INTEGRATION PACK FOR CITRIX VIRTUAL APPS AND DESKTOPS

For Microsoft System Center Orchestrator

For System Center 2016 and 2019, you must use the 32-bit version of the integration pack, which has the name **Kelverion_Integration_Pack_for_Citrix_Virtual_Apps_and_Desktops_2.0**

For System Center 2022 and later, you must use the 64-bit version of the integration pack, which has the name **Kelverion_IP_Citrix_Virtual_Apps_and_Desktops_x64_2.0**

User Guide

Version 2.0

Kelverion Integration Pack for Citrix Virtual Apps and Desktops

Published: May 2023

Feedback

Send suggestions and comments about this document to support@kelverion.com

Contents

Getting Started

The **Kelverion Integration Pack for Citrix Virtual Apps and Desktops** is an add-on for System Center Orchestrator that enables you to integrate with Citrix Virtual Apps and Desktops environment and automate virtual desktop configuration and management processes.

System Requirements

The Integration Pack for Citrix Virtual Apps and Desktops requires the following software to be installed and configured prior to implementing the integration. For more information about installing and configuring Orchestrator, refer to the respective product documentation.

Kelverion_Integration_Pack_for_Citrix_Virtual_Apps_and_Desktops (32-bit)

- Microsoft System Center Orchestrator 2016, 2019
- Microsoft .NET Framework 4.7.2
- Microsoft Windows PowerShell 3.0
- Microsoft Windows Remote Management (WinRM)
- Citrix Virtual Apps and Desktops 7 2103, 2203

Kelverion_IP_for_Citrix_Virtual_Apps_and_Desktops_x64 (64-bit)

- Microsoft System Center Orchestrator 2022
- Microsoft .NET Framework 4.7.2
- Microsoft Windows PowerShell 3.0
- Microsoft Windows Remote Management (WinRM)
- Citrix Virtual Apps and Desktops 7 2103, 2203

Registering and Deploying the Integration Pack

After you download the integration pack file, you must register it with the Orchestrator management server and then deploy it to Runbook Servers and Runbook Designers. For more information about how to install integration packs, see the How to Install an Integration Pack in the online documentation for System Center Orchestrator.

IMPORTANT: Ensure that you are deploying the correct version of the Integration Pack.

- For System Center 2016 and 2019, you must use the 32-bit version of the integration pack, which has the name **Kelverion_Integration_Pack_for_Citrix_Virtual_Apps_and_Desktops**
- For System Center 2022 and later, you must use the 64-bit version of the integration pack, which has the name **Kelverion_IP_Citrix_Virtual_Apps_and_Desktops_x64**

To register the integration pack:

1. On the management server, copy the **.OIP** file for the integration pack to a local hard drive or network share.

2. Confirm that the file is not set to **Read Only** to prevent unregistering the integration pack later.
3. Start the **Deployment Manager**.
4. In the navigation pane of the Deployment Manager, expand **Orchestrator Management Server**, right-click **Integration Packs** to select **Register IP with the Orchestrator Management Server**. The **Integration Pack Registration Wizard** opens.
5. Click **Next**.
6. In the **Select Integration Packs or Hotfixes** dialog box, click **Add**.
7. Locate the **.OIP** file that you copied locally from step 1, click **Open** and then click **Next**.
8. In the **Completing the Integration Pack Wizard** dialog box, click **Finish**.
9. On the **End User Agreement** dialog box, read the Kelverion License Terms**,** and then click **Accept**.
10. The **Log Entries** pane displays a confirmation message when the integration pack is successfully registered.

To deploy the integration pack:

1. In the navigation pane of the **Deployment Manager**, right-click **Integration Packs**, click **Deploy IP to Runbook Server or Runbook Designer**.
2. Select the integration pack you want to deploy, and then click **Next**.
3. Enter the name of the runbook server or computers with the Runbook Designer installed, on which you want to deploy the integration pack, click **Add**, and then click **Next**.
4. Continue to add additional runbook servers and computers running the Runbook Designer, on which you want to deploy the integration pack. Click **Next**.
5. In the **Installation Options** dialog box, configure the following settings.
6. To choose a time to deploy the integration pack, select the **Schedule installation** check box, and then select the time and date from the **Perform installation** list.
7. Click one of the following:
    a. **Stop all running runbooks before installing the integration pack** to stop all running runbooks before deploying the integration pack.
    b. **Install the Integration Packs without stopping the running Runbooks** to install the integration pack without stopping any running runbooks.
8. Click **Next**.
9. In the **Completing Integration Pack Deployment Wizard** dialog box, Click **Finish**.
10. When the integration pack is deployed, the Log Entries pane displays a confirmation message.

Licensing the Integration Pack

After you register and deploy the integration pack you must provide a valid Kelverion license before running any runbooks that contain activities from the integration pack

To deploy the integration pack license file to System Center Orchestrator 2019 or earlier:

1. Copy the .KAL license file to %PROGRAMFILES(X86)%\Kelverion Automation\Licenses
2. Repeat for each Orchestrator Runbook Server and Runbook Designer host system.

To deploy the integration pack license file to System Center Orchestrator 2022 or later:

1. Copy the .KAL license file to %PROGRAMFILES%\Kelverion Automation\Licenses
2. Repeat for each Orchestrator Runbook Server and Runbook Designer host system.

Orchestrator Configuration

A configuration establishes a reusable link between Orchestrator and Citrix Virtual Apps and Desktops. You can create multiple connections, as you require, specifying links to multiple Virtual Apps and Desktops servers.

To set up a Citrix Virtual Apps and Desktops configuration:

1. In the Client, click the **Options** menu, and select **KA Citrix Virtual Apps and Desktops**. The **KA Citrix Virtual Apps and Desktops** dialog box appears.
2. On the **Configurations** tab, click **Add**. The **Add Configuration** dialog box appears.
3. In the **Name** box, enter a name for the configuration. This could be the name of the Citrix Virtual Apps and Desktops server or a descriptive name to distinguish the type of configuration.
4. Click the ellipsis button (…) next to the **Type** box and select **Connection Configuration**.
5. In the **XenDesktop Server** box, enter the FQDN or the IP address of the machine where your Virtual Apps and Desktops server (controller) is installed.
6. In the **XenDesktop Server Port** box enter the port used to communicate with the Virtual Apps and Desktops server. Typical values are 80 for HTTP and 443 for HTTPS.
7. In the **XenDesktop SDK Host** box enter the FQDN of the machine where the Virtual Apps and Desktops PowerShell SDK has been installed. For optimal performance it is recommended to install the Virtual Apps and Desktops SDK on the Orchestrator Runbook Service machine.
8. In the **XenDesktop SDK Host Port** box enter the port used to communicate with the machine where the Virtual Apps and Desktops PowerShell SDK has been installed. Typical values are 5985 for HTTP and 5986 for HTTPS.
9. In the **XenDesktop Admin User** box enter a domain user with permissions to administer the Virtual Apps and Desktops environment, in the form *DOMAIN\user.*

10. In the **XenDesktop Admin User Password** box enter the password of the Virtual Apps and Desktops admin user.
11. The **Use SSL** box specifies whether the IP uses HTTPS or HTTP to communicate with the SDK Host. Select **True** to use SSL over HTTPS. Select **False** to use HTTP. Note that configuring this also requires the **SDK Host Port** to be configured appropriately.
12. The **Skip CA Check** box specifies whether the client does not validate that the server certificate is signed by a trusted certificate authority (CA) when connecting over HTTPS (**Use SSL** box is **True**).
13. The **Skip CA Check** box specifies whether the client does not validate that the server certificate is signed by a trusted certificate authority (CA) when connecting over HTTPS (**Use SSL** box is **True**). Select **True** when the remote server is trusted by using another mechanism, such as when the remote computer is part of a network that is physically secure and isolated or when the remote computer is listed as a trusted host in a WinRM configuration.
14. The **Skip CN Check** box specifies whether the certificate common name (CN) of the server does not need to match the hostname of the server, when connecting over HTTPS (**Use SSL** box is **True**). Select **True** for trusted servers.
15. The **Skip Revocation Check** box specifies whether the revocation status of the server certificate is validated or not.
16. Click **OK**, and then click **Finish**.

Installing and Configuring WinRM

The integration pack requires Windows Remote Management (WinRM) to be installed and configured for the integration pack to connect and communicate with the machine where the Virtual Apps and Desktops PowerShell SDK has been deployed. The PowerShell SDK is typically installed on the machine where Citrix Studio is installed. However, for optimal performance, it is recommended to install the Power SDK on the Orchestrator machine and make this machine part of the domain where your desktop infrastructure is running.

To configure WinRM when the PowerShell SDK is running on the Orchestrator Machine:

1. Install and configure Windows Remote Management (WinRM) on the Orchestrator machine. This machine should be configured as a WinRM client and a WinRM server. Refer to http://msdn.microsoft.com/en-us/library/aa384372%28v=vs.85%29.aspx and to WinRM Configuration Steps.
2. Install the Virtual Apps and Desktops PowerShell SDK on the Orchestrator machine. You can install the SDK by installing Citrix Studio - refer to Install instructions (https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/install-configure/install-core.html).
3. Specify the Orchestrator machine as the **XenDesktop SDK Host** in the integration pack configuration options.

4. Set PowerShell script execution policy to Remote Signed on the Orchestrator machine – start Windows PowerShell (x86) and run PS command *Set-ExecutionPolicy RemoteSigned*.

To configure WinRM when the PowerShell SDK is running on Citrix Studio machine:

1. Install and configure Windows Remote Management (WinRM) on the Orchestrator machine. This machine should be configured as a WinRM client. Refer to http://msdn.microsoft.com/en-us/library/aa384372%28v=vs.85%29.aspx and to WinRM Configuration Steps.
2. Install and configure Windows Remote Management (WinRM) on the machine where the Virtual Apps and Desktops PowerShell SDK has been installed. This machine should be configured as a WinRM server. Refer to http://msdn.microsoft.com/en-us/library/aa384372%28v=vs.85%29.aspx and to WinRM Configuration Steps.
3. Specify the machine where the Virtual Apps and Desktops PowerShell SDK is installed as the **XenDesktop SKD Host** in the integration pack configuration options. The PowerShell SDK is typically installed on the machine where Citrix Studio is installed.
4. Set PowerShell script execution policy to Remote Signed on the Orchestrator machine – start Windows PowerShell (x86) and run PS command *Set-ExecutionPolicy RemoteSigned*.

WinRM Server Configuration

The Integration Pack requires WinRM to be installed and configured in order for the Orchestrator machine (WinRM Client) to communicate with the machine where the Virtual Apps and Servers PowerShell SDK has been installed (WinRM server).

To configure a WinRM server:

Follow these steps to configure a WinRM server machine – the machine where the Virtual Apps and Desktops PowerShell SDK has been installed.

1. Configure a WinRM HTTP listener on the SDK Host machine (WinRM server) by opening a PowerShell console (Run as Administrator) and running the *winrm quickconfig*.

```
PS C:\Users\orchadmin> winrm quickconfig
WinRM service is already running on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
Enable the WinRM firewall exception.

Make these changes [y/n]? y

WinRM has been updated for remote management.

Created a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.
WinRM firewall exception enabled.
```

2. If you want to configure a HTTPS listener, use *winrm quickconfig –transport:https*. Note that HTTPS requires a valid SSL certificate to be configured on the server machine.
3. Make sure that CredSSP authentication is enabled. This can be accomplished either by running a PowerShell command or by via the group policy configuration utility (gpedit.msc).
    a. PowerShell command: ***Enable-WSMANCredSSP -Role Server***

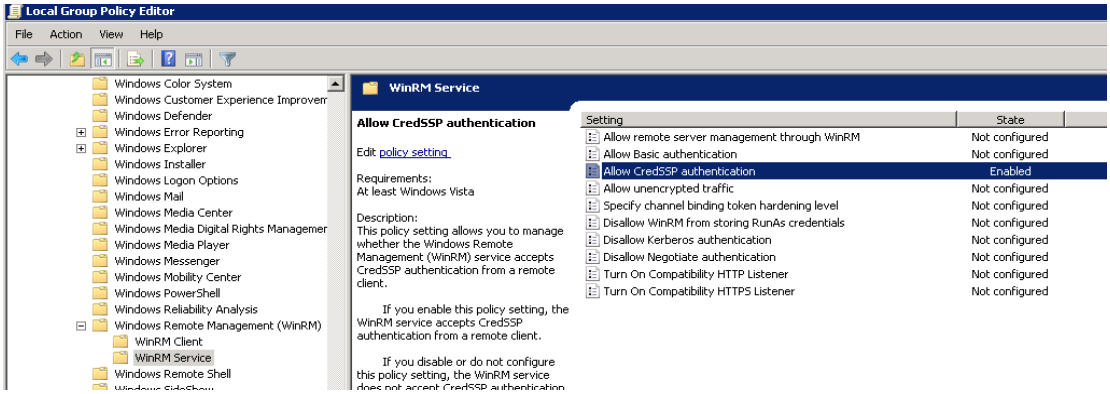
```
PS C:\Windows\system32> Get-WSManCredSSP
The machine is not configured to allow delegating fresh credentials.
This computer is not configured to receive credentials from a remote client computer.
PS C:\Windows\system32> Enable-WSManCredSSP -Role Server

CredSSP Authentication Configuration for WS-Management
CredSSP authentication allows the server to accept user credentials from a remote computer. If you enable CredSSP
authentication on the server, the server will have access to the user name and password of the client computer if the
client computer sends them. For more information, see the Enable-WSManCredSSP Help topic.
Do you want to enable CredSSP authentication?
[Y] Yes  [N] No  [S] Suspend  [?] Help (default is "Y"): y


cfg               : http://schemas.microsoft.com/wbem/wsman/1/config/service/auth
lang              : en-US
Basic             : false
Kerberos          : true
Negotiate         : true
Certificate       : false
CredSSP           : true
CbtHardeningLevel : Relaxed


PS C:\Windows\system32> _
```

b. Alternatively, navigate to **Computer Configuration -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Service** and enable **Allow CredSSP authentication**.



WinRM Client Configuration

Follow these steps to configure a WinRM client machine – the machine where the Orchestrator Runbook Service is running:

On the WinRM client machine, make sure that CredSSP authentication is enabled and allow delegation of credentials to WinRM Server machine. This can be accomplished in either with a PowerShell command or via the group policy configuration utility (gpedit.msc):

To configure the WinRM client:

Open PowerShell and run the following PowerShell command:

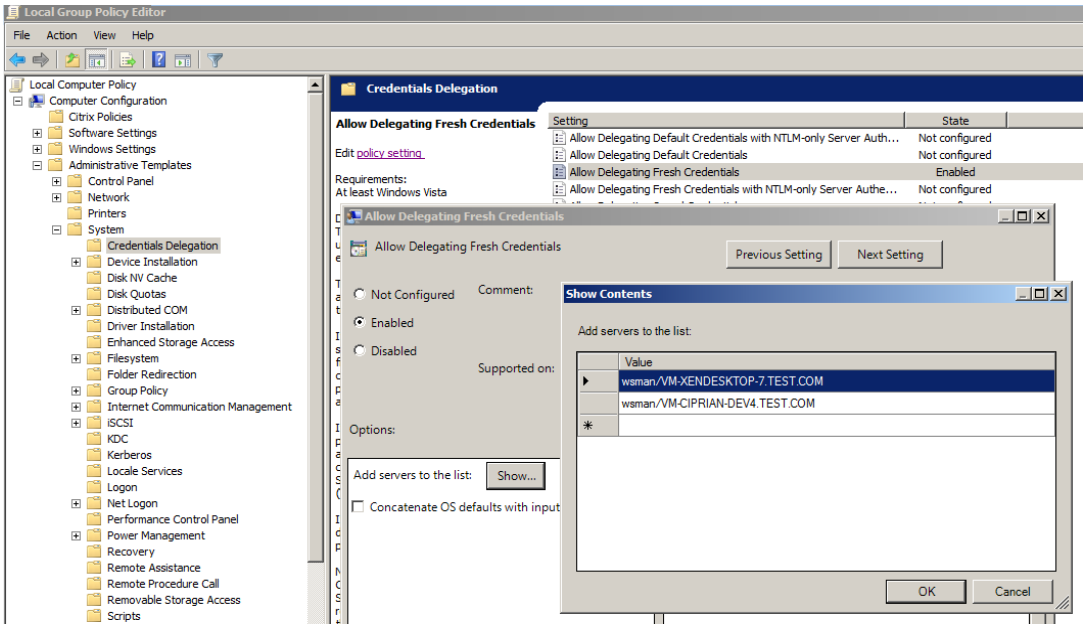
Enable-WSManCredSSP -Role Client -delegatecomputer <WinRM Server FQDN> -force

OR

1. Open **gpedit.msc**.

2. Navigate to **Computer Configuration -> Administrative Templates -> Windows Components -> Windows Remote Management (WinRM) -> WinRM Client** and enable **Allow CredSSP authentication**.
3. Navigate to **Computer Configuration -> Administrative Templates -> System -> Credentials Delegation** and enable **Allow Delegating Fresh Credentials.**
4. Add the WinRM server machine to the list of servers. This must be in the form wsman/<WinRM server FQDN>.

Important: If your WinRM server and WinRM client machines are not part of the same domain, you may have to configure *Allow Delegating Fresh Credentials with NTLM-only server authentication* in a similar fashion.



Citrix Virtual Apps and Desktops Activities

This integration pack adds the KA Citrix Virtual Apps and Desktops category to the **Activities** pane in the Client. This category contains the following activities:

- Add Machine
- Assign User
- Get Desktop Group
- Get Machine
- Get Machine Catalog
- Get Session
- Remove Machine
- Remove User
- Restart Machine
- Run Power Shell Script
- Set Maintenance Mode
- Shut Down Machine
- Start Machine
- Stop Session

Common Configuration Instructions for All Activities

The following configuration instructions apply to all activities in this integration pack. Links to this section are included in the configuration instructions for each activity.

Activity Properties

Each activity has a set of required or optional properties that define the configuration of that activity. This includes how it connects to other activities or how the activity performs its actions. You can view or modify activity properties in the Orchestrator Client.

To configure the properties for an activity:

1. Double-click the activity. Alternatively, you can right-click the activity, and then click **Properties**.
2. To save your configuration entries, click **Finish**.

In the activity properties dialog box, several tabs along the left side provide access to general and specific settings for the activity. Although the number of available tabs for activity properties differs from activity to activity, all activities will have a **General** tab, a **Properties** tab and/or **Filters** tab, and a **Run Behavior** tab. Some activities may have additional tabs.

General Tab

This tab contains the **Name** and **Description** properties for the activity. By default, the **Name** of the activity is the same as its activity type, and the **Description** is blank. You can modify these properties to create more descriptive names or provide detailed descriptions of the actions of the activity.

Properties/Filters Tab

These tabs contain properties that are specific to the activity.

All activities in this integration pack have the **Configuration Name** property at the top of the **Properties** tab. This property is used to specify the connection to a desktop server.

To configure the Configuration Name property:

1. Click the ellipsis **(…)** button next to the **Name** field, and then select the applicable connection name. Connections displayed in the list have been previously configured as described in Orchestrator Configuration.

Filter Behavior

The Monitor and Get activities use filters to determine the values that will invoke a runbook or retrieve activities. Property values of potential candidates are compared to the values of the filters to determine if they meet the criteria. When matching against values, you select one of the available methods of comparison. An option is provided to either match or not match the filter using each method. For example, the "Does not" version of a method causes alerts that do not match the filter to trigger the runbook.

- **Equals**: the property of the object exactly matches the text or number specified in the filter.
- **Does not equal**: the property of the object does not exactly match the text or number specified in the filter.
- **Is less than**: the property of the object is less than the number specified in the filter.
- **Is less than or equal to**: the property of the object is less than or equal to the number specified in the filter.
- **Is greater than**: the property of the object is greater than the number specified in the filter.
- **Is greater than or equal to**: the property of the object is greater than or equal to the number specified in the filter.
- **Contains**: the property of the object contains the exact text specified in the filter. Unlike the Equals behavior, there can be other text surrounding the matching text.
- **Does not contain**: the property of the object does not contain the exact text specified in the filter. Unlike the Equals behavior, there can be other text surrounding the matching text.
- **Starts with**: the property of the object starts with the exact text specified in the filter. Unlike the Equals behavior, there can be other text following the matching text.
- **Ends with**: the property of the object ends with the exact text specified in the filter. Unlike the Equals behavior, there can be other text preceding the matching text.
- **$null** is accepted as a filter value and can be used to build filter conditions which test for properties being equal or not equal to PowerShell $null.

When building DateTime filter conditions it is recommended to use inequality comparison operators. If you use equals or does not equal to compare with DateTime values, ensure the filter value is specified with millisecond precision, otherwise the comparison evaluation may fail.

Run Behavior Tab

This tab contains the properties that determine how the activity handles multi-value published data and what notifications will be sent if the activity fails or runs for an excessive period of time.

Multi-Value Published Data Behavior

The Get activities retrieve information from another activity or outside source and can return one or more values in the published data. For example, when you use the Get Collection Member activity, the data output from that activity might be a list of computers that belong to the specified collection.

By default, the data from the Get activity will be passed on as multiple individual outputs. This invokes the next activity as many times as there are items in the output. Alternatively, you can provide a single output for the activity by enabling the **Flatten** option. When you enable this option, you also choose a formatting option:

- **Separate with line breaks**. Each item is on a new line. This format is useful for creating human-readable text files for the output.
- **Separate with _** . Each item is separated by one or more characters of your choice.
- **Use CSV format**. All items are in CSV (comma-separated value) format. This format is useful for importing data into spreadsheets or other applications.

The activity will produce a new set of data every time it runs. The **Flatten** feature does not flatten data across multiple instances of the same activity.

Event Notifications

Some activities are expected to take a limited amount of time to complete. If they do not complete within that time they may be stalled or there may be another issue preventing them from completing. You can define the number of seconds to wait for completion of the action. After this period a platform event will be sent, and the issue will be reported. You can also choose whether to generate a platform event if the activity returns a failure.

To be notified when the activity takes longer than a specified time to run or fails to run:

1. In the **Event Notifications** box, enter the **number of seconds** of run time before a notification is generated.
2. Select **Report if activity fails to run** to generate run failure notifications.

For more information about Orchestrator events, see the “Event Notifications " topics in the Runbook Properties (https://technet.microsoft.com/en-us/library/hh489610.aspx#Event Notifications).

Published Data

Published data is the foundation of a working runbook. It is the data produced as a result of the actions of an activity. This data is published to an internal data bus that is unique for each runbook. Subsequent activities in the runbook can subscribe to this data and use it in their configuration. Link conditions also use this information to add decision-making capabilities to runbooks.

An activity can only subscribe to data from the activities that are linked before it in the runbook. You can use published data to automatically populate the property values needed by activities.

To use published data:

1. Right-click the property value box, click **Subscribe**, and then click **Published Data**.
2. Click the **Activity** drop-down box and select the activity from which you want to obtain the data.
3. To view additional data elements common to all activities, select **Show Common Published Data**.
4. Click the published data element that you want to use, and then click **OK**.

For a list of the data elements published by each activity, see the Published Data tables in the activity topic. For information about the common published data items, see the Published Data (http://technet.microsoft.com/en-us/library/hh403821.aspx).

Important: when publishing activity-specific data items that represent **date and time values**, the integration pack uses the format **yyyy-MM-ddTHH:mm:ss.fff**. For example: 2021-03-21T10:15:00.345.

1Add Machine Activity

The **Add Machine** activity is used in a runbook to add a virtual machine to a Machine Catalog or a Desktop (Delivery) Group.

Required Properties

You must configure the following properties.

Add Machine To	Specifies whether the machine is to be added to a Machine Catalog or to a Delivery Group.
Desktop Group UID	Identifies the Delivery Group the machine is to be added to. Available only when adding machine to a delivery group.
Hosted Machine ID	Identifies the VM within the hosting hypervisor. Available only when adding machines to a catalog. ***Important:*** Obtaining the **Hosted Machine ID** depends on the hypervisor that you are using. • For Microsoft Hyper-V with VMM, this ID is a GUID which can be found at **Hyper-V Manager > VM > Settings > Management > Name > Notes**. • In cases where the machine has not yet been added to the desktop server, the ID can be obtained using the **Get-Item** PowerShell command from the Citrix.Host.Admin snapin. For example: `Get-Item –LiteralPath XDhyp:\Connections\<path to VM >.vm) –AdminAddress <desktop controller>` • In cases where the machine has been previously added to the desktop server, the ID can be obtained by using the **Get Machine** Activity.
Hypervisor Connection Name	Name of the Virtual Apps and Desktops hypervisor connection to be used when adding the VM. Available only when adding VM to a catalog.
Machine Catalog UID	Identifies the machine catalog the VM is to be added to. Available only when adding machines to a catalog.
Machine Name	Name of the machine to be added, in the form *domain\machine.*

Published Data

This activity publishes the following activity-specific data.

Machine UID	The UID of the machine that has been added to a Machine Catalog or Delivery Group
Machine Name	The name of the machine that has been added to a Machine Catalog or Delivery Group

Assign User Activity

The **Assign User** activity is used in a runbook to assign a user to a Private (Static) Desktop or Shared (Random) Delivery Group or a Machine.

Required Properties

You must configure the following properties.

Assign User To	Specifies whether the user is to be assigned to a Private Desktop or to a Shared Group or to a Machine.
Machine Name	Name of the machine the user is to be assigned to, in the form *domain**machine*. Available only when adding a user to a machine.
Private (Static) Desktop Name	Name of the private desktop the user is to be assigned to, in the form *domain**machine*. Available only when adding a user to private desktop.
Shared (Random) Group UID	Identifies the shared delivery group the user is to be assigned to. Available only when adding a user to a shared delivery group.
User Name	Name of the user to be assigned, in the form *domain**user.*

Published Data

This activity publishes the following activity-specific data.

Machine Name	Name of the machine the user has been assigned to.
Machine UID	UID of the machine the user has been assigned to.
Private (Static) Desktop Name	Name of the private desktop the user has been assigned to.
Private (Static) Desktop UID	UID of the private desktop the user has been assigned to.
Shared (Random) Group Name	Name of the shared group the user has been assigned to.
Shared (Random) Group UID	UID of the shared group the user has been assigned to.
User Name	Name of the user that has been assigned.

Get Desktop Group Activity

The **Get Desktop Group** activity is used in a runbook to return desktop (delivery) groups.

Required Properties

You must configure the following properties.

Max Record Count	Specifies the maximum number of records to be returned.
Property	Specifies which object properties are to be returned, in the form of a comma separated list of property names.
Return Total Record Count	Specifies whether the activity should return the total number of records available.
Skip	Skips the specified number of records before returning the results.
Sort By	Sorts the results by the specified list of properties, in the form of a comma separated list of property names. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Filters

This activity provides the following filters, that you can use to control which desktop group records to retrieve.

Application UID	Filters results by UID of applications published.
Automatic Power On for Assigned	Filters results by Automatic Power on For Assigned value.
Automatic Power On For Assigned During Peak	Filters results by Automatic Power on For Assigned During Peak value.
Color Depth	Filters results by Color Depth value.
Delivery Type	Filters results by Delivery Type value.
Description	Filters results by Description value.
Desktop Kind	Filters results by Desktop Kind value.
Enabled	Filters results by Enabled value.
In Maintenance Mode	Filters results by In Maintenance Mode value.
Is Remote PC	Filters results by Is Remote PC value.
Machine Configuration UID	Filters results by Machine Configuration UID.
Metadata	Filters results by Metadata value.

Minimum Functional Level	Filters results by Minimum Functional Level value.
Name	Filters results by Name value.
Off Peak Buffer Size Percent	Filters results by Off Peak Buffer Size Percent value.
Off Peak Disconnect Action	Filters results by Off Peak Disconnect Action value.
Off Peak Disconnect Timeout	Filters results by Off Peak Disconnect Timeout value.
Off Peak Extended Disconnect Action	Filters results by Off Peak Extended Disconnect Action value.
Off Peak Extended Disconnect Timeout	Filters results by Off Peak Extended Disconnect Timeout value.
Off Peak Log Off Action	Filters results by Off Peak Log Off Action value.
Off Peak Log Off Timeout	Filters results by Off Peak Log Off Timeout value.
Peak Buffer Size Percent	Filters results by Peak Buffer Size Percent value.
Peak Disconnect Action	Filters results by Peak Disconnect Action value.
Peak Disconnect Timeout	Filters results by Peak Disconnect Timeout value.
Peak Extended Disconnect Action	Filters results by Peak Extended Disconnect Action value.
Peak Extended Disconnect Timeout	Filters results by Peak Extended Disconnect Timeout value.
Peak Log Off Action	Filters results by Peak Log Off Action value.
Peak Log Off Timeout	Filters results by Peak Log Off Timeout value.
Power Time Scheme UID	Filters results by Power Time Scheme UID value.
Published Name	Filters results by Published Name value.
Scope ID	Filters results by Scope ID value.
Scope Name	Filters results by Scope Name value.
Secure ICA Required	Filters results by Secure ICA Required value.
Session Support	Filters results by Session Support value.
Shutdown Desktops After Use	Filters results by Shutdown Desktops After Use value.

Tag	Filters results by Tag value.
Tag UID	Filters results by Tag UID value.
Time Zone	Filters results by Time Zone value.
Total Applications	Filters results by Total Applications value.
Turn on Added Machine	Filters results by Turn on Added Machine value.
UID	Filters results by UID.
UUID	Filters results by UUID.

Published Data

This activity publishes the following activity-specific data.

Automatic Power on For Assigned	Specifies whether assigned desktops in the group are automatically started at the start of peak time periods. Only relevant for groups with **Desktop Kind** as **Private**.
Automatic Power on For Assigned During Peak	Specifies whether assigned desktops in the group are automatically started throughout peak time periods. Only relevant for groups with **Desktop Kind** as **Private** and which have **Automatic Power on For Assigned** enabled.
Color Depth	Default color depth of sessions started with machines in the desktop group.
Configuration Slot UIDs	UIDs of any configuration slots which hold machine configurations associated with the desktop group as a JSON array. The order of slot UIDs in this list correspond with the order of items in the associated Machine Configuration Names and Machine Configuration UIDs list properties, and so the same slot UID can appear more than once.
Delivery Type	The type of resources being published by the desktop group.
Description	Description of the desktop group.
Desktop Group Count	Number of desktop groups returned.
Desktop Kind	The type of desktops being published by the desktop group.
Desktops Available	The number of desktops in the group that are available for new sessions.
Desktops Disconnected	The number of desktops in the group that have disconnected sessions.
Desktops in Use	The number of desktops in the group that are currently in use.
Desktops Never Registered	The number of desktops in the group that have never registered.
Desktops Preparing	The number of desktops in the group that are currently preparing sessions.
Desktops Unregistered	The number of desktops in the group that are currently unregistered.

Enabled	Specifies whether the desktop group is enabled or not. Only enabled groups appear to users.
Icon UID	The UID of the icon to be used as a default for desktops in the desktop group. Individual desktops can override this default by setting the Icon UID parameter on the desktop object.
In Maintenance Mode	Specifies whether the machines in the group are in maintenance mode or not.
Is Remote PC	Specifies whether the desktop group is a Remote PC desktop group.
Machine Configuration Names	The Machine Configuration names associated with the desktop group.
Machine Configuration UIDs	The Machine Configuration UIDs associated with the desktop group.
Metadata Map	Metadata associated with the desktop group.
Minimum Functional Level	The minimum Functional Level required for the machines in the desktop group to be able to register with the Citrix Broker Service.
Name	Description
Name	Name of the desktop group.
Off Peak Buffer Size Percent	The percentage of machines that are kept available in an idle state outside of peak hours.
Off Peak Disconnect Action	The action that is performed after a configurable period of a user session disconnecting outside peak hours.
Off Peak Disconnect Timeout	The number of minutes before the configured action is performed after a user session disconnects outside peak hours.
Off Peak Extended Disconnect Action	The action performed after a second configurable period of a user session disconnecting outside peak hours.
Off Peak Extended Disconnect Timeout	The number of minutes before the second configured action is performed after a user session disconnects outside peak hours.
Off Peak Log Off Action	The action performed after a configurable period of a user session ending outside peak hours.
Off Peak Log Off Timeout	The number of minutes before the configured action is performed after a user session ends outside peak hours.
Peak Buffer Size Percent	The percentage of machines in the desktop group that are kept available in an idle state in peak hours.
Peak Disconnect Action	The action performed after a configurable period of a user session disconnecting in peak hours.
Peak Disconnect Timeout	The number of minutes before the configured action is performed after a user session disconnects in peak hours.

Peak Extended Disconnect Action	The action performed after a second configurable period of a user session disconnecting in peak hours.
Peak Extended Disconnect Timeout	The number of minutes before the second configured action is performed after a user session disconnects in peak hours.
Peak Log Off Action	The action performed after a configurable period of a user session ending in peak hours.
Peak Log Off Timeout	The number of minutes before the configured action is performed after a user session ends in peak hours.
Protocol Priority	A list of protocol names in the order in which they are attempted for use during connection.
Published Name	The name of the desktop group as it is to appear to the user in Store Front.
Scopes	The list of the delegated admin scopes to which the desktop group belongs.
Secure ICA Required	Specifies whether the Secure ICA encryption of the HDX protocol is required for sessions of desktops in the desktop group.
Session Support	Specifies the session support of the machines in the desktop group. Machines with the incorrect session support for the desktop group will be unable to register with the Citrix Broker Service.
Sessions	The total number of user sessions currently running on all the machines in the desktop group.
Shutdown Desktops After Use	Specifies whether the desktops will shut down after they have been used and there are no sessions running on the machine.
Tags	Tags associated with the desktop group
Time Zone	The time zone that desktops in the desktop group are in.
Total Applications	Total number of applications associated with the desktop group.
Total Desktops	Total number of desktops associated with the desktop group.
Total Record Count	Total number of records available. This is published when Return Total Record Count is True.
Turn on Added Machine	Specifies whether power-managed machines should be attempted to be turned on when they are added to the desktop group.
UID	UID if the desktop group.
UUID	UUID if the desktop group.

Get Machine Activity

The **Get Machine** activity is used in a runbook to retrieve information about Virtual Apps and Desktops machines, including both private and shared desktops.

Required Properties

This activity does not have any properties that you must configure.

Optional Properties

This activity provides the following optional properties that you can configure, as necessary.

Max Record Count	Specifies the maximum number of records to be returned.
Property	Specifies which object properties are to be returned, in the form of a comma separated list of property names.
Return Total Record Count	Specifies whether the activity should return the total number of records available.
Skip	Skips the specified number of records before returning the results.
Sort By	Sorts the results by the specified list of properties, in the form of a comma separated list of property names. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Filters

This activity provides the following filters, that you can use to control which machine records to retrieve and publish.

Agent Version	Filters results by Agent Version value.
Allocation Type	Filters results by Allocation Type value.
Application in Use	Filters results by Application in Use value.
Assigned Client Name	Filters results by Assigned Client Name value.
Assigned IP Address	Filters results by Assigned IP Address value.
Assigned User SID	Filters results by Assigned User SID value.
Associated Use UPN	Filters results by Associated Use UPN value.
Associated User Full Name	Filters results by Associated User Full Name value.
Associated User Name	Filters results by Associated User Name value.
Associated User SID	Filters results by Associated User SID value.
Catalog Name	Filters results by Catalog Name value.
Catalog UID	Filters results by Catalog UID value.
Catalog UUID	Filters results by Catalog UUID value.

Color Depth	Filters results by Color Depth value.
Controller DNS Name	Filters results by Controller DNS Name value.
Delivery Type	Filters results by Delivery Type value.
Description	Filters results by Description value.
Desktop Condition	Filters results by Desktop Condition value.
Desktop Group Name	Filters results by Desktop Group Name value.
Desktop Group UID	Filters results by Desktop Group UID value.
Desktop Group UUID	Filters results by Desktop Group UUID value.
Desktop Kind	Filters results by Desktop Kind value.
Desktop UID	Filters results by Desktop UID value.
DNS Name	Filters results by DNS Name value.
Fault State	Filters results by Fault State value.
Functional Level	Filters results by Functional Level value.
Hosted Machine ID	Filters results by Hosted Machine ID value.
Hosted Machine Name	Filters results by Hosted Machine Name value.
Hosting Server Name	Filters results by Hosting Server Name value.
Hypervisor Connection Name	Filters results by Hypervisor Connection Name value.
Hypervisor Connection UID	Filters results by Hypervisor Connection UID value.
HypHypervisor Connection UID	Filters results by HypHypervisor Connection UID value.
Icon UID	Filters results by Icon UID value.
Image Out of Date	Filters results by Image Out of Date value.
In Maintenance Mode	Filters results by In Maintenance Mode value.
IP Address	Filters results by IP Address value.
Is Assigned	Filters results by Is Assigned value.
Is Physical	Filters results by Is Physical value.
Last Connection Failure	Filters results by Last Connection Failure value.
Last Connection Time	Filters results by Last Connection Time value.
Last Connection User	Filters results by Last Connection User value.
Last Deregistration Reason	Filters results by Last Deregistration Reason value.

Last Deregistration Time	Filters results by Last Deregistration Time value.
Last Error Reason	Filters results by Last Error Reason value.
Last Error Time	Filters results by Last Error Time value.
Last Hosting Update Time	Filters results by Last Hosting Update Time value.
Load Index	Filters results by Load Index value.
Machine Internal State	Filters results by Machine Internal State value.
Machine Name	Filters results by Machine Name value.
Metadata	Filters results by Metadata value.
OS Type	Filters results by OS Type value.
OS Version	Filters results by OS Version value.
Persist User Changes	Filters results by Persist User Changes value.
Power Action Pending	Filters results by Power Action Pending value.
Power State	Filters results by Power State value.
Provisioning Type	Filters results by Provisioning Type value.
Published Application	Filters results by Published Application value.
Published Name	Filters results by Published Name value.
PVD Stage	Filters results by PVD Stage value.
Registration State	Filters results by Registration State value.
Scheduled Reboot	Filters results by Scheduled Reboot value.
Secure ICA Required	Filters results by Secure ICA Required value.
Session Autonomously Brokered	Filters results by Session Autonomously Brokered value.
Session Client Address	Filters results by Session Client Address value.
Session Client Name	Filters results by Session Client Name value.
Session Client Version	Filters results by Session Client Version value.
Session Connected Via Host Name	Filters results by Session Connected Via Host Name value.

Session Connected Via IP	Filters results by Session Connected Via IP value.
Session Count	Filters results by Session Count value.
Session Device ID	Filters results by Session Device ID value.
Session Hardware ID	Filters results by Session Hardware ID value.
Session Hidden	Filters results by Session Hidden value.
Session Key	Filters results by Session Key value.
Session Launched Via Host Name	Filters results by Session Launched Via Host Name value.
Session Launched Via IP	Filters results by Session Launched Via IP value.
Session Protocol	Filters results by Session Protocol value.
Session Secure ICA Active	Filters results by Session Secure ICA Active value.
Session Smart Access Tag	Filters results by Session Smart Access Tag value.
Session Start Time	Filters results by Session Start Time value.
Session State	Filters results by Session State value.
Session State Change Time	Filters results by Session State Change Time value.
Session Support	Filters results by Session Support value.
Session UID	Filters results by Session UID value.
Session User Name	Filters results by Session User Name value.
Session User SID	Filters results by Session User SID value.
Sessions Established	Filters results by Sessions Established value.
Sessions Pending	Filters results by Sessions Pending value.
SID	Filters results by SID value.
Summary State	Filters results by Summary State value.
Tag	Filters results by Tag value.
UID	Filters results by UID value.
UUID	Filters results by UUID value.
VM Tools State	Filters results by VM Tools State value.
Will Shut Down After Use	Filters results by Will Shut Down After Use value.
Windows Connection Setting	Filters results by Windows Connection Setting value.

Published Data

This activity publishes the following activity-specific data. ***Note:*** machine session properties are always null for multi-session machines.

Agent Version	Version of the Citrix Virtual Delivery Agent (VDA) installed on the machine.
Allocation Type	Indicates how the machine is allocated to the user.
Applications in Use	List of applications in use on the machine (in the form of browser name).
Assigned Client Name	The name of the endpoint client device that the machine has been assigned to.
Assigned IP Address	The IP address of the endpoint client device that the machine has been assigned to.
Associated User Full Names	Full names of the users that have been associated with the machine.
Associated User Names	Usernames of the users that have been associated with the machine, as a JSON array.
Associated User SIDs	The SIDs of the users that have been associated with the machine, as a JSON array.
Associated User UPNs	The User Principal Names of the users that have been associated with the machine, as a JSON array.
Capabilities	List of the capabilities that the machine support, as a JSON array.
Catalog Name	Name of the catalog the machine is a member of.
Catalog UID	UID of the catalog the machine is a member of.
Catalog UUID	UUID of the catalog the machine is a member of.
Color Depth	The color depth setting configured on the machine.
Controller DNS Name	The DNS host name of the controller that the machine is registered to.
Delivery Type	Specifies whether the machine delivers desktops only, apps only or both.
Description	Description of the machine.
Desktop Conditions	List of outstanding desktop conditions for the machine, as a JSON array.
Desktop Group Name	Name of the desktop group the machine is a member of.
Desktop Group UID	UID of the desktop group the machine is a member of.
Desktop Group UUID	UUID of the desktop group the machine is a member of.
Desktop Kind	Indicates whether the machine is private or shared.

Desktop UID	The UID of the associated desktop object.
DNS Name	The DNS host name of the machine.
Fault State	Summary state of any current fault state of the machine.
Functional Level	Functional level of the machine, if known.
Hosted Machine ID	Unique ID within the hosting unit of the target managed machine.
Hosted Machine Name	The friendly name of a hosted machine as used by its hypervisor.
Hosting Server Name	DNS name of the hypervisor that is hosting the machine if managed.
Hypervisor Connection Name	The name of the hypervisor connection that the machine has been assigned to, if managed.
Hypervisor Connection UID	The UID of the hypervisor connection that the machine's hosting server is accessed through.
HypHypervisor Connection UID	The UUID of the hypervisor connection that the machine's hosting server is accessed through.
Icon UID	The UID of the machine's icon that is displayed in Store Front.
Image Out of Date	Specifies whether the VM image for a hosted machine is out of date.
In Maintenance Mode	Specifies whether the machine is in maintenance mode.
IP Address	IP address of the machine
Is Assigned	Specifies whether a private desktop has been assigned to a user/users, or a client name/address. Users can be assigned explicitly or by assigning on first use of the machine.
Is Physical	Indicates whether the machine is physical or not.
Last Connection Failure	The reason for the last failed connection between a client and the machine.
Last Connection Time	Date and time of the last detected connection attempt that either failed or succeeded.
Last Connection User	The SAM name (in the form DOMAIN\user) of the user that last attempted a connection with the machine. If the SAM name is not available, the SID is used.
Last Deregistration Reason	The reason for the last deregistration of the machine with the broker.
Last Deregistration Time	Time of the last deregistration of the machine from the controller.
Last Error Reason	The reason for the last error detected in the machine.
Last Error Time	The time of the last detected error.

Last Hosting Update Time	Date and time of last update to any hosting data (such as power states) for this machine reported by the hypervisor connection.
Load Index	Gives current effective load index for multi-session machines.
Load Indexes	Gives the last reported individual load indexes that were used in the calculation of the **LoadIndex** value. Note that the **LoadIndex** value may have been subsequently adjusted due to session brokering operations. This value is only set for multi-session machines.
Machine Count	Number of machines returned.
Machine Internal State	The internal state of the machine; reported while the machine is registered to a controller, plus some private Citrix Broker Service states while the machine is not registered.
Machine Name	DNS host name of the machine.
Metadata Map	Any metadata that is associated with the machine, as a JSON array.
OS Type	Operating system running on the machine.
OS Version	Version of the operating system running on the machine.
Persist User Changes	Describes whether/how the user changes are persisted.
Power Action Pending	Indicates whether there are any pending power actions for the machine.
Power State	The current power state of the machine.
Provisioning Type	Indicates how the machine was provisioned.
Published Applications	List of applications published by the machine.
Published Name	The name of the machine that is displayed in Store Front, if the machine has been published.
PVD Stage	Indicates the stage of Personal vDisk (PvD) image preparation, for machines that support it.
Registration State	Indicates the registration state of the machine.
Scheduled Reboot	Indicates the state of any scheduled reboot operation for a machine.
Secure ICA Required	Indicates whether SecureICA is required or not when starting a session on the machine.
Session Autonomously Brokered	Session property indicating if the current session was started without the use of the broker.
Session Client Address	Session property indicating the IP address of the client connected to the machine.
Session Client Name	Session property indicating the host name of the client connected to the machine.

Session Client Version	Session property indicating the host name of the client connected to the machine.
Session Connected Via Host Name	Session property indicating the host name of the connection gateway, router or client.
Session Connected Via IP	Session property indicating the IP address of the connection gateway, router or client.
Session Count	Number of sessions on the machine.
Session Device ID	Session property indicating a unique identifier for the client device that has most recently been associated with the current session.
Session Hardware ID	Session property indicating a unique identifier for the client hardware that has been most recently associated with the current session.
Session Hidden	Session parameter that indicates if a session is hidden.
Session Key	Session property indicating the key of the current session.
Session Launched Via Host Name	Session property that denotes the host name of the Store Front server used to launch the current brokered session.
Session Launched Via IP	Session property that denotes the IP address of the Store Front server used to launch the current brokered session.
Session Protocol	Session property that denotes the protocol that the current session is using, can be either "HDX" or "RDP".
Session Secure ICA Active	Session property that indicates whether SecureICA is active on the current session.
Session Smart Access Tags	Session property that indicates the Smart Access tags for the current session.
Session Start Time	Session property that indicates the start time of the current session. Session properties are always null on multi-session machines.
Session State	Session property indicating the state of the current session.
Session State Change Time	The date and time of the last state change of the current session.
Session Support	Indicates the session support of the machine.
Session UID	Session property indicating the UID of the current session.
Session User Name	Session property indicates the name of the current sessions' user (in the form DOMAIN\user).
Session User SID	Session property indicates the SID of the current sessions' user.
Sessions Established	Number of established sessions on this machine. For multi-session machines this excludes established sessions which have not yet completed their logon processing.

Sessions Pending	Number of pending (brokered but not yet established) sessions on this machine. For multi-session machines this also includes established sessions which have not yet completed their logon processing.
SID	The SID of the machine.
Summary State	Indicates the overall state of the desktop associated with the machine. The overall state is a result of other more specific states such as session state, registration state and power state.
Tags	List of tags for the machine.
Total Record Count	Total number of records available. This is published when Return Total Record Count is True.
UID	UID of the machine object.
UUID	UUID of the machine object.
VM Tools State	State of the hypervisor tools present on the VM (if any).
Will Shut Down After Use	Indicates whether this machine is tainted and will be shut down after all sessions on the machine have ended. This flag should only ever be true on power managed, single-session machines.
Windows Connection Setting	The logon mode reported by Windows itself (multi-session machines only). For single-session machines the value is always hardwired to LogonEnabled.

Get Machine Catalog Activity

The **Get Machine Catalog** activity is used in a runbook to return Virtual Apps and Desktops machine catalogs.

Optional Properties

This activity provides the following parameters that you can configure as required.

Max Record Count	Specifies the maximum number of records to be returned.
Property	Specifies which object properties are to be returned, in the form of a comma separated list of property names.
Return Total Record Count	Specifies whether the activity should return the total number of records available.
Skip	Skips the specified number of records before returning the results.
Sort By	Sorts the results by the specified list of properties, in the form of a comma separated list of property names. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Filters

This activity provides the following filters that you can use to control which Machine Catalog records to retrieve and publish.

Allocation Type	Filters results by Allocation Type value.
Assigned Count	Filters results by Assigned Count value.
Available Assigned Count	Filters results by Available Assigned Count value.
Available Count	Filters results by Available Count value.
Available Unassigned Count	Filters results by Available Unassigned Count value.
Description	Filters results by Description.
Hypervisor Connection UID	Filters results by Hypervisor Connection UID value.
Is Remote PC	Filters results by Is Remote PC value.
Machine UID	Filters results by Machine UID value.
Machines Are Physical	Filters results by Machines Are Physical value.
Metadata	Filters results by Metadata value.
Minimum Functional Level	Filters results by Minimum Functional Level value.

Name	Filters results by Name.
Persist User Changes	Filters results by Persist User Changes value.
Provisioning Scheme ID	Filters results by Provisioning Scheme ID value.
Provisioning Type	Filters results by Provisioning Type value.
PVS Address	Filters results by PVS Address value.
PVS Domain	Filters results by PVS Domain value.
Remote PC Desktop Group Priority	Filters results by Remote PC Desktop Group Priority value.
Remote PD Desktop Group UID	Filters results by Remote PD Desktop Group UID value.
Scope ID	Filters results by Scope ID value.
Scope Name	Filters results by Scope Name value.
Session Support	Filters results by Session Support value.
UID	Filters results by UID value.
Unassigned Count	Filters results by Unassigned Count value.
Used Count	Filters results by Used Count value.
UUID	Filters results by UUID value.

Published Data

This activity publishes the following activity-specific data.

Allocation Type	Specifies how the machines in the catalog are allocated to a user.
Assigned Count	The number of assigned machines (machines that have been assigned to a user/users or a client name/address).
Available Assigned Count	The number of available machines (not in a desktop group), that are also assigned to users.
Available Count	The number of available machines (those not in any desktop group).
Available Unassigned Count	The number of available machines (those not in any desktop group) that are not assigned to users.
Description	Description of the catalog
Hypervisor Connection UID	The UID of the hypervisor connection that is associated with the machines in the catalog. This only applies for MCS provisioned catalogs as with other provisioning types, the machines can be from one or more different hypervisor connections.
Is Remote PC	Specifies if the catalog is a Remote PC catalog or not. Remote PC catalogs automatically configure appropriate machines without the need for manual configuration.
Machine Catalog Count	Number of Machine Catalog objects returned.
Machines Are Physical	Specifies if the machines in the catalog can be power-managed by the broker or not.
Metadata Map	Holds any metadata associated with the catalog.
Minimum Functional Level	The expected minimal functional level of the machines in the catalog.
Name	The name of the catalog.
Persist User Changes	Specifies how the user changes are persisted on the machines in the catalog.
Provisioning Scheme ID	The GUID of the provisioning scheme (if any) associated with the catalog. This only applies if the provisioning type is MCS.
Provisioning Type	Specifies how the machines are provisioned in the catalog.
PVS Address	IP address of the PVS server to be used in a catalog with a PVS Provisioning Type.
PVS Domain	he domain of the PVS server to be used in a catalog with a PVS Provisioning Type.
Remote PC Desktop Group Priorities	Remote PC desktop groups association priorities.

Remote PD Desktop Group UIDS	UIDs of the Remote PC desktop groups associated with this catalog.
Scopes	The list of the delegated admin scopes to which the catalog belongs.
Session Support	Specifies the session support of the machines in the catalog.
Total Record Count	Total number of records available. This is published when Return Total Record Count is True.
UID	UID of the catalog.
Unassigned Count	The number of unassigned machines (machines not assigned to users).
Used Count	The number of machines in the catalog that are in a desktop group.
UUID	The number of machines in the catalog that are in a desktop group.

Get Session Activity

The **Get Session** activity is used in a runbook to return running desktop sessions.

Required Properties

This activity does not have any required properties that you must configure.

Optional Properties

This activity provides the following optional properties that you can configure as necessary.

Max Record Count	Specifies the maximum number of records to be returned.
Property	Specifies which object properties are to be returned, in the form of a comma separated list of property names.
Return Total Record Count	Specifies whether the activity should return the total number of records available.
Skip	Skips the specified number of records before returning the results.
Sort By	Sorts the results by the specified list of properties, in the form of a comma separated list of property names. Optionally, prefix each name with a + or - to indicate ascending or descending order. Ascending order is assumed if no prefix is present.

Filters

This activity provides the following filters, that you can use to control which session records to retrieve and publish.

Agent Version	Filters results by Agent Version value.
Application in Use	Filters results by Application in Use value.
Application UID	Filters results by Application UID.
Autonomously Brokered	Filters results by Autonomously Brokered value.
Brokering Duration	Filters results by value.
Brokering Time	Filters results by Brokering Duration value.
Brokering User Name	Filters results by Brokering User Name value.
Brokering User SID	Filters results by Brokering User SID value.
Catalog Name	Filters results by Catalog Name value.
Client Address	Filters results by Client Address value.
Client Name	Filters results by Client Name value.
Client Version	Filters results by Client Version value.
Connected Via Host Name	Filters results by Connected Via Host Name value.

Connected Via IP	Filters results by Connected Via IP value.
Controller DNS Name	Filters results by Controller DNS Name value.
Desktop Group Name	Filters results by Desktop Group Name value.
Desktop Group UID	Filters results by Desktop Group UID value.
Desktop Kind	Filters results by Desktop Kind value.
Desktop SID	Filters results by Desktop SID.
Desktop UID	Filters results by Desktop UID.
Device ID	Filters results by Device ID.
DNS Name	Filters results by DNS Name.
Establishment Duration	Filters results by Establishment Duration value.
Establishment Time	Filters results by Establishment Time value.
Hardware ID	Filters results by Hardware ID.
Hidden	Filters results by Hidden value.
Hosted Machine Name	Filters results by Hosted Machine Name.
Hosting Server Name	Filters results by Hosting Server Name.
Hypervisor Connection Name	Filters results by Hypervisor Connection Name.
Image Out of Date	Filters results by Image Out of Date value.
In Maintenance Mode	Filters results by In Maintenance Mode value.
IP Address	Filters results by IP Address value.
Is Physical	Filters results by Is Physical value.
Launched Via Host Name	Filters results by Launched Via Host Name value.
Launched Via IP	Filters results by Launched Via IP value.
Machine Name	Filters results by Machine Name.
Machine Summary State	Filters results by Machine Summary State value.
Machine UID	Filters results by Machine UID.
Metadata	Filters results by Metadata value.
OS Type	Filters results by OS Type.
Persist User Changes	Filters results by Persist User Changes value.
Power State	Filters results by Power State value.

Protocol	Filters results by Protocol value.
Provisioning Type	Filters results by Provisioning Type value.
Secure ICA Active	Filters results by Secure ICA Active value.
Session Id	Filters results by Session Id.
Session Key	Filters results by Session Key.
Session State	Filters results by Session State value.
Session State Change Time	Filters results by Session State Change Time value.
Session Support	Filters results by Session Support value.
Session Type	Filters results by Session Type value.
Shared Desktop UID	Filters results by Shared Desktop UID value.
Start Time	Filters results by Start Time value.
UID	Filters results by UID.
User Full Name	Filters results by User Full Name.
User Name	Filters results by User Name.
User SID	Filters results by User SID.
User UPN	Filters results by User UPN.

Published Data

This activity publishes the following activity-specific data.

Agent Version	Version of the Citrix Virtual Delivery Agent (VDA) installed on the machine.
Applications in Use	List of applications in use in the session as a JSON array.
Autonomously Brokered	Indicates if the session was started without the use of the broker.
Brokering Duration	Time taken to broker the session.
Brokering Time	The date and time when the session was.
Brokering User Name	The username of the brokering user.
Brokering User SID	The SID of the brokering user.
Catalog Name	The name of the catalog that the machine hosting the session is assigned to.
Client Address	The IP address of the client connected to the desktop.
Client Name	The host name of the client connected to the session.
Client Version	The version of the Citrix Receiver running on the client connected to the session.
Connected Via Host Name	The host name of the incoming connection. This is usually a gateway, router or client.
Connected Via IP	The IP address of the incoming connection This is usually a gateway, router or client.
Controller DNS Name	The DNS host name of the controller that the session's hosting machine is registered with.
Desktop Group Name	Name of the desktop group of the machine the session is on.
Desktop Group UID	UID of the desktop group of the machine the session is on.
Desktop Kind	Indicates if the session is shared or private.
Desktop SID	The Windows SID of the machine the session is on.
Desktop UID	For a desktop session, the unique identifier of the desktop.
Device ID	Unique identifier for the client device that has most recently been associated with the session.
DNS Name	The DNS host name of the machine hosting the session.
Establishment Duration	Duration that it took to establish the session.
Establishment Time	Date and time at which the session was established.
Hardware ID	Unique identifier for the client hardware that has been most recently associated with the session.

Hidden	Indicates if the session is currently hidden from the user and not to be reconnected to.
Hosted Machine Name	The friendly name of a hosted machine running the session, as used by its hypervisor. This does not necessarily match either the DNS or AD name of the machine.
Hosting Server Name	DNS name of the hypervisor that is hosting the machine hosting the session.
Hypervisor Connection Name	The name of the hypervisor connection that the machine hosting the session has been assigned to.
Image Out of Date	Indicates whether the VM image for a hosted machine is out of date and due to be updated to a new master image when the machine next reboots.
In Maintenance Mode	Specifies whether the machine hosting the session is in maintenance mode.
IP Address	The IP address of the machine hosting the session.
Is Physical	Indicates if the machine hosting the session can be power managed.
Launched Via Host Name	The host name of the Store Front server used to launch the session.
Launched Via IP	The IP address of the Store Front server used to launch the session.
Machine Name	DNS host name of the machine hosting the session.
Machine Summary State	The summary state of the machine.
Machine UID	UID of the machine hosting the session.
Metadata Map	Map of metadata for this session.
OS Type	String that can be used to identify the operating system that is running on the machine hosting the session.
Persist User Changes	Indicates whether/how the user changes are persisted.
Power State	The current power state of the machine hosting the session.
Protocol	The protocol that the session is using, can be either **HDX** or **RDP**.
Provisioning Type	Specifies how the machine hosting the session was provisioned.
Secure ICA Active	Indicates whether Secure ICA is active on the session.
Session Count	Number of Session objects returned.
Session Id	A unique identifier that Remote Desktop Services uses to track the session, but it is only unique on that machine.
Session Key	Identifies the session object.
Session State	The state of the session.

Session State Change Time	The date and time of the most recent state change for the session
Session Support	Indicates if the machine hosting the session supports multiple or single sessions.
Session Type	Indicates if this is an Application or Desktop session. Possible values include Application and Desktop.
Smart Access Tags	The Smart Access tags for this session as a JSON array.
Start Time	Indicates the date and time that the session was started
Total Record Count	Total number of records available. This is published when Return Total Record Count is True.
UID	Unique identifier of this session.
User Full Name	The full name of the user.
User Name	The name of the user.
User SID	The user's Windows SID.
User UPN	The user's User Principal Name

Remove Machine Activity

The **Remove Machine** activity is used in a runbook to remove a machine from a Machine Catalog or a Desktop (Delivery) Group. If a machine is part of a Desktop (Delivery) Group, it must be removed from that group first, before it can be removed from the Machine Catalog.

Note: when removing a machine from a Machine Catalog, the underlying VM is not deleted from the hypervisor. The following tables list the required properties for this activity.

Required Properties

You must configure the following properties.

Delivery Group UID	Identifies the Delivery Group the machine is to be removed from. Available only when removing a machine from a delivery group.
Machine Name	Name of the machine to be removed, in the form *domain\machine.*
Remove Machine From	Specifies whether the machine is to be removed from a Machine Catalog or from a Delivery Group.

Published Data

This activity publishes the following activity-specific data.

Machine Name	The name of the machine that has been removed from the Machine Catalog or Delivery Group
Machine UID	The UID of the machine that has been removed from the Delivery Group. Machine UID value is not published after removing a machine from a catalog since the machine UID is no longer valid.

Remove User Activity

The **Remove User** activity is used in a runbook to remove a user from a Private (Static) Desktop or Shared (Random) Delivery Group or a Machine.

Required Properties

You must configure the following properties.

Machine Name	Name of the machine the user is to be removed from, in the form *domain**machine*. Available only when removing a user from a machine.
Private (Static) Desktop Name	Name of the private desktop the user is to be removed from, in the form *DOMAIN**machine*. Available only when removing a user from a private desktop.
Remove User From	Specifies whether the user is to be removed from a Private Desktop or from a Shared Group or from a Machine.
Shared (Random) Group UID	Identifies the shared delivery group the user is to be removed from. Available only when removing a user from a shared delivery group.
User Name	Name of the user to be removed, in the form *domain**user.*

Published Data

This activity publishes the following activity-specific data.

Machine Name	Name of the machine the user has been removed from.
Machine UID	UID of the machine the user has been removed from.
Private (Static) Desktop Name	Name of the private desktop the user has been removed from.
Private (Static) Desktop UID	UID of the private desktop the user has been removed from.
Shared (Random) Group Name	Name of the shared group the user has been removed from.
Shared (Random) Group UID	UID of the shared group the user has been removed from.
User Name	Name of the user that has been removed.

Restart Machine Activity

The **Restart Machine** activity is used in a runbook to restart a running machine. The activity initiates a machine restart action with the underlying hypervisor and may complete before the machine is restarted.

Required Properties

You must configure the following properties.

Force	Indicates whether to forcefully restart the machine or not.
Machine Name	Name of the machine to be restarted, in the form *domain**machine*.

Published Data

This activity publishes the following activity-specific data.

Machine Name	The name of the machine that has been restarted.
Machine UID	The UID of the machine that has been restarted.

Run PowerShell Script Activity

The **Run PowerShell Script** activity is used in a runbook to run Virtual Apps and Desktops specific PowerShell commands. Use this activity to run commands which are not implemented by specific activities in the integration pack.

Required Properties

You must configure the following properties.

Script Text	Virtual Apps and Desktops specific PowerShell script to be executed.

Published Data

This activity publishes the following activity-specific data.

Result Object	Object properties returned from running the script, if the script returned any objects (for example, from Get commands). Object properties formatted in JSON.
Result Object Count	Number of objects returned from running the script, if any (for example, from Get commands).
Result Text	Text representation of the script output. This field is useful in cases when the script prints information to the output stream.
Warnings	Warnings returned from running the script, if any.

Set Maintenance Mode Activity

The **Set Maintenance Mode** activity is used in a runbook to enable or disable maintenance mode for a Virtual Apps and Desktops machine.

Required Properties

You must configure the following properties.

Machine Name	Identifies the machine for which maintenance mode is to be enabled or disabled, in the form *domain**machine.*
Machine UID	Identifies the machine for which maintenance mode is to be enabled or disabled. Takes precedence over Machine Name.
Maintenance Mode Enabled	Indicates whether maintenance mode is to be enabled or disabled.

Published Data

This activity publishes the following activity-specific data.

Machine Name	The name of the machine that has been placed in maintenance mode.
Machine UID	The UID of the machine that has been placed in maintenance mode.

Shut Down Machine Activity

The **Shut Down Machine** activity is used in a runbook to shut down a running machine. The activity initiates a machine shut-down action with the underlying hypervisor and may complete before the machine shuts down.

Required Properties

You must configure the following properties.

Force	Indicates whether to forcefully shut down the machine or not.
Machine Name	Name of the machine to be shut down, in the form *domain**machine*.
Machine UID	Identifies the machine to be shut down. Takes precedence over Machine Name.

Published Data

This activity publishes the following activity-specific data.

Machine Name	The name of the machine that has been shut down.
Machine UID	The UID of the machine that has been shut down.

Start Machine Activity

The **Start Machine** activity is used in a runbook to start a machine. The activity initiates a machine start action with the underlying hypervisor and may complete before the machine starts. You can use the **Get Machine** activity to verify the current machine Power State.

Required Properties

You must configure the following properties.

Machine Name	Name of the machine to be started, in the form *domain\machine.*
Machine UID	Identifies the machine to be started. Takes precedence over Machine Name.

Published Data

This activity publishes the following activity-specific data.

Machine Name	The name of the machine that has been started.
Machine UID	The UID of the machine that has been started.

Stop Session Activity

The **Stop Session** activity is used in a runbook to stop (logoff) a running desktop session. The activity executes a non-blocking operation, and it may finish before the operation completes. You can use the **Get Session** activity to verify the state of the session.

Required Properties

You must configure the following properties.

Session UID	Identifies the session to be stopped

Published Data

This activity does not publish any activity-specific data.