opentext™

Universal Policy Administrator CE24.3(v3.5)

Administration Guide

November 2024

Legal Notice

Contents

About This Guide 7

1 Introduction 9

Understanding Universal Policy Administrator . . . 9
Benefits of Using Universal Policy Administrator . . . 9
Understanding the Universal Policy Administrator Architecture . . . 10
Universal Policy Administrator Components . . . 10
Understanding the Workflow . . . 11
Using the Web Console . . . 12

2 Installing Universal Policy Administrator 13

Installation Checklist . . . 13
Installing Universal Policy Administrator Components . . . 14
Installing the Universal Policy Administrator all-in-one On Premises Gateway . . . 15
Least Privilege Account (LPA) for Installation . . . 17
Account to install UPA Server . . . 17
Least Privilege Account for Runtime . . . 17
Installing the Universal Policy Administrator On Premises Gateway . . . 19
Configuring the Universal Policy Administrator Syslog Provider . . . 20
Installing the Universal Policy Administrator Windows Agent . . . 21
Installing Citrix GPO Snap-in to Manage the Citrix Policies . . . 22
Non Windows Agent Requirements and Installations . . . 22
Installing the Universal Policy Administrator Linux Agent . . . 23
Installing the Universal Policy Administrator Mac Agent . . . 26
Joining Linux Agent Configuration Type Post Installation . . . 27
Licensing Universal Policy Administrator On Premises Gateway and Agents . . . 27
Evaluation Licenses . . . 28
Enterprise Licenses . . . 28

3 Configuring Universal Policy Administrator 29

Service Accounts . . . 29
Importing Linux Custom Configuration File Settings . . . 29
Example of Deployment and Initial Setup . . . 30
Configuring UPA to use a Third-Party Identity Provider . . . 30
Install the UPA Gatekeeper and Gateway . . . 31
Configure the UPA application in the identity provider . . . 31
Configure UPA to use SAML or OIDC Authentication . . . 32
Configure Provisioning . . . 33
Assigning the UPA global Administrator Role to a User . . . 34
Configuring UPA Agent Login to use SAML/OIDC Login . . . 35
Windows Agent . . . 35
Linux Agent . . . 35
Configuring SAML Authentication with Microsoft ENTRA . . . 36
Configuring OIDC Authentication with Microsoft Entra . . . 38

Configuring SAML Authentication with ENTRA . . . 39
Configuring OIDC Authentication with OKTA . . . 41
Configuring SAML Authentication with Ping Identity . . . 43
Configuring OIDC Authentication with Ping Identity . . . 44
Configuring SAML Authentication with Amazon IAM . . . 46
Configuring OIDC Authentication with Ping Identity . . . 47

4 Working with Universal Policies 51

Creating and Checking In Universal Policies . . . 52
Editing and Deleting Universal Policies . . . 53
Merging Universal Policies . . . 53
Approving Universal Policies . . . 53
Managing Universal Policy versions . . . 54
Rolling Back Universal Policies . . . 54
Support for ADMX Templates . . . 54
Exporting Universal Policies and Updating OU Links . . . 55
Replicating and Migrating Universal Policies . . . 56
Managing Non Windows Agent Services with Universal Policies . . . 56
Managing Non Windows Applications with Universal Policies . . . 57
Migrating from GPA to UPA . . . 58
Managing Security Filtering . . . 58
Executing Commands with Universal Policies . . . 59
Managing User Logins with Universal Policies . . . 60
Managing Gold Universal Policy . . . 60
Managing Windows Preferences . . . 61

5 Working with Universal Policy Administrator Delegation 65

Understanding Roles, Views, and Assignments . . . 65
Adding and Editing Roles . . . 65
Using Delegation OUs to Grant Access . . . 66
Creating and Editing Views . . . 66
Creating and Editing Assignments . . . 67
Applying Role Notifications . . . 67

6 Working with Cloud OUs and Domains 69

Importing Domains and OUs . . . 69
Accessing Domains and OUs . . . 70
Creating, Editing and Deleting WMI Filters . . . 70
Adding and Removing Cloud OUs . . . 70
Linking and Activating Universal Policies and Including Agents in Cloud or Domain OUs . . . 71
Removing Linked Universal Policies and Agents from Cloud OUs . . . 71

7 Reporting on Universal Policies 73

Viewing RSoP Analysis Reports . . . 73
Adding and Viewing RSoP Planning Reports . . . 73
Conflict Analysis Report . . . 73
Setting Uniqueness For Conflicts . . . 74

Universal Policy Differences Report 77
Universal Policy Settings Report 78

8 Uninstalling Universal Policy Administrator 81

A Automating Universal Policy Administrator Operations with PowerShell Cmdlets 83

Importing The PowerShell Snap-In 83
Listing PowerShell Snap-In Cmdlets 83
Viewing A Sample Cmdlet Detail 83
To View Comparison and Differential Reports with PowerShell 85

B Appendix 91

Linux Agent Commands and Lookups 91
Supported PowerShell Cmdlets 92
Troubleshooting 96
Unable to manage child, trusted, and untrusted domains. 96

About This Guide

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

Audience

This guide is written for administrators and users who will use Open Text 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 9
- "Understanding the Universal Policy Administrator Architecture" on page 10
- "Using the Web Console" on page 12

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
- Lets you quickly roll back to a last known good version of a Universal Policy
- 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.

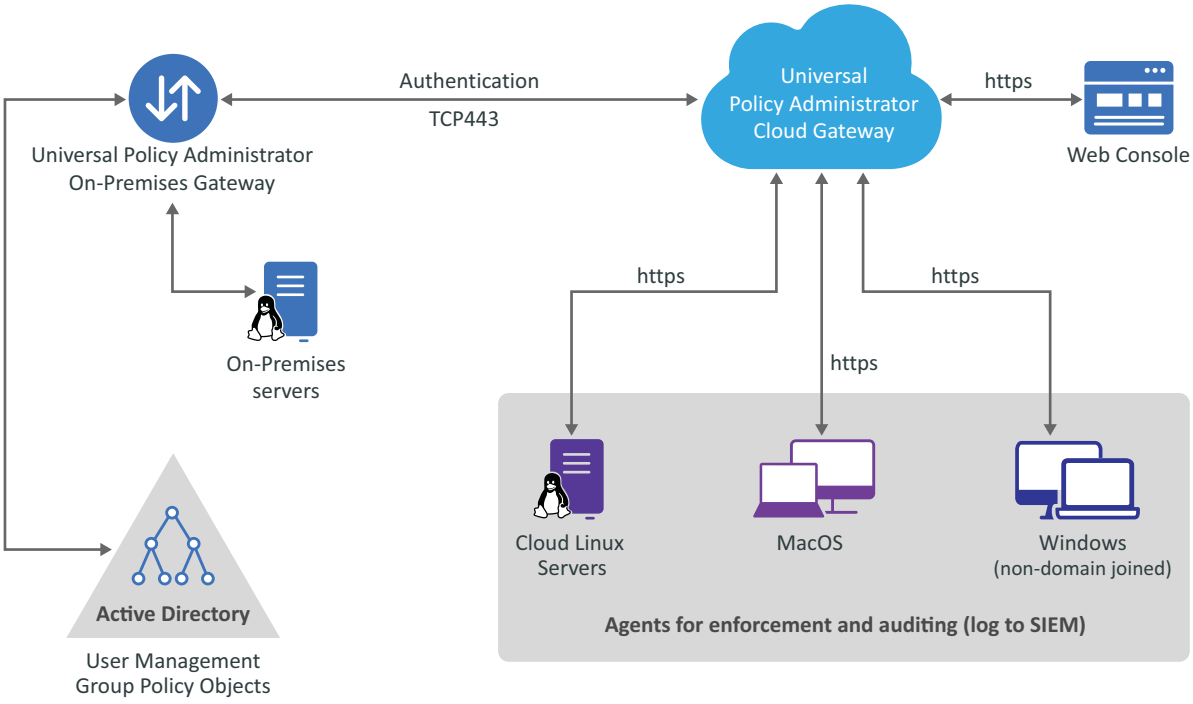
Universal Policy Administrator Components

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 performs most of the operations, including storing Universal Policies and interacting with AD.
Universal Policy Administrator Cloud Gateway	A Windows server that can be on-premises or in the cloud, interacts with the SQL database, hosts the web UI, and meters calls to the on-premises gateway.

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, unlock the Universal Policy and update 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, 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, domain-based OUs, and delegation OUs, and can link UPs and agents to those OUs
- **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 13
- "Installing Universal Policy Administrator Components" on page 14
- "Installing the Universal Policy Administrator all-in-one On Premises Gateway" on page 15
- "Least Privilege Account (LPA) for Installation" on page 17
- "Installing the Universal Policy Administrator On Premises Gateway" on page 19
- "Installing the Universal Policy Administrator Windows Agent" on page 21
- "Installing Citrix GPO Snap-in to Manage the Citrix Policies" on page 22
- "Non Windows Agent Requirements and Installations" on page 22
- "Licensing Universal Policy Administrator On Premises Gateway and Agents" on page 27

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
❑	Review the information about how Universal Policy Administrator works.	"Understanding Universal Policy Administrator" on page 9
❑	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.	Hardware Requirements Software Requirements

	Task	See
❑	Determine and install Universal Policy Administrator components.	"Installing the Universal Policy Administrator all-in-one On Premises Gateway" on page 15 "Installing the Universal Policy Administrator all-in-one On Premises Gateway" on page 15 "Installing the Universal Policy Administrator On Premises Gateway" on page 19 "Installing Citrix GPO Snap-in to Manage the Citrix Policies" on page 22 "Installing the Universal Policy Administrator Linux Agent" on page 23 "Installing the Universal Policy Administrator Windows Agent" on page 21 "Installing the Universal Policy Administrator Mac Agent" on page 26
❑	Make any post-installation configurations.	Chapter 3, "Configuring Universal Policy Administrator," on page 29

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 and On Premises Gateway

  For more information, see "Installing the Universal Policy Administrator all-in-one On Premises Gateway" on page 15
- Universal Policy Administrator Cloud Gateway, On Premises

  For more information, see "Installing the Universal Policy Administrator all-in-one On Premises Gateway" on page 15
- Universal Policy Administrator On Premises Gateway

  For more information, see "Installing the Universal Policy Administrator On Premises Gateway" on page 19
- Universal Policy Administrator Windows Agent

  For more information, see "Installing the Universal Policy Administrator Windows Agent" on page 21
- Support for Citrix Policies in Universal Policy Administrator

  For more information, see "Installing Citrix GPO Snap-in to Manage the Citrix Policies" on page 22
- Universal Policy Administrator Linux Agent

  For more information, see "Installing the Universal Policy Administrator Linux Agent" on page 23

- Universal Policy Administrator Mac Agent

  For more information, see "Installing the Universal Policy Administrator Mac Agent" on page 26

Installing the Universal Policy Administrator all-in-one On Premises Gateway

You can install Universal Policy Administrator on Cloud and on-premises using the Cloud Gateway (Gatekeeper) and Gateway installer.

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

- Domain Administrator account access
- WebServer (IIS)

The Universal Policy Administrator On Premises Gateway installer also installs Microsoft .Net Framework 4.8.x and the Microsoft-Windows-GroupPolicy-ServerAdminTools-Update.

For information about the minimum rights of the account entered during the installation, see "Least Privilege Account (LPA) for Installation" on page 17.

NOTE: The Universal Policy Administrator On Premises Gateway installation on a Microsoft Windows Server 2016 or later computer upgrades Microsoft Windows PowerShell to version 5.1 through a Windows Management Framework (WMF) 5.1 update.

NOTE: SQL Reporting component is not recommended to be installed on the same server as UPA to ensure a successful Gatekeeper installation.

To install the Universal Policy Administrator (Gatekeeper) 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 `AD Bridge Gateway.exe` from the Open Text Downloads website.
3. Execute the downloaded `AD Bridge Gateway.exe file.`
4. When the installation wizard opens, select both **Install Gatekeeper** and **Install Gateway** options and click **Install**.
5. Click **Next**.
6. Read and accept the license agreement, and click **Next**.
7. Specify a certificate in the .pfx format and enter the password for the certificate on the Certificate File Page. Click **Next**.

   NOTE: You need an SSL certificate that is trusted by clients (agents, gateways, any machine running the Web UI, and any machine one which you want to run our PowerShell cmdlets) and matches the hostname you plan to use. We recommend using an SSL certificate from a major issuer such as Sectigo or Verisign to ensure compatibility with all client platforms. If the customer is issuing their own certificate, then SNI is required.

   ---

8 Specify the connection string and SSL hostname on the Configuration wizard, and click **Next**.

9 Accept the default installation location or specify the alternate location for the installation. Click **Next**.

10 Click **Install**.

11 Click **Finish** to complete the Gatekeeper setup.

NOTE: After the Gatekeeper installation completes, the Gateway installation automatically starts.

---

12 Click **Next**.

13 Read and accept the license agreement, and click **Next**.

14 Select an installation option. The available options are:

- NAT Traversal
- DMZ or Port Forward

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

---

15 Click **Next**.

16 Enter domain administrator credentials on the Domain Credentials Page and click **Next**.

17 Enter the Cloud Gateway URL and Universal Policy Administrator On Premises Gateway owner account credentials for your tenant on the Login page and click **Next**.

NOTE: If you do not have an administrator or owner account for the tenant, click **Register** to create a new account.

---

18 Accept the default installation location or specify the alternate location for the installation. Click **Next**.

19 Click **Install**.

20 Click **Finish** to complete the Gateway installation.

To set up the Universal Policy Administrator (Gatekeeper) Cloud Gateway:

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.

1 Log in to a Member server as a domain administrator.

2 Download the Universal Policy Administrator On Premises Gateway installer `AD Bridge Gateway.exe` file from the Open Text Downloads website.

3 Execute the downloaded `AD Bridge Gateway.exe` file.

4 When the installation wizard opens, select **Install Gatekeeper** option and click **Install**.

5 Click **Next** when the Gatekeeper Installation wizard opens.

6 Read and Accept the License Agreement, and click **Next**.

7 Browse your system to select a certificate in the .pfx file format, specify the password, and click Next.

8 Specify the connection string, SSL hostname in the Configuration wizard, and click Next.

9 Select the destination folder for the installation files and click **Next**.

10 Click **Install** to copy the Gatekeeper files.

11 Click **Finish** to complete the Gatekeeper setup.

Least Privilege Account (LPA) for Installation

Account to install UPA Server

Table 2-1 *1*

Target Object	Permissions
Computer	Administrator (Local Administrator Privilege)
Database	SYSADMIN
AD Group for UPA Admin	Add Member(). LPA account should be member of the group

Least Privilege Account for Runtime

Table 2-2 *2*

Target Object	Permissions
Computer	Administrator (Local Administrator Privilege)
AD SYSTEM Container	Read Permission
AD SYSTEM Container	Write Permission
AD SYSTEM Container	Read Property
AD SYSTEM Container	Modify Property
AD SYSTEM Container	Delete Subtree
AD SYSTEM Container	Create Container Objects
AD SYSTEM Container	Delete Container Objects
AD SYSTEM Container	Create Service Connection Point Objects
AD SYSTEM Container	Delete Service Connection Point Objects
Group Policy Creator Owners Group in AD	Add Member
All GPOs in the domain	Edit, Modify, Delete. For more information, see "To Grant Full Edit Permissions for GPOs" on page 18
AD DOMAIN	RSoP Planning
AD DOMAIN	RSoP Logging

Target Object	Permissions
AD DOMAIN	Read gpLink
AD DOMAIN	Write gpLink
AD DOMAIN	Read gpOptions
AD DOMAIN	Write gpOptions
AD SITE	Read gpLink
AD SITE	Write gpLink
AD SITE	Read gpOptions
AD SITE	Write gpOptions

SQL Permissions

None (UPA installers grants the GSA when the installation is in progress).

Granting Permissions in Domain

To Grant Full Edit Permissions for GPOs

1. Grant the Export Only account FullEdit permission on all the GPOs in Active Directory using PS CmdLet "Set-GPPermission".

   Script:

   ```
   $params = @{
      All           = $true
     TargetName     = "<<Export Only account Name>>"
     TargetType     = 'User'
     PermissionLevel = 'GpoEditDeleteModifySecurity'
     Replace        = $true
   }
   Set-GPPermission @params
   ```

2. Grant the Export Only account "Link GPOs" permission on the AD Domain. For more information, see Delegate Permissions for Group Policy.

Installing the Universal Policy Administrator On Premises Gateway

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:

- Domain Administrator account access
- WebServer (IIS)

The Universal Policy Administrator On Premises Gateway installer also installs Microsoft .Net Framework 4.8.x and the Microsoft-Windows-GroupPolicy-ServerAdminTools-Update.

NOTE: The Universal Policy Administrator On Premises Gateway installation on a Microsoft Windows Server 2016 or later 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 `AD Bridge Gateway.exe` from the Open Text Downloads website.
3. Execute the downloaded `AD Bridge Gateway.exe` file. The installation wizard is displayed.
4. Select the **Install Gateway** option and click **Install**.
5. Click **Next**.
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 on the Domain Administrator Credentials page and click **Next**.

10 Enter the Cloud Gateway URL and Universal Policy Administrator On Premises Gateway owner account credentials for your tenant page on the Login page, and click **Next**.

NOTE: If you do not have an administrator or owner account for the tenant, click Register to create an account.

---

11 Accept the default installation location or specify an alternate location for installation. Click **Next**.

12 Click **Install**.

13 Click **Finish** to complete the Gateway 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\OpenText\AD Bridge\Gateway\WebApp\Web.Config` file.

2 Modify the highlighted text in the following code snippet according to your environment:

```
<syslogSettings CEFVendor="Open Text" 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 3.5 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

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 2016 or later, installed and running.
- Domain Administrator Account.

The Universal Policy Administrator Windows Agent installer also installs Microsoft .NET Framework 4.8.x.

NOTE: The Universal Policy Administrator Windows Agent installation on a Microsoft Windows Server 2016 or later 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 2016 or later as a local administrator.
2. Download the Universal Policy Administrator Windows Agent installer file `AD Bridge Agent.exe` from the Open Text Downloads website and copy onto the non-domain joined Windows Server.
3. Execute the downloaded `AD Bridge Agent.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 4.8.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.

Installing Citrix GPO Snap-in to Manage the Citrix Policies

The Citrix Policy Management snap-in allows you to manage a Citrix environment. You must install the Citrix GPO snap-in and use the web console to create a new Universal Policy and add a Citrix policy to it. Approve this policy and export the policy to the Active Directory to manage the Citrix environment.

Complete the following requirements before you install the Citrix GPO Snap-in:

- Install Gateway using the `ADBridge.exe` file. For more information, see "Installing the Universal Policy Administrator On Premises Gateway" on page 19
- Install `VC_redist.x64.msi` from the Open Text Downloads website.

To Install Citrix GPO snap-in:

1. Log in to Microsoft Windows Server 2016 or later as a local administrator.
2. Download the Universal Policy Administrator Citrix installer file `CitrixGroupPolicyManagement_x64.msi` from the Open Text Downloads website and copy onto the non-domain joined Windows Server.
3. Execute the downloaded `CitrixGroupPolicyManagement_x64.msi` file. The installation wizard is displayed.
4. Read and accept the license agreement and click **Next**.
5. Click **Finish** to complete the setup.

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 Other 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

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 6, 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_3_5_`LinuxAgents.tar.gz` file applicable to your distribution onto the Linux machine.

Installer file	Linux distribution
`UPA_3_5_LinuxAgents.tar.gz` `UPA_3_5_UbuntuAgents.tar.gz`	◆ RHEL 7, 8 and 9 ◆ SLES 12 and 15 ◆ Ubuntu 18 ◆ Ubuntu 20 ◆ Ubuntu 22

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.tar`	◆ RHEL 9 ◆ RHEL 8 ◆ RHEL 7
`Ubuntu22.tar`	Ubuntu 22
`Ubuntu20.tar`	Ubuntu 20
`Ubuntu18.tar`	Ubuntu 18
`SLES15.tar`	SLES 15
`SLES12.tar`	SLES 12

4 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:

```
(a) - Join the agent to Active Directory
(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-6` installation displays a problem dependency for `libicu52-1`.

Enter 2 to ignore the dependency and enter y when prompted to install “NEW packages.”

---

5 (Optional) Enter a, 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 later. For information about joining Agent Configuration Type after installation, see Joining Linux Agent Configuration Type Post Installation.

---

6 (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 91.

Adding a GoDaddy SSL Certificate

To add a GoDaddy SSL certificate, you must download the certificate, copy it 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 certificate from the GoDaddy Repository.

For RHEL 7:

1. Copy the gdig2.crt. and ca-certificates.crt files 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 and RHEL 9:

1. Copy the `Go Daddy Secure Certificate Authority - G2.crt` and ca-certificates.crt files 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 gdig2.crt. and ca-certificates.crt files to `/etc/pki/trust/anchors/`.
2. Type `update-ca-certificates` and press Enter.
3. Restart the agent.

For Ubuntu 18, 20 and 22:

1. Copy the `certificate.crt and gdig2.crt` 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 12, 13 or 14 installed and running.
- Domain Administrator Account.

The Universal Policy Administrator Windows Agent installer also installs Microsoft .NET Framework 4.8.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 Open Text Downloads website and copy it onto the non-domain joined Mac computer.
3. Execute the downloaded `adb-agent-macOS-3.5-arm64.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 the 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:

   ```
   (a) - Join the agent to Active Directory
   (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 a, g, h, or n.

   NOTE: This step is optional if you want to join the 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 28
- "Enterprise Licenses" on page 28

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 Open Text Sales.

To download this product, go to the Open Text 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%\Open Text\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 29
- "Importing Linux Custom Configuration File Settings" on page 29
- "Example of Deployment and Initial Setup" on page 30
- "Configuring UPA to use a Third-Party Identity Provider" on page 30

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**.

NOTE: While adding a custom configuration file using **Add Custom Configuration File**, you can use a hyphen(-) in the file name.

---

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**.

To overwrite the existing settings:

1 Click **SSH** or **Sudoers** or a file in the Configuration Files node.

2 Select **Overwrite** check box to modify an existing rule. The existing values of the **Setting** and **Rule** get overwritten with the new values.

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 delegates policies to his coworkers to perform policy management from the browser-based web console which he can 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.

Configuring UPA to use a Third-Party Identity Provider

- “Install the UPA Gatekeeper and Gateway” on page 31
- “Configure the UPA application in the identity provider” on page 31
- “Configure UPA to use SAML or OIDC Authentication” on page 32
- “Configure Provisioning” on page 33
- “Assigning the UPA global Administrator Role to a User” on page 34
- “Configuring UPA Agent Login to use SAML/OIDC Login” on page 35
- “Windows Agent” on page 35

- “Linux Agent” on page 35
- “Configuring SAML Authentication with Microsoft ENTRA” on page 36
- “Configuring OIDC Authentication with Microsoft Entra” on page 38
- “Configuring SAML Authentication with ENTRA” on page 39
- “Configuring OIDC Authentication with OKTA” on page 41
- “Configuring SAML Authentication with Ping Identity” on page 43
- “Configuring OIDC Authentication with Ping Identity” on page 44
- “Configuring SAML Authentication with Amazon IAM” on page 46
- “Configuring OIDC Authentication with Ping Identity” on page 47

Install the UPA Gatekeeper and Gateway

Install the UPA Gatekeeper and Gateway. For more information, see Chapter 2, “Installing Universal Policy Administrator,” on page 13.

Configure the UPA application in the identity provider

1. Create the Application for UPA in the identity provider’s console.
2. If the identity provider requires it, assign or grant users and groups permission to use the application.
3. Configure the authentication settings in the identity provider application.

SAML Authentication Settings

1. If the identity provider allows for importing SAML metadata, import the UPA SAML metadata into the identity provider Application or Integration.
2. The UPA SAML metadata is available at (https://<gatekeeper>/Portal/SSO/GetSPMetadata) or by clicking the **Get SAML Metadata** link in the SSO page of the UPA Owner Portal (https://<gatekeeper>/Portal/Account).
3. If the identity provider does not provide an option to import a metadata XML file, use the following values:
   - Entity ID: https://<gatekeeper>
   - Single Signon (SSO) URL: (https://<gatekeeper>/Portal/SSO/SamlACS)
   - Name ID Format: EmailAddress (recommended)
   - Single Logout (SLO) URL: (https://<gatekeeper>/Portal/SSO/SLO)

Configuring Relay State

Choose a provider name for the SAML connection. Provider name is used when configuring the SAML connection in UPA. The connection name should consist of only alphanumeric characters. Set the SAML Relay State parameter to the provider name.

Federation Metadata

Download the federation metadata from the identity provider. You will need this metadata to configure UPA in the next step.

OIDC Authentication Settings

1. Set the Redirect URI to: (https://<gatekeeper>/Portal/SSO/OIDC)
2. Set the logout URI to: (https://<gatekeeper>/Portal/SSO/Logout)
3. Make a note of the Client ID 'OpenID Connect metadata document URL'
4. Set claim type to token.

Configure UPA to use SAML or OIDC Authentication

- Sign in to the Owner portal (https://<gatekeeper>/Portal/Account) using the Owner account created during the Gatekeeper installation.
- Click the **SSO** button.

UPA SAML Authentication Settings

1. Click the **Add SAML Provider** button.
2. Specify the provider name (the same name used in the Relay State)
3. Set the Tenancy ID to 1.

IsDefault: Use this provider as the default identity provider. If IsDefault is checked, the UPA web console will use this provider for logins. If IsDefault is not checked, to log in to the UPA web console using this provider, you will need to use this URL: https://<gatekeeper>/Portal/SSO/SamlLogin?provider=<ProviderName>.

NameIdFormat: The format of the SAML NameID. This value should match the value configured on the identity provider. In most cases, EmailAddress is the recommended value.

SignatureAlgorithm: The encryption algorithm used to sign SAML requests and responses. This setting should match the configuration of the identity provider. The recommended setting is SHA_256.

Provisioning Mode

The provisioning mode determines how users and groups are imported or provisioned into UPA.

- **Automatic provisioning:** The identity provider's provisioning service makes calls to the UPA SCIM endpoint to provision users or groups.
- **SCIM connector:** UPA queries the identity provider's SCIM endpoint to retrieve user or group information.
- **Match to AD account:** In scenarios where there is a local Active Directory with user accounts synchronized with the identity provider, the SAML-authenticated user will be matched to an existing Active Directory user. In this scenario, UPA permissions can be delegated to the Active Directory users and groups.

- **Just In Time provisioning:** In this model, the customer adds a custom attribute to the user accounts, specifying the name of the UPA role assignment to which the user should be added. This value is then sent as a claim during login. When the user logs on, the user account is created in UPA and added to the specified role assignment.
- **Manual provisioning:** If the identity provider does not support automatic provisioning, the customer can use a PowerShell script to create the user and group accounts.

SAML Claims Mapping

Specify the names of the SAML claims that correspond to the user properties:

- **Require signed requests:** This setting causes all SAML requests, including logout requests, to be signed.
- **Logout URL:** If the identity provider provides a URL for single sign-out, specify it here. This setting overrides the Single Sign-out (SSO) endpoint specified in the SAML metadata.

UPA OIDC Authentication Settings

To use OIDC authentication:

1. Click the **"Add OIDC Provider"** button
2. Specify the provider name.
3. Set the Tenancy ID to 1.

IsDefault: Use this provider as the default identity provider. If IsDefault is checked, the UPA web console will use this provider for logins. If IsDefault is not checked, to log in to the UPA web console using this provider, use the following URL: https://<gatekeeper>/Portal/SSO/OIDCLogin?provider=<ProviderName>.

Config URL: The OpenID Connect metadata URL provided by the Identity Provider.

Identity Claim: The name of the OpenID Connect claim that contains the identity of the user. (Refer to the identity provider's documentation for details).

Additional Parameters

If the identity provider requires additional information to be sent with the request (such as a tenancy id, you can add it in the Additional Parameters.

Configure Provisioning

Before external users can log in to the UPA console, they must be provisioned or imported into the UPA database. UPA provides two methods for provisioning users.

Automatic Provisioning

Automatic Provisioning requires the identity provider to support SCIM provisioning. In this scenario, the identity provider's provisioning service makes SCIM calls to the UPA SCIM service to provision users and groups.

To configure automatic provisioning, you will need to configure the following settings in the identity provider's provisioning settings:

- **Scim Endpoint:** https://<gatekeeper>/api/scim
- **Authentication or Secret Token:**
  - Navigate to the SSO page in the UPA owner portal.
  - Click **Edit** for the identity provider.
  - Click **Configure Provisioning**
  - On the Configure Provisioning page, click Get SCIM Token.

Scim Connector

If the identity provider does not provide a SCIM provisioning service but exposes a SCIM endpoint, you can use the UPA SCIM Connector to import users and groups. The UPA SCIM connector queries the identity provider's SCIM endpoint to provision users and groups.

Configure the UPA SCIM Connector with the following settings:

- **Server URL:** The server name portion of the Identity Provider's SCIM endpoint (e.g., https://server.domain.com)
- **Base URL:** The relative URL to the SCIM endpoint on the identity provider (e.g., "/scim/v2").
- **AuthToken:** The authentication token (client secret) provided by the identity provider for SCIM access.
- **Import Users:** Indicates whether user information should be imported.
- I**mport Groups:** Indicates whether group information should be imported.
- **Refresh Interval:** The interval, in minutes, at which the UPA SCIM Connector should query the identity provider for changes to users and groups.

Assigning the UPA global Administrator Role to a User

- Allow time for the initial provisioning cycle to complete. (If using automatic provisioning, you can check the provisioning status in the Identity Provider's portal)
- Once the initial provisioning cycle is complete, go to the UPA Owner Portal
- Navigate to the SSO page
- Select the identity provider, and click **List Users**
- Examine the list of users to verify the imported data
- Select a user from the dropdown list and click **Set User as Global Admin**.

This user will now be able to log in to UPA at https://<gatekeeper>. On the Administration tab of the UPA web portal, this user can delegate UPA permissions to other users and groups as desired.

Configuring UPA Agent Login to use SAML/OIDC Login

For cloud/hybrid Windows or Linux agents, this feature enables users to log in to the device using their AD credentials. If SAML/OIDC login is configured, they can also use their SAML/OIDC credentials.

Since SAML/OIDC authentication requires users to authenticate directly with the identity provider, the login interface will display a URL: https://<gatekeeper>/Portal/SSO/OOB?id=<requestId>.

Users must visit this URL, which will redirect them to the identity provider to complete the login process. Afterward, a Passcode will be displayed. Users must then enter this passcode in the login interface on the client machine to complete the login.

Windows Agent

To log in using the UPA Agent Login feature, select 'UPA Login' on the login screen. By default, the UPA Agent Login feature will use the default identity provider for the gatekeeper (so if SAML/OIDC is selected as default, SAML/OIDC will be used). To allow login using a non-default provider, set AllowMultipleProviders=1.

The Windows Agent Login feature includes two components: HAPIAUTH, a custom LSA authentication package, which performs the login operations, and HAPICredentialProvider, a custom credential provider, which provides the UI displayed for the UPA Login. The settings for both these components are stored under the registry key HKLM\Software\OpenText\HAPIAUTH.

The following settings can be configured:

- GatekeeperUrl (REG_SZ): The URL of the HAPI gatekeeper.
- LogPath (REG_SZ): The path for the HAPIAuth log file (C:\ProgramData\OpenText\Logs\HapiAuth.log).
- LogLevel (REG_DWORD) (1=Debug, 2=Info, 3=Warning, 4=Error, 5=Critical): Determines the minimum severity of events to write to the log file.
- EventLogLevel (REG_DWORD) (1=Debug, 2=Info, 3=Warning, 4=Error, 5=Critical): Determines the minimum severity of events to write to the event log.
- AllowMultipleProviders (REG_DWORD) (0=Disabled, 1=Enabled): If enabled, UPA Login will display a dropdown list of identity providers (including SAML/OIDC and AD), and the user can select which provider to use for login.
- ShowQRCode (REG_DWORD) (0=Disabled, 1=Enabled): If enabled, UPA will display a link that will open a window containing a QR code. The QR code represents the login URL that the user must visit to complete the login.

NOTE: Only administrators can read the HAPIAuth.log. To view the HAPIAuth.log, use "Run as Administrator.

Linux Agent

During installation, the settings are configured to use the default identity provider. To switch to a different identity provider, update the DomainName and DomainSid properties in /etc/nss_hapi.conf.

The following settings can be configured:

1. **GatekeeperUrl:** The URL of the gatekeeper.
2. **GenerateUids:** (yes/no) Generates UID numbers for external users. If set to no, only user accounts that have a value specified in the uidNumber property are allowed to log in.
3. **UidBase:** (default=10000) - The starting number for Generated UIDs.
4. **DomainName:** The name of the Active Directory domain or SAML/OIDC provider to use for authentication.
5. **DomainSid:** For AD domains, the Domain SID. For SAML/OIDC providers, this should be set to TenancyId_ProviderId (in the HAPI Owner portal, select the identity provider, and click List Users – the DomainSid will be the first half of the unique ID for each user).

The Linux Agent Login feature includes a PAM module and NSS module. The settings for these modules are defined in /etc/nss_hapi.conf and can be configured via Universal Policy using the Linux/AD Logins/Cloud/Custom settings.

Configuring SAML Authentication with Microsoft ENTRA

1 Install the UPA Gatekeeper and Gateway.

2 Create and configure an ENTRA Enterprise Application for UPA:

- In the ENTRA console, navigate to Enterprise Applications, and select **Create a new Application**.
  - Give the application a name, and select “Integrate any other application you don't find in the gallery (Non-gallery).
  - Click Create.
- In the ENTRA console, assign Users and Groups to the Enterprise Application.
- Configure the Enterprise Application to use SAML authentication.
- In the ENTRA Enterprise Application Settings, go to Single Sign On, and select **SAML**.
- Download the HAPI SAML metadata:
  - In the UPA owner portal (https://<gatekeeper>/portal/account) (https://<gatekeeper>/portal/account), select **SSO**.
  - Click **Get SAML Metadata**.
  - Save the metadata to a file.
- In the ENTRA Application SAML settings,
  - Select **Upload metadata file** and upload the **HAPI SAML metadata**.
  - Under “Relay State” specify a domain name for UPA to use for the ENTRA users and groups (for example “ENTRA” or “MYDOMAIN”).
  - (Optional) Set Sign on URL to (https://<gatekeeper>/Portal/SSO/SamlLogin?provider=<ProviderName>) where ProviderName is the name of the SAML provider in UPA – the name you specified for RelayState.
  - Select **Download Federation Metadata** XML and save the metadata to a file.

3 Configuring UPA to use SAML authentication:

- In the UPA Owner Portal, navigate to SSO settings and click **Add SAML Provider**.

- Set the provider name to the same value used for Relay State.
- Check the IsDefault checkbox. This will set the UPA web console to use this SAML provider as the default identity provider for logins. To login with a non-default SAML provider, go to https://<gatekeeper>/Portal/SSO/SamlLogin?provider=<ProviderName>.
- Set NameIdFormat to Email Address.
- Set SignatureAlgorithm to SHA_256.
- Set provisioning mode to AutomaticProvisioning.
- Set the following values for SAML claims:

  DisplayName: (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/displayname)

  Email: (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name)

  Unique ID: (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name)
- Save the changes.

4 Setting up SCIM provisioning:

- Get a SCIM Authentication Token:
  - In the UPA Owner Portal, navigate to the SSO page
  - Select the SAML provider and click **Edit**
  - Click **Edit Provisioning**, then Get SCIM Token.
- Configure Provisioning in the Entra Console:
  - Go to the Enterprise Application's Provisioning tab.
  - Select Provisioning Mode: Automatic.
  - Under Admin Credentials/Tenant URL, specify the SCIM endpoint: https://<gatekeeper>/api/scim.
  - For Admin Credentials/Secret Token, paste the SCIM Auth Token from the first step.
  - Click **Save Changes**.
  - Click **Start Provisioning**.

5 Assigning UPA Global Administrator role:

- Wait for the initial provisioning:
  - Allow time for the initial provisioning cycle to complete. You can check the provisioning status in the Microsoft Entra portal.
- Assign Global Admin Role:
  - Once the provisioning cycle is complete, go to the UPA Owner Portal, SSO page.
  - Select the List Users button for the SAML provider.
  - Confirm that the users or groups have been imported correctly.
  - Select the user to grant Global Administrator permissions to and click **Set User** as Global Admin.

Configuring OIDC Authentication with Microsoft Entra

1. Install the UPA Gatekeeper/Gateway.
2. Create an ENTRA Enterprise Application for UPA:
   - Create an ENTRA Enterprise Application:
     - In the ENTRA console, navigate to Enterprise Applications
     - Select **Create a new Application**
     - Give the application a name and select Integrate any other application you don't find in the gallery (Non-gallery)
     - Click **Create.**
3. Assign Users and Groups:
   - In the ENTRA console, assign users and groups to the newly created Enterprise Application.
4. Configure Application Authentication:
   - In the ENTRA console, go to Applications/App Registrations
   - Select the application
   - Under Authentication, select Add a Platform and add the Web platform
   - Set Redirect URI to https://<gatekeeper>/Portal/SSO/OIDC
   - Set Front Channel Logout URL to https://<gatekeeper>/Portal/SSO/Logout
   - Check the Identity Tokens checkbox.
5. Configure UPA to use OIDC authentication.
   - You will need the following information from the ENTRA App Registration:
     - Application (client) ID
     - Directory (tenant) ID
     - OpenID Connect metadata document URL (Click on Endpoints)
   - In the UPA owner portal, on the SSO page, click **Add OIDC Provider,** and configure the following settings:
     - **Provider Name:** Specify a name for this identity provider.
     - **Tenancy ID:** Must be 1.
     - **Is Default:** Set to checked.
     - **Provisioning Mode:** Automatic Provisioning
     - **Config URL:** The OpenID Connect metadata document URL.
     - **Client ID:** The Application (client) ID
     - **Claims Mapping:** Click Configure Claims Mapping and set the following values:
       - Match login claims to users using this property: EmailAddress
       - Unique ID: email
       - Username: email
       - Email Address: email
     - **ExtraPropertyName:** tenancyId
     - **ExtraPropertyValue1:** The Directory (tenant) ID

- **ExtraPropertyName2:** scope
- **ExtraPropertyValue2:** openid email
- Click **Save Changes.**

6 Set up SCIM provisioning
- In the UPA owner portal, get a SCIM authentication token:
  - On the SSO page, select the SAML provider, and click **Edit**.
  - Click **Edit Provisioning**, then click **Get SCIM Token**.
- In the Entra console: go to the Enterprise Application's Provisioning tab.
  - Select Provisioning Mode: Automatic.
  - Under Admin Credentials/Tenant URL, specify the SCIM endpoint: https://<gatekeeper>/api/scim
- For the Admin Credentials or Secret Token:
  - Paste the Scim Auth Token from the first step
  - Click **Save Changes**
  - Click **Start Provisioning.**

7 Assign UPA Global Administrator role
- Wait for the initial provisioning cycle to complete.
- In the UPA owner portal:
  - Go to the SSO page, and select the **List Users** button for the OIDC provider.
- Confirm that the users/groups have been imported correctly:
  - Select the user to grant Global Administrator permissions to
  - Click Set User as Global Admin.

Configuring SAML Authentication with ENTRA

1 Install the UPA Gatekeeper and Gateway.

2 Create and configure an ENTRA Enterprise Application for UPA.
- In the OKTA console, go to Applications, and click "Create App Integration"
  - Select "SAML 2.0" as the authentication type.
  - Give the application a name and click Next.
  - Configure the SAML settings:
    - Single Signon URL: https://<gatekeeper>/Portal/SSO/SamlACS
    - Use this for Recipient URL and Destination URL: Checked
    - Audience URI: https://<gatekeeper>
    - Default Relay State specify a domain name for UPA to use for the ENTRA users and groups (for example "ENTRA" or "MYDOMAIN")
    - NameIDFormat: EmailAddress
    - Application Username: ENTRA Username
    - Update application username on: Create and Update

        - Under Advanced Options, upload the HAPI certificate: (On the Gatekeeper machine, the certificate can be found in C:\Program Files\OpenText\UPA\Gatekeeper\nginx\conf\certificate.crt)
        - Check the “Allow application to initiate single logout” checkbox Single Logout URL: https://<gatekeeper>/Portal/SSO/SLO
    - In the ENTRA console, Assign Users and Groups to the Application.
    - Under “Relay State” specify a domain name for UPA to use for the ENTRA users and groups (for example “ENTRA” or “MYDOMAIN”)
    - Download the ENTRA SAML metadata and save the metadata to a file.

3. Configure UPA to use SAML authentication.
    - In the UPA Owner Portal, SSO settings, click “Add SAML Provider”.
        - Set the provider name to the same value used for Relay State.
        - Check the IsDefault checkbox. This causes the UPA web console to use this SAML provider as the default identity provider for logins. To login with a non-default SAML provider, go to https://<gatekeeper>/Portal/SSO/SamlLogin?provider=<ProviderName>
        - Set NameIdFormat to Email Address.
        - Set SignatureAlgorithm to SHA_256.
        - Set provisioning mode to AutomaticProvisioning.
        - Save Changes
4. Set up SCIM provisioning
    - In the UPA owner portal, get a SCIM authentication token:
        - On the SSO page, select the SAML provider, and click Edit.
        - Click “Edit Provisioning”, then “Get SCIM Token”.
    - In the OKTA console, go to the UPA Application, and check the “Enable SCIM Provisioning” checkbox.
    - In the Provisioning/Integration tab, set the following values:
        - Scim Connector Base URL: https://<gatekeeper>/api/scim
        - Unique Identifier field for Users: username
        - Push New Users
        - Push Profile Updates
        - Push Groups
        - Authentication Mode: Http Header Token: <the SCIM token from UPA
    - Under Provisioning/To App/Attribute Mappings, remove the following mappings:
        - Manager Value

          Employee Number

          Cost Center

          Organization

          Division

Department

Manager Display Name

- Click “Save Changes.
- Click “Force Sync”

5 Assign UPA Global Administrator role

- Wait for the initial provisioning cycle to complete. Once the provisioning cycle has completed, go to the UPA owner portal, SSO page, and select the “List Users” button for the SAML provider.
- Confirm that the users/groups have been imported correctly, then select the user to grant Global Administrator permissions to, and click “Set User as Global Admin”.

Configuring OIDC Authentication with OKTA

1 Install the UPA Gatekeeper/Gateway.

2 Create and configure an OKTA Application for UPA

- In the OKTA console, click “Create App Integration”
  - Select Sign-in Method: OIDC – Open ID Connect
  - Select Application Type: Web Application
  - Specify an application name
  - Select grant types “Authorization Code”, “Refresh Token” and “Implicit (hybrid)
  - Set Sign-in redirect URI: https://<gatekeeper>/Portal/SSO/OIDC
  - Set Sign-out redirect URI: https://<gatekeeper>/Portal/SSO/Logout
- Set user/group assignments as desired.

3 Configure UPA to use OIDC authentication.

- You will need the Client ID from the OKTA Application properties.
- In the UPA owner portal, SSO page, click “Add OIDC Provider”, and configure the following settings:
  - Provider Name: Specify a name for this identity provider.
  - Tenancy ID: Must be 1.
  - Is Default: Set to checked.
  - Provisioning Mode: Automatic Provisioning
  - Config URL: https://${yourOktaDomain}/.well-known/openid-configuration (see https://developer.okta.com/docs/reference/api/oidc/#well-known-openid-configuration)
  - Client ID: The Application (client) ID
  - Configure Claims Mapping: Click "Configure Claims Mapping" and set the following values:
    - Match login claims to users using this property: EmailAddress
    - Unique ID: email

        - Username: email
        - Email Address: email
    - Click Save Changes.

4 Automatic Provisioning:

- Configure SCIM provisioning
- OKTA does not currently support SCIM provisioning for OIDC applications. In order to use OKTA provisioning, you must create a SAML Application in OKTA.
    - Create an additional Application in OKTA. Choose SAML 2.0.
    - Specify a name for the application. Specify the gatekeeper URL in the required URL fields (these values will not be used, because this App will only be used for provisioning, not authentication). Check “Enable SCIM Provisioining” and “Do not display application icon to users”.
    - In the Provisioning/Integration tab, set the following values:
        - Scim Connector Base URL: https://<gatekeeper>/api/scim
        - Unique Identifier field for Users: username
        - Push New Users
        - Push Profile Updates
        - Push Groups
        - Authentication Mode: Http Header
        - Token: <the SCIM token from UPA>
    - Under Provisioning/To App/Attribute Mappings, remove the following mappings:
        - Manager Value

          Employee Number

          Cost Center

          Organization

          Division

          Department

          Manager Display Name

          Click “Save Changes”.

          Click “Force Sync”
    - Alternatively, instead of Automatic Provisioning, you can use JustInTime provisioining to enable JustInTime provisioning:
        - In the OKTA console, in Directory/Profile Editor, create a custom attribute “UPARole” (the name of the attribute doesn’t matter).
        - Add a mapping for the custom property to the Application profile for the application.
        - Populate the UPARole for each user with the name of a role assignment in UPA.

NOTE: When the user attempts to log in to the UPA console, a SCIM user will be created for them, if one doesn't already exist. If the SCIM user has not been assigned to any roles, it will be assigned to the role specified in the UPARole property.

- In the UPA owner portal, set the provider's ProvisioiningMode to "JustInTime".
- For additional properties enter: scope "openid email profile"
- Add the following Attribute Mappings:
  - DisplayName="name"

    Email="email"

    UserName="email"

    RoleAssignment="UPARole"

5 Assign UPA Global Administrator role

- Wait for the initial provisioning cycle to complete. Once the provisioning cycle has completed, go to the UPA owner portal, SSO page, and select the "List Users" button for the OIDC provider.
- Confirm that the users/groups have been imported correctly, then select the user to grant Global Administrator permissions to, and click "Set User as Global Admin".

Configuring SAML Authentication with Ping Identity

1 Install the UPA Gatekeeper and Gateway.

2 Create and configure a Ping Identity Application for UPA.

- In the Ping Identity console, Select Applications, and click the "+" button.
  - Give the application a name, and select "SAML Application"
  - Click Configure.
- Select "Import from URL". Enter the following url: https://<gatekeeper>/Portal/SSO/GetSPMetadata and click Import, then Save.
- On the attribute mappings tab, specify the following mappings:
  - saml-subject: User ID

    email: Email Address

    username: Username
- On the configuration tab, click "Download Metadata"

3 Configure UPA to use SAML authentication.

- In the UPA Owner Portal, SSO settings, click "Add SAML Provider".
  - Specify a name for the identity provider.
  - Check the IsDefault checkbox. This causes the UPA web console to use this SAML provider as the default identity provider for logins. To login with a non-default SAML provider, go to https://<gatekeeper>/Portal/SSO/SamlLogin?provider=<ProviderName> .
  - Set NameIdFormat to Email Address.
  - Set SignatureAlgorithm to SHA_256

- Set provisioning mode to AutomaticProvisioning.
- Set the following values for SAML claims:
  - DisplayName: userName

    Email: email

    Unique ID: userName
- Save Changes.

4 Set up SCIM provisioning
- In the UPA owner portal, get a SCIM authentication token: On the SSO page, select the SAML provider, and click Edit. Click “Edit Provisioning”, then “Get SCIM Token”.
- In the PingIdentity console, go to Integrations/Provisioning/New Connection.
- Choose Connection Type: Identity Store, then choose “SCIM Outbound”.
- Specify a name for the connection and click Next.
- Set the following properties on the Configure Authentication page:
  - Scim Base URL: https://<gatekeeper>/api/scim

    Users Resource: /Users

    SCIM Version: 2.0

    Authentication method: “OAuth 2 Bearer token”

    Auth type header: Bearer

    Oauth Access Token: <the SCIM token from UPA>
- Integrations/Provisioning/Rules/New Rule.
  - Select the SCIM connection you created in the previous step.

    Configure the user filter and attribute mappings, if desired.

    Enable the rule.

5 Assign UPA Global Administrator role:
- Wait for the initial provisioning cycle to complete. You can check the provisioning status in provisioning rule on the Ping Identity portal.
- Once the provisioning cycle has completed, go to the UPA owner portal, SSO page, and select the “List Users” button for the SAML provider.
- Confirm that the users/groups have been imported correctly, then select the user to grant Global Administrator permissions to, and click “Set User as Global Admin”.

Configuring OIDC Authentication with Ping Identity

1 Install the UPA Gatekeeper and Gateway.

2 Create and configure a Ping Identity Application for UPA.
- In the Ping Identity console, Select Applications, and click the “+” button.
  - Give the application a name, and select “OIDC Web App”

    Click Save.
- Edit Configuration:
  - Response Type: Code, ID Token

Grant Type : Authorization Code

Redirect URIs: https://<gatekeeper>/Portal/SSO/OIDC https://<gatekeeper>

Token endpoint authentication method: Client Secret Basic

Initiate Login URI: https://<gatekeeper>/Portal/SSO/OIDCLogin?provider=<UPAProviderName>

- On the attribute mappings tab, specify the following mappings:
  - ub, UserID, openid
  - email, Email Address,openid
  - userName: Username, openid

3 Configure UPA to use OIDC authentication.

- You will need the following information from the configuration tab of the PingIdentity Application:
  - Application ID

    OpenID Connect metadata document URL
- In the UPA owner portal, SSO page, click “Add OIDC Provider”, and configure the following settings:
  - Provider Name: Specify a name for this identity provider.

    Tenancy ID: Must be 1.

    Is Default: Set to checked.

    Provisioning Mode: Automatic Provisioning

    Config URL: The OpenID Connect metadata document URL.

    Client ID: The Client ID

    Identity Claim: email

    Click Save Changes.

4 Set up SCIM provisioning

- In the UPA owner portal, get a SCIM authentication token: On the SSO page, select the SAML provider, and click Edit.

  Click “Edit Provisioning”, then “Get SCIM Token”.

  In the PingIdentity console, go to Integrations/Provisioning/New Connection.

  Choose Connection Type: Identity Store, then choose “SCIM Outbound”.

  Specify a name for the connection and click Next.

  Set the following properties on the Configure Authentication page:

  Scim Base URL: https://<gatekeeper>/api/scim
  - Users Resource: /Users

    SCIM Version: 2.0

    Authentication method: “OAuth 2 Bearer token”

    Auth type header: Bearer

    Oauth Access Token: <the SCIM token from UPA>

- Integrations/Provisioning/Rules/New Rule.
  - Select the SCIM connection you created in the previous step.

    Configure the user filter and attribute mappings, if desired.

    Enable the rule.

5 Assign UPA Global Administrator role:

- Wait for the initial provisioning cycle to complete. You can check the provisioning status in provisioning rule on the Ping Identity portal.

  Once the provisioning cycle has completed, go to the UPA owner portal, SSO page, and select the “List Users” button for the OIDC provider.

  Confirm that the users/groups have been imported correctly, then select the user to grant Global Administrator permissions to, and click “Set User as Global Admin”.

Configuring SAML Authentication with Amazon IAM

1 Install the UPA Gatekeeper and Gateway.

2 Create and configure an Amazon IAM Application for UPA.

- In the Amazon IAM console, Select Applications, and click "Add Application”.
  - Select “I have an application I want to set up”

    Select Application type “SAML 2.0”, and click “Next”
- Specify a name for the Application.
- Click the link to download the IAM Identity Center SAML metadata file.
- Specify the Application Start URL and Relay State:
  - Application Start URL: https://<gatekeeper>/Portal/SSO/SamlLogin?provider=<ProviderName>
  - Relay State: <ProviderName>

    Where ProviderName is the name you will give this SAML provider in the UPA owner portal.
- Download the UPA SAML metadata from: https://<gatekeeper>/Portal/SSO/GetSPMetadata and save it to a file.
- In the IAM Application Metadata section, select “Upload Application SAML Metadata file”, and select the downloaded UPA SAML metadata.
- Assign users and groups to the application as desired.

3 Configure UPA to use SAML authentication.

- Specify a name for the identity provider.

  Check the IsDefault checkbox. This causes the UPA web console to use this SAML provider as the default identity provider for logins. To login with a non-default SAML provider, go to https://<gatekeeper>/Portal/SSO/SamlLogin?provider=<ProviderName>

  Set NameIdFormat to Email Address.

  Set SignatureAlgorithm to SHA_256.

  Set provisioning mode to AutomaticProvisioning.

- Set the following values for SAML claims:
  - DisplayName: name

    Email: email

    Unique ID: name
- Save Changes.

4 Set up SCIM provisioning

- In the UPA owner portal, get a SCIM authentication token: On the SSO page, select the SAML provider, and click Edit. Click “Edit Provisioning”, then “Get SCIM Token”.

  In the PingIdentity console, go to Integrations/Provisioning/New Connection.

  Choose Connection Type: Identity Store, then choose “SCIM Outbound”.

  Specify a name for the connection and click Next.
- Set the following properties on the Configure Authentication page:
  - Scim Base URL: https://<gatekeeper>/api/scim

    Users Resource: /Users

    SCIM Version: 2.0

    Authentication method: “OAuth 2 Bearer token”

    Auth type header: Bearer

    Oauth Access Token: <the SCIM token from UPA>
- Integrations/Provisioning/Rules/New Rule.
  - Select the SCIM connection you created in the previous step.

    Configure the user filter and attribute mappings, if desired.

    Enable the rule.

5 Assign UPA Global Administrator role:

- Wait for the initial provisioning cycle to complete. You can check the provisioning status in provisioning rule on the Ping Identity portal.
- Once the provisioning cycle has completed, go to the UPA owner portal, SSO page, and select the “List Users” button for the SAML provider.
- Confirm that the users/groups have been imported correctly, then select the user to grant Global Administrator permissions to, and click “Set User as Global Admin”.

Configuring OIDC Authentication with Ping Identity

1 Install the UPA Gatekeeper and Gateway.

2 Create and configure a Ping Identity Application for UPA.

- In the Ping Identity console, Select Applications, and click the “+” button.
  - Give the application a name, and select “OIDC Web App”

    Click Save.
- Edit Configuration:
  - Response Type: Code, ID Token

    Grant Type : Authorization Code

Redirect URIs: https://<gatekeeper>/Portal/SSO/OIDChttps://<gatekeeper>

Token endpoint authentication method: Client Secret Basic Initiate Login URI: https://<gatekeeper>/Portal/SSO/OIDCLogin?provider=<UPAProviderName>

- On the attribute mappings tab, specify the following mappings:
  - ub, UserID, openid

    email, Email Address,openid

    userName: Username, openid

3 Configure UPA to use OIDC authentication.

- You will need the following information from the configuration tab of the PingIdentity Application:
  - Application ID

    OpenID Connect metadata document URL
- In the UPA owner portal, SSO page, click “Add OIDC Provider”, and configure the following settings:
  - Provider Name: Specify a name for this identity provider.

    Tenancy ID: Must be 1.

    Is Default: Set to checked.

    Provisioning Mode: Automatic Provisioning

    Config URL: The OpenID Connect metadata document URL.

    Client ID: The Client ID

    Identity Claim: email

    Click Save Changes.

4 Set up SCIM provisioning

- In the UPA owner portal, get a SCIM authentication token:

  On the SSO page, select the SAML provider, and click Edit.

  Click “Edit Provisioning”, then “Get SCIM Token”.

  In the PingIdentity console, go to Integrations/Provisioning/New Connection.

  Choose Connection Type: Identity Store, then choose “SCIM Outbound”.

  Specify a name for the connection and click Next.
- Set the following properties on the Configure Authentication page:
  - Scim Base URL: https://<gatekeeper>/api/scim

    Users Resource: /Users

    SCIM Version: 2.0

    Authentication method: “OAuth 2 Bearer token”

    Auth type header: Bearer

    Oauth Access Token: <the SCIM token from UPA>
- Integrations/Provisioning/Rules/New Rule.
  - Select the SCIM connection you created in the previous step.

Configure the user filter and attribute mappings, if desired.

Enable the rule.

5 Assign UPA Global Administrator role:

- Wait for the initial provisioning cycle to complete. You can check the provisioning status in provisioning rule on the Ping Identity portal.

  Once the provisioning cycle has completed, go to the UPA owner portal, SSO page, and select the “List Users” button for the OIDC provider.

  Confirm that the users/groups have been imported correctly, then select the user to grant Global Administrator permissions to, and click “Set User as Global Admin”.

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 2016.

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 52
- "Editing and Deleting Universal Policies" on page 53
- "Merging Universal Policies" on page 53

- “Approving Universal Policies” on page 53
- “Managing Universal Policy versions” on page 54
- “Support for ADMX Templates” on page 54
- “Exporting Universal Policies and Updating OU Links” on page 55
- “Replicating and Migrating Universal Policies” on page 56
- “Managing Non Windows Agent Services with Universal Policies” on page 56
- “Managing Non Windows Applications with Universal Policies” on page 57
- “Migrating from GPA to UPA” on page 58
- “Managing Security Filtering” on page 58
- “Executing Commands with Universal Policies” on page 59
- “Managing User Logins with Universal Policies” on page 60
- “Managing Gold Universal Policy” on page 60
- “Managing Windows Preferences” on page 61

Creating and Checking In Universal Policies

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.

NOTE: To create a Universal Policy, you must be an Administrator or have Create UP permission either at global or domain level to which the UP is linked.

To create a Universal Policy from the web console:

1. Log in 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 Log in 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 Log in 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. Log in 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.

NOTE: You need to reexport the Universal Policy to the Active Directory whenever you make changes such as linking, activating, and enforcing the Universal Policies in the Domain OU. For more information, see "Linking and Activating Universal Policies and Including Agents in Cloud or Domain OUs" on page 71.

Managing Universal Policy versions

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. Log in 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.

Support for ADMX Templates

ADMX files are XML-based administrative template files, which were introduced with Microsoft Windows Vista Service Pack 1 and used instead of ADM files. ADMX files are language-neutral and support multilingual display of policy settings. The file structure comprises a language-neutral

(.admx) file and a language-specific (.adml) resource file. Multilingual support allows administrators in different countries to work with the same ADMX files and see the descriptions of the Group Policy settings in the local language. You can only manage ADMX file-based Group Policy settings on computers running Microsoft Windows Vista Service Pack 1 or later. You can create and edit ADMXfiles using any XML-compatible editor.

Microsoft Windows manages ADMX files from the central store that is a central location in the domain. Before you install the UPA Console on a computer running Microsoft Windows Vista Service Pack 1 or later, manually create a central store on the domain controller. The central store enables you to read ADMX files from a single domain-level location on the domain controller. You cannot manage ADMX files if you do not create a central store. For more information about creating the central store, see the Microsoft Windows documentation.

The ADMX and ADML files are available in the default local policy definition folder, C:\Windows\SYSVOL\sysvol\%Domain%\Policies\PolicyDefinitions. When you install the UPA Console on a computer running Microsoft Windows Vista Service Pack 1 or later, the installation process replaces the default local policy definition folder with a local folder, \installDir\Local UPA\domain name\, and redirects all future ADMX files to the local folder. UPA uses this local folder to temporarily store and work with ADMX files.

To Include ADMX Files in the Web Console

1. Login to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a **Universal Policy**.
4. Click **+**.
5. In the **Add Policies** tab, click **Include Policy Templates.**
6. Select the templates to be included in the Universal Policy.
7. Click **Include**, to include the ADMX template to the Universal Policy.

Exporting Universal Policies and Updating OU Links

You must export the Universal Policy to the Active Directory for the approver to review and approve, and use in the system.

To export a Universal Policy from the web console:

1. Log in to the **Web Console** as an Administrator or Exporter and navigate to the **Universal Policies** tab.

   NOTE: The Universal Policy must be in Approved State to export to the Active Directory.

2. Select a Universal Policy for which you want to update the GPO and OU links and click **Export to Active Directory**.
3. Specify when you want to export the Universal Policy. Select **Now** to export the policy immediately. Select **Later** to export the policy at the specified Date and Time.
4. Click **+Include GPO**.
   - Select a GPO from the list. If the GPO that you want to include is not in the list, click New GPO to add the GPO to the list.

- Enter a name for the GPO and click Add.
- Click **Include**.

5 Select **Update All Links of This Universal Policy** to update the GPOs and OU links.

6 You can verify the linked OUs in GPMC.

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 Log in 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 Select the **Target** for the OU to which the Universal Policy is linked and click **Next**. This step is applicable only if the Universal Policy has an OU.

8 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 am 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.

Migrating from GPA to UPA

The GPA to UPA Migration feature enables administrators to seamlessly transition Group Policy Objects (GPOs) from the Group Policy Administrator (GPA) platform to the Universal Policy Administrator (UPA) environment. By leveraging this functionality, administrators can efficiently import categories and GPOs, from their Active Directory domains into UPA, ensuring a smooth migration process.

To Migrate GPO to UPA

1. Make sure, same domain is managed in the UPA.
2. In the Import-GPA-GPOs.ps1 file update the following connection strings for your specific environment:
   - $connstr - A SQL connection string (e.g. server:db:username:password)
   - $share - The share where the ps1 file is located and shared
   - $upaurl - The URL to the UPA server
   - $domain - The NETBIOS name of the domain.
3. Run the PowerShell command Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass file to bypass the digital sign.
4. Run the powershell command `.\Import-GPA-GPOs.ps1` to import the GPOs.
5. Repository GPOs are migrated to Universal Policies in UPA.
6. The GPA categories will be imported as delegation OUs in the UPA web console.

Managing Security Filtering

Using Universal Policy Administrator, you can manage the scope of policy application to selected users or groups with Security Filtering. Security filtering functions depend on the Universal Policy's source and setup.

When you import an Universal Policy from a Group Policy Object in Active Directory, by default, the imported Universal Policy applies the security filter for Authenticated Users, which targets all authenticated users in the domain. You can modify this setting as needed to apply the policy to specific users or groups.

When you create an Universal Policy without importing a Group Policy Object in Active Directory, no default security filter is applied. You must manually configure security filtering to specify the intended users or groups. If no security filters are added, the Authenticated Users group is automatically added to the Security Filtering on the Group Policy Object, upon export to Active Directory to ensure appropriate policy application.

After configuring the security filtering, you can export the policy to a GPO in AD, retaining the defined security filters.

You can view detailed insights into security filter changes through the Settings Report and Differences Report.

To Include Security Filtering from the web console:

1. Log in to the **Web Console** as an Administrator.

2 Navigate to the **Universal Policies** tab.

3 Select an **Universal Policy.**

4 On the policy tab, navigate to the **Details** menu.

5 Click **Security Filtering**.

6 In the **Security Filtering** tab, click **Include.**

7 In the dialog box, specify the users or groups to which you want to apply the policy. You can search for users or groups by entering their names in the search field.

8 Click **Include.**

9 Click **Save,** to keep your changes.

Security filtering is now configured for the selected universal policy. This configuration can be modified as needed.

To Exclude Security Filtering from the web console:

1 Log in to the **Web Console** as an Administrator.

2 Navigate to the **Universal Policies** tab.

3 Select an **Universal Policy.**

4 On the policy tab, navigate to the **Details** menu.

5 Click **Security Filtering**.

6 In the **Security Filtering** tab, click **Exclude.**

7 In the dialog box, specify the users or groups you want to exclude from the policy. You can search for users or groups by entering their names in the search field.

8 Click **Exclude.**

9 Click **Save,** to keep your changes.

The security filtering configuration is now updated for this universal policy and can be adjusted as requirements change.

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 to sign in to Linux computers in your Active Directory domain. Configure login privileges for specific users or groups to manage access effectively.

NOTE: For cloud AD computers, 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: 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`

Managing Gold Universal Policy

Using Universal Policy Administrator, you can create a Gold Universal Policy that serves as a template for other universal policies.

The Gold Universal Policy serves as the primary universal policy, containing a comprehensive set of configurations. Once a universal policy is replicated from the Gold Universal Policy, it automatically inherits all settings from the Gold Universal Policy, ensuring consistent configurations across multiple universal policies.

To Include Universal Policy Settings from Gold Universal Policy from the web console:

1. Log in to the **Web Console** as an Administrator.

2 Navigate to the **Universal Policies** tab.

3 Select a **Universal Policy** that you want to be the Gold Universal Policy.

4 On the policy tab, navigate to the **Details** menu.

5 Click **Synchronization**.

6 In the **Synchronization** tab, click **Include.**

7 Select the universal policy to inherit the settings of the Gold Universal Policy.

8 Click **Include.**

9 Click **Save,** to keep your changes.

10 In the **Synchronization** tab, select the universal policy and click **Synchronize** > **Synchronize**.

11 You can view the synchronized policies of the Gold Universal Policy in the synchronization tab.

NOTE:

- The Gold Universal Policy must be checked out to perform Synchronization.
- If the policy settings of the Gold Universal Policy is modified and synchronization is not processed for the inherited universal policies, the status of the inherited universal policies will be 'not synced'.
- The policy settings of a universal policy is overwritten by the policy settings of the Gold Universal Policy when it is synchronized with the Gold Universal Policy.
- The target UP will not show as out of sync until the status check job runs again. The job runs once a day, or you can set the 'UPGPOSyncCheckIntervalMinutes' app setting in the configuration to shorten the time.

To Exclude Universal Policy Settings from Gold Universal Policy from the web console:

1 Log in to the **Web Console** as an Administrator.

2 Navigate to the **Universal Policies** tab.

3 Select the **Gold Universal Policy.**

4 On the policy tab, navigate to the **Details** menu.

5 Click **Synchronization.**

6 In the **Synchronization** tab, select the universal policy that needs to be excluded from the Gold Universal Policy.

7 Click **Exclude.**

8 Click **Save,** to keep your changes.

Managing Windows Preferences

Using Universal Policy Administrator, you can now configure and manage various settings for Windows operating systems.

The Windows Preferences allows administrator to configure and set preferences rather than enforce policies, giving users more flexibility while still maintaining administrative control. Windows Preferences can be used to manage settings related to the Windows registry, files and folders, shortcuts, printers, network shares, and more.

The Windows Preferences lets you create multiple preference items with each preference extension. The preference items are categorized as Computer Preferences and User Preferences. The Computer Preferences and User Preferences are further categorized as Windows Settings and Control Panel Settings.

NOTE: Preference items exist only if a administrator creates them, and each preference item contains multiple properties.

Computer Preferences - Windows Settings	Computer Preferences - Control Panel Settings
Environment	Data Sources
Files	Devices
Folders	Folder Options
Ini Files	Local Users and Groups
Registry	Network Options
Network Shares	Power Options
Shortcuts	Printers
	Scheduled Tasks
	Services

User Preferences - Windows Settings	User Preferences - Control Panel Settings
Drive Maps	Data Sources
Environment	Devices
Files	Folder Options
Folders	Internet Settings
Ini Files	Local User and Groups
Registry	Network Options
shortcuts	Power Options
	Printers
	Regional Options
	Scheduled Tasks
	Start Menu

Preference Extension	Description
Environment	Creates, modifies, or deletes a persistent user or system environment variable.
Drive Maps	Creates, configures, or deletes dynamic a drive mapping.
Files	Copies or replaces files and configures their attributes, or deletes files.
Folders	Creates folders and configures their attributes, or deletes folders and their contents.
Ini Files	Creates or changes a property/value pair in an .ini file, or deletes part or all of an .ini file.
Registry	Creates, modifies, or deletes a setting in the Windows registry.
Network Shares	Creates, modifies, or deletes a share. Can configure Access-Based Enumeration.
Shortcuts	Creates, modifies, or deletes a shortcut to a file system object (such as a file, folder, drive, share, or computer), a shell object (such as a printer, desktop item, or control panel item), or a URL (such as a Web page or an FTP site).
Data Sources	Configures an ODBC system or other user data source.
Devices	Enables or disables a class or type of hardware device.
Folder Options	Modifies Folder Options in Windows Explorer, associates a file extension with a particular program, or associates a file extension with a particular class of files.
Local Users and Groups	Creates, modifies or deletes local users (performing tasks such as setting passwords) or local security groups (performing tasks such as creating restricted groups and modifying the list of members).
Network Options	Creates, modifies, or deletes a virtual private network (VPN) or dial-up network (DUN) connection.
Power Options	Configures power management options, either modifying power options or creating, modifying, or deleting a power scheme.
Printers	Creates, modifies, or deletes a local, shared, or TCP/IP printer connection.
Scheduled Tasks	Creates, modifies, or deletes a scheduled task in the Control Panel.
Services	Modifies an operating system service.

Preference Extension	Description
Internet Settings	Modifies Internet settings.
Regional Options	Configures how most programs format numbers, currencies, dates, and times for end users.
Start Menu	Modifies the look and feel of the Start menu.

To Create Windows Preference Settings:

1. Log in to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a Universal Policy from the Universal Policies tab in the Web Console and click **Windows Group Policy**.
4. In the **Windows Group Policy** tab click **Windows Preferences** to view the preference items categorized as Computer Preferences and User Preferences.
5. Select the preference settings you want to include in your policy.
6. Click **+New** to open the **Properties** tab.
7. On the **Properties** tab, select the settings needed for the preference item and click **OK**.
8. In the **Windows Preferences** tab, click **Save.**

NOTE: Specifications with * are mandatory to be entered.

To Update Windows Preference Settings:

1. Log in to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a Universal Policy from the Universal Policies tab in the Web Console and click **Windows Group Policy**.
4. In the Windows Group Policy tab click **Windows Preferences** to view the preference items categorized as Computer Preferences and User Preferences.
5. Select the preference setting you want to update in your policy.
6. In the **Preferences** tab, click on the preference you want to update.
7. Update the setting as per requirements (Edit, Delete, Enable, Disable, Move Up, Move Down and Share).
8. In the **Windows Preferences** tab, click **Save.**

5 Working with Universal Policy Administrator Delegation

The Delegation model in UPA enables you to define who can use Universal Policies, OUs, and GPOs. It allows to define who can view, create, modify, delete domains, export to, or import Universal Policies from the Active Directory. Depending on the permissions defined for a role, the user gets access to and can perform the actions on the defined selected list, such as UPs, OUs, and GPOs.

- "Understanding Roles, Views, and Assignments" on page 65
- "Adding and Editing Roles" on page 65
- "Using Delegation OUs to Grant Access" on page 66
- "Creating and Editing Views" on page 66
- "Creating and Editing Assignments" on page 67
- "Applying Role Notifications" on page 67

Understanding Roles, Views, and Assignments

Under the **Administrator** tab there are three sub-nodes, **Roles**, **Views**, and **Assignments**.

You can use these three sub-nodes to:

- Define access roles, using built-in or custom roles
- Create a View and define the scope of permissions (where permissions get applied)
- Select users and assign them to the roles on the View that you have defined

Adding and Editing Roles

Roles define a set of actions that users can perform. You can create roles and assign permissions to them. You can also modify and delete roles.

To add a role and define permissions:

1. Log in to the **Web Console** as an Administrator and navigate to the **Administrator** tab.
2. In the left pane, click **Roles**.
3. Click **New** and specify a name for the Role and click **Create**.
4. In the **Role Details** pane, Select the permissions that you want to assign to the role and click **Save**.
5. (Optional) To edit the role, select the role click **Edit** and specify a name, select or deselect permissions for the user.
6. (Optional) To delete a role, select the role and click **Delete**.

Using Delegation OUs to Grant Access

Delegation OUs are used to grant access to a set of Universal Policies. Create structured OUs to delegate abilities and add these OUs in the **Administration** tab to delegate which Universal Policies, Cloud OUs, and Repository OUs are available to each of the Delegation OUs.

To add a Delegation OU:

1. Log in to the **Web Console** as an Administrator and navigate to the **Organization** tab.
2. In the left pane, click **Delegation**.
3. To create a top-level Delegation OU, do one of the following:
   - In the left pane, click the three dots icon within the **Delegation** tab, and click **New Delegation OU**.
   - In the right pane, click **New Delegation OU.** Specify a name for the Delegation OU and click **Create**.
4. To link Universal Policies, click **Linked Universal Policies.** For more information, see "Linking and Activating Universal Policies and Including Agents in Cloud or Domain OUs" on page 71.
5. To create one or more nested OUs within the top-level Delegation OU, do one of the following:
   - In the left pane, click the three dots icon within the top-level Delegation OU, click **New Delegation OU**.
   - In the right pane, click **New**. Specify a name for the nested Delegation OU and click **Create**.

   NOTE: Create as many nested Delegation OUs as required and link Universal Policies within the Delegation OUs and nested OUs to define the scope of delegation.

Creating and Editing Views

Views define a list of universal policies, OUs, and AD OUs that be managed by users or groups. You can add, modify, and delete views.

To add a View:

1. Log in to the **Web Console** as an Administrator and navigate to the **Administrator** tab.
2. In the left pane, click **Views**.
3. Click **New.** In the **New View** window:
   1. Specify a name for the View. Click the **Universal Policies** tab. Select one or more Universal Policies.
   2. Click the **OUs** tab and select one or more OUs to **Include**.
   3. Click the **AD OUs** tab and select an AD OU. Click **Save**.
4. (Optional) To edit a View, select the View and click **Edit**. Make the required changes and click **Save**.
5. (Optional) To delete a Role, select the role and click **Delete**.

Creating and Editing Assignments

Assignments define who can perform which actions on the objects in a view. You can add, modify, and delete views.

To add an Assignment:

1. Log in to the **Web Console** as an Administrator and navigate to the **Administrator** tab.
2. In the left pane, click **Assignments**.
3. Click **+New**. In the **New Assignment** window:
    1. Specify a name for the Assignment. Click the **Include Role** tab. Select a Role.
    2. Click the **Include Views** tab and select a View to **Include**.
    3. Click the **Include Groups** tab and search for the Group you want to include or select a Group from the list to Include.
    4. Click **Include Users** tab and search for the User you want to include or select a User from the list to Include. Click **Save**.
4. (Optional) Select an Assignment and click **Edit**. Make the required changes and click **Save**.
5. (Optional) To delete an Assignment, select the Assignment and click **Delete**.

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 to 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 69
- "Accessing Domains and OUs" on page 70
- "Creating, Editing and Deleting WMI Filters" on page 70
- "Adding and Removing Cloud OUs" on page 70
- "Linking and Activating Universal Policies and Including Agents in Cloud or Domain OUs" on page 71
- "Removing Linked Universal Policies and Agents from Cloud OUs" on page 71

Importing Domains and OUs

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

1. Log in 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 fully qualified domain name (FQDN) 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. Supply the UPN name. For more information, see To access domains and associated OUs in the web console.
5. Click **OK**.

NOTE: Reimport Domain adds a job to reimport that domain. If you select a Repository OU, you can select Reimport OU to add a job to reimport that OU and it's children.

Accessing Domains and OUs

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

For information about the minimum rights of the account entered during the installation, see Least Privilege Account for Installation.

To access domains and associated OUs in the web console:

1. Log in to the **Web Console** as an Administrator, navigate to the **Organization** tab, and select an imported domain.
2. Enter the User Principle Name (UPN) and **Password** to set up *Read* or *Read /Write* access to the selected domain.

NOTE: UPN is your unique sign in name in the format username@domain.com.

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. Log in 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, the existing WMI filter is overridden when you save.

Adding and Removing Cloud OUs

To add a Cloud OU from the web console:

1. Log in 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 or Domain 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 then, from the web console:

1 Log in to the **Web Console** as an Administrator, and navigate to the **Organization** tab.

2 Select a Cloud or Domain OU and click **UPs** or **Links** respectively 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 **Save**.

5 For a Domain OU, select the linked Universal Policy on the **Linked Universal Policies** pane. Toggle the associated switch to enabled for **Active** and **Enforce** to activate the policy. This step is optional for the Cloud OUs.

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 Log in 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. Log in 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 Report and Planning**.
3. (Optional) Select a **Domain** OU with Universal Policies assigned and click **RSoP Report and Planning**.
4. View the **RSoP Report**.

Adding and Viewing RSoP Planning Reports

You can add and view RSoP planning reports that allow simulating links for both Cloud and Domain OUs.

To view RSoP Planning Reports in the web console:

1. Log in to the **Web Console** as an Administrator and navigate to the **Organization** tab.
2. Select a cloud OU with Universal Policies assigned and click **RSoP Report and Planning**.
3. To add new simulating link, click **Add Planning Item** and select the following values:
    1. A universal policy to simulate linking to OU.
    2. The target OU for the simulated link.
    3. Clear the **Enforced Settings** check box.
    4. (Optional) Specify a link order for the policy to be included in the link list.

NOTE: You can see both simulated and the linked policies in the **Contributed Policies** section.

Conflict Analysis Report

A Conflict Analysis Report shows any other Universal Policies that have the same settings as this Universal Policy but have one or more values on that setting that differ. Universal Policies with identical settings do not appear in this report. This provides for an easy method for administrators to clean up and consolidate policies across the repository.

To view Conflict Analysis Report in the Web Console:

1. Login to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a **Universal Policy**, to open the policy tab.
4. On the policy tab, navigate to the **Reports** menu.
5. Click **Conflicts**, to open the **Conflict Analysis Report** tab.
6. View the **Conflicts Analysis Report**.

To Search Specific Settings in the Conflict Analysis Report in the Web Console:

1. Login to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a **Universal Policy**, to open the policy tab.
4. On the policy tab, navigate to the **Reports** menu.
5. Click **Conflicts**, to open the **Conflict Analysis Report** tab.
6. In the **Conflict Analysis Report** tab, navigate to the search bar.
7. Click on the search bar to activate it.
8. Type in the keyword or setting name you are looking for.
9. Press **Enter** or click on the search icon to initiate the search.
10. Review the search results to find the relevant setting (The keywords are highlighted).

To Share Conflict Analysis Report in the Web Console:

1. Login to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a **Universal Policy**, to open the policy tab.
4. On the policy tab, navigate to the **Reports** menu.
5. Click **Conflicts**, to open the **Conflict Analysis Report** tab.
6. In the **Conflict Analysis Report** tab, click on the **Share Report** icon, a print dialog box will appear.
7. Choose **Save as PDF** or select the PDF printer option from the list of available printers.
8. Click the **Print** or **Save** button. A new dialog box will prompt you to choose the destination where you want to save the PDF file.
9. Select the desired location on your device and enter a file name for the PDF.
10. Click **Save** to generate the report as a PDF file.

Setting Uniqueness For Conflicts

To effectively view and use conflict reports, it is important to understand the significance of each setting type to differentiate between uniqueness and identical settings.

Table 7-1 *Registry Based Settings*

Settings	Specifications
Registry	Hive, Key, and ValueName

Table 7-2 *Linux\Mac OS Settings*

Settings	Specifications
Execute Commands	Command, Shell
Firewall	Ports, Inbound\Outbound
Configuration Files and AD Logins	Filename, SettingName (setting name for custom can be Setting Variable plus Delimiter)
Services	Name

Table 7-3 *Preference Settings*

Settings	Specifications
Environment Variable Preferences	Action, VariableName, PathValue
File Preferences	Action, SourceFile, DestinationFile
Folder Preferences	Action, PathValue
IniFile Preferences	Action, Path, Section, Property
Registry Preferences	Action, Hive, Key, ValueName
Registry Collection Preferences	Name
Shortcut Preferences	Action, Location, TargetPath, TargetType, Arguments
DataSource Preferences	Action, DSN, UserDSN, Driver
Device Preferences	DeviceClass, DeviceType
Folder Option FileType Preferences	FileExt
Folder Option Global Preferences	Always unique
Folder Option Vista Preferences	Always unique
Folder Option OpenWith Preferences	Action, FileExtension
Local Group Preferences	Action, GroupName
Local User Preferences	Action, UserName
Network DialUp Preferences	Action, ConnectionName
Network VPN Preferences	Action, ConnectionName
Power Power Options Preferences	Always Unique
Power Power Scheme Preferences	Action, Name, PowerScheme

Settings	Specifications
Power Power Plan Preferences	Name, NameGuid
Printer Local Preferences	Action, Name
Printer Port Preferences	Action, IPAddress
Printer Shared Preferences	Action, Path
Task Trigger	Type
Task Scheduled Preferences	Action, TaskName, AppName, Args
Task Immediate Preferences	TaskName, AppName, Args
Time Trigger	Type
Daily Trigger	Type, DaysInterval
Weekly Trigger	Type, WeeksInterval
Monthly Trigger	Type, MonthsOfYear, DaysOfMonth
MonthlyDOW Trigger	Type, MonthsOfYear, DaysOfWeek, WeeksOfMonth
Event Trigger	Type, EventLog, EventSource, EventId
Idle Trigger	Type
Logon Trigger	Type, UserID
Boot Trigger	Type
Registration Trigger	Type
Session State Change Trigger	Type, UserID, GroupID
Run Program Action	Action, Program, Arguments
Send Email Action	Action, To, From, Subject
Display Message Action	Action, Title
Task Scheduled V2 Preferences	Action, TaskName, Actions
Task Immediate V2 Preferences	Action, TaskName, Actions
Network Share Preferences	Action, ShareName (if action is delete), Path (if action not delete)
Services Preferences	ServiceName
Drive Preferences	Action, Drive Letter
Regional Options Preferences	LocaleId
Start Menu Preferences	Always Unique
Start Menu Vista Preferences	Always Unique
IE Preferences	Always Unique

Universal Policy Differences Report

Using Universal Policy Administrator, you can view the Universal Policy Differences report between the current version of a specific universal policy and the last checked-in version, the last approved version, any two versions, and the version present in the GPO in AD.

NOTE: The Universal Policy Differences Report described is only available for Universal Policies that were created from a GPO in AD. If you create a brand new Universal Policy and export it to AD, this type of Difference report is not available.

To View Universal Policy Differences Report in the web console:

1. Login to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a **Universal Policy**, to open the policy tab.
4. On the policy tab, navigate to the **Reports** menu.
5. Click **Differences** to open the **Differences** tab.
6. On the Differences tab, click on the type of differences report you need to open the **Comparing Changes** tab.
7. View the **Universal Policy Differences Report**.

To Search Specific Settings in the Universal Policy Differences Report in the web console:

1. Login to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a **Universal Policy**, to open the policy tab.
4. On the policy tab, navigate to the **Reports** menu.
5. Click **Differences** to open the **Differences** tab.
6. On the Differences tab, click on the type differences report you need to open the **Comparing Changes** tab.
7. In the **Comparing Changes** tab, navigate to the search bar.
8. Click on the search bar to activate it.
9. Type in the keyword or setting name you are looking for.
10. Press **Enter** or click on the search icon to initiate the search.
11. Review the search result to find the relevant setting (The keywords are highlighted).

To Share Universal Policy Differences Report in the Web Console:

1. Login to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a **Universal Policy**.
4. On the policy tab, navigate to the **Reports** menu.
5. Click **Differences**, to open the **Differences** tab.

6. In the **Differences** tab, click on the type differences report you need, to open the **Comparing Changes** tab
7. In the **Comparing Changes** tab, click on the **Share Report** icon, a print dialog box will appear.
8. Choose **Save as PDF** or select the PDF printer option from the list of available printers.
9. Click the **Print** or **Save** button. A new dialog box will prompt you to choose the destination where you want to save the PDF file.
10. Select the desired location on your device and enter a file name for the PDF.
11. Click **Save** to generate the report as a PDF file.

Universal Policy Settings Report

You can view settings report for Universal Policies. This helps administrators quickly access and review the settings of any Universal Policy, ensuring effective policy management.

To view Universal Policy Settings Report in the Web Console:

1. Login to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a **Universal Policy**, to open the policy tab.
4. On the policy tab, navigate to the **Reports** menu.
5. Click **Settings**, to open the **Settings Report** tab.
6. In the **Settings Report** tab, click on the release of the Universal Policy, to open the **Universal Policy Settings Report** tab.
7. View the **Universal Policy Settings Report**.

To Search Specific Settings in the Universal Policy Settings Report in the Web Console:

1. Login to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.
3. Select a **Universal Policy**, to open the policy tab.
4. On the policy tab, navigate to the **Reports** menu.
5. Click **Settings**, to open the **Settings Report** tab.
6. In the **Settings Report** tab, click on the release of the Universal Policy, to open the **Universal Policy Settings Report** tab.
7. In the Universal Policy Settings Report tab, navigate to the search bar.
8. Click on the search bar to activate it.
9. Type in the keyword or setting name you are looking for.
10. Press **Enter** or click on the search icon to initiate the search.
11. Review the search results to find the relevant setting (The keywords are highlighted).

To Share Universal Policy Settings in the Web Console:

1. Login to the **Web Console** as an Administrator.
2. Navigate to the **Universal Policies** tab.

3 Select a **Universal Policy**, to open the policy tab.

4 On the policy tab, navigate to the **Reports** menu.

5 Click **Settings**, to open the **Settings Report** tab.

6 In the **Settings Report** tab, click on the release of the Universal Policy, to open the **Universal Policy Settings Report** tab.

7 In the Universal Policy Settings Report tab, click on the **Share Report** icon, a print dialog box will appear.

8 Choose **Save as PDF** or select the PDF printer option from the list of available printers.

9 Click the **Print or Save** button. A new dialog box will prompt you to choose the destination where you want to save the PDF file.

10 Select the desired location on your device and enter a file name for the PDF.

11 Click **Save** to generate the report as a PDF file.

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 83

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 92

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"
```

To View Comparison and Differential Reports with PowerShell

1. Open the PowerShell console.
2. Navigate to the PowerShell Snapin folder path.
3. Enter the following command to load the HAPI.ProviderPowershellSnapin snap-in:

   Add-PSSnapin HAPI.ProviderPowershellSnapin
4. Use the scripts below to view the Differential Reports:

NOTE: The UP Id is obtained by selecting the universal policy for which you need the report and navigating to the ‘Advanced’ tab.

Differential Report between two Different Universal Policies

Synopsis

Retrieve a differential report between two different Universal Policies using the Get-DiffReport cmdlet.

Syntax

```
$resp = Get-DiffReport -UPId '<UPId>' -SecondUPId '<SecondUPId>'
$resp.Changes.Count
$resp.Changes
```

Description

The Get-DiffReport cmdlet generates a differential report between two Universal Policies (UPs). This report highlights the changes between the specified UPs, providing details on the number of changes and the specific differences.

Parameters

Attribute / Description	Parameters / Values				
	Required	**Position**	**Default Value**	**Accept Pipeline input?**	**Accept wildcard characters?**
UPId <String>	true	named		false	false
The unique identifier of the first Universal Policy.					
Second UPId <String>	true	named		false	false
An array of existing Active Directory groups to assign specified by distinguished name.					

Example A-1 *1*

```
$resp = Get-DiffReport -UPId 'bdc31f11-0683-42e3-9c72-2157ad2c9393' -
SecondUPId '657583b1-f749-4b8c-a3a5-45b5e9bbb425'
$resp.Changes.Count
$resp.Changes
```

In this example, the Get-DiffReport cmdlet is used to generate a differential report between two Universal Policies (UPs). The command $resp = Get-DiffReport -UPId 'bdc31f11-0683-42e3-9c72-2157ad2c9393' -SecondUPId '657583b1-f749-4b8c-a3a5-45b5e9bbb425' compares the two specified UPs and stores the result in the variable $resp.

Differential Report between Current Version and the last Checkedin Version of the same Universal Policy

Synopsis

Retrieve a differential report for a specific Universal Policy between the current version and the last checked-in version using the Get-DiffReport cmdlet.

Syntax

```
$resp = Get-DiffReport -UPId 'XXX' -CheckedOutVersusCheckedIn
```

Description

The Get-DiffReport cmdlet generates a differential report for a specific Universal Policy, comparing the current version of the Universal Policy with its last checked-in version. This report highlights the changes made since the last check-in, providing details on the number of changes and the specific differences.

Parameters

Attribute / Description	Parameters / Values				
	Required	**Position**	**Default Value**	**Accept Pipeline input?**	**Accept wildcard characters?**
UPId <String>	true	named		false	false
The unique identifier of the Universal Policy.					
CheckedOutVersusCheckedIn <SwitchParameter>	true	named		false	false
Compares the current version with the last checked-in version.					

Example A-2 *2*

```
$resp = Get-DiffReport -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' -
CheckedOutVersusCheckedIn
```

In this example, the Get-DiffReport cmdlet is used to generate a differential report for a specific Universal Policy (UP), comparing its current version with the last checked-in version. The command $resp = Get-DiffReport -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' -CheckedOutVersusCheckedIn specifies the unique identifier of the UP with -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' and uses the -CheckedOutVersusCheckedIn switch parameter to indicate that the comparison should be between the current version and the last checked-in version.

Differential Report between Current Version and the last Approved Version of the same Universal Policy

Synopsis

Retrieve a differential report for a specific Universal Policy between the current version and the last approved using the Get-DiffReport cmdlet.

Syntax

```
$resp = Get-DiffReport -UPId 'XXX' -CheckedOutVersusApproved
```

Description

The Get-DiffReport cmdlet generates a differential report for a specific Universal Policy, comparing the current version of the Universal Policy with its last approved version. This report highlights the changes made since the last approval, providing details on the number of changes and the specific differences.

Parameters

Attribute / Description	Parameters / Values				
	Required	**Position**	**Default Value**	**Accept Pipeline input?**	**Accept wildcard characters?**
UPId <String>	true	named		false	false
The unique identifier of the Universal Policy.					
CheckedOutVersusApproved <SwitchParameter>	true	named		false	false
Compares the current version with the last approved version.					

Example A-3 *3*

```
$resp = Get-DiffReport -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' -
CheckedOutVersusApproved
```

In this example, the Get-DiffReport cmdlet is used to generate a differential report for a specific Universal Policy (UP), comparing its current version with the last approved version. The command $resp = Get-DiffReport -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' -CheckedOutVersusApproved specifies the unique identifier of the UP with -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' and uses the -CheckedOutVersusApproved switch parameter to indicate that the comparison should be between the current version and the last approved version.

Differential Report between Current Version and the last Two Versions of the same Universal Policy

Synopsis

Retrieve a differential report for a specific Universal Policy between the current version and the last two versions using the Get-DiffReport cmdlet.

Syntax

```
$resp = Get-DiffReport -UPId 'XXX' -CheckedOutVersusLast2Versions $True$
```

Description

The Get-DiffReport cmdlet generates a differential report for a specific Universal Policy, comparing the current version of the Universal Policy with its last two versions. This report highlights the changes made over the last two versions, providing details on the number of changes and the specific differences.

Parameters

Attribute / Description	Parameters / Values				
	Required	**Position**	**Default Value**	**Accept Pipeline input?**	**Accept wildcard characters?**
UPId <String>	true	named		false	false
The unique identifier of the Universal Policy.					
CheckedOutVersusLast2Versions <SwitchParameter>	true	named		false	false
Compares the current version with the last two versions.					

Example A-4 *4*

```
$resp = Get-DiffReport -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' -
CheckedOutVersusLast2Versions $True$
```

In this example, the Get-DiffReport cmdlet is used to generate a differential report for a specific Universal Policy, comparing its current version with the last two versions. The command $resp = Get-DiffReport -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' -CheckedOutVersusLast2Versions $True$ specifies the unique identifier of the Universal Policy with -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' and uses the -CheckedOutVersusLast2Versions $True$ switch parameter to indicate that the comparison should be between the current version and the last two versions.

Differential Report between Current Version and the Version in GPO in AD

Synopsis

Retrieve a differential report for a specific Universal Policy between the current version and the version in Group Policy Object in Active Directory using the Get-DiffReport cmdlet.

Syntax

```
$resp = Get-DiffReport -UPId 'XXX' -CheckedOutVersusGPOInAD
```

Description

The Get-DiffReport cmdlet generates a differential report for a specific Universal Policy (UP), comparing the current version of the UP with the version stored in the Group Policy Object (GPO) in Active Directory (AD). This report highlights the changes made between the two versions, providing details on the number of changes and the specific differences.

Parameters

Attribute / Description	Parameters / Values				
	Required	**Position**	**Default Value**	**Accept Pipeline input?**	**Accept wildcard characters?**
UPId <String>	true	named		false	false
The unique identifier of the Universal Policy.					
CheckedOutVersusGPOInAD <SwitchParameter>	true	named		false	false
Compares the current version with the version in GPO in AD					

Example A-5 *5*

```
$resp = Get-DiffReport -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' -
CheckedOutVersusGPOInAD
```

In this example, the Get-DiffReport cmdlet is used to generate a differential report for a specific Universal Policy (UP), comparing its current version with the version stored in the Group Policy Object (GPO) in Active Directory (AD). The command $resp = Get-DiffReport -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' -CheckedOutVersusGPOInAD specifies the unique identifier of the UP with -UPId '1971ceca-7875-4a5f-8365-faa4bcdf07fa' and uses the -CheckedOutVersusGPOInAD switch parameter to indicate that the comparison should be between the current version and the version in GPO in AD.

B Appendix

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

- "Linux Agent Commands and Lookups" on page 91
- "Supported PowerShell Cmdlets" on page 92
- "Troubleshooting" on page 96

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-Role	Creates a new delegation Role.
10	Add-ViewScope	Creates a new delegation View.
11	Add-DelegationAssignment	Creates a new delegation Assignment.
12	Approve-UniversalPolicy	Approves or Unapproves a Universal Policy.
13	Assign-UniversalPolicy	Assigns new Universal Policy to an agent or OU.
14	Checkin-UniversalPolicy	Checks in changes to a Universal Policy.
15	Checkout-UniversalPolicy	Checks out a Universal Policy.
16	Clone-UniversalPolicy	Clones a Universal Policy.
17	Deploy-UniversalPolicy	Deploys a Universal Policy.
18	Find-UniversalPolicy	Finds Universal Policies using the given search filters.
19	Find-UniversalPolicySettings	Finds settings in a given Universal Policy.
20	Get-ADComputers	Gets one or more Active Directory computers.
21	Get-ADDomainControllers	Gets the list of Active Directory Domain Controllers for the specified domain.
22	Get-ADDomains	Gets the set of Active Directory domains that can be managed by HAPI.
23	Get-ADGroups	Gets one or more Active Directory groups.
24	Get-AdmFiles	Gets ADMX definitions for policy settings.
25	Get-ADUsers	Gets one or more Active Directory users.
26	Get-AgentPolicy	Gets the policy settings for a specified agent. This cmdlet is for internal use only.
27	Get-AllOUs	Gets Repository and Cloud OUs.

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

54	Get-Roles	Gets the list of Roles.
55	Get-RolesForUsers	Get the delegation Roles that the currently logged on user has been granted.
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-ViewScopes	Get one or more delegation Views.
61	Get-WMIFilter	Gets one or more WMI Filters from Active Directory.
62	Get-WMINamespaces	Gets the set of WMI Namespaces.
63	Import-UniversalPolicy	Imports a Universal Policy.
64	Link-UniversalPolicy	Updates all the AD OU Links that the given Universal Policy is linked to.
65	Load-ADRepository	The name of the domain to load into the Repository.
66	Lock-Policy	The Lock-Policy cmdlet helps insure that the settings in a GPO match the settings in the associated Universal Policy.
67	Merge-UniversalPolicies	Merges two Universal Policies into a new Universal Policy.
68	New-AgentComputer	The name of the agent computer to add.
69	New-GPONameFilter	Creates a filter that allows you to search for a Group Policy object by name.
70	New-Group	Creates a new Active Directory group.
71	New-LdapFilter	Creates a filter that allows you to search for a User, Group, or Computer based on its properties.
72	New-LdapPropertyValue	Creates an LdapPropertyValue object.
73	New-PolicyLink	Links a Universal Policy to a Scope.
74	New-UniversalPolicy	Creates a new Universal Policy in the repository.
75	New-User	Creates a new Active Directory user.
76	New-WMIFilter	Creates a new WMI Filter in Active Directory.
77	Remove-AgentComputer	Removes an agent.
78	Remove-DelegationAssignment	Deletes a delegation Assignment.
79	Remove-Group	Deletes a group from Active Directory.
80	Remove-GroupMember	Removes a member from a group in Active Directory.
81	Remove-HapiGPO	Removes a GPO from Active Directory.
82	Remove-HapiGPOLink	Removes a GPO Link from Active Directory.

83	Remove-HapiGPOPermission	Removes the specified permission entry from a GPO's permissions.
84	Remove-MigrationMap	Removes one or more Migration Maps from storage.
85	Remove-OU	Removes a Cloud or Repository OU.
86	Remove-OUChild	Removes one or more children from a Cloud or Repository OU.
87	Remove-PolicyAssignment	Removes one or more children from a Cloud or Repository OU.
88	Remove-RepWMIFilter	Removes a WMI Filter from the Repository.
89	Remove-Role	Deletes a delegation Role.
90	Remove-UniversalPolicy	Removes a Universal Policy.
91	Remove-User	Deletes a user from Active Directory.
92	Remove-ViewScope	Deletes a delegation View.
93	Remove-WMIFilter	Removes a WMI Filter from Active Directory.
94	Rename-OU	Renames a Cloud or Delegation OU.
95	Revert-PolicyCheckout	Reverts the Checkout of a Universal Policy.
96	Rollback-UniversalPolicy	Rolls back a Universal Policy to a previous version
97	Set-DomainCredential	Specifies credentials to manage a domain.
98	Set-Group	Updates an Active Directory group.
99	Set-HapiGPOProperties	Sets the properties of a GPO in Active Directory.
100	Set-HapiGPOSettings	Updates the Policy Settings defined in the specified GPO.
101	Set-MigrationMap	Creates or updates a Migration Map in storage.
102	Set-PolicyActivation	Activates or Deactivates a Policy Assignment.
103	Set-RepWMIFilter	Creates or Updates a WMI Filter in the Repository.
104	Set-User	Updates an Active Directory user.
105	Set-WMIFilter	Updates a WMI Filter in Active Directory.
106	Stop-LoadRepositoryJob	Stops a job that is loading AD OUs and GPOs into the repository.
107	Submit-UniversalPolicy	Checks out a Universal Policy.
108	Test-WMIFilter	Runs a WMI Filter to determine whether the filter is valid.
109	Unlink-PolicyFromScope	Unlinks a Policy from a Scope.
110	Update-DelegationAssignment	Updates an existing delegation Assignment.
111	Update-HapiGPOLink	Updates the settings of a GPO Link.
112	Update-HapiGPOPermissions	Updates the Permissions for the specified GPO.
113	Update-Role	Updates an existing delegation Role.

114	Update-OULinkOrder	Updates the link order for a child Universal Policy to a Cloud or Repository OU.
115	Update-UniversalPolicy	Updates the properties of a Universal Policy.
116	Update-UPPolicy	Updates a Policy within a Universal Policy.
117	Update-UPSection	Updates a Policy Section within a Universal Policy.
118	Update-ViewScope	Updates an existing delegation View.

Troubleshooting

Unable to manage child, trusted, and untrusted domains.

The errors encountered during domain import were related to the failure to import the only two GPOs in that domain, because of UNC Hardening.

Follow the instructions below to grant the Gateway machine access to SYSVOL on the domain controllers (DCs) in that untrusted domain:

- UNC hardening policy (For Untrusted Domains):
  - Open the local group policy editor on the gateway machine (gpedit.msc).
  - Navigate to Computer Configuration > Administrative Templates > Network > Network Provider > Hardened UNC Paths.
  - Enable the policy and add the following entry:
    1. Path: \\adbdemo.local\SYSVOL
    2. Settings: RequireMutualAuthentication=0,RequireIntegrity=0,RequirePrivacy=0
    3. Alternatively, you can use \\dcname.adbdemo.local or *.adbdemo.local for testing purposes (the GUID will change).
  - Browse from the gateway to the untrusted domain using the following path:

    \\adbdemo.local\SysVol\adbdemo.local\Policies\{3b547bb5-ad82-485f-8c39-405d4bcdb0bc}
  - Replace "adbdemo" with the domain you want to configure.