



# Universal Policy Administrator 3.0 Administration Guide

October 2020

## Legal Notice

© Copyright 2020 Micro Focus or one of its affiliates.

The only warranties for products and services of Micro Focus and its affiliates and licensors (“Micro Focus”) are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Micro Focus shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

For additional information, such as certification-related notices and trademarks, see <http://www.microfocus.com/about/legal/>.

---

# Contents

<b>About This Guide</b>	<b>5</b>
<b>1 Introduction</b>	<b>7</b>
Understanding Universal Policy Administrator	7
Benefits of Using Universal Policy Administrator	7
Understanding the Universal Policy Administrator Architecture	8
Universal Policy Administrator Components	8
Understanding the Workflow	9
Using the Web Console	10
<b>2 Installing Universal Policy Administrator</b>	<b>11</b>
Installation Checklist	11
Installing Universal Policy Administrator Components	12
Installing the Universal Policy Administrator Cloud Gateway in Microsoft Azure	12
Installing the Universal Policy Administrator Cloud Gateway, On Premises	15
Installing the Universal Policy Administrator On Premises Gateway	16
Configuring the Universal Policy Administrator Syslog Provider	17
Installing the Universal Policy Administrator Windows Agent	18
Non Windows Agent Requirements and Installations	19
Installing the Universal Policy Administrator Linux Agent	20
Installing the Universal Policy Administrator Mac Agent	23
Joining Linux Agent Configuration Type Post Installation	24
Licensing Universal Policy Administrator On Premises Gateway and Agents	25
Evaluation Licenses	25
Enterprise Licenses	25
<b>3 Configuring Universal Policy Administrator</b>	<b>27</b>
Service Accounts	27
Importing Linux Custom Configuration File Settings	27
Example of Deployment and Initial Setup	28
<b>4 Working with Universal Policies</b>	<b>29</b>
Creating and Checking In Universal Policies	30
Editing and Deleting Universal Policies	30
Merging Universal Policies	31
Approving Universal Policies	31
Managing Universal Policy versions	32
Rolling Back Universal Policies	32
Exporting Universal Policies	32
Replicating and Migrating Universal Policies	33
Managing Non Windows Agent Services with Universal Policies	33
Managing Non Windows Applications with Universal Policies	34

Executing Commands with Universal Policies . . . . .	34
Managing User Logins with Universal Policies . . . . .	35
<b>5 Working with Universal Policy Administrator Roles</b>	<b>37</b>
Understanding Universal Policy Administrator Roles . . . . .	37
Adding Users to Roles . . . . .	39
Adding Groups to Roles . . . . .	39
Applying Role Notifications . . . . .	40
<b>6 Working with Cloud OUs and Domains</b>	<b>41</b>
Importing Domains and OUs . . . . .	41
Accessing Domains and OUs . . . . .	41
Creating, Editing and Deleting WMI Filters . . . . .	42
Adding and Removing Cloud OUs . . . . .	42
Linking and Activating Universal Policies and Including Agents in Cloud OUs . . . . .	43
Removing Linked Universal Policies and Agents from Cloud OUs . . . . .	43
<b>7 Reporting on Universal Policies</b>	<b>45</b>
Viewing RSoP Analysis Reports . . . . .	45
Viewing Conflict Analysis Report . . . . .	45
Viewing Comparison and Differential Reports . . . . .	45
<b>8 Uninstalling Universal Policy Administrator</b>	<b>47</b>
<b>A Automating Universal Policy Administrator Operations with PowerShell Cmdlets</b>	<b>49</b>
Importing The PowerShell Snap-In . . . . .	49
Listing PowerShell Snap-In Cmdlets . . . . .	49
Viewing A Sample Cmdlet Detail . . . . .	49
<b>B Appendix</b>	<b>53</b>
Linux Agent Commands and Lookups . . . . .	53
Supported PowerShell Cmdlets . . . . .	54
<b>C Appendix</b>	<b>59</b>

# About This Guide

The *Universal Policy Administrator Administration Guide* provides information to help you understand, install, configure, and use the Micro Focus Universal Policy Administrator product to help manage your hybrid enterprise environment.

## **Audience**

This guide is written for administrators and users who will use Micro Focus Universal Policy Administrator to more effectively manage Active Directory and universal policies in a hybrid environment.

## **Feedback**

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the User Comments feature at the bottom of each page of the online documentation.

## **Additional Documentation**

Universal Policy Administrator is supported by other documentation (in both PDF and HTML formats) that you can use to learn about and implement the product. For additional documentation, see the [Universal Policy Administrator documentation website](#).



# 1 Introduction

To leverage Universal Policy and comply with necessary regulations without human intervention, you need ways to:

- ◆ Model changes to Universal Policies safely without interrupting services.
- ◆ Test Universal Policies and secure approval from all stakeholders before deploying them.
- ◆ Deploy tested Universal Policies into trusted or untrusted Active Directory domains and hybrid environments.
- ◆ Maintain consistent Universal Policies across business units, regions, worldwide locations or cloud resources.
- ◆ Roll back to a last known good Universal Policy to quickly recover from errors.

Universal Policy Administrator is an enterprise-wide universal policy administration solution to help administrators to centrally manage thousands of resources on premises or on cloud. It can also help meet compliance objectives, especially those that require you to document changes that affect network security or access to sensitive files, such as financial, business or personnel data.

The following sections provide more information:

- ◆ [“Understanding Universal Policy Administrator” on page 7](#)
- ◆ [“Understanding the Universal Policy Administrator Architecture” on page 8](#)
- ◆ [“Using the Web Console” on page 10](#)

## Understanding Universal Policy Administrator

Universal Policy Administrator has an offline repository where you can test and manage changes to Universal Policies before rolling them out into the live environment. This helps in avoiding potentially catastrophic changes that can impact network or service availability.

Universal Policy Administrator has a change management workflow and delegation model to safely involve all Universal Policy stakeholders and built in tools to analyze, compare, troubleshoot, and test Universal Policies. The comprehensive reporting capability helps in documenting regulatory compliances.

## Benefits of Using Universal Policy Administrator

The benefits of using the Universal Policy Administrator are:

- ◆ Provides a buffer from making errors in a live Active Directory environment
- ◆ Lets you compare and view differences between Universal Policies
- ◆ Performs health checks to ensure Universal Policies are not corrupted
- ◆ Lets you quickly roll back to a last known good version of a Universal Policy
- ◆ Stores backup copies of Universal Policies including WMI filters and links

- ◆ Lets you centrally manage Universal Policies in untrusted domains
- ◆ Lets you migrate Universal Policies from one domain to another
- ◆ Lets you delegate Universal Policy changes to appropriate people while limiting Active Directory permissions

Universal Policy Administrator helps manage policies in a hybrid environment with the help of a Web Console. By deploying Universal Policy Administrator in your hybrid environment, you can:

- ◆ Enforce secure password and account policies
- ◆ Ensure access to network resources
- ◆ Secure network and wireless communications
- ◆ Comply with government and industry regulations such as HIPAA, PCI DSS and many others

It helps secure and unify hybrid environment operations across multiple policy silos including Active Directory, Linux, Mac, and Cloud.

It helps large enterprises with hybrid environments to automate the following types of tasks:

- ◆ Enforcing consistent use of Universal Policies across the enterprise
- ◆ Managing and maintaining Universal Policies across trust barriers
- ◆ Automatically deploying Universal Policies during non peak hours
- ◆ Diagnosing problems and differences between Universal Policies

## Understanding the Universal Policy Administrator Architecture

Universal Policy administrator extends the Active Directory (AD) capabilities by enabling domain controllers to add Linux and Mac servers along with Cloud resources to the AD environment, which can interface with identity services, Universal policies, and domains.

### Universal Policy Administrator Components

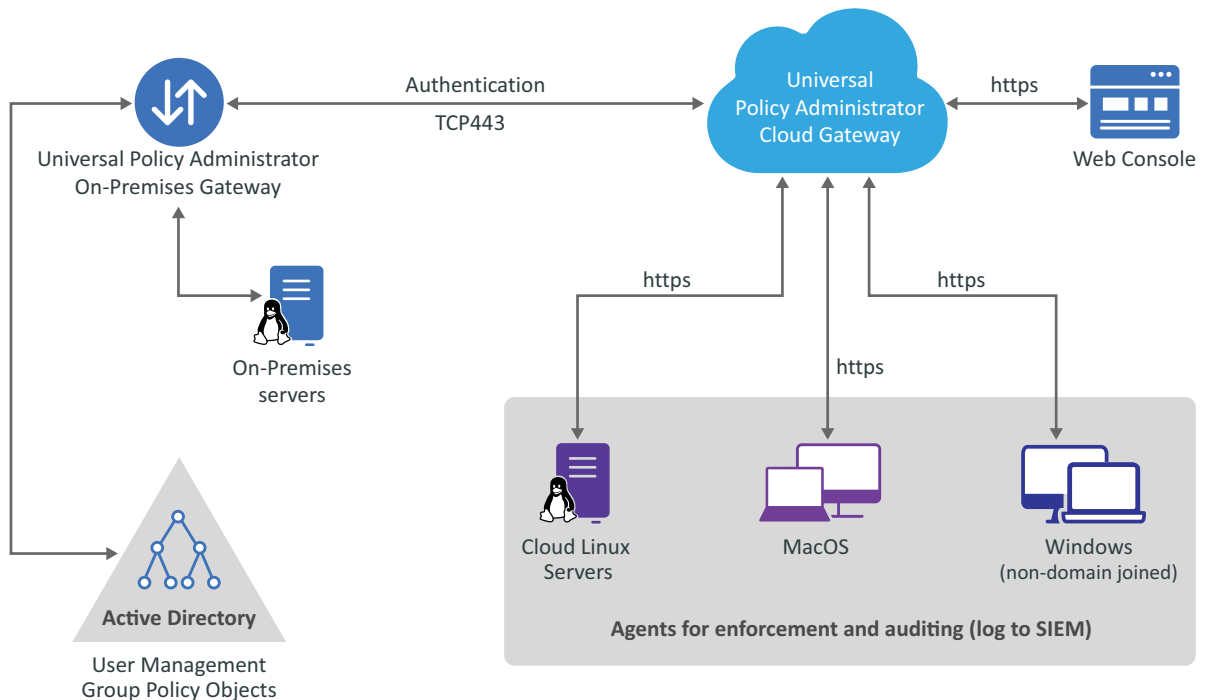
Universal Policy Administrator Components	Description
Universal Policy Administrator Agents	Windows, Linux or Mac based software that enforce universal policies and audit logs; the Windows agent manages a non-domain joined Windows computer.
Universal Policy Administrator On Premises Gateway	A Windows server that is used to push policies from Active Directory to the Universal Policy Administrator Cloud Gateway.
Universal Policy Administrator Cloud Gateway	A component that provides the ability to bridge VMs in the cloud with the Universal Policy Administrator On Premises Gateway in order to apply universal policies to cloud VMs.



Universal Policy Administrator Components	Description
Web Console	A browser based console that Interfaces dashboards and management consoles for universal policies, associated roles, domains, OUs, users, groups, agent versions, environments, view session and event details and so on.

## Understanding the Workflow

Universal Policy Administrator has multiple components depicted in the architecture diagram below:



A high-level Universal Policy Administrator change management workflow includes the following steps:

- 1 Create a new Universal Policy in the Web Console or import GPOs from your production Active Directory environment into the Web Console of the Universal Policy Administrator and save as a Universal Policy.
- 2 Check out a Universal Policy, locking it from changes by other users.
- 3 Edit the Universal Policy as needed.
- 4 Check in the updated Universal Policy, unlocking the Universal Policy and updating its version number.
- 5 Analyze the Universal Policy to verify your changes (for example, RSoP analysis), and then approve the policy.
- 6 Export to Active Directory.

# Using the Web Console

You can identify and manage domain joined Mac and Linux devices, both on premises and cloud, on a browser to improve security and provide better visibility into the infrastructure from any supported device and location.

You can sort devices to list by **Environments**, **Agent Versions** and **Connections**. Environments include Windows and non Windows; Connections include devices joined on premises, Cloud AD along with Domain or Cloud non joined. Thus, this single dashboard centralizes device and policy management beyond your organization as well

To add a web console, you must first set up your web server in Microsoft Azure. Following tabs and associated information is displayed in the Web Console, to an Administrator:

- ◆ **Administration:** You can search and view roles, role details, and subscribed role notifications.
- ◆ **Organization:** You can view and manage Cloud based OUs and Domain based OUs and GPOs.
- ◆ **Universal Policies:** You can view and manage Linux, Mac and Windows policies and also create **Universal Policies** or import existing policies from a GPO in Active Directory and save them as universal policies. You can also:
  - ◆ Modify, approve, deploy (to agent machines) and export (to AD as GPOs) existing policies
  - ◆ Delete policies
  - ◆ Refresh policies
- ◆ **Devices:** You can view a dashboard and manage environments, agents versions and connection types across the Universal Policy Administrator infrastructure on premises, cloud and devices.

---

**NOTE:** You can link an available Universal Policy to a selected device.

---

- ◆ **Auditing:** You can search for and view User Session and Event audit information from a consolidated user interface.

# 2 Installing Universal Policy Administrator

This section contains information that will help you understand the following:

- [“Installation Checklist” on page 11](#)
- [“Installing Universal Policy Administrator Components” on page 12](#)
- [“Installing the Universal Policy Administrator Cloud Gateway in Microsoft Azure” on page 12](#)
- [“Installing the Universal Policy Administrator Cloud Gateway, On Premises” on page 15](#)
- [“Installing the Universal Policy Administrator On Premises Gateway” on page 16](#)
- [“Installing the Universal Policy Administrator Windows Agent” on page 18](#)
- [“Non Windows Agent Requirements and Installations” on page 19](#)
- [“Licensing Universal Policy Administrator On Premises Gateway and Agents” on page 25](#)

## Installation Checklist

The following checklist provides Universal Policy Administrator installation tasks. Review the information in this section before installing non Windows Universal Policy Administrator Agents.

	Task	See
<input type="checkbox"/>	Review the information about how Universal Policy Administrator works.	<a href="#">“Understanding Universal Policy Administrator” on page 7</a>
<input type="checkbox"/>	Ensure your user account has the necessary permissions to complete the installation and the computers on which you want to install Universal Policy Administrator components meet minimum hardware and software requirements.	<a href="#">Hardware Requirements</a> <a href="#">Software Requirements</a>
<input type="checkbox"/>	Determine and install Universal Policy Administrator components.	<a href="#">“Installing the Universal Policy Administrator Cloud Gateway in Microsoft Azure” on page 12</a> <a href="#">“Installing the Universal Policy Administrator On Premises Gateway” on page 16</a> <a href="#">“Installing the Universal Policy Administrator Linux Agent” on page 20</a> <a href="#">“Installing the Universal Policy Administrator Windows Agent” on page 18</a> <a href="#">“Installing the Universal Policy Administrator Mac Agent” on page 23</a>
<input type="checkbox"/>	Make any post-installation configurations.	<a href="#">Chapter 3, “Configuring Universal Policy Administrator,” on page 27</a>

# Installing Universal Policy Administrator Components


To complete an installation of Universal Policy Administrator you must install the following components and agents relevant to your environment:

- ◆ Universal Policy Administrator Cloud Gateway  
For more information, see [“Installing the Universal Policy Administrator Cloud Gateway in Microsoft Azure” on page 12](#)
- ◆ Universal Policy Administrator On Premises Gateway  
For more information, see [“Installing the Universal Policy Administrator On Premises Gateway” on page 16](#)
- ◆ Universal Policy Administrator Windows Agent  
For more information, see [“Installing the Universal Policy Administrator Windows Agent” on page 18](#)
- ◆ Universal Policy Administrator Linux Agent  
For more information, see [“Installing the Universal Policy Administrator Linux Agent” on page 20](#)
- ◆ Universal Policy Administrator Mac Agent  
For more information, see [“Installing the Universal Policy Administrator Mac Agent” on page 23](#)

## Installing the Universal Policy Administrator Cloud Gateway in Microsoft Azure

The Universal Policy Administrator Cloud Gateway is used to bridge non Windows virtual machines (VMs) in the cloud with the Universal Policy Administrator on premises Gateway and push universal policies created on the Cloud Gateway to cloud non Windows VMs.

### To set up the Universal Policy Administrator Cloud Gateway:

- 1 Create a Resource Group.  
For more information, see [Create Resource Groups on Azure](#).
- 2 Create an Azure SQL Database.  
For more information, see [Create a SQL Database on Azure](#).
- 3 Prepare the Azure Environment:
  1. Click  from the blade to open the Azure Cloud Shell.
  2. Execute the following commands in the Azure Cloud Shell to create a deployment directory in the Azure Shell Cloud Drive with your deployment name:

```
PS /home/your-account-name> cd clouddrive
PS /home/your-account-name/clouddrive> mkdir your-deployment-name
PS /home/your-account-name/clouddrive> cd your-deployment-name
PS /home/your-account-name/clouddrive/ your-deployment-name>
```

#### 4 Deploy the Cloud Gateway:

1. Execute the following command from the directory created in the Azure Cloud Shell, to copy Cloud Gateway into the Azure Cloud Drive:

```
Invoke-WebRequest -Uri https:// Your Registry Name /yaml/gatekeeper.yaml  
-OutFile gatekeeper.yaml
```

2. Edit the `gatekeeper.yaml` file with the Azure Cloud Shell editor to update the fields listed in the following table:

Field Name	Existing Field Name	Updated Name
Deployment Name	mydeployment-gatekeeper	deployment-name-gatekeeper
Database Connection String	'configure-me'	Azure SQL database connection string and database password
SSL Certificate Value	'mydeployment.com'	Wildcard SSL certificate used in the deployment
Registry Credentials	username: someuser password: password	Registry username and password assigned.
Deployment DNS Name	mydeployment-gatekeeper	deployment-name-gatekeeper

3. Execute the following command in the Azure Cloud Shell from the same directory.

```
az container create -g myResourceGroup --file gatekeeper.yaml
```

Replace *myResourceGroup* with the name of the resource group in use.

---

**NOTE:** It takes several minutes to create the Cloud Gateway container in the Resource Group and for it to begin to run.

---

#### 5 Deploy the Traversal Server:

1. Execute the following command in the Azure Cloud Shell from the directory created in the previous step, to copy the `traversal.yaml` file into the Azure Cloud Drive.

```
Invoke-WebRequest -Uri https:// Your Registry Name /yaml/traversal.yaml  
-OutFile traversal.yaml
```

2. Edit the `traversal.yaml` file with the Azure Cloud Shell editor to update the fields listed in the following table:

Field Name	Existing Field Name	Updated Name
Deployment Name	mydeployment-traversal	deployment-name-traversal
Database Connection String	'configure-me'	Azure SQL database connection string and database password
Registry Credentials	username: someuser password: password	Registry username and password assigned.
Deployment DNS Name	mydeployment-traversal	deployment-name-traversal

- Execute the following command in the Azure Cloud Shell from the same directory.

```
az container create -g myResourceGroup --file traversal.yaml
```

Replace *myResourceGroup* with the name of the resource group in use.

**NOTE:** It takes several minutes to create the Traversal Server container in the Resource Group and for it to begin to run.

- Create a Storage Account and File Share within.

For more information, see [Create a Storage Account in Azure](#) and [Create a File Share in Azure](#).

- Deploy the Front-end:

- Execute the command shown in the snippet below, in the Azure Cloud Shell from the directory created in the previous steps, to copy the `nginx.yaml` file into the Azure Cloud Drive.
- Edit the `nginx.yaml` file with the Azure Cloud Shell editor to update the fields indicated below:

Field Name	Existing Field Name	Updated Name
Deployment Name	mydeployment-nginx	deployment-name-nginx
Traversal URL Value	'https://mydeployment-traversal.eastus.azurecontainer.io'	Must be the FQDN of the Traversal Server container created in previous steps
Gatekeeper URL Value	'https://mydeployment-gatekeeperl.eastus.azurecontainer.io'	Must be the FQDN of the Cloud Gateway Server container created in previous steps
PFX file Password Value	'somepassword321'	Must be the password of your certificate.pfx file uploaded to your storage account
Registry Credentials	username: someuser password: password	Registry username and password assigned.
Deployment DNS Name	mydeployment-nginx	-deployment-name-nginx

Field Name	Existing Field Name	Updated Name
Storage Account and File Share information	myShare	Your share name created in previous steps
	someuser	
	somekey	Your Storage Account name created in previous steps
		Your Storage Account Access Key created with the Storage Account

3. Execute the following command in the Azure Cloud Shell from the same directory.

```
az container create -g myResourceGroup --file nginx.yaml
```

Replace *myResourceGroup* with the name of the resource group in use.

**NOTE:** It takes several minutes to create the NGINX Server container in the Resource Group and for it to begin to run.

## Installing the Universal Policy Administrator Cloud Gateway, On Premises

Ensure the following prerequisites are met before you install the Universal Policy Administrator Cloud Gateway, on premises:

- ◆ Microsoft SQL Server installed and running SQL Server 2016 or later.
- ◆ Microsoft Hyper-V running Docker for Desktop on a hardware system and not VM.
- ◆ Linux system or VM running Docker.

### To set up the Universal Policy Administrator Cloud Gateway, On Premises:

- 1 Create a Database on the SQL server with default settings.
- 2 Create a database connection string.
- 3 Deploy the Cloud Gateway on Docker Desktop:
  1. Create an ENV file with your database connection strings and the domain with SSL certificate where:
 

```
DATABASE_CONNECTION=Your Databse Connection String
WILDCARD_DOMAIN=Your Domain with SSL Certificate
```
  2. Login to Docker with *Your Registry Name* and run:
 

```
docker run --name Your Cloud Gateway Container Name --Your ENV file Name -p 8080:80 -d Your Registry Name/gatekeeper: Your Build Name
```
- 4 Deploy the Traversal Server on a Linux Docker System:
  1. Create an ENV file with your database connection strings and the domain with SSL certificate where:
 

```
DATABASE_CONNECTION=Your Databse Connection String
WILDCARD_DOMAIN=Your Domain with SSL Certificate
```

2. Login to Docker with *Your Registry Name* and run:

```
docker run --name Your Traversal Gateway Container Name --Your ENV file Name -p 8081:80 -d cert:/mnt/cert -d /traversal: Your Build Name
```

## 5 Deploy the NGINX Server on a Linux Docker System:

1. Create an ENV file with your database connection strings and the domain with SSL certificate where:

```
DATABASE_CONNECTION=Your Databse Connection String
```

```
WILDCARD_DOMAIN=Your Domain with SSL Certificate
```

```
TRAVERSAL_URL=http://address or IP of Traversal Host Server:8081
```

```
GATEKEEPER_URL=http://address or IP of Gatekeeper Host Server:8080
```

```
PFX_PASSWORD=Your Certificate Password
```

2. Copy your PFX to a local folder on the Linux host
3. Run the container:

```
docker run --name Your NGINX Gateway Container Name --Your ENV file Name -p 443:443 -v Your local PFX folder/cert:/mnt/cert -d Your Registry Name/nginx:Your Build Name
```

---

**NOTE:** Your certificate must be named `certificate.pfx`.

---

# Installing the Universal Policy Administrator On Premises Gateway



<http://www.youtube.com/watch?v=deTneiXynSA>

The Universal Policy Administrator On Premises Gateway is used to push policies from Active Directory to the Cloud Gateway.

When using Universal Policy Administrator to work with Universal Policies, you can use the Universal Policy Repository to effectively plan and evaluate your Universal Policy before implementing it in your production environment. The Universal Policy Repository also provides change management features.

---

**NOTE:** The Offline Repository is built and configured during the installation of the Universal Policy Administrator Gateway. After the installation, the repository is built and the Universal Policy Administrators can use the Web Console to manage domains, users, groups and Cloud OUs.

---

Ensure that the following prerequisites are met before you install the Universal Policy Administrator On-Premises Gateway:

- ◆ Microsoft Windows Server 2012 R2 or later installed and running
- ◆ Domain Administrator account access

The Universal Policy Administrator On Premises Gateway installer also installs Microsoft .Net Framework 4.7.x.



---

**NOTE:** The Universal Policy Administrator On Premises Gateway installation on a Microsoft Windows Server 2012 R2 computer upgrades Microsoft Windows PowerShell to version 5.1 through a Windows Management Framework (WMF) 5.1 update.

---

**To install the Universal Policy Administrator On Premises Gateway:**

- 1 Log in to a Member server as a domain administrator.
- 2 Download the Universal Policy Administrator On Premises Gateway installer file UPAOPG\_3.exe from the [Micro Focus Downloads](#) website.
- 3 Execute the downloaded UPAOPG\_3.exe file.
- 4 When the installation wizard opens, click **Install**.  
If .NET Framework 4.7.x is not already installed on the server, it is installed as part of the prerequisite check before the Universal Policy Administrator On Premises Gateway installation starts.
- 5 Click **Next** when the Universal Policy Administrator On Premises Gateway setup wizard opens.
- 6 Read and Accept the License Agreement, and click **Next**.
- 7 Select an installation option. The available options are:
  - ◆ NAT Traversal
  - ◆ DMZ or Port Forward

---

**NOTE:** In most cases, select **NAT Traversal**.

---

- 8 Click **Next**.
- 9 Enter domain administrator credentials and click **Next**.
- 10 Enter the Cloud Gateway URL and Universal Policy Administrator On Premises Gateway owner account credentials, and click **Next**.

---

**NOTE:** Click **Register** and create a new account if one does not exist.

---

- 11 Retain or change the default location for program installation, and then click **Next**.
- 12 Click **Install** to copy the Gateway installer files.
- 13 Click **Finish** on the last screen of the wizard to complete the installation.

## Configuring the Universal Policy Administrator Syslog Provider

You can configure Universal Policy Administrator to forward events and syslog messages to one or more SIEM solutions.

**To configure the Universal Policy Administrator Syslog Provider:**

- 1 Open the C:\Program Files\MicroFocus\AD Bridge\Gateway\WebApp\Web.Config file.
- 2 Modify the highlighted text in the following code snippet according to your environment:

```
<syslogSettings CEFVendor="Micro Focus" CEFProduct="AD Bridge"
CEFVersion="2.0">
  <Forwarders>
    <add host="localhost" port="514" senderType="UDP"
rfcType="Rfc5242" filterType="None" />
  </Forwarders>
</syslogSettings>
```

The available options for each of these attributes are:

- ◆ **senderType:** The default value is UDP.
  - ◆ TCP
  - ◆ UDP
- ◆ **rfcType:** The default value is Rfc5242.
  - ◆ Rfc5242
  - ◆ Rfc3164
- ◆ **filterType:** The default value is None.
  - ◆ SyslogOnly
  - ◆ AuditOnly
  - ◆ None

---

**NOTE:** Universal Policy Administrator 3.0 only supports the filterType attribute value, AuditOnly.

---

- 3 Set CEFVendor, CEFProduct, and CEFVersion to values of your choice.

---

**NOTE:** You can specify multiple forwarders in the same Web.Config file.

---

## Installing the Universal Policy Administrator Windows Agent

 <http://www.youtube.com/watch?v=bvA25ECLUYk>

The Universal Policy Administrator Windows Agent allows you to manage a non-domain joined Windows computer. You configure these settings in the Web Console, when installed in Cloud or Hybrid mode.

Ensure the following prerequisites are met before you install the Universal Policy Administrator Windows Agent:

- ◆ Microsoft Windows Server 2012 R2 or later, installed and running.
- ◆ Domain Administrator Account.

The Universal Policy Administrator Windows Agent installer also installs Microsoft .NET Framework 4.7.x.

---

**NOTE:** The Universal Policy Administrator Windows Agent installation on a Microsoft Windows Server 2012 R2 computer upgrades Microsoft Windows PowerShell to version 5.1 through a Windows Management Framework (WMF) 5.1 update.

---

**To install the Universal Policy Administrator Windows Agent:**

- 1 Log in to a non-domain joined Microsoft Windows Server 2012 R2 or later as a local administrator.
- 2 Download the Universal Policy Administrator Windows Agent installer file `UPA_3WindowsAgent.exe` from the [Micro Focus Downloads](#) website and copy onto the non-domain joined Windows Server.
- 3 Execute the downloaded `UPA_3WindowsAgent.exe` file.
- 4 Click **Next** when the Agent setup wizard opens.
- 5 Read and Accept the License Agreement, and click **Next**.
- 6 Select Installation Options. The available options are:
  - ◆ Hybrid
  - ◆ Cloud
- 7 Click **Next**.
- 8 Enter domain administrator credentials and click **Next**.

---

**NOTE:** The Cloud Gateway URL is pre-populated.

---

- 9 Retain or **Change** the default location for program installation, and click **Next**.
- 10 Click **Install** to begin copying files.

---

**NOTE:** If .NET Framework 4.7.x is not already installed on your Domain Controller, it is installed as a part of the prerequisite check, before the Universal Policy Administrator Windows Agent installation starts.

---

- 11 Click **Finish** on the last screen of the wizard to complete the installation.

## Non Windows Agent Requirements and Installations

Complete the following requirements before you install the Linux Agent and join Active Directory:

- ◆ Install the Linux Agent with `root` (requires administrator password)
- ◆ DNS name servers on the Linux Agent must list the Active Directory DNS servers
- ◆ The Active Directory domain is listed as one of the default search domains
- ◆ Download and install prerequisite Linux packages from respective vendors during or prior to running the Linux Agent installation. For more information, see [Additional Linux Requirements](#).

---

**NOTE:** If a prerequisite package check or installation fails, the failure notice will identify any missing prerequisites.

---

# Installing the Universal Policy Administrator Linux Agent

 <http://www.youtube.com/watch?v=JHFD2RmXaz0>

After you download the Universal Policy Administrator Linux Agent installer, unpack the installer for your specific Linux distribution. Following is an example of the files included with the final distribution installer:

- ◆ `Package_Name.rpm`
- ◆ `install.sh`
- ◆ `uninstall.sh`

---

**NOTE:** The Universal Policy Administrator Linux Agent installer also installs .Net Core 2.2, that is used during an uninstall.

---

## To install the Universal Policy Administrator Linux Agent on a Linux machine:

- 1 Copy the Linux Agent installer `UPA_3LinuxAgent.tar.gz` file applicable to your distribution onto the Linux machine.

---

Installer file	Linux distribution
<code>UPA_3LinuxAgent.tar.gz</code>	<ul style="list-style-type: none"><li>◆ RHEL 7 and 8</li><li>◆ CentOS 7 and 8</li><li>◆ Oracle Linux 7 and 8</li><li>◆ SLES 12 and 15</li><li>◆ Ubuntu 16</li><li>◆ Ubuntu 18</li></ul>

---

- 2 On the command line, log in as the `root` user and type the following command to unpack the applicable installation package: `tar xvzf <file name>`.
- 3 For all distributions except Ubuntu, execute the command again using the file name specific to your platform from the table below.  
For example: `tar xvf <file name>`

Installer file	Linux distribution
RHEL_CENT_Oracle8.tar	<ul style="list-style-type: none"> <li>◆ RHEL 8</li> <li>◆ CentOS 8</li> <li>◆ Oracle 8</li> </ul>
RHEL_CENT_Oracle7.tar	<ul style="list-style-type: none"> <li>◆ RHEL 7</li> <li>◆ CentOS 7</li> <li>◆ Oracle 7</li> </ul>
Ubuntu18.tar	Ubuntu 18
Ubuntu16.tar	Ubuntu 16
SLES15.tar	SLES 15
SLES12.tar	SLES 12

4 Verify all installer files are on the computer with the list command: `# ls`.

5 Run the `install.sh` script file as `root` to set up the Linux Agent. For example:

- ◆ `# ./install.sh`
- ◆ `#bash install.sh`

Available agent configuration types are:

(g) - Join the agent to the Cloud Gateway Only

(h) - Join the agent to the Cloud Gateway, and create an AD object for this computer (Hybrid Mode)

(n) - Don't join the agent to anything

Installation time varies depending on your environment and prerequisites that need installation. Warning messages during the installation are informational and do not necessarily require action unless you experience an installation failure.

---

**IMPORTANT:** For SUSE installations, you may receive a confirmation prompt `y/n` before the installation starts. For SUSE 15 installations, the `dotnet-runtime-2.1` installation displays a problem dependency for `libicu52-1`.

Enter `2` to ignore the dependency and enter `y` when prompted to install "NEW packages."

---

6 (Optional) Enter `g`, `h`, or `n` when prompted to join Active Directory.

---

**NOTE:** This step and the following step are optional if you want to join agent configuration type at a later time. For information about joining Agent Configuration Type after installation, see [Joining Linux Agent Configuration Type Post Installation](#).

---

7 (Optional) When prompted, provide the full domain name, the AD account with rights to join a domain, and AD account password. For example:

```
myCompany.local
administrator
<password>
```

---

**NOTE:** A fully qualified domain name (FQDN) is only required to join the agent to Active Directory.

---

During the installation, the Linux Agent is added by default to the Computers OU in Active Directory. After the installation is complete, the Linux Agent service runs on the Linux system, as demonstrated in the following example of an installation on a Red Hat distribution.

```
[root@dev-rhat22 ~]# systemctl status linuxagent.service
● linuxagent.service - LinuxAgent Service
  Loaded: loaded (/etc/systemd/system/linuxagent.service; enabled; vendor preset: disabled)
  Active: active (running) since Wed 2019-02-06 10:35:54 EST; 1min 32s ago
  Main PID: 1739 (scl)
  CGroup: /system.slice/linuxagent.service
          └─1739 /usr/bin/scl enable rh-dotnet21 /opt/rh/rh-dotnet21/root/bin/dotnet LinuxAgent.dll
            └─1740 /bin/bash /var/tmp/scl61RG3I
              └─1743 /opt/rh/rh-dotnet21/root/bin/dotnet LinuxAgent.dll

Feb 06 10:35:54 dev-rhat22.adanywhere.local systemd[1]: Started LinuxAgent Service.
Feb 06 10:35:54 dev-rhat22.adanywhere.local systemd[1]: Starting LinuxAgent Service...
[root@dev-rhat22 ~]# █
```

---

**NOTE:** For information about how to start the Linux Agent Service or verify if it is running, see [“Linux Agent Commands and Lookups”](#) on page 53.

---

## Adding a GoDaddy SSL Certificate

To add a GoDaddy SSL certificate, you must download the certificate, copy to the necessary agent machine and manually assign trust to the certificate.

---

**NOTE:** The GoDaddy SSL certificate is a prerequisite for Linux Agent installation in Cloud Gateway or Hybrid mode only.

---

### Prerequisite

Download the [gdig2.crt.pem](#) certificate from the GoDaddy Repository.

#### For RHEL 7 or CentOS 7 or Oracle Linux 7:

- 1 Copy the `gdig2.crt.pem` file to `/etc/pki/tls/certs`.
- 2 Type `ln -s /etc/pki/tls/certs/gdig2.crt.pem /etc/pki/tls/certs/27eb7704.0` and press Enter.
- 3 Type `certutil -d sql:/etc/pki/nssdb -A -t "C,C,C" -n "Go Daddy Secure Certificate Authority - G2" -i /etc/pki/tls/certs/gdig2.crt.pem` and press Enter.

#### For RHEL 8 or CentOS 8 or Oracle Linux 8:

- 1 Copy the Go Daddy Secure Certificate Authority - G2.pem file to `/usr/share/pki/ca-trust-source/anchors`.
- 2 Type `update-ca-trust` and press Enter.

### For SLES 12 and SLES 15:

- 1 Copy the certificate to `/etc/pki/trust/anchors/`.
- 2 Type `update-ca-certificates` and press Enter.
- 3 Restart the agent.

### For Ubuntu 16 and 18:

- 1 Copy the `certificate.pem` to `/usr/local/share/ca-certificates/certificate.crt`.
- 2 Type `dpkg-reconfigure ca-certificates` and press Enter.

## Installing the Universal Policy Administrator Mac Agent

The Universal Policy Administrator Mac Agent allows you to manage non-domain joined Mac computers with universal policies configured in the web user interface and installed in Cloud Gateway Only mode or native group policy tools in Hybrid mode.

Ensure the following prerequisites are met before you install the Universal Policy Administrator Mac Agent:

- ♦ macOS 10.13, 10.14 or 10.15 installed and running.
- ♦ Domain Administrator Account.

The Universal Policy Administrator Windows Agent installer also installs Microsoft .NET Framework 4.7.x.

### To install the Universal Policy Administrator Mac Agent:

- 1 Log in to a non-domain joined Mac computer as a local administrator.
- 2 Download the Universal Policy Administrator Mac Agent installer file from the [Micro Focus Downloads](#) website and copy onto the non-domain joined Mac computer.
- 3 Execute the downloaded `UPA_3MacAgent.dmg` file.
- 4 Click **Continue** when the Universal Policy Administrator Mac Agent setup wizard opens.
- 5 Click **Install** to begin copying files.
- 6 Enter the local macOS password if prompted to start `Terminal` and proceed with installation.

---

**NOTE:** ASP.NET Core 2.1 is installed as part of the prerequisite check, if not installed already and before the Universal Policy Administrator Mac Agent installation starts.

---

- 7 Choose an agent configuration type. The available options are:

- (g) - Join the agent to the Cloud Gateway Only
- (h) - Join the agent to the Cloud Gateway, and create an AD object for this computer (Hybrid Mode)
- (n) - Don't join the agent to anything

---

**NOTE:** Installation time varies depending on your environment and prerequisites that need installation. Warning messages during the installation are informational and do not necessarily require action unless you experience an installation failure.

---

8 Enter g, h, or n.

---

**NOTE:** This step optional if you want to join agent configuration type at a later time.

---

9 (Optional) Execute the `configure.sh` file from the `/opt/adb-agent/install` directory to choose from agent configuration type options as in the previous step, at a later time.

## Joining Linux Agent Configuration Type Post Installation

If you did not join your Linux computer to Active Directory or Cloud Gateway in Gateway Only or Hybrid mode when installing the Universal Policy Administrator Linux Agent, follow these instructions on the Linux Agent at a later time:

1 Open the Linux Terminal and locate the agent directory. For example:

```
cd /opt/adb-agent.
```

2 Type respective commands for given agent configuration types:

- ♦ **Active Directory:** `dotnet LinuxJoinAD.dll <full domain name> <AD Admin account name> [distinguished name of the computer OU]`

For example: `dotnet LinuxJoinAD.dll myCompany.com administrator.`

---

**NOTE:** The Linux server is on a corporate network and you choose to join Active Directory for management with native AD tools and GPOs.

---

- ♦ **Cloud Gateway:** `dotnet CloudLinuxJoin.dll <gatekeeperServer[:port]> <traversalServer[:port]> <domainUser>`

---

**NOTE:** The Linux server is in the cloud (outside the corporate network) and does not have a computer object in Active Directory. You can manage this Linux server only from the Universal Policy Administrator web console using Universal Policies.

---

- ♦ **Hybrid Mode:** `dotnet CloudLinuxJoin.dll <gatekeeperServer[:port]> <traversalServer[:port]> <domainUser> [-create-ad-object]`

---

**NOTE:** The Linux server is in the cloud (outside the corporate network) and will have a computer object in Active Directory linked to the Universal Policy Administrator Secure Gateway. Choose this option to manage your cloud Linux server with native Active Directory tools and GPOs.

---

3 Enter the AD account password when prompted.

---

**NOTE:** You can also choose to join a specified OU of Active Directory.

---



# Licensing Universal Policy Administrator On Premises Gateway and Agents

This section provides information about the following:

- ♦ [“Evaluation Licenses” on page 25](#)
- ♦ [“Enterprise Licenses” on page 25](#)

## Evaluation Licenses

The Universal Policy Administrator and associated Windows, Linux and Mac agents come with an independent built-in 30-day evaluation period for each component to use the complete functionality. To continue using after 30 days, purchase and apply the product and agents before the 30 days elapse for each installation.

For more information, contact [Micro Focus Sales](#).

To download this product, go to the [Micro Focus Downloads](#) or [Customer Care](#) website.

## Enterprise Licenses

The Universal Policy Administrator license is applied on the Universal Policy Administrator On Premises Gateway, which in turn enables the Universal Policy Administrator Web Console on the Universal Policy Administrator Cloud Gateway.

---

**NOTE:** You must purchase agent license types and numbers according to the need in your environment.

---

### To activate a Universal Policy Administrator Gateway and appropriate Agent license:

- 1 Copy the associated license file into the Universal Policy Administrator On Premises Gateway location `%PROGRAMDATA%\Micro Focus\AD Bridge\License`.
- 2 Copy the associated license file into the Windows Agent install directory.
- 3 Copy the associated license file into the Linux or Mac Agent install directory `/opt/adb-agent`.

---

**NOTE:** After the license file is copied for each component, the system picks up the licenses at license check iterations, that are run every 15 minutes.

---



# 3 Configuring Universal Policy Administrator

Universal Policy Administrator is used to manage Universal Policies, it provides a security model to ensure the safety and reliability of your Active Directory environment. This security model, implemented in the Offline Repository, enables you to enforce a secure workflow for creating, modifying, testing, approving, and deploying Universal policies to your production Active Directory environment:

- ◆ [“Service Accounts” on page 27](#)
- ◆ [“Importing Linux Custom Configuration File Settings” on page 27](#)
- ◆ [“Example of Deployment and Initial Setup” on page 28](#)

## Service Accounts

Accounts with special privileges in Universal Policy Administrator to access AD or Cloud services to accomplish specific tasks are Service Accounts. For example, an Account that exports Universal Policies to AD.

---

**NOTE:** The account you use to access AD, when you install the Universal Policy Administrator On Premises Gateway, functions as a Service Account.

---

## Importing Linux Custom Configuration File Settings

From the Configuration Files node, you can import custom settings for Configuration Files into your Linux Agent. This enables you to create Universal Policies to manage the configuration of custom or legacy applications. When you import Configuration File settings, you can do the following:

- ◆ Add new settings without removing existing settings
- ◆ Change existing settings
- ◆ Overwrite existing settings
- ◆ Create a new configuration file

### To import custom Configuration File settings:

- 1 Click **+** to add policies from the Web Console and expand the **Linux** folder.
- 2 Expand the **Linux** and the **Configuration Files** folders, then select **Add Custom Configuration File**.
- 3 Provide the path and file name for the file you want to import, and click **Add**.

If the specified configuration file does not exist, you have the option to create a new file from which you can create new custom Configuration File settings.

### To modify Configuration File settings:

- 1 Click **SSH** or **Sudoers** or a file in the Configuration Files node that you imported and do one of the following:
  - ♦ Select an existing rule and modify the attributes as desired.
  - ♦ Add a custom rule and specify the attributes as desired.
- 2 Click **Add**.

## Example of Deployment and Initial Setup

Jack a policy administrator at MF Corporation is responsible to install and configure Universal Policy Administrator across the enterprise. Therefore he runs through the installation checklist and meets the necessary hardware and software requirements, downloads and installs various Universal Policy Administrator components and agents on end points across the enterprise:

- ♦ Universal Policy Administrator Cloud Gateway in Microsoft Azure
- ♦ Universal Policy Administrator On Premises Gateway
- ♦ Universal Policy Administrator Agents (Windows, Linux or Mac)

Jack applies license keys to the Universal Policy Administrator On Premises Gateway and the Agents and configures Universal Policy Administrator within his enterprise, adds in various policy tenants in the central repository and delegate policies to his coworkers to perform policy management from the browser based web console which he is able to audit.

Jack is pleased with the consolidated and simplified policy management solution, with the oversight and assurance of security policies applied to all enterprise endpoints.

# 4 Working with Universal Policies

A Universal Policy is defined in one of two different forms - Windows or cross platform environments to centrally manage and configure user and computer objects to manage applications, operating systems, discreet individual settings on premises or in the cloud. Cross platform environments include Mac or Linux managed on premises or in the cloud. You can apply and use Mac and Linux policies interchangeably. To ease management and avoid confusion, it is recommended to define, apply and manage cross platform policies by operating system. For example: Apply Linux policies to Linux systems only.

Additional benefits of Universal Policy Administrator include the following:

- ◆ Implements a process to create, test, and deploy Universal Policies and minimize risks to your production environment
- ◆ Tracks the history of changes made to Universal Policies and restore prior versions
- ◆ Avoids changing Universal Policies directly in your production environment
- ◆ Takes advantage of features such as version control and reports
- ◆ Delegates Universal Policy administration capabilities and control the tasks each user can perform

---

**NOTE:** Universal Policy Administrator obtains descriptions of policies and permissible value ranges from Windows Server 2012 R2.

---

You can use the Universal Policy Repository to plan and evaluate your Universal Policies before implementing them in your production environment. Using the Universal Policy Repository enables you to perform a number of tasks that assist to manage Universal Policies in your Active Directory environment.

---

**NOTE:** A sub-string search in the Universal Policies tab of the web console lists all Universal Policies from the domain, if the search string matches the domain name.

---

You can view and manage Universal Policies with the Universal Policy Administrator web console. After you create, import or modify a Universal Policy, you can export it to Active Directory.

After you create, edit or merge a Universal Policy, you must check in the policy and submit for approval from the **Universal Policies** tab of the Web Console. The system then moves the policy to the appropriate approver. If approved, the policy becomes available for application in Active Directory.

---

**NOTE:** The option to submit a Universal Policy for approval becomes available only if the policy is in a checked in state.

---

- ◆ [“Creating and Checking In Universal Policies” on page 30](#)
- ◆ [“Editing and Deleting Universal Policies” on page 30](#)
- ◆ [“Merging Universal Policies” on page 31](#)

- ◆ “Approving Universal Policies” on page 31
- ◆ “Managing Universal Policy versions” on page 32
- ◆ “Exporting Universal Policies” on page 32
- ◆ “Replicating and Migrating Universal Policies” on page 33
- ◆ “Managing Non Windows Agent Services with Universal Policies” on page 33
- ◆ “Managing Non Windows Applications with Universal Policies” on page 34
- ◆ “Executing Commands with Universal Policies” on page 34
- ◆ “Managing User Logins with Universal Policies” on page 35

## Creating and Checking In Universal Policies

 <http://www.youtube.com/watch?v=hZbQaRDwSv4>

When you create a Universal Policy, Universal Policy Administrator automatically links it to the domain or OU in which you are working.

- ◆ AD
- ◆ Linux
- ◆ Cloud
- ◆ Mac
- ◆ Non Domain Windows

---

**NOTE:** The browser-based web console allows you to check out and check in universal policies as there are no external dependencies involved or any limitations on account of untrusted domain scenarios. You can also search for and edit policies simultaneously, saving both time and effort.

---

### To create a Universal Policy from the web console:

- 1 Login to the **Web Console** as an Administrator and navigate to the **Universal Policies** tab.
- 2 Click **+** to open the **New Universal Policy** dialog box.
- 3 Enter a **Name** for the New Universal Policy.
- 4 (Optional) Select **Import policies from a GPO in Active Directory** and choose policies to import.
- 5 Enter a **Domain** name.
- 6 (Optional) Select a **WMI Filter for Domain OUs** from the drop-down list.
- 7 Click **Create**.
- 8 Click **+** to select and add platform specific policies to the created Universal Policy.
- 9 Click **Add**.

## Editing and Deleting Universal Policies

### To modify a Universal Policy from the web console:

- 1 Login to the **Web Console** as an Administrator and navigate to the **Universal Policies** tab.

- 2 Select a Universal Policy and click **Checkout** if not already.
- 3 Click **Edit** to open the **Edit Universal Policy** dialog box.
- 4 Make necessary changes to the selected policy name, **Description** and **WMI Filter for Domain OUs**.
- 5 Click **Save**.
- 6 (Optional) To edit Universal Policy settings only, select a Universal Policy and select associated **Platforms**, **Sections** and **Machine Security Settings** or **Machine Policies**.
- 7 Make necessary changes and click **Save**. Alternatively click **Undo** changes or **Remove** linked settings or policies.
- 8 (Optional) To delete a Universal Policy, select a Universal Policy and click **Delete** to open the **Delete Universal Policy** dialog box.
- 9 Click **Delete**.

## Merging Universal Policies

Merge policies to reduce the number of policies, consolidate and remove redundancies to make policy management simpler.

### To merge a Universal Policy from the web console:

- 1 Login to the **Web Console** as an Administrator and navigate to the **Universal Policies** tab.
- 2 Select a Universal Policy and click **Merge**.
- 3 Enter a name for the newly merged Universal Policy.
- 4 To delete the original Universal Policy and retain only the merged Universal Policy, select the **Delete Originals** check box
- 5 Select the Universal Policy to merge with and click **Select**.
- 6 Choose to **Delete Originals** if you must.
- 7 Select a method from the **Any conflicting settings during merge should** drop down menu to resolve any conflict that might arise during the merging process.
- 8 Click **Merge**.
- 9 Select the created policy and click + to add additional settings.

## Approving Universal Policies

An approver must approve a Universal Policy, before you can use it.

### To approve a Universal Policy from the web console:

- 1 Login to the **Web Console** as an Administrator or Approver and navigate to the **Universal Policies** tab.
- 2 Select a new Universal Policy from the Universal Policies tab in the Web Console and click **Submit for Approval**.
- 3 Enter comments about your changes and click **Submit**.
- 4 The approver can **Approve** or **Reject** the policy.

---

**NOTE:** The system checks for conflicts before approval.

---

- 5 Click **Checkout** to make changes to the policy.
- 6 Select the created policy and click + to add a policy and settings.
- 7 Click **Checkin** or **Revert** to undo.

## Managing Universal Policy versions

 <http://www.youtube.com/watch?v=TNVkeK7OyoQ>

Universal Policy Administrator allows you to manage different versions of the same policy.

### Rolling Back Universal Policies

You can roll back to an earlier version of a Universal Policy.

**To roll back to a Universal Policy version from the web console:**

- 1 Login to the **Web Console** as an Administrator and navigate to the **Universal Policies** tab.
- 2 Click **Roll back** and select the policy version to roll back to open the **Roll Back Universal Policy** dialog box.
- 3 Enter **Comments** and click **Roll Back**.
- 4 Click **Submit for Approval** to open the **Submit Universal Policy for Approval** dialog box.
- 5 Click **Submit**.
- 6 The approver can **Approve** or **Reject** the policy.

---

**NOTE:** The system checks for conflicts before approval.

---

## Exporting Universal Policies

**To export a Universal Policy from the web console:**

- 1 Login to the **Web Console** as an Administrator or Exporter and navigate to the **Universal Policies** tab.
- 2 Select a Universal Policy and click **Export to Active Directory**.
- 3 Click + to open the **Export Universal Policy** dialog box.
- 4 Click + to open the **Add GPO Deployment Targets** dialog box.
- 5 Click + to open the **New GPO** dialog box.
- 6 Enter a name for the GPO and click **Add**.
- 7 Select a deployment target and click **Add**.
- 8 Click to select a **Schedule**. The available options are:
  - ◆ **Now**
  - ◆ **Later**



- 9 (Optional) To schedule for later, select an appropriate **Date** and **Time**.
- 10 Click **Save**.

## Replicating and Migrating Universal Policies

You can replicate and migrate Universal Policies between two domains managed by Universal Policy Administrator.

**To migrate a Universal Policy from one domain to another from the web console:**

- 1 Login to the **Web Console** as an Administrator and navigate to the **Universal Policies** tab.
- 2 Select an existing Universal Policy from the Universal Policies tab in the Web Console and click **Replicate**.
- 3 Enter a **New Policy Name** for the Universal Policy.
- 4 Select a **Target Domain** from the drop-down list.
- 5 Click **Next**.
- 6 Enter a **Target** role to migrate settings.
- 7 Click **Next** and then **Close**.

## Managing Non Windows Agent Services with Universal Policies

You can monitor, start, stop, and restart services on Non Windows Agent computers with Universal Policies. You can use an existing or a new policy, but the Universal Policy needs to be linked with the OU that has the agents where you want to perform the action.

---

**NOTE:** You can use the command-line interface to refresh policies.

---

Agents deliver flexible installation and configuration capability to work across enterprise and cloud. Supported Agent Install modes include agent machines joined to:

- ♦ On Premises AD
- ♦ Cloud AD
- ♦ Cloud Non AD

This allows you to monitor files in real time and for persistence of local Configuration files, outside of the Universal Policy and the Sysvol check cycle.

In addition, the cloud agent helps extend on premises AD management capabilities to cloud based resources. This permits you to leverage on premises AD authorization and authentication to improve security and reduce the number of unmanaged identities.

**To start, stop, or restart a service on an Agent computer:**

- 1 Select a Universal Policy and click **Policies** to open the **Add Policies** dialog box.
- 2 Expand the **Services** node and enter the service name. This must be the actual service name as opposed to the friendly name of the service.

3 Select the desired option and click **Add**. The available options are:

- ◆ **Start**
- ◆ **Restart**
- ◆ **Stop**

## Managing Non Windows Applications with Universal Policies

You can deploy application files on non Windows Agent computers by using Universal Policies to harden, manage, and persist application settings on these computers. With these Universal Policies in place, any attempts to modify an application configuration from the Agent computer will be overwritten by the Universal Policy configuration.

This is done from the Deploy Files node by importing existing application files into one or more Universal Policies and assigning the Universal Policies to the non Windows Agent OU. All changes going to these applications can then be managed from the Universal Policies in Active Directory.

For example, if you have a Web Service in your enterprise environment that manages user access on the Internet or Intranet by restricting communication based on IP addresses, you can modify these settings in the Universal Policy.

Before you can manage a non Windows Agent application by using a Universal Policy, the following prerequisites need to be met:

- ◆ Universal Policies must be linked to applicable non Windows agents
- ◆ You need to know the relative path for deploying the configuration file on the agent
- ◆ You need to know the location of the application file you will use to configure the group policy

### To begin managing Non Windows applications using Universal Policies:

- 1 Select a Universal Policy and click **Policies** to open the **Add Policies** dialog box.
- 2 Expand the **Linux** folder, and click the **Deploy Files** node.
- 3 Click the browse button and locate the application file.
- 4 Enter the relative path on the Linux Agent(s) where you will deploy the GPO configuration file.
- 5 Click **Add**.
- 6 Once you have the application file added to the Universal Policy make any required configuration changes from the Web Console and save your changes to apply the policy to the non Windows Agent computers.

---

**NOTE:** You can add and deploy more than one application configuration to a Universal Policy.

---

## Executing Commands with Universal Policies

You can create Universal Policies to execute commands or run shell scripts on your local computer, once or every hour.

**To execute a command:**

- 1 Click + to add policies from the Web Console and expand the **Linux** folder.
- 2 Click the **Execute Command** node.
- 3 Add a command and select **Run Once** if you choose to.
- 4 Add and save your changes.

## Managing User Logins with Universal Policies

Using universal policies, you can control which users and groups are allowed or denied to log in on Linux Agent computers in your Active Directory domain. This is accomplished by creating or modifying one or more Universal Policies and setting the login privileges for specified users or groups.

---

**NOTE:** For cloud AD logins, users or groups must be part of the MFPolicy-Users group.

---

**To configure and apply Universal Policy login settings on Linux agents:**

- 1 Click + to add policies from the Web Console and expand the **Linux** folder.
- 2 Expand the **Linux** and then the **AD Login** folders.
- 3 Select the **On-Premise** or **Cloud** folders, then **AD login provider mode**, and then select a mode in the pull-down menu.

For example, select **Simple allow/deny list**.

- 4 Click **Add** again, and select the desired rule.

---

**IMPORTANT:** When you configure a Universal Policy to prevent users or groups from logging in, this is in effect an exclusionary list for Active Directory objects. However, when you configure to “Allow AD users or groups” those objects will be the only AD users or groups that will be able to login on the Linux agents that have the Universal Policy applied. You cannot have both Allow and Deny logins in the policy at the same time.

---

- 5 Click the browse button, and use the **Select Users** dialog box to (a) define if the rule is for users or groups, (b) choose the applicable domain, and (c) locate required users and or groups that are applicable to the policy.
- 6 Save the changes to apply the policy to applicable Linux agents.

---

**NOTE:** In order for the policy to be applied to Linux Agent computers, the Linux Agent Service must be running on those devices. If the service is not running, use one of the commands below, applicable to the platform, to start the service:

- ♦ `systemctl start adb-agent.service`
  - ♦ `service adb-agent start`
-

---

**NOTE:** In order for the policy to be applied to Linux Agent computers, the Linux Agent Service must be running on those devices. If the service is not running, use one of the following commands, applicable to the platform, to start the service:

- ♦ `systemctl start adb-agent.service`
  - ♦ `service adb-agent start`
-

# 5 Working with Universal Policy Administrator Roles

You can assign several roles to Universal Policy Administrator users. Each role corresponds to one of the job functions a user performs in Universal Policy Administrator. Each role defines the security permissions required to perform the tasks in the Universal Policies Repository for associated job functions.

- ♦ [“Understanding Universal Policy Administrator Roles” on page 37](#)
- ♦ [“Adding Users to Roles” on page 39](#)
- ♦ [“Adding Groups to Roles” on page 39](#)
- ♦ [“Applying Role Notifications” on page 40](#)

## Understanding Universal Policy Administrator Roles

Universal Policy Administrator provides the following roles and permissions for one or more given platforms:

**Table 5-1** *Universal Policy Administrator Roles and Permissions*

Role	Platform	Permissions
Universal Policy Administrator Admins	All Platforms	Is the top level administrator with permissions to do everything with the system.
Windows Admin	Windows	Is the top level administrator with permission to do everything with Windows group policies.
Windows Approver	Windows	Has permission to approve, reject, or unapprove GPOs for export from the Universal Policy Repository to Active Directory. This role also has permissions to approve or unapprove ADMX files for export from the Universal Policy Repository to the central store.
Windows Auditor	Windows	Has permission to audit, GPOs exported from the Universal Policy Repository to Active Directory and ADMX files from the Universal Policy Repository to the central store.

<b>Role</b>	<b>Platform</b>	<b>Permissions</b>
Windows Editor	Windows	Has permission to send for approval and modify GPOs in the Universal Policy Repository and add ADMX files.
Windows Importer	Windows	Has permission to import GPOs from Active Directory into the Universal Policy Repository and synchronize ADMX files from the central store.
Windows Exporter	Windows	Has permission to export, GPOs from the Universal Policy Repository to Active Directory and ADMX files to the central store.
Mac Admin	Mac	Is the top level administrator with permission to do everything with Mac policies.
Mac Approver	Mac	Has permission to approve, reject, or unapprove Mac policy objects for export from the Universal Policy Repository to Active Directory.
Mac Auditor	Mac	Has permission to audit, Mac policy objects exported from the Universal Policy Repository to Active Directory.
Mac Editor	Mac	Has permission to send for approval and modify Mac policy objects in the Universal Policy Repository.
Mac Importer	Mac	Has permission to import Mac policy objects from Active Directory into the Universal Policy Repository.
Mac Exporter	Mac	Has permission to export, Mac policy objects from the Universal Policy Repository to Active Directory.
Mac Importer		Has permission to import Mac policy objects from Active Directory into the Universal Policy Repository.
Mac Exporter	Mac	Has permission to export, Mac policy objects from the Universal Policy Repository to Active Directory.

Role	Platform	Permissions
Linux Admin	Linux	Is the top level administrator with permission to do everything with Linux policies.
Linux Approver	Linux	Has permission to approve, reject, or unapprove Linux policy objects for export from the Universal Policy Repository to Active Directory.
Linux Auditor	Linux	Has permission to audit, Linux policy objects exported from the Universal Policy Repository to Active Directory.
Linux Editor	Linux	Has permission to send for approval and modify Linux policy objects in the Universal Policy Repository.
Linux Importer	Linux	Has permission to import Linux policy objects from Active Directory to the Universal Policy Repository.
Linux Exporter	Linux	Has permission to export, Linux policy objects from the Universal Policy Repository to Active Directory.

**NOTE:** If a user is assigned to multiple roles, each role is additive and permissions for the least restrictive role apply at any given time.

## Adding Users to Roles

Universal Policy Administrators can add users to roles or remove them.

### To add Users from the Web Console:

- 1 From the Web Console, select the Administration tab.
- 2 Select the relevant role to which you want to add a user, then click **Members** from the **Role Configuration** section.
- 3 To add groups, click **Include Users** to open the **Include Members** dialog box.
- 4 Select **Include Users** to add members to a role and click **Add**. Repeat to add more users.
- 5 To remove member from a role, select a user and click **Remove**.

## Adding Groups to Roles

Universal Policy Administrators can add groups to roles or remove them.

### To add Groups from the Web Console

- 1 From the Web Console, select the Administration tab.
- 2 Select the relevant role to which you want to add a group, then click **Members** from the **Role Configuration** section.
- 3 To add groups, click **Include Groups** to open the **Include Members** dialog box.
- 4 Select a **Group** and click **Add**. Repeat to add more groups.
- 5 To remove members from a role, select a group and click **Remove**.

## Applying Role Notifications

Subscribe to email role notifications to be notified of each of the Actions listed below. Each Role can select a given Action and click + to subscribe to associated Role Notifications. The available Actions are:

- ◆ Create Repository
- ◆ Delete Repository
- ◆ Checkout
- ◆ Checkin
- ◆ Revert
- ◆ Create Release



# 6 Working with Cloud OUs and Domains

Universal Policy Administrator allows you import domains and associated OUs from Active Directory. You can also add Cloud resources and save them in the familiar OU format.

---

**NOTE:** If GPO imports fail for an untrusted domain, you must configure a local group policy to disable mutual authentication for the SYSVOL share of the untrusted domain on the Universal Policy Administrator On Premises Gateway.

For more information, see [UNC Path Configuration](#)

---

- ◆ “Importing Domains and OUs” on page 41
- ◆ “Accessing Domains and OUs” on page 41
- ◆ “Creating, Editing and Deleting WMI Filters” on page 42
- ◆ “Adding and Removing Cloud OUs” on page 42
- ◆ “Linking and Activating Universal Policies and Including Agents in Cloud OUs” on page 43
- ◆ “Removing Linked Universal Policies and Agents from Cloud OUs” on page 43

## Importing Domains and OUs

 [http://www.youtube.com/watch?v=tsAVQZPZq\\_o](http://www.youtube.com/watch?v=tsAVQZPZq_o)

**To import a domain or OU into Universal Policy Administrator from the web console:**

- 1 Login to the **Web Console** as an Administrator, navigate to the **Organization** tab and click **Import** to open the **Load Active Directory OU into Repository** dialog box.
- 2 Enter the name of a **Domain** or **OU**.  
Click to select a schedule. The available options are:
  - ◆ **Now**
  - ◆ **Later**
- 3 (Optional) To schedule for later, select an appropriate **Date** and **Time**.

---

**NOTE:** You may schedule time consuming domain imports to run at night.

---

- 4 Click **OK**.

---

**NOTE:** **Reimport OU** adds a job to reimport the entire domain.

---

## Accessing Domains and OUs

You can set up Read or Read /Write Access to domains and associated OUs.

**To access domains and associated OUs in the web console:**

- 1 Login to the **Web Console** as an Administrator, navigate to the **Organization** tab, and select an imported domain.
- 2 Enter a **Username** and **Password** to set up *Read* or *Read /Write* access to the selected domain.

## Creating, Editing and Deleting WMI Filters

Windows Management Instrumentation (WMI) filters let you dynamically detect the scope of Universal Policies, based on the attributes of the targeted computer.

**To create a WMI filter:**

- 1 Login to the **Web Console** as an Administrator, navigate to the **Organization** tab, select a domain and **WMI Filters**.
- 2 Click **+** to open the **New WMI Filter** dialog box.
- 3 Enter a Filter name and click **+** to open the **Add WMI Query** dialog box.
- 4 Enter a Query.
- 5 Click **Save**.
- 6 (Optional) To edit an existing WMI filter, click **Edit** to open the **New WMI Filter** dialog box.
- 7 Make necessary changes and click **Save**.
- 8 (Optional) To delete an existing WMI filter, click **Delete** to open the **Delete WMI Filter** dialog box.
- 9 Click **Delete**.

---

**NOTE:** If the name entered for a new WMI filter already exists, upon save the existing WMI filter is overridden.

---

## Adding and Removing Cloud OUs

**To add a Cloud OU from the web console:**

- 1 Login to the **Web Console** as an Administrator, navigate to the **Organization** tab, click **Cloud** and then **+** to open the **New Cloud OU** dialog box.
- 2 Enter a **Cloud OU name** and **Description**.
- 3 Click **Create**.
- 4 (Optional) To remove a Cloud OU, select and click **Remove**.
- 5 Select created Cloud OU and click **Include Universal Policies** to open the **Edit Linked Universal Policies for the OU** dialog box.
- 6 Select one or more linked Universal Policies and click **Link**. You can also **Unlink**, **Move Up** or **Move Down**, selected Universal Policies.
- 7 Click **OK**.
- 8 Select created Cloud OU again and click **Include Agents** to open the **Include Agents** dialog box.
- 9 Select an Agent and click **Include**.

# Linking and Activating Universal Policies and Including Agents in Cloud OUs

You can link Universal Policies to a Cloud OU and also include Agents in them.

To link Universal Policies to a Cloud OU and also include Agents in them, from the web console:

- 1 Login to the **Web Console** as an Administrator, and navigate to the **Organization** tab.
- 2 Select a Cloud OU and click **Include Universal Policies** to open the **Edit Linked Universal Policies for the OU** dialog box.
- 3 Select one or more linked Universal Policies and click **Link**. You can also **Unlink**, **Move Up** or **Move Down**, selected Universal Policies.
- 4 Click **OK**.
- 5 (Optional) Select the linked Universal Policy on the **Linked Universal Policies** pane. Toggle the associated switch to **Enabled** to activate the policy.
- 6 Click **Save**.
- 7 (Optional) To include agents, select a created Cloud OU and click **Include Agents** to open the **Include Agents** dialog box.
- 8 Select an Agent and click **Include**.

---

**NOTE:** Only Universal Policies with release versions > 1 are available to link in the **Edit Linked Universal Policies for the OU** dialog box.

---

## Removing Linked Universal Policies and Agents from Cloud OUs

To remove Universal Policies and Agents from a Cloud OU using the web console:

- 1 Login to the **Web Console** as an Administrator, navigate to the **Organization** tab.
- 2 Select a Cloud OU, click **Linked Universal Policies** and click **Edit** to open the **Edit Linked Universal Policies for the OU** dialog box.
- 3 Select one or more linked Universal Policies and click **Unlink**.
- 4 Click **OK**.
- 5 Select a Cloud OU and **Agents**.
- 6 (Optional) To remove an agent type from an OU, select an agent and click **Remove Agent Type from OU**.
- 7 (Optional) To delete an agent from the system, select an agent and click **Delete Agent from System**.

---

**NOTE:** You can delete Universal Policies linked to Cloud OUs; ensure you delete only those you must.

---



# 7 Reporting on Universal Policies

Universal Policy Administrator offers reporting for Universal Policies in the Universal Policy Repository and in Active Directory, including reports that provide the following information.

## Viewing RSoP Analysis Reports

You can view RSoP analysis reports for both Cloud and Domain OUs.

**To view RSoP Analysis Reports in the web console:**

- 1 Login to the **Web Console** as an Administrator, navigate to the **Organization** tab.
- 2 (Optional) Select a **Cloud** OU with Universal Policies assigned and click **RSoP for Cloud OU**.
- 3 (Optional) Select a **Domain** OU with Universal Policies assigned and click **RSoP for Domain OU**.
- 4 View the **RSoP Report**.

---

**NOTE:** RSoP is supported for Windows Universal Policies only.

---

## Viewing Conflict Analysis Report

You can view conflict analysis reports for Universal Policies. This provides for an easy method for administrators to clean up and consolidate policies across the repository.

**To view Conflict Analysis Reports in the web console:**

- 1 Login to the **Web Console** as an Administrator, navigate to the **Universal Policies** tab.
- 2 Select a **Universal Policy** and click **Conflict Analysis**.
- 3 View the **Conflict Analysis Report**.

## Viewing Comparison and Differential Reports

You can view comparison and differential reports between two versions of the same Universal Policy.

**To view Comparison and Differential Reports in the web console:**

- 1 Login to the **Web Console** as an Administrator, navigate to the **Universal Policies** tab.
- 2 Select a **Universal Policy** and click **Changes**.
- 3 Click **Compare last two versions**.
- 4 View the changes.



# 8

## Uninstalling Universal Policy Administrator

Complete the following tasks to uninstall Universal Policy Administrator:

1. Uninstall the Universal Policy Administrator agents from respective devices.
2. Uninstall Universal Policy Administrator On Premises Gateway from the Windows Control Panel on the installed computer.
3. Delete the Universal Policy Administrator Cloud Gateway and Web User Interface container installation instances from the hosted account in Microsoft Azure.





# A Automating Universal Policy Administrator Operations with PowerShell Cmdlets

The PowerShell command-line and scripting language can be used to automate many Universal Policy tasks, including configuring registry-based policy settings. To help you perform these tasks, the Universal Policy Administrator snap-in for PowerShell provides the cmdlets covered in the following sections:

- ♦ [“Importing The PowerShell Snap-In” on page 49](#)

## Importing The PowerShell Snap-In

You must import the PowerShell snap-in for use with Universal Policy Administrator. To import, execute the cmdlet from a PowerShell prompt as in the following snippet:

```
add-pssnapin HAPI.ProviderPowershellSnapin
```

## Listing PowerShell Snap-In Cmdlets

After you load the PowerShell snap-in, to view the list of supported cmdlets you must execute the cmdlet from a PowerShell prompt as in the following snippet:

```
get-command -module HAPI.ProviderPowershellSnapin
```

The outputs provides a complete list of cmdlets that Universal Policy Administrator supports. For more information, see [“Supported PowerShell Cmdlets” on page 54](#)

## Viewing A Sample Cmdlet Detail

You can view a sample cmdlet detail from a PowerShell prompt as in the following command:

```
get-help Get-UniversalPolicy -detailedNAME
Get-UniversalPolicy
```

#### SYNTAX

```
Get-UniversalPolicy [-AllDetails <SwitchParameter>] [-BranchName
<string>] [-Domain <string>] [-LoadGPOId
<string>] [-PolicyId <string>] [-PreviousVersion <bool>] [-SectionId
<string>] [-SpecificVersion <int>] [-UPId
<string>] [<CommonParameters>]
```

#### DESCRIPTION

The `Get-UniversalPolicy` cmdlet gets the properties for a specified Universal Policy, or all Universal Policies.

#### PARAMETERS

`-LoadGPOId <string>`

Obsolete. Use `New-UniversalPolicy + Import-UniversalPolicy` instead.  
(optional) Specifies the Guid of a GPO to import into a new UP.

`-load <string>`

Obsolete. Use `New-UniversalPolicy + Import-UniversalPolicy` instead.  
(optional) Specifies the Guid of a GPO to import into a new UP.

This is an alias of the `LoadGPOId` parameter.

`-UPId <string>`

Id of the UP to retrieve. If not specified, all UPs will be retrieved.

`-PolicyId <string>`

If specified, Policy within the UP to retrieve.

`-SectionId <string>`

If specified, Section within the UP to retrieve.

`-AllDetails <SwitchParameter>`

If this flag is set, the results will include the Policies, Sections, and Settings within the UP. Otherwise, only the UP properties will be returned.

`-PreviousVersion <bool>`

True to retrieve a previous version of the UP.

`-SpecificVersion <int>`

If specified, Version of the UP to retrieve.

`-BranchName <string>`

(Optional) The branch where the Universal Policy is retrieved from.

`-Domain <string>`

(Optional) The name of the domain where the Universal Policy is

retrieved from.

*<CommonParameters>*

*This cmdlet supports the common parameters: Verbose, Debug, ErrorAction, ErrorVariable, WarningAction, WarningVariable, OutBuffer, PipelineVariable, and OutVariable. For more information,*

*see*

*about\_CommonParameters (https://go.microsoft.com/fwlink/?LinkID=113216).*

*----- EXAMPLE 1 -----*

*This example opens a HAPI session, and then retrieves all Universal Policies from the domain*

*'mydomain.com'Get-Credential | Get-HAPIConnection -url "https://dev.hapidevelopment.com"*



# B Appendix

This appendix provides information about Linux Agent commands, lookups and PowerShell cmdlets that Universal Policy Administrator supports.

- ♦ [“Linux Agent Commands and Lookups” on page 53](#)
- ♦ [“Supported PowerShell Cmdlets” on page 54](#)

## Linux Agent Commands and Lookups

The items in this section contain useful Linux commands and lookups pertaining to the Universal Policy Administrator Linux Agent.

### Start the Linux Agent Service

If the Linux Agent Service is not running, use one of the following commands, applicable to your platform, to start the service:

- ♦ `systemctl start adb-agent.service`
- ♦ `service adb-agent start`

### Verify the Linux Agent Service is running

If you want to verify that the Linux Agent Service is running, use one of the following commands, applicable to your platform, to check the status:

- ♦ `systemctl status adb-agent.service`
- ♦ `service adb-agent status`

### Check for the Linux Agent version

If you need to know what version of the Linux Agent is installed on a given Linux device, access `/opt/adb-agent` and type a `tail` command for the `version` file to show the agent version.

For example:

1. `cd /opt/adb-agent`
2. `tail version`

### View the Universal Policy Update Schedule

Installed Linux Agents are configured by default to run a pull from Active Directory every 60 minutes to check for any changes to Universal Policies. This configuration is set in the `appsettings.json` file at `/opt/adb-agent` on the Linux Agent using the “PullIntervalInMins” element.

While this configuration can be changed, modifying this file is not recommended and may involve some risk.

# Supported PowerShell Cmdlets

Universal Policy Administrator supports PowerShell cmdlets listed below:

---

1	Add-ChildToOU	Adds agents or Universal Policies to a Cloud or Repository OU.
2	Add-CloudOU	Adds a new Cloud OU into the Cloud OU tree.
3	Add-GlobalPolicySetting	Adds a policy setting to a Universal Policy.
4	Add-GroupMember	Adds a member to an Active Directory group.
5	Add-HapiGPO	Creates a Group Policy Object in Active Directory.
6	Add-HapiGPOLink	Links a GPO to a Scope.
7	Add-HapiGPOPermission	Grants the specified User/Group Permissions on a GPO.
8	Add-Notification	Enables notifications for the specified operation for members of the specified role.
9	Add-RoleMember	Adds a member to the specified role.
10	Approve-UniversalPolicy	Approves or Unapproves a Universal Policy.
11	Assign-UniversalPolicy	Assigns new Universal Policy to an agent or OU.
12	Checkin-UniversalPolicy	Checks in changes to a Universal Policy.
13	Checkout-UniversalPolicy	Checks out a Universal Policy.
14	Check-Permissions	Checks whether the logged on user is granted the specified permission.
15	Clone-UniversalPolicy	Clones a Universal Policy.
16	Deploy-UniversalPolicy	Deploys a Universal Policy.
17	Find-UniversalPolicy	Finds Universal Policies using the given search filters.
18	Find-UniversalPolicySettings	Finds settings in a given Universal Policy.
19	Get-ADComputers	Gets one or more Active Directory computers.
20	Get-ADDomainControllers	Gets the list of Active Directory Domain Controllers for the specified domain.
21	Get-ADDomains	Gets the set of Active Directory domains that can be managed by HAPI.
22	Get-ADGroups	Gets one or more Active Directory groups.
23	Get-AdmFiles	Gets ADMX definitions for policy settings.
24	Get-ADUsers	Gets one or more Active Directory users.
25	Get-AgentPolicy	Gets the policy settings for a specified agent. This cmdlet is for internal use only.
26	Get-AllOUs	Gets Repository and Cloud OUs.

---

---

27	Get-AvailablePermissions	Gets the set of permissions that are supported by a HAPI Provider.
28	Get-Categories	Gets the set of permission categories.
329	Get-CloudOU	Gets one or more Cloud OUs.
30	Get-DiffReport	Generates a report that compares two versions of a Universal Policy.
31	Get-GPSettings	Gets the policy settings for a Universal Policy.
32	Get-HAPIConnection	Logs in the user with the credentials specified.
33	Get-HapiGPO	Gets one or more Group Policy objects from Active Directory.
34	Get-HapiGPOLinks	Gets the Scopes a GPO is linked to, or the GPOs linked to a specified scope.
35	Get-HapiGPOPermissions	Gets the Scopes a GPO is linked to, or the GPOs linked to a specified scope.
36	Get-HapiGPOReport	Gets the Settings report for the specified GPO.
37	Get-HapiGPORSOPReport	Generates an RSOP report for the specified Computer and/or User.
38	Get-HapiGPSettings	Gets the Policy Settings that are defined in the specified GPO.
39	Get-JobProgress	Retrieves the completion percentage for a given job.
40	Get-LinkSites	Gets the set of objects a Universal Policy can be linked to.
41	Get-LinkSiteType	Gets the types of scopes a specified policy type can be linked to.
42	Get-MaxPermissions	Gets the set of permissions that are supported by a HAPI Provider.
43	Get-MigrationMap	Gets one or more Migration Maps from storage.
44	Get-Notification	Gets the configured notifications that match the specified criteria.
45	Get-NotificationAction	Gets the list of Actions for which Notifications can be configured.
46	Get-OUChild	Gets the child objects in a Cloud or Repository OU.
47	Get-OULinks	Gets the Universal Policies and/or Agents that are linked to a Cloud or Repository OU.
48	Get-PolicyAssignment	Gets the Policy Assignments for a Universal Policy, or Assignee.
49	Get-PolicyLink	Gets the Policy Links for a Universal Policy, or Assignee.
50	Get-PosixUsers	Gets posix attributes for one or more Active Directory users.
51	Get-RepositoryOU	Gets one or more Repository OUs.
52	Get-RepWMIFilter	Retrieves one or more WMI filters from storage.
53	Get-RoleMembers	Gets the members of the specified Role.

---

---

54	Get-Roles	Gets the list of Roles.
55	Get-RolesForUser	Gets the Roles that the currently logged on user is a member of.
56	Get-RSOPReport	Generates an RSOP report for a Universal Policy.
57	Get-SettingsReport	Generates a Settings report for a Universal Policy.
58	Get-UnassignedGlobalPolicies	Retrieves all unassigned Universal Policies.
59	Get-UniversalPolicy	Gets the properties for a specified Universal Policy, or all Universal Policies.
60	Get-WMIFilter	Gets one or more WMI Filters from Active Directory.
61	Get-WMINamespaces	Gets the set of WMI Namespaces.
62	Import-UniversalPolicy	Imports a Universal Policy.
63	Load-ADRepository	The name of the domain to load into the Repository.
64	Lock-Policy	The Lock-Policy cmdlet helps insure that the settings in a GPO match the settings in the associated Universal Policy.
65	Merge-UniversalPolicies	Merges two Universal Policies into a new Universal Policy.
66	New-AgentComputer	The name of the agent computer to add.
67	New-GPONameFilter	Creates a filter that allows you to search for a Group Policy object by name.
68	New-Group	Creates a new Active Directory group.
69	New-LdapFilter	Creates a filter that allows you to search for a User, Group, or Computer based on its properties.
70	New-LdapPropertyValue	Creates an LdapPropertyValue object.
71	New-PolicyLink	Links a Universal Policy to a Scope.
72	New-UniversalPolicy	Creates a new Universal Policy in the repository.
73	New-User	Creates a new Active Directory user.
74	New-WMIFilter	Creates a new WMI Filter in Active Directory.
75	Remove-AgentComputer	Removes an agent.
76	Remove-Group	Deletes a group from Active Directory.
77	Remove-GroupMember	Removes a member from a group in Active Directory.
78	Remove-HapiGPO	Removes a GPO from Active Directory.
79	Remove-HapiGPOLink	Removes a GPO Link from Active Directory.
80	Remove-HapiGPOPermission	Removes the specified permission entry from a GPO's permissions.
81	Remove-MigrationMap	Removes one or more Migration Maps from storage.
82	Remove-OU	Removes a Cloud or Repository OU.

---



---

83	Remove-OUChild	Removes one or more children from a Cloud or Repository OU.
84	Remove-PolicyAssignment	Removes one or more children from a Cloud or Repository OU.
85	Remove-RepWMIFilter	Removes a WMI Filter from the Repository.
86	Remove-RoleMember	Removes a member from the specified role.
87	Remove-UniversalPolicy	Removes a Universal Policy.
88	Remove-User	Deletes a user from Active Directory.
89	Remove-WMIFilter	Removes a WMI Filter from Active Directory.
90	Revert-PolicyCheckout	Reverts the Checkout of a Universal Policy.
91	Rollback-UniversalPolicy	Rolls back a Universal Policy to a previous version
92	Set-DomainCredential	Specifies credentials to manage a domain.
93	Set-Group	Updates an Active Directory group.
94	Set-HapiGPOProperties	Sets the properties of a GPO in Active Directory.
95	Set-HapiGPOSettings	Updates the Policy Settings defined in the specified GPO.
96	Set-MigrationMap	Creates or updates a Migration Map in storage.
97	Set-PolicyActivation	Activates or Deactivates a Policy Assignment.
98	Set-RepWMIFilter	Creates or Updates a WMI Filter in the Repository.
99	Set-User	Updates an Active Directory user.
100	Set-WMIFilter	Updates a WMI Filter in Active Directory.
101	Submit-UniversalPolicy	Checks out a Universal Policy.
102	Test-WMIFilter	Runs a WMI Filter to determine whether the filter is valid.
103	Unlink-PolicyFromScope	Unlinks a Policy from a Scope.
104	Update-HapiGPOLink	Updates the settings of a GPO Link.
105	Update-HapiGPOPermissions	Updates the Permissions for the specified GPO.
106	Update-OULinkOrder	Updates the link order for a child Universal Policy to a Cloud or Repository OU.
107	Update-UniversalPolicy	Updates the properties of a Universal Policy.
108	Update-UPPolicy	Updates a Policy within a Universal Policy.
109	Update-UPSection	Updates a Policy Section within a Universal Policy.

---



# C Appendix

This appendix provides information about the list of videos embedded in this guide.

1. On Premises Gateway Installation
2. Windows Agent Installation
3. Linux Agent Installation
4. Import a Domain
5. Create a Universal Policy
6. Import a GPO into Universal Policy Administrator
7. Merge Universal Policies
8. Versioning of Universal Policies
9. Conflict Analysis Report
10. Comparison Report

