Quick-Start Tutorial for VMware Horizon JMP Integrated Workflow
# Table of Contents

Technical Introduction ................................................................................................................................. 3
  Overview ...................................................................................................................................................... 4
  Introduction to JMP .................................................................................................................................... 5

Installation ..................................................................................................................................................... 7
  Set Up the JMP Server Database ..................................................................................................................... 8
  Install the JMP Server .................................................................................................................................. 19

Initial Configuration ..................................................................................................................................... 27
  Synchronize Time with Connection Server ...................................................................................................... 28
  Place the Root Certificate from the AD Server in the JMP Configuration Folder .............................................. 31
  Place the Certificate for Connection Server in the JMP com Folder ................................................................. 41
  Place the Certificate for App Volumes Server in the JMP com Folder ............................................................. 52
  Use the Horizon Console to Add the JMP Server ............................................................................................. 58
  Configure the Browser to Accept the Default JMP Server Certificate ............................................................ 67
  Add the Other Servers to the JMP Settings .................................................................................................... 82

Basic JMP Integrated Workflow .................................................................................................................. 92
  Create a JMP Assignment ............................................................................................................................. 93

Summary and Next Steps ............................................................................................................................ 101
  Introduction ................................................................................................................................................ 102
  Terminology Used in This Tutorial ............................................................................................................... 103
  Additional Resources .................................................................................................................................... 104
  About the Author and Contributors .......................................................................................................... 105
Technical Introduction
Overview

JMP (pronounced *jump*), which stands for Just-in-Time Management Platform, represents capabilities in VMware Horizon® 7 Enterprise Edition that deliver Just-in-Time Desktops and Apps in a flexible, fast, and personalized manner. JMP is composed of the following VMware technologies:

- **VMware Instant Clone Technology** for fast desktop and RDSH provisioning
- **VMware App Volumes™** for real-time application delivery
- **VMware User Environment Manager™** for contextual policy management

The JMP approach provides several key benefits, including simplified desktop and RDSH image management, faster delivery and maintenance of applications, and elimination of the need to manage “full persistent” desktops. JMP is supported with both on-premises and cloud-based Horizon 7 deployments, providing a unified and consistent management platform regardless of your deployment topology.

With the Horizon Console and the VMware Horizon JMP Integrated Workflow features, you can use a single console to define and manage desktop workspaces for users or group of users. You create a desktop workspace by defining a JMP assignment that includes information about the desktop pool, the App Volumes AppStacks, and User Environment Manager settings. After you submit the JMP assignment, the JMP automation engine communicates with the Connection Server, App Volumes, and User Environment Manager systems to entitle the user to a desktop.

Purpose of This Tutorial

The *Quick-Start Tutorial for VMware Horizon JMP Integrated Workflow* helps you evaluate JMP Integrated Workflow features by providing a discussion of the product and offering practical exercises.

**Important**: This tutorial is designed for evaluation purposes only, based on using the minimum required resources for a basic deployment, and does not explore all possible features. This evaluation environment should not be used as a template for deploying a production environment. To deploy a production environment, see the [VMware Horizon 7 documentation](#).

Audience

This tutorial is intended for IT administrators and product evaluators who are familiar with VMware vSphere® and VMware vCenter Server®. Familiarity with networking and storage in a virtual environment, Active Directory, identity management, and directory services is assumed. Knowledge of other technologies, such as [VMware Horizon 7](#) is also helpful.
Introduction to JMP

In the early years of VDI, the operating system (OS) for each virtual desktop had to be managed and patched regularly, and applications had to be updated, just as if the VM were a physical machine. In recent years, linked-clone technology sped up VM creation, provisioning, and maintenance, but maintenance windows were still required for refreshing the VM back to its original disk size. The VM also had to go through a lengthy recompose operation to apply OS and application updates. And at regular intervals VMs had to be rebalanced across datastores.

Today with JMP, components of a desktop or RDSH server are decoupled and managed independently in a centralized manner, yet reconstituted on demand to deliver a personalized user workspace when needed. For example, because VMs can be cloned in seconds, they no longer need to persist when the user logs out. App Volumes, a container-style technology, can attach applications to a VM when the user logs in. User preferences and settings for each application are applied when the user launches the application.

How JMP Works

JMP offers an alternative to managing per virtual machine. JMP decouples each aspect of a desktop to allow it to be managed on a per-user or per-group basis. As illustrated in the following figure, application-management containers are managed separately from the desktop OS. Similarly, user data files and OS- and application-specific configurations are decoupled from the OS and kept on separate file shares.

![JMP Management Strategy](image)

**Figure 1**: How JMP Technologies Manage Virtual Desktops, Settings, and User Data
The following components of JMP work together to compose a just-in-time personalized desktop:

- **User Environment Manager share** A file share that stores user-specific desktop and application settings, making them available across multiple devices, Windows versions, and application instances.

  Application settings are imported and applied at application launch. Windows settings (such as the desktop background, desktop screensaver, keyboard settings) are imported at login. When a user quits an application, or logs out of the OS, settings are exported and saved on a file share.

- **User data share** A file share that stores personal user data, documents, pictures, and so on that are redirected from specific folders inside the VM. This strategy minimizes the number of files that must be copied to the VM when the user logs in.

- **AppStack** A read-only container for one-to-many delivery of IT-managed applications. For virtual desktops, AppStacks are assigned to an Active Directory user or group, and assigned AppStacks are attached to the desktop when a user logs in.

- **Writable volume** A one-to-one, user-specific, read-and-write container for user-installed applications or for applications that require a local cache, since a writable volume appears as part of the local C: drive.

- **Instant clone** A new type of cloned VM that is created using vSphere vmFork technology to rapidly clone both the memory and the disk of a running parent VM.

You use the Horizon Console to access the JMP integrated workflow. With this one user interface, you create an assignment that defines which elements to use from all three products: View in Horizon 7, App Volumes, and User Environment Manager.

### Component Requirements

The JMP integrated workflow requires that the following versions of the Horizon 7 components be installed and set up:

- **Horizon 7 version 7.5 or later** – For instructions for installing and configuring the Connection Server, see Reviewer’s Guide for View in VMware Horizon 7: Installation and Configuration. For instructions on creating instant-clone desktop pools, see Reviewers Guide for View in Horizon 7: Instant Clones.

- **App Volumes 2.14 or later** – For instructions for installing and configuring App Volumes Manager, see Reviewer’s Guide for VMware App Volumes, and see the VMware App Volumes documentation.

- **User Environment Manager 9.2.1 or later** – For instructions for installing and configuring User Environment Manager, see Quick-Start Tutorial for User Environment Manager.

**Note**: Although you can also integrate JMP with VMware Workspace ONE through VMware Identity Manager, such integration is beyond the scope of the exercises in this tutorial. For more information about this integration, see the VMware Horizon 7 documentation.
Installation
Set Up the JMP Server Database

Before you can run the JMP installer, you must create a database and two database logins.

Prerequisites for Setting Up the JMP Server Database

To perform this exercise, you need the following:

- **User account** – AD credentials for the user account that will be used for installing the JMP server. To run the installer, you must use a domain user account with local administrative privileges on the host system of the JMP server VM.
- **SQL Server instance** – This is the database server on which you will create the database for the JMP server. For the example in this exercise, we used Microsoft SQL Server 2016. For a list of all supported databases, see Database Requirements for JMP Server.
- **Microsoft SQL Server Management Studio** – For the example in this exercise, we used Microsoft SQL Server Management Studio v17.7. The instructions might differ slightly for different versions of SQL Server Management Studio.
- **SA credentials** – To create the necessary logins for the JMP server database, you will log in to the SQL Server instance as the sysadmin (SA) or as a user account with SA privileges.

1. Open Microsoft SQL Server Management Studio

   1. On the VM where SQL Server and SQL Server Management Studio are installed, click the **Start** button.
   2. Navigate to and select **Microsoft SQL Server Management Studio**.
2. Log In to a SQL Management Studio Session as SA

1. Select SQL Server instance. By default your Windows login credentials are used, but you are not required to use Windows authentication.
2. Log in as the sysadmin (SA) or using a user account with SA privileges.
3. Click Connect.

3. Create a Database for the JMP Server

1. [Diagram of creating a new database]

   1. Right-click the databases folder and select New Database.
   2. Name the database and select options as needed.

1. In the Object Explorer, right-click **Databases**.
2. Select **New Database**.

### 4. Name the Database

1. For the database name, enter **JMPDB**. You must use only ASCII characters. Use the default settings.
2. Click **OK**.

### 5. Create a Database Login for the JMP Server Machine

The JMP server installer needs to access the database when it runs. You must create a login for this purpose.
5.1. Create a Login

1. Expand the Security folder, and right-click Logins.
2. Select New Login.

5.2. Complete the General Settings
1. Enter a login name to use for the JMP server machine, using ASCII characters only; for example, JMPSERVER.
2. Select SQL Server authentication, and create a password.
3. De-select Enforce password policy. For the purposes of this exercise, you do not need to use password policies.
4. Select a default language.

You can leave the default database set to master, or you can select the JMPSERVER database.

5.3. Assign the sysadmin Server Role

1. Select the Server Roles page.
2. Select the sysadmin check box.
5.4. Map the Login to the JMP Server Database

1. Select the User Mapping page.
2. Select the JMPDB database.
3. Click OK.

The new login is added under the Security > Logins folder in the Object Explorer pane, and the user is added under the Databases > JMPDB > Security > Users folder.
6. Create a Login for the User Account That Will Install the JMP Server

1. Expand the Security folder, and right-click Logins.
2. Select New Login.
6.1. Select the AD Credentials

1. Click Search.
2. Enter a valid Active Directory user account that you plan to use to install JMP Server.
3. Click Check Names to validate the account name.
4. Click OK.
6.2. Assign the sysadmin Server Role

1. Select the Server Roles page.
2. Select the sysadmin check box.
6.3. Grant the User the db_owner Role for the JMPDB Database

1. Select the User Mapping page.
2. Select the JMPDB database.
3. Select the db_owner role.
4. Click OK.

The new login is added under the Logins folder in the Object Explorer pane, and the user is added under the Databases > JMPDB > Security > Users folder.
Install the JMP Server

Installing the JMP server is a simple process of running the installation wizard and pointing to the JMP server database you created.

Prerequisites for Installing the JMP Server

To perform this exercise, you need the following:

- **Horizon 7 components** – Before you install the JMP server, you need to have installed and configured the following components:
  - **Connection Server** – The required version is Horizon 7 version 7.5 or later. For installation instructions, see [Reviewer's Guide for View in VMware Horizon 7: Installation and Configuration](https://vmware.com/horizon).  
  - **VMware App Volumes 2.14 or later** – For installation instructions, see [Reviewer’s Guide for VMware App Volumes](https://vmware.com/).  
  - **VMware User Environment Manager 9.2.1 or later** – For installation instructions, see [Quick-Start Tutorial for VMware User Environment Manager](https://vmware.com/).  

- **User account** – To run the installer, you must use a domain user account with administrative privileges on the host system of the JMP server VM. For this exercise, you will use the user account for which you created a database login during the previous exercise.

- **Database** – Verify that you have performed all the steps in the exercise [Set Up the JMP Server Database](https://vmware.com/), which include creating the database and the various logins required for the JMP server to communicate with the database.

- **Installer** – The JMP Server installer file is included when you download VMware Horizon 7 version 7.5 or later. If necessary, you can download the installer from the [Product Evaluation Center](https://vmware.com/) or the [VMware Downloads](https://vmware.com/) page.

- **VM to host the JMP server** – Like all server VMs, the JMP server has certain hardware, OS, and network requirements. For the example in this exercise, we used a Windows Server 2016 VM with 4 vCPUs, 4 GB of memory, and 25 GB of storage. For a production environment, see [Hardware Requirements for JMP Server](https://vmware.com/) and [Supported Operating System for JMP Server](https://vmware.com/).

For a complete list of system requirements, see [System Requirements for JMP Server](https://vmware.com/), in the [VMware Horizon JMP Server Installation and Setup Guide](https://vmware.com/).

**Note:** If the VM has McAfee Antivirus installed, add the following files to the McAfee Antivirus exclusion list before you install the JMP server.

```plaintext
C:\Program Files (x86)\VMware\JMP\nssm-2.24\nssm-2.24\win32\nssm.exe
C:\Program Files (x86)\VMware\JMP\com\xmp\node_modules\winser\bin\nssm.exe
```
1. Copy or Download the Installer to the JMP Server VM

For this example, we downloaded the installer to a VM hosted on a VMware ESXi server. To connect to this VM, called CA-JMP, you would select the VM in the inventory list and select Launch Web Console.

For the example in this exercise, we copied the file to the JMP server system, but you can alternatively copy it to a location accessible to the system.

2. Start the Installer
1. Log in to the JMP server host system as a domain user with administrative privileges on the host system, and double-click the installer file.
2. Follow the prompts until you get to the Allow HTTP Traffic on Port 80? page.

3. Click Next

![Screenshot of the Allow HTTP Traffic on Port 80? screen]

The JMP server uses port 443 and, optionally, ports 80, 3000–3004, 888, and 8889. The choice of whether to allow port 80 is up to you. For the purposes of this exercise, and for some POC (proof-of-concept) installations, enabling HTTP traffic on port 80 helps avoid having to troubleshoot issues with encryption.
4. Click Browse to Select the Database Server

Although you can type in the name of the server, using the **Browse** button ensures that the server is accessible and avoids typing mistakes.

**Note:** By default, the connection uses Windows authentication. This is correct, assuming you logged in to the system as the same domain user that you used for creating the database login, as described in [Set Up the JMP Server Database](#).
5. Select the Database Server

Select the database server you used when completing the exercise Set Up the JMP Server Database, and click OK.

6. Enter Credentials for SQL Server Authentication
1. Select Server authentication using Login ID and password below. This was the type of authentication used in the exercise Set Up the JMP Server Database.
2. Enter the login ID name (JMPSERVER) and password you used when you created this ID.

7. De-select Enable SSL Connection and Click Browse

1. Click to remove the check mark from the Enable SSL Connection? check box.

   **Important**: When this check box is selected, the TLS/SSL certificate used in SQL Server must be imported into the Windows local certificate store on the JMP Server host before you run the installer. Otherwise, the JMP server installation process fails with the error "Failed to execute uem_migrate.bat file," and when you click OK in the error dialog box, installation is rolled back. In a production environment, for security purposes, you would leave this check box selected, but for this exercise, de-select the check box.

2. Click **Browse** to select the database from a list.
8. Select the JMPDB Database

1. Select the database you created when completing the exercise Set Up the JMP Server Database.
2. Click OK to close the dialog box, and click Next on the wizard page.

9. Click Install
After installation is complete, the wizard notifies you that installation was successful.

10. Verify Installation

1. Navigate to the **Programs and Features** control panel.
2. Verify that the **VMware JMP Server** program appears in the list.
Initial Configuration
Synchronize Time with Connection Server

The clock in both the Connection Server and JMP server hosts must be synchronized in order for the authentication process between the two servers to be successful.

**Important:** For the purposes of this quick-start, we assume that you are performing these exercises in a test environment. Changing the time-synchronization configuration of a Connection Server or ESXi host in a test environment does not carry the same risks as changing the configuration of a production environment component. If you are performing this exercise using a production Connection Server or ESXi host, consult with the proper administrators before changing time-synchronization settings.

Prerequisites for Synchronizing Time

To complete this exercise, you will need:

- **VMware Tools** – You will use VMware Tools command-line options to turn on time synchronization with the ESXi host for the Connection Server VM and the JMP server VM. Therefore, VMware Tools must be installed in the VMs.
- **Connection Server version** – To use the JMP integrated workflow, the Connection Server version must be Horizon 7 version 7.5 or later.

1. Use the timesync Option to Turn On Time Synchronization for the VMs

1. On the Connection Server system, open a command prompt, and change directories to the `C:\Program Files\VMware\VMware Tools` directory.
2. Run the following command to find out whether time synchronization is disabled:
   ```
   VMwareToolboxCmd.exe timesync status
   ```
3. If `Disabled` is returned, run the following command:
   ```
   VMwareToolboxCmd.exe timesync enable
   ```
4. Repeat these steps on the JMP server system.
Both the JMP server and the Connection Server now synchronize time with the ESXi host.

2. Configure Time Synchronization on the ESXi Host or Hosts

1. In vSphere Client, select the ESXi host for the Connection Server and the JMP server.
   
   If you do not know which ESXi host to use, select the VM for the Connection Server or JMP server and use the Summary tab to determine the ESXi host.

   **Note:** The JMP server might use a different host from the Connection Server.

2. Select the Configure tab.
3. Under the System settings, select Time Configuration.
4. Click Edit.
3. Enable NTP

1. Select **Use Network Time Protocol (Enable NTP client)**.
2. Enter the IP address or fully qualified domain name of one or more NTP servers to synchronize with.
3. Click **OK**.
4. If the JMP server VM and the Connection Server VM use different ESXi hosts, repeat the steps to configure NTP on the other ESXi host. Be sure to use the same NTP server or servers.
Place the Root Certificate from the AD Server in the JMP Configuration Folder

In this exercise, you will export the root CA certificate of the Active Directory domain controller into a certificate file named `adCA.pem` and place this file in a configuration folder on the JMP server.

Prerequisites for Obtaining the AD Server's Root Certificate

Active Directory must be configured for LDAP over SSL (LDAPS) or StartTLS (LDAP over TLS).

1. Start the Microsoft Management Console

   1. Log in to the operating system of the Active Directory server, and right-click the Windows Start icon.
   2. Select Run.
   3. Type `mmc`.
   4. Click OK.
2. Add Snap-in for Certificate Manager

Select File > Add/Remove Snap-in.

3. Select the Certificates Snap-in

1. Select Certificates.
2. Click Add.
4. Select Computer Account

Because you want to export the root certificate for the server, select **Computer account**, and click **Next**.
5. Select the Local Computer

Select Local Computer (the computer this console is running on), and click Finish.
6. Click OK in the Snap-in Dialog Box

With the Certificates snap-in added to the Selected snap-ins list, click OK.

7. Locate the Server's Certificate in the Personal Folder
1. Expand the **Certificates** > **Personal** folder, and select the **Certificates** folder.
2. Right-click a certificate name and select **Open**. You can select any of the certificates in this folder to determine the root certificate.
3. On the **Certification Path** tab, note the top-most item. The name of the root certificate is displayed.

8. **Locate and Export the Root Certificate**

1. Expand the **Trusted Root Certification Authorities** folder, and select the **Certificates** folder.
2. Right-click the certificate name. This is the certificate that was listed on the **Certification Path** tab in the previous step.
3. Select **All Tasks > Export**.
9. Export a Base-64 Encoded Certificate

In the Certificate Export Wizard, select **Base-64 encoded X.509 (.CER)**, and click **Next**.
10. Name the File adCA.pem

Type the file name `adCA.pem`, and click Next.
11. Complete the Wizard

Note that the completion page displays the location of the file, and click Finish.
12. Copy the Exported Certificate to the JMP Server

Copy the **adCA.pem** file to the JMP Server XMS configuration folder, in the following location:

```
C:\Program Files (x86)\VMware\JMP\com\XMS\config\adCA.pem
```

**Note:** To verify that the file uses the **.pem** extension rather than the **.cer** extension, you can click the View tab at the top of the window and select the File name extensions check box. For example, if the file name is **adCA.cert.pem.cer**, rename the file to remove the **.cer** at the end of the file name. The file must have a **.pem** file extension.
Place the Certificate for Connection Server in the JMP com Folder

In this exercise, you will export the server certificate of the Connection Server into a certificate file named `horizon.cert.pem` and place this file in the `com` folder on the JMP server.

Prerequisites for Placing the Connection Server Certificate on the JMP Server

You must have credentials for a user account that has administrator privileges on the Connection Server system and on the JMP server system.

1. Start the Microsoft Management Console

1. Log in to the operating system of the Connection Server, and right-click the Windows Start icon.
2. Select Run.
3. Type `mmc`.
4. Click OK.
2. Add Snap-in for Certificate Manager

Select File > Add/Remove Snap-in.

3. Select the Certificates Snap-in

1. Select Certificates.
2. Click Add.
4. Select Computer Account

Because you want to export the server certificate for the server, select Computer account, and click Next.

5. Select the Local Computer
Select Local Computer (the computer this console is running on), and click Finish.

6. Click OK in the Snap-in Dialog Box

With the Certificates snap-in added to the Selected snap-ins list, click OK.
7. Locate the Server's Certificate in the Personal Folder

1. Expand the Certificates > Personal folder, and select the Certificates folder.
2. Right-click the certificate name and select Properties.
3. Verify that the friendly name of the certificate is `vdm`. If not, find the certificate in that folder that has the friendly name `vdm`.
4. Close the dialog box.
8. Export the Server Certificate

Right-click the certificate and select All Tasks > Export.
9. Do Not Export a Private Key

In the Certificate Export Wizard, on the Export Private Key page, select **No, do not export the private key**, and click **Next**.
10. Export a Base-64 Encoded Certificate

In the Certificate Export Wizard, select **Base-64 encoded X.509 (.CER)**, and click **Next**.
11. Name the File horizon.cert.pem

Type the file name `horizon.cert.pem` and click Next.
12. Complete the Wizard

Note that the completion page displays the location of the file, and click Finish.

13. Copy the Exported Certificate to the JMP Server
Copy the `horizon.cert.pem` file to the JMP server home folder (`com`), in the following location:

C:\Program Files (x86)\VMware\JMP\com\horizon.cert.pem

**Note:** To verify that the file uses the `.pem` extension rather than the `.cer` extension, you can click the View tab at the top of the window and select the File name extensions check box. For example, if the file name is `horizon.cert.pem.cer`, rename the file to remove the `.cer` at the end of the file name. The file must have a `.pem` file extension.
Place the Certificate for App Volumes Server in the JMP com Folder

In this exercise, you will export the self-signed certificate of the App Volumes Manager instance into a certificate file named `av-selfsigned.cert.pem` and place this file in the `com` folder on the JMP server.

Prerequisites for Placing the App Volumes Manager Certificate on the JMP Server

To perform this exercise, you need the following:

- App Volumes Manager is installed and set up. For instructions for installing and configuring App Volumes Manager, see [Reviewer's Guide for VMware App Volumes](#), and see the VMware App Volumes documentation. App Volumes 2.14 or later is required.
- To save the certificate file to the correct location, you must have credentials for a user account that has administrator privileges on the JMP server system.

1. Log In to App Volumes Manager from the JMP Server

Log in to the JMP server system as an administrator, open a browser and type in the URL to the App Volumes Manager host; for example,
For the example in this exercise, we used a Firefox browser.

In the production environment, this URL might point to a load balancer fronting two App Volumes Managers.

2. Open the Site Information Dialog Box

Click the Show Site Information icon to access the certificate information.
3. View the Certificate

On the Security tab, click View Certificate.
4. Export the Certificate

On the Details tab, click Export.
5. Save the Exported Certificate to the JMP Server

1. For **Save as type**, select a PEM-formatted certificate type.
2. For **File name**, type `av-selfsigned.cert.pem`.
3. For the folder on the local drive, navigate to `C:\Program Files (x86)\VMware\JMP\com`.
4. Click **Save**.

6. Open the Services Applet

1. Click **Run**.
2. Type `services.msc` in the **Open** field.
3. Click **OK**.
1. To open the Services applet, right-click the Start button, and select Run.
2. Type `services.msc`.
3. Click OK.

7. Restart the JMP Services

For each of the following JMP services:

- VMware JMP API Service
- VMware JMP File Share Service
- VMware JMP Platform Services

1. Right-click the service name.
2. Select Restart.
Use the Horizon Console to Add the JMP Server

After you have installed the JMP server and placed the certificate files from the various servers in the correct location on the JMP server, you are ready to configure settings for the JMP integrated workflow.

Prerequisites for Adding the JMP Server

Before you perform this exercise, you need:

- **Administrator account** – This is a domain account for the Administrator user (\<domain-name>\Administrator). You will add this user to Horizon Administrator.
- **JMP server URL** – Use the fully qualified domain name of the JMP server machine.
- **Connection Server certificate** – This certificate must be exported in the correct format and placed on the JMP server machine in the correct location. See Place the Certificate for Connection Server in the JMP com Folder.

**Important**: For the purposes of this quick-start, because you are using a test environment rather than a production environment, you do not need to install CA-signed security certificates on your servers. However, if you do not use a CA-signed TLS certificate for the JMP server, your browser most likely will not recognize the default TLS certificate, and you will not be able to successfully complete this exercise. To resolve this issue, use either of the following options:

- Obtain a CA-signed TLS certificate and replace the default TLS certificate installed by the JMP Server installer. See Replace the Default TLS Certificate.
- Configure the browser on the computer you are using for the Horizon Console to accept the default certificate. See Configure the Browser to Accept the Default JMP Server Certificate.

If you do not use either of these options, when you attempt to add the JMP server, you might get the following error message.
1. Add a New User to Horizon Administrator

1. Log in to Horizon Administrator and navigate to View Configuration > Administrators.
2. Click Add User or Group.
2. Add the Domain Administrator User

1. In the Add Administrator or Permission dialog box, click **Add**.
2. In the Find User or Group dialog box, select the domain for the Connection Server and JMP server.
3. In the **Name/Username** text box, enter **Administrator**.
4. Click **Find**.
5. Select the domain Administrator user in the list.
6. Click **OK**.

---

Quick-Start Tutorial for VMware Horizon JMP Integrated Workflow
3. Give the User the Administrators Role

1. On the Select administrators or groups page, click Next.
2. On the Select a role page, select Administrators.
3. Click Next.
4. Select the Root Access Group for the User

1. Select the check box for Root (/).
2. Click Finish.

The domain Administrator account now has full Horizon Administrator permissions.
5. Click Settings in the Horizon Console

Log in to the Horizon Console as the `<domain-name>\Administrator` (not as BUILTIN\Administrator), and click Settings. This `<domain-name>\Administrator` user is the user you just added in the previous steps.

The URL for the Horizon Console uses the following format:

```
https://<connection_server>.<domain>.com/newadmin
```
6. Click Add JMP Server

On the JMP Server tab, click Add JMP Server.
7. Add the JMP Server URL

Use the following format:

https://<jmp_server>.<domain>.com/

If you receive an error message, verify that:

- In Horizon Administrator, you have added the <Domain>\Administrator user and given that user the Administrators role at the root level of Horizon Administrator.
- You have exported the Connection Server certificate with the friendly name vdm to a base-64-encoded .pem file and placed it in the following location on the JMP server: C:\Program Files (x86)\VMware\JMP\com\horizon.cert.pem, as described in Place the Certificate for Connection Server in the JMP com Folder.
- You have either installed a CA-signed TLS certificate on the JMP server, or you have configured your browser to accept the default self-signed certificate. See Configure the Browser to Accept the Default JMP Server Certificate.

If all goes well, the URL is validated.
To complete the JMP set up, please have the URL, user name, and password for the following components:

- VMware Horizon® 7 Pod (required)
- Active Directory (required)
- VMware App Volumes (optional)
- VMware User Environment Manager (UEM) File Share (optional)
Configure the Browser to Accept the Default JMP Server Certificate

If you do not use a CA-signed TLS certificate for the JMP server, your browser most likely will not recognize the default TLS certificate, and when you attempt to use the Horizon Console to add the JMP server, you see the following error message.

![Figure 1: Attempting to Add the JMP Server When Its Certificate Is Not Trusted](image1)

After you succeed in adding the JMP server, if you attempt to use Horizon Console in a different browser or a browser on another computer, you might see the following error message.

![Figure 2: Attempting to Access the JMP Server Settings from a Browser That Does Not Trust the JMP Server Certificate](image2)
You can either configure your browser to accept the self-signed certificate or you can install a CA-signed certificate on the JMP server, as described in Replace the Default TLS Certificate. The procedure for configuring your browser depends on which browser you are using:

- **Procedure for Configuring the Firefox Browser**
- **Procedure for Configuring the Chrome Browser**
- **Procedure for Configuring the Internet Explorer Browser**

**Procedure for Configuring the Firefox Browser**

Browser features and options can change as new versions are released. This procedure uses Firefox 60.0.2.

1. **Browse to the URL for the JMP Server**

As you can see, the browser cannot connect to the JMP server.
2. Open the Firefox Browser Menu

Click the menu button icon.

3. Select Options
4. Open the Privacy & Security Settings

Click **Privacy & Security** in the list of settings.

5. Click View Certificates in the Security Section

Scroll down to the Security section, and click **View Certificates**.
6. Click Add Exception on the Servers Tab

7. Enter an Exception for the JMP Server

1. Enter the URL for the JMP server.
2. Click Get Certificate.
3. Select the **Permanently store this exception** check box.
4. Click **Confirm Security Exception**.

8. **Verify That the JMP Server Has Been Added to the List of Exceptions**

On the **Servers** tab, verify that the JMP server is listed, and click **OK**.

You can now go back to the JMP Settings page in the Horizon Console. When you refresh your browser, the JMP server is validated.
Procedure for Configuring the Chrome Browser

Browser features and options can change as new versions are released. This procedure uses Google Chrome 67.0.3396.99.

1. Browse to the URL for the JMP Server and View Site Information

To view information about the self-signed certificate, click View site information.

2. Click Certificate

To open the Certificate dialog box, click Certificate.
3. Copy the Certificate Information to a File

On the Details tab, click Copy to File.
4. Click Next in the Certificate Export Wizard

5. Select the Base-64 Format
Select Base-64 encoded X.509 (.CER), and click Next.

6. Click Browse
7. Save the File

Name the file, and click Save. You can save the file in any location on your computer.
8. Click Next

9. Click Finish
The certificate file is saved with a .cer extension, as shown in the following screen shot. You do not need to install the certificate.

You can now go back to the JMP Settings page in the Horizon Console. When you refresh your browser, the JMP server is validated.

Procedure for Configuring the Internet Explorer Browser

Browser features and options can change as new versions are released. This procedure uses Internet Explorer 11.2312.14393.0.

1. Disable IE ESC If You Are Using Windows Server

In order to avoid responding to a large number of security alerts, saying that content has been blocked, you can use Windows Server Manager to disable IE enhanced security configuration. See How to Disable Internet Explorer Enhanced Security Configuration.
2. Click JMP Settings in the Horizon Console

Log in to the Horizon Console, and click Settings for the JMP server.
3. Click Yes in the Security Alert

Click Yes when the Security Alert dialog box prompts you. The JMP server is validated.
Add the Other Servers to the JMP Settings

In this exercise, you will add the URLs and credentials for accessing the servers for the components of the JMP integrated workflow, which includes the Connection Server, the Active Directory server, the App Volumes Manager server, and the User Environment Manager Configuration Share file server.

**Note:** The steps for configuring the App Volumes Manager settings and the User Environment Manager configuration share settings are optional. When creating JMP assignments, you are not required to use these components, but later exercises in this quick-start tutorial do use these components.

Prerequisites for Adding the Other Servers to JMP Settings

Before you perform this exercise, you need:

- **Security certificates for the Active Directory and App Volumes machines** – You can use CA-signed certificates or the default self-signed certificates. These certificates must be exported in the correct format and placed on the JMP server machine in the correct location. See Place the Root Certificate from the AD Server in the JMP Configuration Folder and Place the Certificate for App Volumes Server in the JMP com Folder.

- **Server information for the JMP components** – Use the following table to organize the required information about the various servers involved in the JMP integrated workflow.

  **Tip:** The user (service) accounts for each of the components require the administrator-level role for that component. To simplify your setup in a test environment, you could create one account, with the user name *Administrator*, and use that account for all the server components. You could then use the same credentials for all four of the components.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection Server URL</td>
<td>Example: <a href="https://connection_server.mycompany.com">https://connection_server.mycompany.com</a></td>
</tr>
<tr>
<td>Horizon 7 service account credentials</td>
<td>User name and password for a user with the Administrators role in the root level in Horizon Administrator. For this exercise, we will use the domain Administrator user you added when you added the JMP server.</td>
</tr>
<tr>
<td>Horizon Administrator Service Account Domain</td>
<td>NETBIOS domain name for the Horizon 7 service account, which does not include .com. Example: mycompany</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Active Directory NETBIOS Name</td>
<td>The same NETBIOS domain name as was used for the Service Account Domain. You will select this name from a drop-down list.</td>
</tr>
<tr>
<td>Active Directory Protocol</td>
<td>The protocol used by your Active Directory. For the example in this exercise, our lab was set up to use <strong>LDAP (non-secure)</strong>. For a production environment, the protocol is usually <strong>LDAP over TLS</strong>.</td>
</tr>
<tr>
<td>Active Directory Bind User Name and Bind Password</td>
<td>Most likely, these are the credentials for the administrator user.</td>
</tr>
<tr>
<td>App Volumes Manager URL</td>
<td>Example: <a href="https://app_vol_mgr.mycompany.com">https://app_vol_mgr.mycompany.com</a></td>
</tr>
<tr>
<td>App Volumes service account credentials</td>
<td>User name and password for a user with the Administrators role in App Volumes Manager.</td>
</tr>
<tr>
<td>App Volumes Service Account Domain</td>
<td>The NETBIOS domain name for the App Volumes service account, which does not include .com. Example: <a href="http://mycompany">mycompany</a></td>
</tr>
<tr>
<td>User Environment Manager File Share UNC Path</td>
<td>This is the UNC path to the User Environment Manager configuration share. For details on setting up this share, see <a href="https://app_vol_mgr.mycompany.com">Quick-Start Tutorial for User Environment Manager</a>. Example: <a href="http://%5Cfile%5CUEM_Config">\file\UEM_Config</a></td>
</tr>
<tr>
<td>User Environment Manager User Name and Password</td>
<td>User name and password for a User Environment Manager administrator account to connect to the User Environment Manager configuration share.</td>
</tr>
<tr>
<td>Active Directory domain for User Environment Manager</td>
<td>The NETBIOS domain name for the User Environment Manager user account. You will select this name from a drop-down list.</td>
</tr>
</tbody>
</table>

**Table:** Server Information for Configuring JMP Integrated Workflow Settings
1. Add the Connection Server

1. Log in to the Horizon Console, and click **Settings**.
2. Click the **Horizon 7** tab.
3. Click **Add Credentials**.
2. Add Credentials for Horizon Administrator

Add the information you gathered as part of Prerequisites for Adding the Other Servers to JMP Settings. The Connection Server URL is already populated.
3. Add the Active Directory Server

1. Click the **Active Directory** tab.
2. Click **Add**.
4. Add Credentials for the Active Directory Server

Add the information you gathered as part of Prerequisites for Adding the Other Servers to JMP Settings. After you select the domain from the NETBIOS Name list, the DNS Domain Name text box and the Context text box are automatically populated.
5. Add the App Volumes Manager Server

1. Click the **App Volumes** tab.
2. Click **Add**.
6. Add Credentials for App Volumes Manager

Add the information you gathered as part of [Prerequisites for Adding the Other Servers to JMP Settings](#). If you use a load balancer in front of two App Volumes Managers, enter the URL for the load balancer in the **App Volumes Server URL** text box.
7. Add a User Environment Manager File Share

1. Click the UEM tab.
2. Click Add.
8. Add the Credentials for the User Environment Manager Configuration Share

Add the information you gathered as part of Prerequisites for Adding the Other Servers to JMP Settings.

You are now ready to create a JMP assignment. If you ever need to change any of the settings you just configured in this exercise, see Managing JMP Settings.
Basic JMP Integrated Workflow
Create a JMP Assignment

In this exercise, you select the end users, instant-clone desktop pool, App Volumes AppStacks, and User Environment Manager settings to define a JMP assignment. If you have not set up App Volumes or User Environment Manager, you can still do this exercise and skip those components.

Prerequisites for Creating a JMP Assignment

Before you perform this exercise, you need:

- **User or user group** – You must have set up users and user groups in Active Directory. As part of this exercise, you will enter the first two letters of the user or group name.
- **Instant-clone desktop pool** – You must have created an instant-clone desktop pool using Horizon Administrator or the Horizon Console. For instructions, see [Creating Instant-Clone Desktop Pools](#).
- **App Volumes AppStacks** – If you plan to select applications as part of the JMP integrated workflow, you must have created AppStacks that contain the applications you want to deploy and manage. For instructions, see [Reviewer’s Guide for VMware App Volumes](#).
- **User Environment Manager settings** – If you plan to apply granular control policies as part of the JMP integrated workflow, you must have created settings in User Environment Manager. For instructions, see [Quick-Start Tutorial for User Environment Manager](#).
- **JMP server** – You must have installed the JMP server and configured JMP settings by completing the previous exercises in this quick-start guide. The following topic, [Administering JMP Assignments](#), summarizes the JMP server prerequisites.
1. Create a New JMP Assignment

1. Log in to the Horizon Console, and click Assignments.
2. Click New.

2. Type the First Letters of a User or Group Name
1. Type the first two letters of a user or group that you want to assign the desktop workspace to. The domain is already selected.
2. Select the user or group from the list of search results, and click Next.

3. Select a Desktop Pool

Select the desktop pool in the table, and click Next.
4. Select the Applications

Select one or more check boxes next to the applications you want to deploy, and click **Next**.

**Note:** If you are not using App Volumes or did not configure an App Volumes Manager server, you can click **Skip**.
5. Complete the User Environment Settings

Select one or more settings to apply, and click Next. Note which settings you select so that you will be able to verify later whether they have been applied when the user logs in to their desktop.

**Important:** With Disable UEM Settings? set to No, clicking Skip means that all the User Environment Manager settings are going to be applied to the virtual desktop workspaces in this JMP assignment. If you do not want all the settings applied, be sure to select the ones that you do want applied.
6. Name the Assignment and Schedule It

1. Use the default assignment name (as shown in the screen shot), or enter a different name.
2. Select whether to attach the AppStacks immediately or at the next login (recommended).
3. Click **Next**.
7. Submit the Assignment

Review the assignment, and click Submit.
8. Monitor Progress

Hover your pointer over the status indicator. While the new JMP assignment is queued for storage in the JMP database, the status is **Pending**. After the assignment is added to the database, the status changes to **Success**.
Summary and Next Steps
Introduction

This Quick-Start Tutorial introduced you to the JMP integrated workflow, available from the Horizon Console, and enabled you to set up a proof-of-concept environment through practical exercises.

After you have deployed your proof-of-concept implementation, you can explore the product further or plan your production environment by examining Additional Resources.
## Terminology Used in This Tutorial

The following terms are used in this tutorial.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Instant clone</td>
<td>A copy of an existing VM that shares virtual disks with the parent VM, but that, at creation time, shares the memory of the running parent VM from which it is created.</td>
</tr>
<tr>
<td>Instant-clone desktop</td>
<td>A virtual desktop run from a snapshot of a parent VM. An instant-clone desktop is always deleted and re-created when the user logs off.</td>
</tr>
<tr>
<td>Virtual desktop</td>
<td>The user interface of a virtual machine that has been made available to an end user.</td>
</tr>
<tr>
<td>Virtual machine</td>
<td>A software computer running an operating system or application environment that is backed by the physical resources of a host.</td>
</tr>
</tbody>
</table>

For more information about terms, see the [VMware Glossary](https://www.vmware.com/support/glossary.html).

To comment on this paper, contact VMware End-User-Computing Technical Marketing at [euc_tech_content_feedback@vmware.com](mailto:euc_tech_content_feedback@vmware.com).
Additional Resources

For more information about JMP features and the JMP integrated workflow, you can explore the following resources:

- JMP and VMware Horizon 7 Deployment Considerations
- Tech Zone Expert Series - Top Questions on Horizon 7 JMP Technologies (Video)
- VMware Horizon 7 v 7.5 Technical What's New Overview (Video includes a demo of the JMP workflow)
- Just-in-Time Management Platform JMP Archives - VMware Blogs
- Product documentation:
  - VMware Horizon 7 documentation
  - VMware vSphere documentation
  - VMware App Volumes documentation
  - VMware User Environment Manager documentation
- Evaluate VMware Products
- Horizon Support Center
- VMware Knowledge Base articles
- VMware Product Guide
- VMware Product Interoperability Matrices
- VMware Professional Services VMware Workspace ONE and VMware Horizon Packaging and Licensing guide
About the Author and Contributors

Caroline Arakelian is a Senior Technical Marketing Manager, End-User-Computing Technical Marketing, VMware.

The following people contributed to the review of this quick-start guide:

- Josh Spencer is an End-User-Computing Architect in the Technical Marketing group at VMware.
- Jim Yanik is a Senior Manager of End-User-Computing (EUC) Technical Marketing at VMware.

To comment on this paper, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.