until you see the button **Save**
2. Click **Save**

**Confirm the Reverse Proxy Settings Saved**

Reverse Proxy Settings

<table>
<thead>
<tr>
<th>Instance Id</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>itbudget</td>
<td>Enabled</td>
</tr>
</tbody>
</table>
Confirm the **Configuration is saved successfully** message is displayed.

Click **Close**
Configure a Web App in VMware Identity Manager

1. Return to the VMware Identity Manager Admin Console tab.
2. Click the **drop-down arrow** by Catalog.
3. Click **Web Apps**.
4. Click **New**.
Configure the Web App

1. Enter **IT Budget** for Name.
2. Enter **Internal website for IT budget planning** for Description.
3. Click **Next**.
Open the SAML Service Provider Metadata

1. Click the File Explorer icon from the taskbar.
2. Click Downloads.
4. Click Edit with Notepad++.
Copy the SAML XML

1. Right-click on the content and click **Select All**.
2. Right-click on the content and click **Copy**.
3. Click on **X** to close Notepad++.
Paste the SAML XML

Return to the VMware Identity Manager Console,

1. Select SAML 2.0 for the Authentication Type.
2. Right-click in the URL/XML text field.
3. Click Paste, confirm the copied text is entered.
4. Click Next.
Click **Next**.

You will use the default access policy already defined in VMware Identity Manager.
Click **Save & Assign**.

**NOTE:** It may take a moment for the page to update after clicking Save & Assign, please wait a few seconds for the page to update.
Assign Web App to a AD Group

1. Enter **ALL USERS** in the **Users / User Groups** field.
2. Click the **ALL USERS** result.

Update the Deployment Type and Save

1. Change Deployment Type to **Automatic** for the **ALL USERS** group.
2. Click **Save**.
Testing Web Application and SSO through Identity Bridging

You now have the IT Budget Web App configured and added to the catalog.

1. Click on the three dots on the right top side of Google Chrome Browser.
2. Select New incognito window.
Access the itbudget Site

Select the Corp.Local Domain

You will be redirected to VMware Identity Manager for authentication on the CORP.LOCAL domain.

Click **Next**.
Enter Corp.Local User Credentials

1. Enter **aduser** for the username.
2. Enter **VMware1!** for the password.
3. Click **Sign in**.
Confirm Access after Successful Authentication

You should see the IT Budget website now after successfully authenticating.

Validating Kerberos Authentication

Return to the Intranet Web Server machine that you previously accessed through VMWare Remote Console.

1. Click the **MVware Remote Console** icon from the Main Console task bar to return to the Intranet VM.
2. Click the **Event Viewer** icon from the Intranet VM task bar.
View Logon Logs

1. Expand the **Windows Logs** node.
2. Click on **Security**.
3. Select the latest **Logon** Task Category event.
4. Click the **Details** tab.
5. Click the **XML View** toggle.
6. Scroll down to find the EventData section.
7. The Log Details show an authentication on behalf of the user **ADUSER** using Kerberos.
Conclusion

In this module, you've learned how to:

- Deploy the VMware Unified Access Gateway on two NICs with a pre-configured Web Reverse Proxy instance configuration using PowerShell script.
- Configure Internet Information Server (IIS) to support Kerberos Authentication.
- Setup Kerberos Delegation on a Service Account.
- Configure a Web App (SAML) on VMware Identity Manager.
- Configure Identity Bridging for a Web Reverse Proxy instance on Unified Access Gateway to provide Single Sign-on (SSO) to legacy Web Applications.

For additional UAG documentation, be sure to check out the VMware Unified Access Gateway Reference page at https://docs.vmware.com/en/Unified-Access-Gateway/.
Conclusion

Thank you for participating in the VMware Hands-on Labs. Be sure to visit http://hol.vmware.com/ to continue your lab experience online.

Lab SKU: HOL-1957-08-UEM

Version: 20181104-123630