IBM® Security Privileged Identity Manager
Version 2.1.0

Access Agent on a Gateway Guide

IBM

IBM® Security Privileged Identity Manager
Version 2.1.0

Access Agent on a Gateway Guide

Note

Before using this information and the product it supports, read the information in Notices.

Edition notice

Note: This edition applies to Version 2.1.0 of *IBM Security Privileged Identity Manager* **(product number 5725-H30) and to all subsequent releases and modifications until otherwise indicated in new editions.**

Contents

Figures

Tables

Chapter 1. Overview

Learn about automatic checkout, session recording, and single sign-on with Privileged Access Agent on desktop and application virtualization solutions.

The Privileged Access Agent client typically runs on a user's Windows desktop. However, you can also deploy Privileged Access Agent on remote or virtualized Windows server infrastructure, for example, Citrix XenApp, XenDesktop, or Microsoft Remote Desktop Services.

Privileged users must log on to a remote Windows session on Citrix or Terminal Server, and rely on the Privileged Access Agent instance to check out and single sign-on to resources. The Citrix or Terminal Server (Remote Desktop Services) act as a gateway to the protected targets.

Some IBM® Security Privileged Identity Manager deployments might involve accessing their virtualized application solution with a web-based front end. With a web-based front end, privileged users can use a web browser, over port 443, to connect to a terminal session, or to connect directly into an RDP or PuTTY application session. Privileged Access Agent runs in the background, to assist with credential checkouts and single sign-on.

In deployments with virtual desktops, you can also deploy Privileged Access Agent on Microsoft Windows-based virtual desktops that are hosted on virtual desktop infrastructure, for example, Citrix XenDesktop, in the organization. In virtual desktop environments, privileged users must log in to a virtual desktop by using a VDI client on their computer to perform their privileged tasks.

Chapter 2. Access Agent on Virtual Desktop Infrastructure

Learn how to set up single sign-on, and session recording support on Virtual Desktop Infrastructure, and the different user workflows for accessing the virtual desktop.

Virtual desktop infrastructure

A Virtual Desktop Infrastructure consists of desktop operating systems that are hosted within virtual machines on a centralized server. Privileged Access Agent supports single sign-on to applications running on a virtual desktop.

Users can access the virtual desktops and applications from a desktop PC client or thin client.

Access Agent support for Virtual Desktop Infrastructure workflow

The following diagram describes the workflow for Virtual Desktop Infrastructure support.

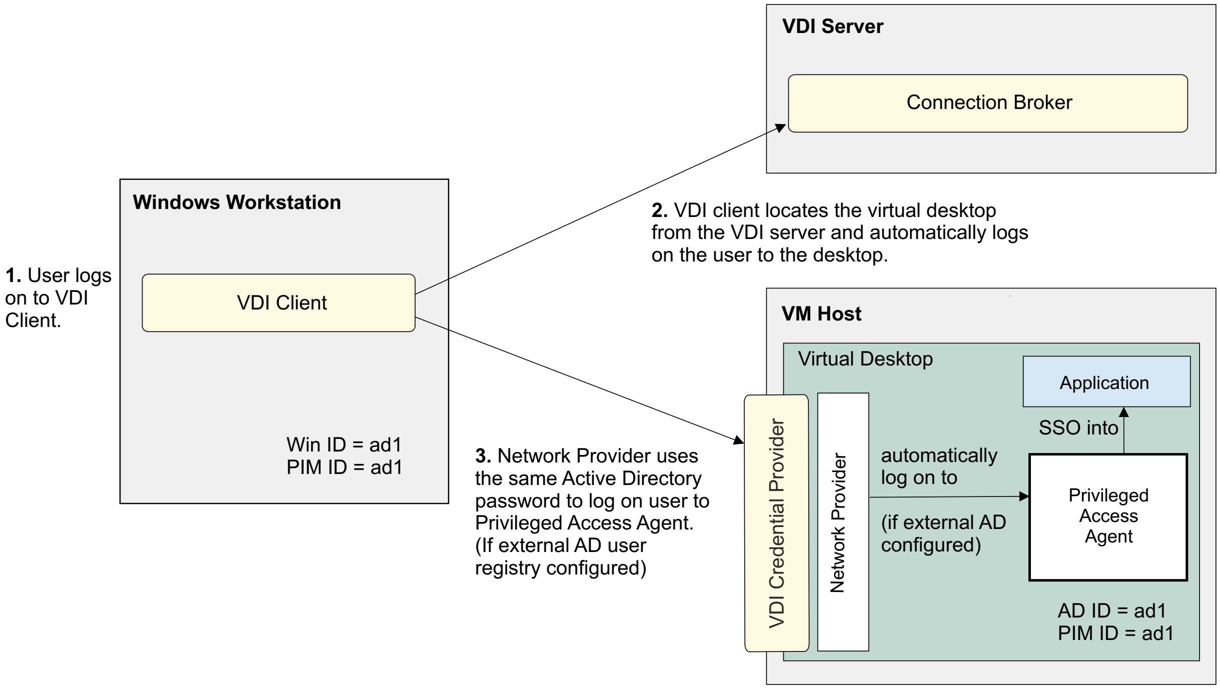
VDI Server
Connection Broker
Windows Workstation
1. User logs on to VDI Client.
VDI Client
Win ID = ad1
PIM ID = ad1
2. VDI client locates the virtual desktop from the VDI server and automatically logs on the user to the desktop.
VM Host
Virtual Desktop
Application
SSO into
3. Network Provider uses the same Active Directory password to log on user to Privileged Access Agent. (If external AD user registry configured)
VDI Credential Provider
Network Provider
automatically log on to
(if external AD configured)
Privileged Access Agent
AD ID = ad1
PIM ID = ad1

Figure 1. Workflow for Virtual Desktop Infrastructure support.

Virtual desktop infrastructure

The following table lists the different VMware Virtual Desktop Infrastructure and Citrix Virtual Desktop Infrastructure components.

Table 1. Component comparison between VMware and Citrix Virtual Desktop Infrastructure solutions.

Component	VMware Virtual Desktop Infrastructure	Citrix Virtual Desktop Infrastructure
Client software	**VMware View Client** This component is installed on all the computers and thin clients through which you want to access the virtual desktops.	**Citrix Receiver** for Citrix XenDesktop: This component provides users with access to their virtual desktops.
Base image agent	**VMware View Agent** This component is installed on all the virtual desktop templates.	**Virtual Delivery Agent** for Citrix XenDesktop. Installed on server or workstation operating systems. The **Virtual Desktop Agent** enables connections for desktops and applications.
Connection server	**VMware View Composer** Use this component to rebalance, recompose, or refresh desktop images regularly.	**Delivery Controller** for Citrix XenDesktop This component creates and manages virtual desktops for users.
Administrative console	**VMware View Administrator** This component is available on the computer where you installed the VMware View Connection Server.	**Studio** for Citrix XenDesktop. The console from which Administrators can install, configure, create, manage virtual desktops, and publish applications.

Planning

Single sign-on on a Virtual Desktop Infrastructure requires configuration. You must know the supported configurations, operating systems, applications, and existing limitations before you proceed with the setup.

Privileged Access Agent configuration

The following configuration is supported:

- See the Software Product Compatibility Report for the supported desktop virtualization solutions.
- The virtual desktop can connect to the IBM Security Privileged Identity Manager server.
- The user is registered to IBM Security Privileged Identity Manager.
- The Machine Policy Template is configured so that Privileged Access Agent logs in using Network Provider configuration.

  Applies only if an external Active Directory user registry is configured. See "Managing the external user registry configuration" in the *IBM Security Privileged Identity Manager Installation and Configuration Guide*.
- Personal desktop mode is supported.
- Single sign-on for applications that are hosted on the virtual desktop are supported.

  Note: Download AccessProfiles for applications from the AccessProfile Library.

Virtual desktop configuration

To manage your virtual desktops:

- Ensure that you configure the `VDIGroupName` and the `MachineTag` in the registry settings. See “VDI registry settings” on page 14.
- Check that the VDI group name that you specified in the registry file is used as the host name for managing the policies in AccessAdmin.
- All computers under the same pool or catalog is shown and managed as one single machine.

Performance configuration

To achieve good performance:

- For deployments with persistent desktops, on the machine policy template, use cached wallets. If not, do not use cached wallets.

  Note: For persistent desktop deployments, set the **Wallet caching option** policy to 2 or always cache.
- Every *N* weeks, recompose the virtual desktop template after Privileged Access Agent synchronizes with the IBM Security Privileged Identity Manager server so that the latest system data is cached into the updated base image. Unnecessary data synchronizations are avoided when new virtual desktops are activated. This step is important for non-persistent desktops.
- For deployments with non-persistent desktops:
  - Allocate more server capacity so that Privileged Access Agent can download the user Wallet upon every logon.
  - Run the cached Wallet pruning script to remove expired and duplicated cached Wallets that are more than 30 days old in the IBM Security Privileged Identity Manager, `essodb`, database.

Limitations

This supported configuration has the following limitations:

- Second-factor authentication is not supported on the virtual desktop.
- PAA Credential Provider is not supported on the virtual desktop.

Configuring

The single sign-on setup tasks are different for VMware View and Citrix XenDesktop. Follow the roadmap that corresponds to your Virtual Desktop Infrastructure.

Set up single sign-on support on Virtual Desktop Infrastructure, by selecting one of the following ways:

- “Roadmap: VMware View configuration”
- “Roadmap: Citrix XenDesktop configuration” on page 6

Roadmap: VMware View configuration

Table 2. VMware View single sign-on setup roadmap.

Step	Task	Reference
1	Verify the VDI environment.	“VDI environment verification” on page 6

Table 2. VMware View single sign-on setup roadmap. (continued)

Step	Task	Reference
2	Create the VDI machine policy template for the base image.	“Creating the VDI machine policy template for the base image”
3	Configure the base image.	“Configuring Access Agent on the base image” on page 7
4	Create virtual desktop pools.	“Creating virtual desktop pools” on page 9 Search for “Creating Desktop Pools” in the VMware website.
5	Optional: Update the base image after changes on the Access Agent.	“Updating the base image after changes on the Access Agent” on page 11

Roadmap: Citrix XenDesktop configuration

Table 3. Citrix XenDesktop single sign-on setup roadmap.

Step	Task	Reference
1	Verify the VDI environment.	“VDI environment verification”
2	Create the VDI machine policy template for the base image.	“Creating the VDI machine policy template for the base image”
3	Configure the base image.	“Configuring Access Agent on the base image” on page 7
4	Create a machine catalog.	“Creating a machine catalog” on page 10
5	Optional: Update the base image after changes on the Access Agent.	“Updating the base image after changes on the Access Agent” on page 11

VDI environment verification

An Administrator must verify the VDI environment before the preparation of the base image and the virtual desktops.

If you are using VMware View

Prepare the VMware View components. Go to the VMware website and search for “VMware View product documentation”.

1. Verify that the View Connection Server is running.
2. Verify that the VMware vCenter Server settings and the **View Composer Settings** are correct.

If you are using Citrix XenDesktop

Prepare the Citrix XenDesktop components. Go to the Citrix website, and search for “Citrix XenDesktop product documentation”

Verify that the Citrix XenController is running.

Creating the VDI machine policy template for the base image

Use a machine policy template to apply a set of policies specific for Virtual Desktop Infrastructure support.

Procedure

1. Log on to AccessAdmin.
2. Select **Machine Policy Templates** > **New template**.
3. Set the name of the new template to `VDI BaseImage MPT`.

   Note: The name is case-sensitive, so **Example** and **example** are two different template names.
4. Specify a criteria to assign a machine policy template. For example: **machine tag**.

   Note:
   - If you use machine tag, assign a name for it. The machine tag name must be the same as the value specified in the `VDI_config.reg` file. The default value is `vdi_tag_example`.
   - You can also use other criteria such as IP address, host name, or others. See "Setting machine criteria" in the *IBM Security Access Manager for Enterprise Single Sign-On Administrator Guide*.
5. Enable Network Provider in this machine policy template.
   a. Navigate to **Access Agent Policies** > **Logon/Logoff Policies**.
   b. Set the value of **Enable Network Provider** to **Yes**.
6. Click **Add** to save the new settings.
7. Under **Machine policy template assignments**, select the **VDI BaseImage MPT** template and click the **Up arrow** icon until the **VDI BaseImage MPT** is at the top of the **Machine policy template assignments** list.
8. Verify that the base image machine name is removed from the IBM Security Privileged Identity Manager server through AccessAdmin.

Configuring Access Agent on the base image

An Administrator must configure Privileged Access Agent on the base image to support single sign-on on a Virtual Desktop Infrastructure.

Before you begin

- Ensure that you created the `VDI BaseImage MPT` machine policy template. See “Creating the VDI machine policy template for the base image” on page 6.
- Complete the “VDI environment verification” on page 6.
- Ensure that the VDI Agent is installed on the virtual machine before Privileged Access Agent.
  – For VMware View: VMware View Agent
  – For Citrix XenDesktop: Virtual Desktop Agent
- Ensure that base image can communicate with VMware View or Citrix XenDesktop server. For example: ping `<server name>`
- Make a copy or know the location of the following files:
  – Privileged Access Agent installer
  – `VDI_config.reg`. See “VDI registry settings” on page 14 for the content of this file.
- Verify that the base image machine name is removed from the IBM Security Privileged Identity Manager server through AccessAdmin.

About this task

All virtual desktops are created from a base image. Different desktop pools use different base image.

This task consists of:

- Pre-configuring and installing Privileged Access Agent.
- Configuring and applying the registry settings.

Procedure

1. Configure the `SetupHlp.ini` file in the Privileged Access Agent installer.
   a. Open the `<`*`Access Agent_installer`*`>\Config\SetupHlp.ini` file with any file editor.
   b. Set **`EnginaEnabled`** to `0`. Default value is 1.
   c. Set **`EncentuateCredentialProviderEnabled`** to `0`. Default value is 1.
   d. Set **`DisableWin7CAD`** to `0`. Default value is 1.
   e. Ensure that **`EncentuateNetworkProviderEnabled`** is set to 1. Default value is 1.
   f. Save the file.
2. Copy the `VDI_config.reg` file into the `<`*`Access Agent_installer`*`>\Reg` folder.

   For steps on preparing the `VDI_config.reg` file, see "VDI registry settings" on page 14.

   Important:

   - Make sure that the **MachineTag** name in this registry file is the same as the machine tag criteria specified in the **VDI BaseImage MPT** machine policy template. See step 4 on page 7 from "Creating the VDI machine policy template for the base image" on page 6.
   - Assign a VDI group name in the registry file. The group name can be your VDI pool name. The VDI group name that you specify in the registry file is used as the host name for managing the policies in AccessAdmin.
3. Install Privileged Access Agent.
   a. Set the IBM Security Privileged Identity Manager server location.
   b. Ensure that the machine Wallet is downloaded.

      Note: The machine Wallet is not downloaded until you restart the computer.

   Privileged Access Agent automatically applies the `SetupHlp.ini` settings and the registry settings to the base image.
4. Verify that the correct **VDI BaseImage MPT** machine policy template is assigned to the base image.
   a. Log on to AccessAdmin.
   b. Search the machine and check the assigned template.
5. Restart the computer.
6. Install the latest fix pack (if any).
7. Log on to the computer.

   Note: If an external Active Directory user registry is configured, log on with a domain account that is registered with the IBM Security Privileged Identity Manager server.

8. Log on to Privileged Access Agent with a IBM Security Privileged Identity Manager user account.

   Note: If an external Active Directory user registry is configured, you do not need to log in manually to Privileged Access Agent.
9. Shut down the computer.
10. Take a snapshot of the virtual machine where you pre-configured and installed Privileged Access Agent.
    a. Assign a name for the virtual machine snapshot and provide a description for it.
    b. Click **OK**.
    c. Ensure that the snapshot is complete before you create a virtual desktop pool.

Results

Privileged Access Agent is installed and with the required policies configured.

You created the base image to be used for the virtual desktops.

What to do next

- For VMware View: Create a virtual desktop pool.
- For Citrix XenDesktop: Create a machine catalog.

Creating virtual desktop pools

Create pools of desktops to deliver View desktop access to users. You can choose from automated pool or manual pool.

Before you begin

Complete the following tasks:
- "VDI environment verification" on page 6.
- "Configuring Access Agent on the base image" on page 7.

About this task

This task is intended for Administrators.

Go to the VMware website and search the VMware View product documentation on "Creating Desktop Pools" and "Entitling Users and Groups".

The following instructions describe an outline of the procedure for VMware Virtual Desktop Infrastructure.

Procedure

1. Log on to the VMware View Administrator with a domain user account.
2. Select **Inventory** > **Pools**.
3. Click **Add** to start the Add Pool wizard.
4. Follow the wizard. Select the settings according to your requirement.
5. When you configure the vCenter settings, select the snapshot of the base image that has the installation of Privileged Access Agent.
6. Follow the wizard. Select the settings according to your requirement.

7. Double-click the desktop pool that you created to view the details and for more configurations.
8. Select the users who can access the desktops in the pool you created.
9. Click **OK**.

Results

The desktop pool is created and users are assigned to the desktop pool.

Users can start accessing the virtual desktops created from the desktop pool.

Creating a machine catalog

In Citrix XenDesktop, create a Catalog of machines and desktop groups to deliver desktops to users.

About this task

This task is intended for Administrators.

For the detailed steps, go to the Citrix website, and search the Citrix XenDesktop product documentation for “Creating a machine catalog”.

The following instructions outline the high-level tasks for Citrix XenDesktop.

Procedure

1. Log on to Citrix Desktop Studio with a domain user account.
2. Click **Machines** > **Create Catalog**.
3. Follow the wizard. Select the settings according to your requirement.

   Note:

   - If you select the random desktop option from the Desktop Experience page, the user is assigned to a random machine during logon. Any changes that are made during the session, such as Privileged Access Agent logs, are discarded after the session is closed.
   - If you select the static desktop option, the user is always connected to the same machine during logon. The user can customize the desktop and can store files on the machine.
4. On the Master Image page, select the snapshot of the base image that has the installation of Privileged Access Agent.
5. Follow the wizard. Select the settings according to your requirement.

Results

You have a Catalog of machines. To deliver desktops to users from your Catalog, allocate the machines to users by creating desktop groups or delivery groups.

For the detailed steps, go to the Citrix website, and search the Citrix XenDesktop product documentation for “Creating desktop groups or delivery groups”.

Users can start accessing the virtual desktops created from your Catalog.

Updating the base image after changes on the Access Agent

Update Privileged Access Agent in the base image to apply a fix pack or change a registry policy.

About this task

This task is intended for Administrators. For more information about updating user desktops, see http:/support.citrix.com/proddocs/topic/xendesktop-rho/cds-update-master-vm-rho.html.

Procedure

1. Log on to the virtual machine you used for the base image.
2. Update Privileged Access Agent in the base image. You can update Privileged Access Agent by doing one of the following tasks:
   - Apply the latest Privileged Access Agent fix pack.
   - Update the registry policies. See “VDI registry settings” on page 14 for the configurable policies.
3. Wait for Privileged Access Agent to synchronize with any changes in the system policies and AccessProfiles.
4. Take a snapshot of the virtual machine where you applied the fix pack.
5. If you are using VMware View, do the following tasks:
   a. Log on to the VMware View Administrator.
   b. Select the desktop pool.
   c. Open VMware View Composer.
   d. Click **Recompose** to apply the new versions of the base image to all users or a subset of the linked clones.
6. If you are using Citrix XenDesktop, do the following tasks:
   a. Log on to the Citrix Desktop Studio.
   b. Click **Machines**.
   c. Select your Catalog.
   d. Click **Update machine**.

Virtual desktop single sign-on experience

Learn what single sign-on users experience to log on to a virtual desktop.

Access a virtual desktop from a client computer without Access Agent

Users can access a virtual desktop from a thin client or from a local computer without an installed Privileged Access Agent. In this scenario, users are not automatically logged on to the virtual machine.

Access through VMware View

1. Verify that you have a VMware View Client installed.
2. Open the VMware View Client.
3. Specify the **Connection Server** IP address or host name.
4. Click **Connect**. The Log On window is displayed.
5. Enter your domain user account password.
6. Click **Login**.

7. Select the virtual desktop to be used.
8. Click **Connect**.

Access through Citrix XenDesktop

1. Verify that you have a Citrix Online Plug-in or Citrix Receiver installed.
2. Ensure that you installed the Citrix plug-in. Otherwise, you are prompted to install the plug-in when you log on to Citrix Web Access.
3. Open Citrix Web Access. For example: `https://<DeliveryController_name>\Citrix\StoreWeb`.
4. Log on with your user name and password.
5. Select the virtual desktop or desktop group.

Results

You are connected to the selected virtual desktop.

You are automatically logged on to Privileged Access Agent in the virtual desktop.

Note: This statement applies only if an external Active Directory user registry is configured with IBM Security Privileged Identity Manager.

You can single sign-on to applications in the virtual desktop.

Troubleshooting virtual desktop issues

You might encounter issues when you log on to Windows in the virtual desktop. Misconfiguration can cause these issues.

Misconfiguration issues

Issue 1: Logon to Windows succeeded. Log on to Privileged Access Agent with EnNetworkProvider failed.

Symptom:

When the user logs on to the virtual desktop, VMware View Client automatically logs on the user to Windows. However, the user is not automatically logged on to Privileged Access Agent.

Cause: Any of these factors can cause this issue:

- Active Directory password synchronization is not enabled.
- The **VDI BaseImage MPT** machine policy template is not applied in the base image.
- The required registry settings are not applied in the base image. See "VDI registry settings" on page 14.
- The virtual machine cannot connect to the IBM Security Privileged Identity Manager server and there is no cached Wallet.

Solution

- Verify that the Active Directory password synchronization is enabled.
- Verify that EnNetworkProvider is enabled in the **VDI BaseImage MPT** machine policy template and that this template is applied

to the base image and virtual desktops. See "Creating the VDI machine policy template for the base image" on page 6.

- Make sure that the **VDI BaseImage MPT** machine policy template is at the **top** of the Machine Policy template assignments list. See step7 on page 7 from "Creating the VDI machine policy template for the base image" on page 6.
- Verify that automatic logon succeeds in the base image.
- The virtual machine can connect to the IBM Security Privileged Identity Manager server.

Issue 2: Logon to Windows failed. PAA Credential Provider is displayed.

Symptom:

When user logs on to the virtual desktop through VMware View Client, the user is not automatically logged on to Windows. The user is prompted with the PAA Credential Provider.

Cause:

The required Privileged Access Agent installer settings are not configured before Privileged Access Agent is installed in the base image.

Solution:

1. Uninstall Privileged Access Agent from the base image.
2. Reconfigure the base image.

   Important: Ensure that the **`EnginaEnabled`** and **`EncentuateCredentialProviderEnabled`** settings in the Privileged Access Agent installer are set to `0`.
3. Log on to the VMware View Administrator.
4. Select the desktop pool.
5. Open VMware View Composer.
6. Click **Recompose** to apply the new versions of the base image to all users or a subset of the linked clones.

Issue 3: Logon to Windows failed. Microsoft Credential Provider is displayed.

Symptom:

When user logs on to the virtual desktop through VMware View Client, the user is not automatically logged on. The user is prompted with the Microsoft Credential Provider. This issue occurs only in Windows 7.

Cause:

The **`DisableWin7CAD`** setting in the Privileged Access Agent installer is not configured correctly.

Solution:

On the base image:

1. Open the Local Security Policy Console.
   a. Click the **Start** menu.
   b. Type `Local Security Policy`.
   c. Press **Enter**.
2. Expand the **Local Policies**.

3. Click **Security Options**.
4. Double-click **Interactive logon: Do not require CTRL+ALT+DEL**.
5. Select **Disabled**.
6. Click **OK**.
7. Log on to the VMware View Administrator.
8. Select the desktop pool.
9. Open VMware View Composer.
10. Click **Recompose** to apply the new versions of the base image to all users or a subset of the linked clones.

VDI registry settings

Ensure that you apply the required registry settings to support Virtual Desktop Infrastructure.

Required registry settings

Prepare a file, enter the following configuration details, and save the file with a `.reg` file extension. For example: `VDI_config.reg`

See the following settings that are required for Virtual Desktop Infrastructure support:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ISPIM\DeploymentOptions]
"VDIGroupName"="vdi_pool_example"
"MachineTag"="vdi_tag_example"
```

Chapter 3. Access Agent on Citrix and Terminal Server

Learn more about the required configurations and supported workflows in the Terminal Services and Citrix Servers.

Access Agent on Citrix and Terminal Servers

IBM Security Privileged Identity Manager supports automatic checkout and single sign-on for applications that are hosted on Citrix and Terminal Servers – Citrix XenApp Servers or Microsoft Remote Desktop Services.

You must install Privileged Access Agent on each Citrix or Terminal Server (Remote Desktop Services).

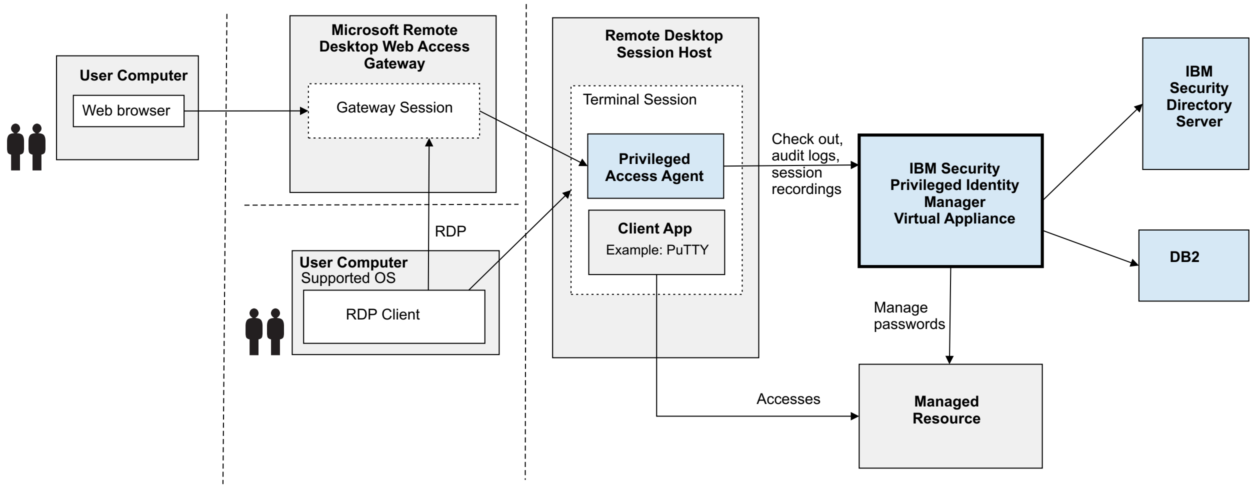
User Computer
Web browser
Microsoft Remote Desktop Web Access Gateway
Gateway Session
RDP
User Computer
Supported OS
RDP Client
Remote Desktop Session Host
Terminal Session
Privileged Access Agent
Client App
Example: PuTTY
Check out, audit logs, session recordings
IBM Security Privileged Identity Manager Virtual Appliance
IBM Security Directory Server
DB2
Manage passwords
Accesses
Managed Resource

Figure 2. Privileged Access Agent support on Terminal Server (Microsoft Remote Desktop Services).

For every remote session on Citrix or Terminal Server (Remote Desktop Services), there is a running Privileged Access Agent instance.

Privileged Access Agent helps users single sign-on to their applications on the particular remote session. Users can later reconnect to the same remote session on the Citrix or Terminal Server (Remote Desktop Services) through any client computer.

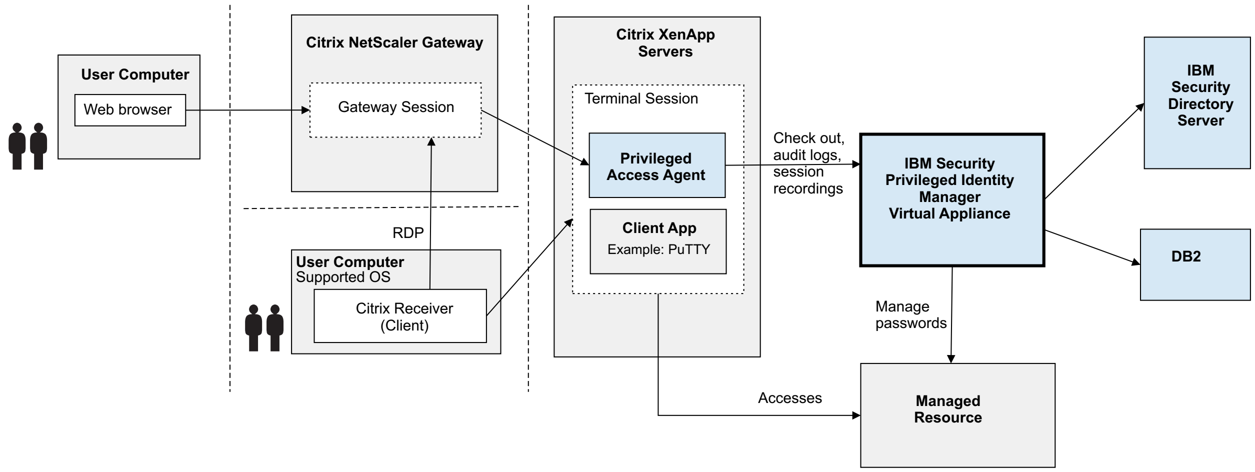

Figure 3. Privileged Access Agent support on Citrix XenApp and XenDesktop.

Configuring

This configuration consists of deploying Privileged Access Agent on the Citrix or Terminal Server (Remote Desktop Services) and enabling the PAA Network Provider.

In this configuration, the Privileged Access Agent automatically logs on the user to IBM Security Privileged Identity Manager upon logon to the Citrix or Terminal Server (Remote Desktop Services) remote session, if IBM Security Privileged Identity Manager is configured with an external Active Directory user registry.

If IBM Security Privileged Identity Manager is not configured with an external Active Directory user registry, you can log on manually to Privileged Access Agent. Launch the Privileged Access Agent tray application, and provide IBM Security Privileged Identity Manager credentials.

Deploying the configuration

Configure the Privileged Access Agent and the Citrix or Terminal Server (Remote Desktop Services) to deploy this configuration.

Before you begin

You must modify the `SetupHlp.ini` file before you install the Privileged Access Agent. You can access this file in the `Config` folder of the Privileged Access Agent installation package.

Specify the following options in the `SetupHlp.ini` file:

Option	Description
`EncentuateNetworkProviderEnabled`	Set to 1 to enable the PAA Network Provider.
`EncentuateCredentialProviderEnabled` and `EnginaEnabled`	Set to `0` to disable the PAA Credential Provider.

Procedure

1. On the Citrix or Terminal Server (Remote Desktop Services), install the Privileged Access Agent on the Citrix or Terminal Server (Remote Desktop Services).
2. Log on to AccessAdmin.
3. Select **Machine Policy Templates** > **New template**.
4. Enter a name. For example: `RDS BaseImage MPT`
5. For machine criteria, set the template as default for new computers.
6. Enable the network provider.
   a. Navigate to **AccessAgent Policies** > **Logon/Log off Policies**.
   b. Set **Enable Network Provider?** to **Yes**.
7. Click **Add**.
8. Under **Machine policy template assignments**, move the `RDS BaseImage MPT` template to the top of the list.

   Note: There is no required installation and configuration on the client machine. There is no optional configuration.

Single sign-on experience

When IBM Security Privileged Identity Manager is configured with an external Active Directory registry, users can automatically log on, single sign-on to profiled applications, and manage credentials.

In this configuration, the user can:

- If an Active Directory is configured and IBM Security Privileged Identity Manager is configured to use an external Active Directory registry, log on to the Citrix or Terminal Server (Remote Desktop Services) remote session with Active Directory credentials. The user is automatically logged on to the Wallet.
- If IBM Security Privileged Identity Manager is not configured with an external Active Directory user registry, you are not logged on automatically to your Wallet. Launch the Privileged Access Agent tray icon and log on manually with IBM Security Privileged Identity Manager credentials.
- Access published applications in seamless mode. The Privileged Access Agent tray icon is added to the client taskbar.
- Single sign-on to profiled applications.

How users experience single sign-on with Privileged Access Agent on Citrix or Terminal Server (Remote Desktop Services)

1. Log in with the appropriate RDP or Citrix client.

   Authenticate with the necessary Windows credentials.
2. Take one of the following actions:
   - If Active Directory credentials are used and the Active Directory is configured as an external user registry with IBM Security Privileged Identity Manager,Privileged Access Agent logs the user in automatically. Continue to step 4.
   - If IBM Security Privileged Identity Manager is not configured with an external Active Directory registry, continue to step 3.
3. If not already prompted, launch the Privileged Access Agent tray application, and enter your configured IBM Security Privileged Identity Manager credentials.

4. Start a supported client application for automatic logon.

   Single sign-on triggers.

Customizing Access Agent on Citrix and Terminal Servers

You can customize the behavior of Privileged Access Agent when users log on to a session on a Citrix or Terminal Server (Remote Desktop Services).

Procedure

1. Log on to AccessAdmin.
2. Go to **Machine Policy Templates** > **Template assignments**.
3. Click a policy template.
4. Go to **AccessAgent Policies** > **Terminal Server Policies**.
5. Complete the following fields:

Option	Description
Enable auto-launching of AccessAgent logon prompt	Identifies whether to launch the Privileged Access Agent logon dialog if Privileged Access Agent is not logged on when a Citrix application or a Terminal Server session is launched.
Option for displaying menu options on remote AccessAgent	Whether to display menu options on Privileged Access Agent user interface in a Citrix or Terminal Server (Remote Desktop Services) session.

6. Click **Update**.
7. Assign the updated machine policy template to the Citrix or Terminal Server (Remote Desktop Services).

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law :

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability
These terms and conditions are in addition to any terms of use for the IBM website.

Personal use
You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use
You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at http://www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

This Software Offering uses other technologies that collect each user's user name, password or other personally identifiable information for purposes of session management, authentication, single sign-on configuration, usage tracking, or functional purposes. These technologies can be disabled, but disabling them will also eliminate the functionality they enable.

This Software Offering does not use cookies to collect personally identifiable information. The only information that is transmitted between the server and the browser through a cookie is the session ID, which has a limited lifetime. A session ID associates the session request with information stored on the server.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details/us/en sections entitled “Cookies, Web Beacons and Other Technologies” and “Software Products and Software-as-a Service”.

Printed in USA