MICRO FOCUS®

AD Bridge 2.0

Administration Guide

December 2019

Legal Notice

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

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

Contents

About This Guide

The *AD Bridge User Guide* provides information to help you understand, install, configure, and employ the Micro Focus AD Bridge product to help manage your enterprise environment.

Audience

This guide is written for administrators and users who will use Micro Focus AD Bridge to more effectively manage Active Directory and group policies in a cross-platform 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

AD Bridge 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 AD Bridge documentation website.

1 Getting Started

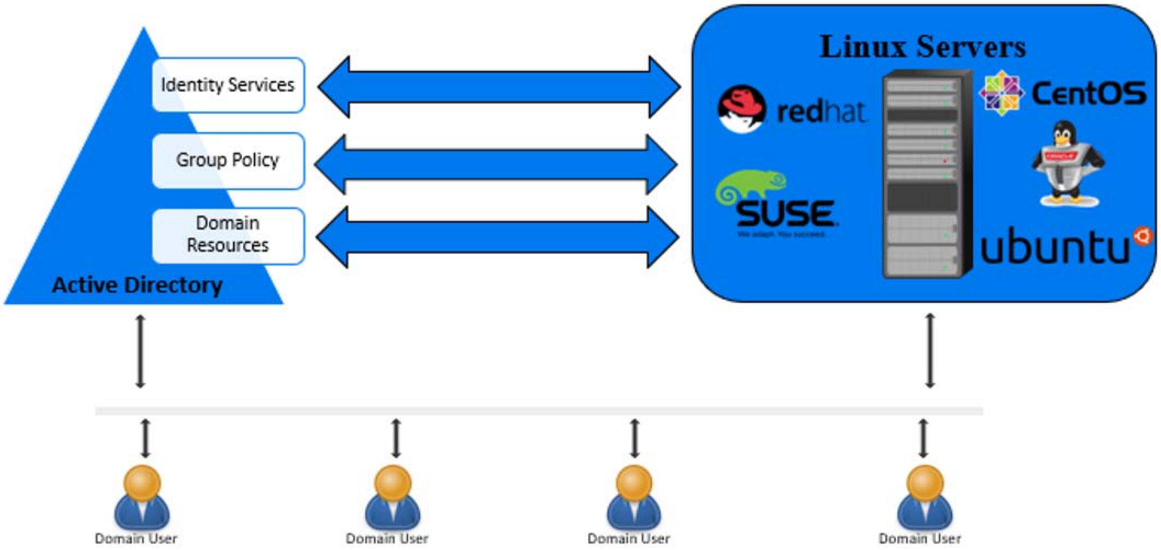
AD Bridge is a solution that extends Active Directory (AD) capabilities by enabling domain controllers to add on premises Linux servers and Linux virtual machines in the Cloud to the AD environment to interface with identity services, group policies, and domain resources. This is accomplished with the installation of an AD Bridge Linux Agent on Linux computers, AD Bridge and Cloud Gateways each and a GPMC snap-in tool “AD Bridge GPEdit Extension” on the domain controller.

After the AD Bridge and Cloud Gateways, AD Bridge Linux Agent and GPEdit Extension are installed on their respective computers, you can configure built-in and custom group policies for Linux agents via the Group Policy Management Console on the domain controller and bridge Linux virtual machines (VMs) in the cloud with the AD Bridge Gateway and push universal policies created on the Cloud Gateway to cloud Linux VMs. Some of the capabilities include the following group policy options for agent computers:

- Configure Allow and Deny controls for Firewall settings
- Start, stop, or restart agent services
- Import and manage Open SSH, Sudoers and Custom Configuration files
- Modify and control agent application files
- Execute commands
- Configure Active Directory login controls

For more information about these settings, see the Linux Agent GPO Settings.

Reference the graphic below for a visual depiction of how AD Bridge will work with your Active Directory environment.



Micro Focus AD Bridge thus delivers unique capabilities, that modern organizations need to capitalize on their investments in the Active Directory and Group Policy space, increasing security while reducing risk.

2 Installing AD Bridge

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

Linux Requirements and Supported Platforms

Review the information in this section before installing the AD Bridge Agent on a Linux server.

Linux Requirements

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 the Linux Agent installation.

  Otherwise, you must install the following Linux packages prior to running the Linux Agent installation:

Linux Distribution	**Required Linux Packages**
All distributions	.NetCore system update to install .NetCore 2.2 and its prerequisites. For more information, see *Linux distribution dependencies*.

RHEL 8, RHEL 7, CentOS 8, CentOS 7, Oracle 8, Oracle 7	`samba`
	`samba-client`
	`samba-winbind`
	`samba-winbind-clients`
	`cifs-utils`
	`openldap-clients`

Linux Distribution	Required Linux Packages

SLES 12, SLES 15	`realmd`
	`adcli`
	`sssd`
	`sssd-tools`
	`sssd-ad`
	`samba-client`
	`krb5-client`
	`openldap2-client`

Ubuntu 18.04	`realmd`
	`sssd`
	`sssd-tools`
	`libnss-sss`
	`libpam-sss`
	`adcli`
	`samba-common-bin`
	`oddjob`
	`oddjob-mkhomedir`
	`packagekit`
	`krb5-user`
	`cifs-utils`
	`keyutils`

Ubuntu 16.04	`ntpdate`
	`samba`
	`krb5-config`
	`krb5-user`
	`winbind`
	`libpm-winbind`
	`libnss-winbind`
	`cifs-utils`

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

Supported Linux Platforms

AD Bridge 2.0 supports the following Linux platforms:

Linux Distribution	Version
RHEL	◆ RHEL 8 ◆ RHEL 7
SLES	◆ SLES 12 ◆ SLES 15
CentOS Enterprise Linux	◆ CentOS 8 ◆ CentOS 7
Ubuntu	◆ Ubuntu 18 ◆ Ubuntu 16

Linux Distribution	Version
Oracle Linux	- Oracle 8 - Oracle 7

NOTE: If your cloud environment uses a GoDaddy SSL certificate on RHEL 7, RHEL 8, CentOS 7, CentOS 8, Oracle Linux 7, Oracle Linux 8, Ubuntu 16, Ubuntu 18, SLES 12, and SLES 15 operating systems, you must copy it to agent machines and manually assign trust.

For more information, see "Adding a GoDaddy SSL Certificate" on page 16.

Installing the Cloud Gateway in Microsoft Azure

The AD Bridge Cloud Gateway is used to bridge Linux virtual machines (VMs) in the cloud with the on premises AD Bridge Gateway and push universal policies created on the Cloud Gateway to cloud Linux VMs.

To set up the AD Bridge Cloud Gateway:

1. Create a Resource Group.

   For more information, see Create Resource Groups on Azure.
2. Create a Virtual Network (Classic).

   For more information, see Create a Virtual Network (Classic) on Azure.
3. Create a Storage Account (Classic).

   For more information, see Create a Storage Account (Classic) on Azure.
4. Create a SQL Database.

   For more information, see Create a SQL Database on Azure.
5. Download the AD Bridge installation files from the Micro Focus Downloads website onto a Windows device.
6. Extract the contents of the `ADBRIDGECLOUD_2.zip` file.
7. Open the `ServiceConfiguration.Release.cscfg` configuration file available in the extracted contents and modify the highlighted text as shown in the snippet below according to your environment:

```
<?xml version="1.0" encoding="utf-8"?>
<ServiceConfiguration serviceName="HAPI.Mvc.Gatekeeper.CloudService"
xmlns="http://schemas.microsoft.com/ServiceHosting/2008/10/
ServiceConfiguration" osFamily="6" osVersion="*" schemaVersion="2015-
04.2.6">
  <Role name="HAPI.Mvc.Gatekeeper.CloudHost">
    <Instances count="1" />
    <ConfigurationSettings>
      <Setting name="DatabaseConnection"
value="Server=tcp:myserver.database.windows.net,1433;Initial
Catalog=ADBridge;Persist Security Info=True;User
ID=myuser@myserver;Password=" />
      <Setting name="WildcardDomain" value="your domain name.com" />
      <Setting name="LogStorageConnectionString"
value="DefaultEndpointsProtocol=https;AccountName=mystorageaccount;Acc
ountKey=" />
      <Setting name="AzureLogShare" value="ADB" />
      <Setting name="AzureLogDirectory" value="Logs" />
      <Setting name="LoggingLevel" value="Error" />
    </ConfigurationSettings>
    <Certificates>
      <Certificate name="Certificate1" thumbprint="<thumbprint here>"
thumbprintAlgorithm="sha1" />
    </Certificates>
  </Role>
  <Role name="HAPI.Mvc.Gatekeeper.TraversalWorker">
    <Instances count="1" />
    <ConfigurationSettings>
      <Setting name="DatabaseConnection"
value="Server=tcp:myserver.database.windows.net,1433;Initial
Catalog=ADBridge;Persist Security Info=True;User
ID=myuser@myserver;Password=" />
      <Setting name="LogStorageConnectionString"
value="DefaultEndpointsProtocol=https;AccountName=somestorageaccount;A
ccountKey=" />
      <Setting name="AzureLogShare" value="ADB" />
      <Setting name="AzureLogDirectory" value="Logs" />
      <Setting name="LoggingLevel" value="Error" />
    </ConfigurationSettings>
    <Certificates>
      <Certificate name="Certificate1" thumbprint="<thumbprint here>"
thumbprintAlgorithm="sha1" />
    </Certificates>
  </Role>
  <NetworkConfiguration>
    <VirtualNetworkSite name="Group resource group virtual network" />
    <AddressAssignments>
      <InstanceAddress roleName="HAPI.Mvc.Gatekeeper.CloudHost">
        <Subnets>
          <Subnet name="subnet name" />
        </Subnets>
      </InstanceAddress>
      <InstanceAddress roleName="HAPI.Mvc.Gatekeeper.TraversalWorker">
        <Subnets>
          <Subnet name="subnet name" />
        </Subnets>
      </InstanceAddress>
    </AddressAssignments>
  </NetworkConfiguration>
</ServiceConfiguration>
```

8 Create a Cloud Service (Classic) and upload the necessary files and certificate.

Configure the SQL firewall to allow the cloud service to access the SQL server.

For more information, see Create a Cloud Service (Classic) on Azure.

9 Create a Virtual Machine (Classic) in Linux.

For more information, see Create a Virtual Machine on Azure.

10 Configure your Linux VM:

10a Install NGINX.

```
# yum update
```

```
# reboot
```

```
# yum install epel-release
```

```
# yum install nginx
```

10b Install your SSL certificate on the NGINX server.

10c Copy the `cors.include` file from extracted contents to the`/etc/nginx` directory of the NGINX server.

10d Copy the `nginx.conf` file from extracted contents to the`/etc/nginx` directory of the NGINX server and replace the existing version of the file.

10e Configure the Azure firewall to allow HTTPS (port 443) traffic to the NGINX server.

11 Open the `/etc/nginx/nginx.conf` file and modify the highlighted text as shown in the snippet below according to your environment:

```
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log;
pid /run/nginx.pid;

# Load dynamic modules. See /usr/share/nginx/README.dynamic.
include /usr/share/nginx/modules/*.conf;

events {
    worker_connections 1024;
}

http {
    log_format  main  '$remote_addr - $remote_user [$time_local]
"$request" '
                      '$status $body_bytes_sent "$http_referer" '
                      '"$http_user_agent" "$http_x_forwarded_for"';

    access_log  /var/log/nginx/access.log  main;

    sendfile            on;
    tcp_nopush          on;
    tcp_nodelay         on;
    keepalive_timeout   65;
    types_hash_max_size 2048;

    include             /etc/nginx/mime.types;
    default_type        application/octet-stream;

    server {
        listen       80 default_server;
        listen       [::]:80 default_server;

        server_name _;
        return 301 https://$host$request_uri;
    }

    server {
        listen       443 ssl http2 default_server;
        listen       [::]:443 ssl http2 default_server;
        server_name  ~$(?<subdomain>\.)?(?<domain>.+)$;
        root         /usr/share/nginx/html;

        #replace with your certificate in the next two lines
        ssl_certificate "/etc/pki/nginx/cert-here.crt";
        ssl_certificate_key "/etc/pki/nginx/cert-here.pem";
ssl_protocols TLSv1.2;
        location ~*
"^/(api|portal|content|scripts|images|swagger)" {
            gzip on;
            gzip_proxied any;
            gzip_types text/html application/json
application/javascript text/xml;
            proxy_redirect off;
            proxy_set_header host $host;
            proxy_set_header X-forward-for $proxy_add_x_forwarded_for;
            proxy_set_header X-real-ip $remote_addr;
            include cors.include;
            rewrite ^/(.*) /$1 break;
            proxy_connect_timeout 300;
            proxy_send_timeout 300;
            proxy_read_timeout 300;
            send_timeout 300;
            proxy_pass http://10.1.0.4;#replace with IP of your Cloud
Host role

}

   location /ws {
            proxy_http_version 1.1;
            proxy_set_header Upgrade $http_upgrade;
            proxy_set_header Connection "Upgrade";
            proxy_redirect off;
            proxy_set_header host $host;
            proxy_set_header X-forward-for $proxy_add_x_forwarded_for;
            proxy_set_header X-real-ip $remote_addr;
            include cors.include;
            proxy_pass https://10.1.0.5/ws; #replace with IP of your
TraversalWorker role

        }

        location /route {
            proxy_connect_timeout 300;
            proxy_send_timeout 300;
            proxy_read_timeout 300;
            send_timeout 300;
            gzip on;
            gzip_proxied any;
          gzip_types text/html application/json application/javascript
text/xml;
            proxy_redirect off;
            proxy_set_header host $host;
            proxy_set_header X-forward-for $proxy_add_x_forwarded_for;
            proxy_set_header X-real-ip $remote_addr;
            proxy_set_header If-Modified-Since "";
            add_header 'Cache-Control' 'no-store, no-cache, must-
revalidate, proxy-revalidate, max-age=0';
            expires off;
            include cors.include;

           proxy_pass https://10.1.0.5/route; #replace with IP of your
TraversalWorker role

        }
    }
}
```

12 Copy compressed files of the web console to the Linux VM and run the following commands:

- **12a** Remove the old HTML files `# rm -rf /usr/share/nginx/html/*`
- **12b** Extract the web console files `# tar -jxvf WebConsole_22472.tar.bz2 -C /usr/share/nginx/html/`.
- **12c** Restart the nginx service`# systemctl restart nginx`.

Adding a GoDaddy SSL Certificate

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

Prerequisite

Download the gdig2.crt.pem certificate from the GoDaddy Repository.

For RHEL 7 or CentOS 7 or Oracle Linux 7:

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

For RHEL 8 or CentOS 8 or Oracle Linux 8:

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

For SLES 12 and SLES 15:

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

For Ubuntu 16 and 18:

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

Installing the AD Bridge Gateway

The AD Bridge Gateway is used to push policies from Active Directory to the Cloud Gateway.

Complete the following prerequisites before you install the AD Bridge Gateway:

- Microsoft Server 2012 r2 or later installed
- Domain Administrator account access

The AD Bridge Gateway installer also installs: Microsoft .Net Framework 4.7.

To install the AD Bridge Gateway:

1. Log in to a Member server as a domain administrator.
2. Execute the downloaded `ADBRIDGE_2.EXE` file.
3. When the installation wizard opens, click **Install**.

   If .NET Framework 4.7.x is not already installed on your Domain Controller, it is installed as part of the prerequisite check before the AD Bridge Gateway installation starts.
4. Click **Next** when the AD Bridge Gateway setup wizard opens.
5. Read and Accept the License Agreement, and click **Next**.
6. Select an installation option. The available options are:
   - NAT Traversal
   - DMZ or Port Forward

   NOTE: In most cases, select **NAT Traversal**.
7. Click **Next**.
8. Enter domain administrator credentials and click **Next**.
9. Enter the Cloud Gateway URL and AD Bridge Gateway owner account credentials, and click **Next**.

   NOTE: Click **Register** and create a new account if one does not exist.
10. Retain or change the default location for program installation, and then click **Next**.
11. Click **Install** to copy the Gateway installer files.
12. Click **Finish** on the last screen of the wizard to complete the installation.

Configuring the AD Bridge Syslog Provider

You can configure AD Bridge 2.0 to forward events and syslog messages to one or more SIEM solutions.

To configure the AD Bridge Syslog Provider:

1. Open the `C:\Program Files\MicroFocus\AD Bridge\Gateway\WebApp\Web.Config` file.
2. Modify the highlighted text as shown in the snippet below according to your environment:

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

The available options for each of these attributes are:

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

  NOTE: AD Bridge 2.0 only supports the filterType attribute value, `AuditOnly`.

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

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

Installing the AD Bridge GPEdit Extension

The native AD Group Policy Management Console (GPMC) manages Group policies for AD Bridge Linux Agents joined to Active Directory, with the AD Bridge GPEdit Extension snap-in installed on the domain controller.

The snap-in adds extensions for Linux-based settings that you can configure within the structure of a Group Policy Object (GPO).

Complete the following prerequisites before installing the GPEdit Extension snap-in:

- Install GPMC on the domain controller
- Access to the domain administrator account
- Install Microsoft .NET Framework 4.7.x (*Can be installed by the snap-in installer*)

To install the AD Bridge GPEdit Extension:

1. Log in to a domain-joined member server with GPMC installed, as an administrator.
2. Execute the downloaded `ADBRIDGE_INSTALLER_2.EXE` file.
3. When the installation wizard opens, click **Change** to change the default copy location for installation files; otherwise, click **Install**.

If .NET Framework 4.7.x is not already installed on your Domain Controller, it is installed as part of the prerequisite check before the snap-in installation starts.

4 Click **Next**.

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

6 Retain or change the default location for program installation, and then click **Next**.

7 Click **Install** to copy the GPEdit extension files.

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

You can now configure GPOs for your Linux endpoints that have the AD Bridge Linux Agent installed. For information about configuring GPOs, see Managing Linux GPO Settings.

Installing the AD Bridge Linux Agent

When you download the AD Bridge Linux Agent installer, you will need to unpack the installer for your specific Linux distribution. An example of the files included with the final distribution installer is shown below:

- `adb-agent-rh7-2.0.rpm`
- `install.sh`
- `uninstall.sh`

NOTE: The AD Bridge Linux Agent installer also installs .Net Core 2.2, which is necessary during uninstallation.

To install the AD Bridge Linux Agent on a Linux machine:

1 Copy the Linux Agent installer file applicable to your distribution onto the Linux machine.

Installer file	Linux distribution
`ADBRIDGE_AGENT_2.TAR.GZ`	◆ RHEL 7 and 8 ◆ CentOS 7 and 8 ◆ Oracle Linux 7 and 8 ◆ SLES 12 and 15
`ADBRIDGE_UBUNTU_AGENT_2.TAR.GZ`	◆ Ubuntu 16 ◆ Ubuntu 18

2 On the command line, log in as the `root` user and type the following command to unpack the applicable installation package from the table above: `tar xvzf <file name>`.

3 For all distributions except Ubuntu, type the command again using the file name specific to your platform from the table below.

For example: `tar xvf <file name>`

Installer file	Linux distribution
`RHEL_CENT_Oracle8.tar`	◆ RHEL 8 ◆ CentOS 8 ◆ Oracle 8
`RHEL_CENT_Oracle7.tar`	◆ RHEL 7 ◆ CentOS 7 ◆ Oracle 7
`Ubuntu18.tar`	Ubuntu 18
`Ubuntu16.tar`	Ubuntu 16
`SLES15.tar`	SLES 15
`SLES12.tar`	SLES 12

4. Verify the installer files are on the machine with a list command: `# ls`.
5. Run the `install.sh` script file as `root` to set up the Linux Agent. For example:
   - `# ./install.sh`
   - `#bash install.sh`

   Available agent configuration types are:

   ```
   (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-2.1` installation displays a problem dependency for `libicu52-1`.

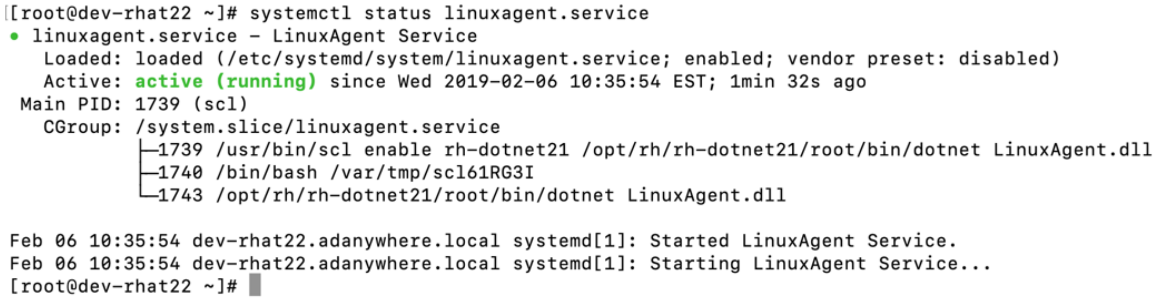
   Enter 2 to ignore the dependency and enter y when prompted to install "NEW packages."
6. (Optional) Enter a, g, h, or n when prompted to join Active Directory.

   NOTE: This step and the following step are optional if you want to join agent configuration type at a later time. For information about joining Agent Configuration Type after installation, see Joining Agent Configuration Type Post Installation.
7. (Optional) When prompted, provide the full domain name, the AD account with rights to join a domain, and AD account password. For example:

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

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

During the installation, the Linux Agent is added by default to the Computers OU in Active Directory. After the installation is complete, the Linux Agent service runs on the Linux system, as demonstrated in the example below 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 it is running, see Linux Agent Commands and Lookups.

Licensing the Linux Agent

The AD Bridge Linux Agent installation comes with a built-in 30-day evaluation period. To continue using AD Bridge after 30 days, purchase the product and install the license before 30 days elapse. For more information, contact Micro Focus Sales.

To download this product, go to the Micro Focus Downloads or Customer Center website.

To activate the AD Bridge license subscription:

1. Copy the license XML file into the Linux Agent directory `/opt/adb-agent`.
2. Restart the Linux Agent Service.

   For more information, see Start the Linux Agent Service.

   Restarting the service replaces the temporary license with the new active license and enables all AD Bridge functionality.

Installing the AD Bridge MAC Agent

The AD Bridge MAC Agent,

Joining 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 AD Bridge 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 AD Bridge 2.0 web console using Universal Policies.

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

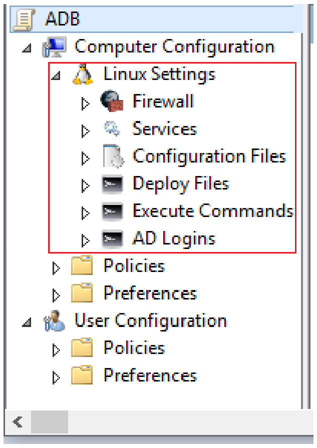
     NOTE: The Linux server is in the cloud (outside the corporate network) and will have a computer object in Active Directory linked to the AD Bridge 2.0 Secure Gateway. Choose this option to manage your cloud Linux server with native Active Directory tools and GPOs.

3. Enter the AD account password when prompted.

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

3 Managing Linux GPO Settings

If you have the AD Bridge GPEdit Extension for the Group Policy Management Console (GPMC) installed on your domain controller, you will see a new node, **Linux Settings**, under Computer Configuration when you open the Group Policy Object (GPO) editor on a GPO. This node has five child nodes, Firewall, Services, Configuration Files, Deploy Files, Execute Commands and AD Logins, which you can use to create, modify, or delete GPO settings for Linux Agent clients in the domain.



When you link a GPO that has rules configured in Linux Settings to an OU that has one or more AD Bridge Linux agents, those GPO settings are applied to the Linux computers in that OU (assuming the Linux Agent Service is running on those computers).

This section demonstrates how to create a new GPO and configure rules in the AD Bridge GPMC snap-in and apply them to your Linux Agent computers. When an AD Bridge Linux Agent is installed on a Linux computer, the computer is automatically added to the Active Directory’s “Computers” OU. As a best practice, you should create a custom OU for linking GPOs to Linux Agent computers in your environment.

IMPORTANT: To minimize the risk of introducing harmful Group Policy errors into your production environment, you should thoroughly test and evaluate Linux Agent GPOs in a non-production environment before you implement them.

For best practice information about configuring GPOs in AD Bridge, see GPO Best Practices.

Accessing or Creating Group Policy Objects

In order to modify, create, or delete group policies for Linux Agent computers in the Active Directory domain, you either need work with existing GPOs or create new GPOs. These GPOs must be linked to any applicable Linux agents in an OU for the group policies to be effective.

When you locate a GPO or create a new one, you open the Group Policy Management Editor, expand the Linux Agent Settings node, and use the AD Bridge GPEdit Extension snap-in to make policy changes in the editor.

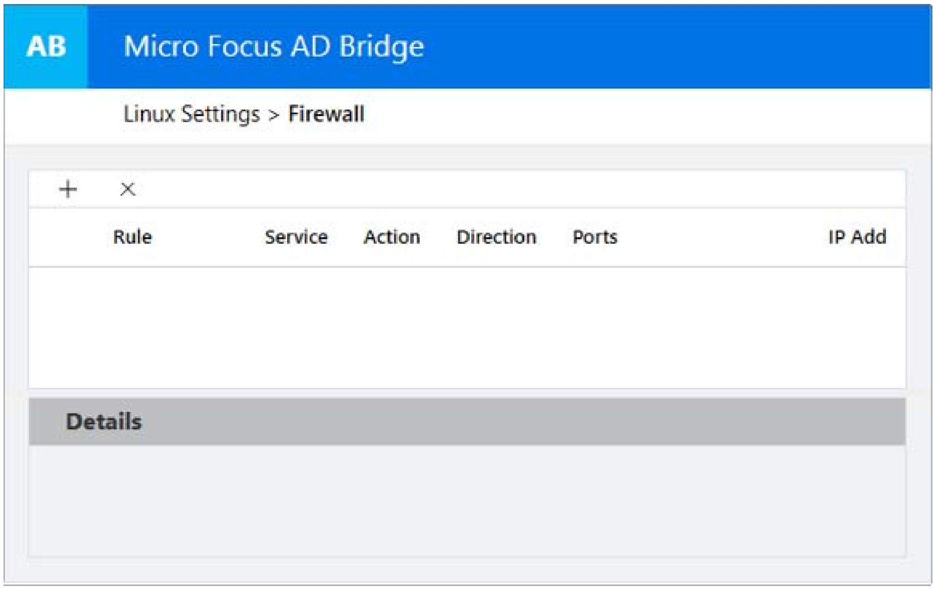
In general, you will use the plus symbol + to add or access settings or rules, if they are not selectable in the snap-in pane, and you will use the delete symbol x to remove them.

To open the GPEdit Extension snap-in on a GPO:

1. Open the GPMC on the domain controller where the GPEdit Extension was installed or from a server in the same domain.
2. Expand the domain tree and OU that contains the Linux Agent.
3. Right-click the applicable GPO, and select **Edit** to open the GPO editor.

   If needed, you can create a new GPO that is linked to the OU and then open the editor from the new object.
4. Expand **Linux Settings** in the GPO editor to access the setting nodes and the GPEdit Extension.

   The GPEdit Extension snap-in is shown below as it appears on a new GPO when first opening the Firewall policy settings.



Configuring Linux GPO Settings

The procedures below provide an example of setting a new Firewall rule in a GPO and applying it to a Linux Agent. For this example we already have a custom OU that contains our Linux Agent.

For information about opening the GPEdit Extension snap-in on a GPO, see Accessing or Creating Group Policy Objects.

To create a Linux Agent Firewall GPO in the AD Bridge GPMC snap-in:

1. Right-click **Group Policy Objects** in the domain tree, and select **New** to create a new GPO.
2. Right-click the new GPO and select **Edit** to open the GPO editor.
3. Expand **Linux Settings** in the GPO editor, and click the **Firewall** node.
4. Click **+** to open the Rule drop-down menu in the AD Bridge snap-in, select **Allow HTTP** from the Rule list, and click **Save** to enable the new rule.

You can also create custom Firewall rules to block or allow Inbound or Outbound traffic based on port, protocol, or IP address.

To add a custom Linux Agent Firewall rule in GPMC:

1. Expand **Linux Settings** in the GPO editor, and click the **Firewall** node.
2. Click **+** to open the Rule drop-down menu in the AD Bridge snap-in, and select **Custom Rule** from the Rule list.
3. Use the Firewall Rule dialog box to name and configure the Action, Direction, Port, Protocol, and IP Address for the custom rule.
4. Add and save your changes.

To apply a new or modified GPO to one or more Linux agents:

1. Select the GPO with the new or modified Linux setting and drag it onto the OU that contains the Linux Agent(s).
2. Click **OK** to link the GPO to the OU and apply the policy to any applicable Linux Agent computers.

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

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

For information about all the GPO settings available in the GPEdit Extension snap-in, see Linux Agent GPO Settings.

Managing Linux Agent Services with GPOs

You can monitor, start, stop, and restart services on Linux Agent computers from a GPO in the GPEdit Extension snap-in. You can use an existing GPO or create a new one, but the GPO needs to be linked with the OU that has the Linux Agent or agents where you want to perform the action.

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

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

- **On Premises AD:** Manage with native tools
- **Cloud AD:** Manage with GPEdit Extension

- **Cloud Non AD:** Manage with web console or third party AD tools

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

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

For information about accessing or creating GPOs in Active Directory, see Accessing or Creating Group Policy Objects.

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

1. Right-click the applicable GPO or GPO link in an OU, and select **Edit** to open the GPO editor.

   If needed, you can create a new GPO that is linked to the OU and then open the editor from the new object.
2. Expand **Linux Settings** in the GPO editor, and click the **Services** node.
3. Click the plus icon **+**, and enter the service name. This must be the actual service name as opposed to the friendly name of the service.
4. Select the desired option (**Start**, **Stop**, or **Restart**), and click **Add**.

NOTE: For information about checking service status on a Linux Agent, see Verify the Linux Agent Service is running.

Importing 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 GPOs 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

For information about accessing or creating GPOs in Active Directory, see Accessing or Creating Group Policy Objects.

To import custom Configuration File settings:

1. Right-click the applicable GPO or GPO link in the OU and select **Edit** to open the GPO editor.

   If needed, you can create a new GPO that is linked to the OU and then open the editor from the new object.
2. In the GPO editor, expand **Linux Settings**, right-click **Configuration Files**, and select **Add Custom Configuration File**.

3 Provide the path and file name for the file you want to import, and click **Add**.

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

To modify Configuration File settings:

1 Click **OpenSSH** or **Sudoers** or a file in the Configuration Files node that you imported as demonstrated above.

2 Click the **+** icon 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.

3 If you want to delete an existing rule, select the rule, and click the **x** icon to delete it.

Managing Linux Applications with GPOs

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

This is done from the Deploy Files node by importing existing application files into one or more GPOs and assigning the GPOs to the Linux Agent OU. All changes going forward for these applications can then be managed from the GPOs 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 GPO.

Before you can manage a Linux Agent application using a GPO, the following prerequisites need to be met:

- The GPO must be linked to applicable Linux 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 Linux applications using GPOs:

1 Expand the domain tree and OU that contains the applicable Linux Agent(s).

2 Right-click the applicable GPO, and select **Edit** to open the GPO editor.

3 Expand **Linux Settings** in the GPO editor, and click the **Deploy Files** node.

4 Click the plus symbol **+** in the GPEdit Extension and do the following:

4a Name the new rule.

4b Click the browse button and locate the application file.

4c Enter the relative path on the Linux Agent(s) where you will deploy the GPO configuration file.

4d Click **Add**.

5. Once you have the application file added to the GPO, make any required configuration changes from the GPEdit Extension options and save your changes to apply the group policy to the Linux Agent computers.

NOTE: You can add and deploy more than one application configuration to a GPO.

Executing Commands with GPOs

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

To execute a command in GPMC:

1. Expand **Linux Settings** in the GPO editor, and click the **Execute Command** node.
2. Click **+** to add a command once if you choose to.
3. Add and save your changes.

Managing User Logins with GPOs

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

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

For information about accessing or creating GPOs in Active Directory, see Accessing or Creating Group Policy Objects.

To configure and apply GPO login settings on Linux agents:

1. Right-click the applicable GPO or GPO link in an OU, and select **Edit** to open the GPO editor.

   If needed, you can create a new GPO that is linked to the OU and then open the editor from the new object.
2. Expand **Linux Settings** in the GPO editor, and click the **AD Login** node.
3. Click the plus icon **+** and select **AD login provider mode**. Then select a mode in the pull-down menu.

   For example, select **Simple allow/deny list**.
4. Click the plus icon **+** again, and select the desired rule.

   For example, select **Prevent these AD users from logging in**.

IMPORTANT: When you configure a GPO to prevent users or groups from logging in, this 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 GPO applied. You cannot have both Allow and Deny logins in the policy at the same time.

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

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

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

Managing User and Group IDs in Linux

You can manage AD objects with Active Directory Users and Computers (ADUC). An ADUC extension based tab **AD Bridge** allows you to manage User ID (UID) and Group ID (GID) for Linux users. The options available to manage are:

- Override ID Mapping
- UID
- GID

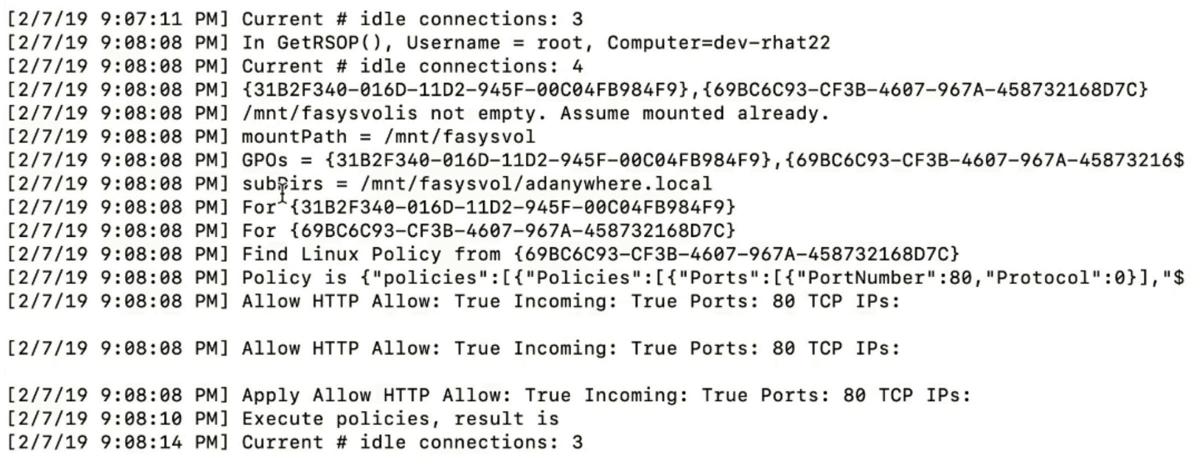
You must follow the steps below to enable this tab:

1. Change directory to `/etc/sssd/sssd.conf`.
2. Edit `sssd.conf` and modify the value of the parameter `ldap_id_mapping` to `False`.
3. Restart the service with either of the commands, `systemctl restart sssd` or `service sssd restart`.

NOTE: You may need to wait for about 15 minutes to see changes take effect.

Viewing Policy Injection on a Linux Agent

When a GPO rule is applied to the OU with one or more AD Bridge Linux agents, that setting is executed on the Linux Agent(s) and can be viewed with a tail of the log at `/var/log/adb-agent.log`, as shown in the example below:



```
[2/7/19 9:07:11 PM] Current # idle connections: 3
[2/7/19 9:08:08 PM] In GetRSOP(), Username = root, Computer=dev-rhat22
[2/7/19 9:08:08 PM] Current # idle connections: 4
[2/7/19 9:08:08 PM] {31B2F340-016D-11D2-945F-00C04FB984F9},{69BC6C93-CF3B-4607-967A-458732168D7C}
[2/7/19 9:08:08 PM] /mnt/fasysvolis not empty. Assume mounted already.
[2/7/19 9:08:08 PM] mountPath = /mnt/fasysvol
[2/7/19 9:08:08 PM] GPOs = {31B2F340-016D-11D2-945F-00C04FB984F9},{69BC6C93-CF3B-4607-967A-45873216$
[2/7/19 9:08:08 PM] subDirs = /mnt/fasysvol/adanywhere.local
[2/7/19 9:08:08 PM] For {31B2F340-016D-11D2-945F-00C04FB984F9}
[2/7/19 9:08:08 PM] For {69BC6C93-CF3B-4607-967A-458732168D7C}
[2/7/19 9:08:08 PM] Find Linux Policy from {69BC6C93-CF3B-4607-967A-458732168D7C}
[2/7/19 9:08:08 PM] Policy is {"policies":[{"Policies":[{"Ports":[{"PortNumber":80,"Protocol":0}],"$
[2/7/19 9:08:08 PM] Allow HTTP Allow: True Incoming: True Ports: 80 TCP IPs:

[2/7/19 9:08:08 PM] Allow HTTP Allow: True Incoming: True Ports: 80 TCP IPs:

[2/7/19 9:08:08 PM] Apply Allow HTTP Allow: True Incoming: True Ports: 80 TCP IPs:
[2/7/19 9:08:10 PM] Execute policies, result is
[2/7/19 9:08:14 PM] Current # idle connections: 3
```

You can also manage policies from the web console including, creation, modification, version control, approval, and deletion of policies for on premises and cloud based resources.

4 Using the Web Console

AD Bridge extends Active Directory (AD) capabilities further by adding a web console to oversee and manage policies and agents. The web console also displays information in figures and charts. This simplifies management and delivers analytics that demonstrate the effectiveness and reach of AD Bridge.

You can identify and manage domain joined Linux devices (both on premises and cloud), on a browser to improve security and provide better visibility into the AD Bridge infrastructure from any supported device and location. 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. The web console displays the following category types with charts:

- **Devices:** You can view and manage environment, agents versions and connection types across the AD Bridge infrastructure and devices.

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

- **Policies:** You can view and manage Linux 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

Creating Universal Policies

To create a Universal Policy from the web console:

1. Click **+** to open the **New Universal Policy** dialog box in the web console.
2. Enter a name for the New Universal Policy.
3. (Optional) Select **Import policies from a GPO in Active Directory** and choose policies to import.
4. Click **Create**.
5. Select the created policy and click **+** to add additional settings.

Exporting Universal Policies

To export a Universal Policy from the web console:

1. Select a Universal Policy and click **Export to Active Directory**.
2. Click **+** to open the **Export Universal Policy** dialog box.

3 Click **+** to open the **Add GPO Deployment Targets** dialog box.

4 Select a deployment target and click **Add**.

5 Troubleshooting

Log files help Micro Focus Technical Support to investigate and isolate the cause of an issue. You can adjust and collect various types of logs that include the following:

- Adjust Global Settings
- Adjust Customer Settings
- Adjust and Collect Gateway Logs
- Adjust and Collect Cloud Gateway Logs
- Adjust and Collect HTTP Call Logs

For detailed contact information, see the Support Contact Information website.

A Appendix

Use this appendix to view the options you have for modifying built-in GPO settings, to view commands and lookups specific to the AD Bridge Linux Agent on Linux devices, and to understand review some best practices for AD Bridge.

Linux Agent GPO Settings

Linux Agent GPO settings include rules for Firewall, Services, OpenSSH, Custom Configuration Files, and managing Active Directory logins. The Firewall settings include default Allow and Deny helper rules that you can configure, but you can also define custom Firewall rules.

Before deploying any configuration changes in your production environment, we strongly recommend that you first deploy GPOs in a Linux test environment to minimize the risk of introducing harmful Group Policy errors.

For examples of how to configure Linux Agent Settings in the GPO editor, see Managing Linux GPO Settings.

Setting Type	Setting Name	Setting Data Type	Input Value (if any)
Firewall	All TCP	Allow/Deny	
	All UDP	Allow/Deny	
	SSH	Allow/Deny	
	HTTP	Allow/Deny	
	HTTPS	Allow/Deny	
	Samba	Allow/Deny	
	SMTP	Allow/Deny	
	MySQL	Allow/Deny	
	FTP	Allow/Deny	
Services	Start	String	
	Stop	String	
	Restart	String	
Configuration Files ◆ SSH ◆ Sudoers			

Setting Type	Setting Name	Setting Data Type	Input Value (if any)
SSH	Log Level	String Enum	QUIET, FATAL, ERROR, INFO, VERBOSE, DEBUG, DEBUG1, DEBUG2, DEBUG3
	Set Login Grace Time	Integer	
	Set Client Alive Count Max	Integer	
	Use GSSAPI Authentication	String Enum	yes, no
	Use GSSAPI KeyExchange	String Enum	yes, no
	Use GSSAPI Cleanup Credentials	String Enum	yes, no
	Use Challenge Response Authentication	String Enum	yes, no
	Use PAM	String Enum	yes, no
	Use Password Authentication	String Enum	yes, no
	Allow Users	String	
	Deny Users	String	
	Deny Groups	String	
Sudoers	Number	Integer	
	Text	String	
	True /False	String Enum	
	Yes /No	String Enum	
Deploy Files	Source File	String	
Execute Commands	Command	String	
AD Logins ◆ On Premises ◆ Cloud			
On Premises	AD login provider mode	String Enum	add, simple, deny
	Allow these AD users to log in	String	
	Allow these AD groups to log in	String	
	Prevent these AD users from logging in	String	
	Prevent these AD groups from logging in	String	

Setting Type	Setting Name	Setting Data Type	Input Value (if any)
Cloud	Allow these AD groups to log in	String	
	Allow users matching this LDAP filter to log in	String	

Linux Agent Commands and Lookups

The items in this section contain useful Linux commands and lookups pertaining to the AD Bridge 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. `/opt/adb-agent`
2. `tail version`

View the GPO 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 Group Policy objects. 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.

GPO Best Practices

Review the best practices in this section when working with Linux Agent GPOs in AD Bridge.

Using the DenyUsers rule in SSH Configuration File settings

SSH DenyUsers for Active Directory user accounts should use '?' in place of '@'. The '?' in sshd is seen as a 1 character to 1 character wildcard. In some Linux platform's the '@' is used only as a Host identifier. Here is an example of the recommended DenyUser SSH Configuration File rule:

```
DenyUser user?domain.local
```

For more information about SSH and the sshd_conf, see https://en.wikibooks.org/wiki/OpenSSH.

Removing GPO SSH Configuration File assignments from Linux agents

Due to the native behavior of working with configuration files in Linux platforms, you should remove the GPO from applicable Linux agents when removing a rule that you previously configured in the GPO. After removing the GPO, you can assign a new GPO if there are additional SSH settings that you require.

For example. If you have a **DenyUsers** SSH rule applied to one or more Linux agents using a Linux Agent GPO and you no longer require this exclusion, you will need to remove the GPO from applicable agents to clear the setting in the SSH configuration file. You can then apply a new GPO that does not have this rule configured.

Understanding the AllowUsers rule in SSH Configuration File settings

When you add the **AllowUsers** rule in SSH Configuration File settings and apply it to one or more Linux agents, you should be aware that those users will be the only Active Directory users that will be able to login using SSH where the Linux agents have the GPO applied.