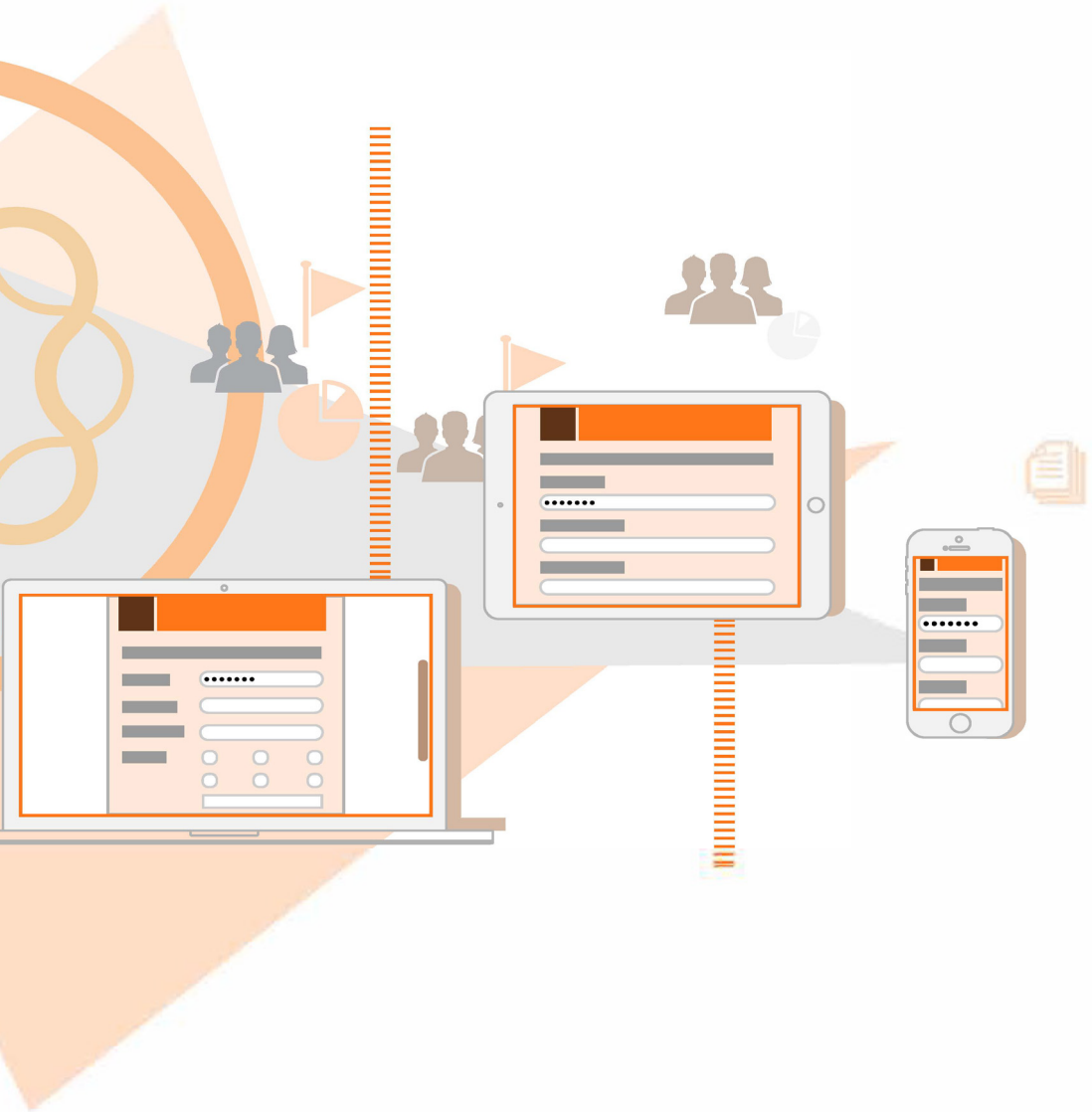
Configuring Adobe Experience Manager Forms on JEE on WebSphere Cluster



AEM 6.3 Forms

Legal notices

Contents

1. About this document

AEM Forms on JEE is an enterprise server platform that helps you automate and streamline business processes. AEM Forms on JEE comprises the following components:

- J2EE-based Foundation provides server capabilities and runtime environment
- Tools to design, develop, and test AEM Forms on JEE Applications
- Modules and Services are deployed on AEM Forms on JEE Server, and provide functional services

For more information about the AEM Forms on JEE capabilities, see Introduction to AEM Forms.

1.1. Who should read this document?

This guide provides information for administrators and developers responsible for installing, upgrading, configuring, administering, or deploying AEM forms on JEE. It is assumed that readers are familiar with J2EE application servers, operating systems, database servers, and web environments.

1.2. Conventions used in this document

The installation and configuration documentation for AEM Forms on JEE uses the following naming conventions for common file paths.

Name	Default value	Description
[aem-forms root]	Windows: C:\Adobe\Adobe_Experience_Manager_Forms Linux, and Solaris: /opt/adobe/Adobe_Experience_Manager_Forms	The installation directory that is used for all AEM Forms on JEE modules. The installation directory contains subdirectories for Configuration Manager. This directory also includes directories related to the SDK and third-party products.
[appserver root]	WebSphere on Windows: C:\Program Files\IBM\WebSphere\AppServer\ WebSphere on Linux and Solaris: /opt/IBM/WebSphere/AppServer/ WebSphere on AIX: /usr/IBM/WebSphere/AppServer	The application server directory that is used for all AEM Forms on JEE modules.
[server name]	server1	
[dbserver root]	Depends on the database type and your specification during installation.	The location where the AEM Forms on JEE database server is installed.

Name	Default value	Description
[*AEM_temp_dir*]	On Windows: C:\Adobe\Adobe_Experience_Manager_Forms\tmp On Linux: /opt/adobe/Adobe_Experience_Manager_Forms/tmp	The temporary directory for AEM Forms on JEE server.
[CRX_home]	On Windows: C:\Adobe\Adobe_Experience_Manager_Forms\crx-repository On Linux: /opt/adobe/Adobe_Experience_Manager_Forms/crx-repository	The directory that is used for installing the CRX repository.

Most of the information about directory locations in this guide is cross-platform (all filenames and paths are case-sensitive on non-Windows operating systems). Any platform-specific information is indicated as required.

1.3. Additional information

The resources in this table can help you learn more about AEM Forms on JEE.

For information about	See
AEM Forms on JEE and the modules	Introduction to AEM Forms
Preparing to Install AEM Forms on JEE	Preparing to Install AEM forms on JEE (ServerCluster)
Performing administrative tasks	Administrationhelp
All the documentation available for AEM Forms on JEE	AEM Forms on JEEdocumentation
Patch updates, technical notes, and additional information about this product version	Adobe EnterpriseSupport

2. Introduction to Installation, Configuration, and Deployment Process

2.1. Installation, configuration, and deployment overview

Installing, configuring, and deploying AEM Forms on JEE involves the following processes:

- **Installing:** Install AEM Forms on JEE by running the installation program. Installing AEM Forms on JEE places all of the required files onto your computer, within one installation directory structure. The default installation directory is C:\Adobe\Adobe_Experience_Manager_Forms (Windows) or /opt/adobe/Adobe_Experience_Manager_Forms (non-windows); however, you can install the files to a different directory.
- **Configuring:** Configuring AEM forms on JEE modifies various settings that determine how AEM Forms on JEE works. Assembling the product places all of the installed components into several deployable EAR and JAR files, according to your configuration instructions. Configure and assemble the components for deployment by running Configuration Manager. You can configure and assemble multiple AEM Forms on JEE modules at the same time.
- **Deploying:** Deploying the product involves deploying the assembled EAR files and supporting files to your application server on which you plan to run your AEM Forms on JEE. If you have configured multiple modules, the deployable components are packaged within the deployable EAR files. Components and AEM Forms on JEE archive files are packaged as JAR files. ***NOTE:*** *AEM Forms on JEE archive file use .lca file extension.*
- **Initializing the database:** Initializing the database to be used with AEM Forms on JEE creates tables for use with User Management and other components. Deploying any module that connects to the database requires you to initialize the database after the deployment process.

Before you begin to install and configure AEM Forms on JEE, ensure that you have prepared your environment as described in the applicable Preparing guides.

2.2. Selecting tasks for configuring and deploying

After you have installed AEM Forms on JEE, you can run Configuration Manager to:

- Configure modules in an EAR file for deploying to the application server or cluster of application servers
- Configure properties of the application server or cluster of application servers to support AEM Forms on JEE
- Validate application server or cluster configuration
- Deploy AEM Forms on JEE EAR files

- Initialize AEM forms on JEE database
- Deploy AEM Forms on JEE components
- Validate AEM Forms on JEE component deployment
- Configure AEM forms on JEE components

2.3. Automatic vs. manual configuration

Although you can use Configuration Manager to configure the application server or cluster and set up data sources to the database, you may prefer to complete these steps manually for the following reasons:

- You have other applications running on the application server or cluster, and are concerned about possible conflicting configurations.
- Corporate security procedures for configuration management dictate finer control.
- You are performing deployments where automatic configuration is not available.

In the manual configuration case, do these tasks:

- Use Configuration Manager to configure AEM Forms on JEE components with the required font, temp, and GDS directories
- Manually configure the application server, configure data sources, and deploy AEM Forms on JEE EAR files
- Run Configuration Manager to initialize the database
- Run Configuration Manager to deploy AEM Forms on JEE components and validate the AEM forms on JEE component deployment.
- Configure AEM forms on JEE components.

2.4. AEM Forms on JEE installation, configuration, and deployment lists

This section includes lists that you can use to step through the installation and configuration process. A list is provided for installing and configuring when using either the automatic method or the manual method.

- **Automatic method:** Refers to using Configuration Manager to configure the application server, configure and deploy AEM Forms on JEE EAR files, initialize the database, and deploy the modules to the server. Use the automatic method if you want to have limited input into the installation, configuration, and deployment of AEM Forms on JEE.
- **Manual method:** Refers to using Configuration Manager only to configure AEM Forms on JEE EAR files, initialize the database, and deploy the modules to the server. Configuring the application server, connecting to the database, and deploying AEM Forms on JEE EAR files to the server is done manually by the administrator by following the instructions later in this document. Use the manual method if you want to have precise input into the installation, configuration, and deployment of AEM Forms on JEE. For example, this method may be used in a locked-down server environment.

NOTE: In a clustering environment, all application server configurations must be performed on each node of the cluster.

Automatic installation and deployment list

The following list includes the steps that are required for installing AEM Forms on JEE modules by using the automatic method. Note that your application server or cluster must be installed before you perform the installation:

- Ensure that you have the required software installed on each machine in the target environment. See the appropriate preparing guide at http://www.adobe.com/go/learn_aemforms_documentation_63.
- Run the installation program only on one machine. (See InstallingAEMformsonJEE.)
- Run Configuration Manager and select all the tasks on the Task Selection screen. It configures the AEM Forms on JEE EAR files, configures application server settings, deploys the EAR files and other components to the application server, initializes the AEM Forms on JEE database, and verifies the deployment. (See Configuring AEM Forms on JEE for Deployment chapter in this guide.)
- Access the administration console and User Management. (See AccessingAdministrationConsole.)
- (Optional) Configure LDAP access. (See ConfiguringLDAPaccess.)
- Ensure that your clustering environment is prepared.

Manual installation and deployment list

- Ensure that you have the required software installed and configured in the target environment.
- Ensure that you created and configured the cluster in the target environment.
- Run the installation program only on one machine.
- Run Configuration Manager and select the Configure AEM Forms on JEE EARs task. This task configures AEM Forms on JEE.

  Run the manual configuration steps on the machines where AEM Forms on JEE is not installed. For example, copy content repository.
- Configure the Application Server cluster for AEM Forms on JEE.
- Deploy the EAR files to the application server. You can do this manually or use Configuration Manager. ***NOTE:*** *(**Cluster only**) Ensure that you deploy ear files to the application server on every node of the cluster. When deploying ear files to the application server, ensure that the deployment scope is Cluster .* ***NOTE:*** *(**Cluster only**) Ensure that you deploy ear files to the application server on every node of the cluster, When deploying ear files to the application server, ensure that you map modules to the Cluster and the webserver.*
- Run Configuration Manager to initialize the AEM Forms on JEE database and deploy AEM forms on JEE component files.
- Access administration console and User Management.
- (Optional) Configure LDAP access.

3. Creating a WebSphere Application Server Cluster

You must install the WebSphere Application Server Network Deployment software to create your WebSphere cluster. Perform the following tasks:

- Ensure that you properly prepared all computers in the cluster. (See Preparingtoinstall.)
- Install the WebSphere Application Server Network Deployment software. (See InstallingWebSphereNetworkDeploymentsoftware.)
- Create your WebSphere Application Server cluster. (See CreatingandconfiguringtheWebSphere-cluster.)
- Test the WebSphere Application Server cluster configuration. (See TestingtheWebSphereApplicationServercluster.)

3.1. Preparing to install

Before you install WebSphere Application Server on the computers of your cluster, ensure that your system meets the following configuration requirements:

Disk space: Ensure that the partition that will hold the application server has a minimum of 10 GB of free disk space. In addition to the space required to install the product, your environment variable `TEMP` or `TMP` must point to a valid temporary directory with at least 500 MB of free disk space. The downloadable executable requires approximately 500 MB, plus an additional 1.0 GB to unpack the images.

IP address settings: All the computers must have a fixed IP address that is managed through a single DNS.

IP multicast: All the computers must fully support IP multicast packet propagation, which means that all routers and other tunneling technologies must be configured to propagate multicast messages to clustered server instances. The network latency must be low enough to ensure that most multicast messages reach their final destination within 200 to 300 milliseconds. Also, the multicast time-to-live (TTL) value for the cluster must be high enough to ensure that routers do not discard multicast packets before they reach their final destination.

Versions: All the computers in the cluster must have the same version and same service pack of WebSphere Application Server software.

Horizontal clustering: If your configuration is horizontally clustered (that is, instances of WebSphere Application Server are installed on separate computers), ensure that all computers are on the same network subnet and that the computer clocks are synchronized. (See Preparing to InstallAEM-Forms(ServerCluster).)

Account privileges:(Windows) You must install and run WebSphere Application Server under a user account that has administrator privileges.

Shared network drive: You must have a secure shared network drive created that all computers in the cluster can access with read and write permissions. (See Preparing to InstallAEMForms(ServerCluster).)

Clocks of all the systems on the cluster might be synchronized to a common time server. In Windows domain, clock synchronization is done automatically. You must set-up Network Time Protocol on non-windows systems.

3.2. Installing WebSphere Network Deployment software

You must install WebSphere Application Server Network Deployment software on each node of the cluster to create your WebSphere Deployment Manager and application server instances.

WebSphere Deployment Manager allows you to manage your WebSphere Application Server cluster. You can install WebSphere Application Server Network Deployment on a dedicated administrative computer or on any node in the cluster that has sufficient capacity to install and run the Deployment Manager. (See WebSphere Application Server site).

Modes of installing the WebSphere Network Deployment software

You can install the WebSphere Network Deployment software in one of the following ways:

- Choose **None** on the **WebSphere Application Server Environments**screen to install the WebSphere Network Deployment Software without creating any profiles. Later, you can create a Deployment Manager or application server profile using the `manageprofiles`script. See CreatingWebSphere-profiles.
- Choose **Application server** on the **WebSphere Application Server Environments**screen to install the WebSphere Network Deployment software along with a single application server profile.
- Choose **Management** on the **WebSphere Application Server Environments** screen to install the WebSphere Network Deployment software along with the Deployment Manager profile.
- Select the **Cell (Deployment Manager and a Managed Node)** option on the **WebSphere Application Server Environments** screen to install the WebSphere Network Deployment software along with a cell that includes a Deployment Manager and a managed node application server profile.

  Selecting this option during installation saves the effort of manually creating the profiles later.

For more information about installing WebSphere Application Server software, see this WebSphere ApplicationServer site.

NOTE: While installing the WebSphere Network Deployment software on nodes where you want to host only the application server, choose the **Application server** option on the **WebSphere Application Server Environments**screen.

NOTE: You can use the `manageprofiles` script to create Deployment Manager or application server profiles any time after installing WebSphere Network Deployment software in one of the above ways.

3.3. Installing WebSphere Application Server Base software

Install and configure WebSphere Application Server Base software on each node of the cluster.

You can also consider the following special cases if they apply to your topology:

- If you employ horizontal clustering and your topology has a managed WebSphere Application Server on the same node where you installed WebSphere Deployment Manager, you do not need to install the WebSphere Base software on that node.

  NOTE: While installing the WebSphere Base software on the other nodes, choose the **Application server** option on the **WebSphere Application Server Environments** screen.
- For information about the service releases, see Java SDK 1.5 SR8 Cumulative Fix for WebSphere Application Server or Java SDK 1.6 SR5 Cumulative Fix for WebSphere Application Server.

3.4. Creating and configuring the WebSphere cluster

Configure your WebSphere Application Server cluster by performing the following tasks:

- Create WebSphere Deployment Manager and WebSphere Application Server profiles. (See CreatingWebSphereprofiles.)
- Federate the nodes to the Deployment Manager. (See FederatingWebSphereApplicationServerprofiles.)
- Create the cluster. (See CreatingtheWebSpherecluster.)
- Modify the SOAP connection time-out. (See ModifyingtheSOAPconnectiontime-outsettings.)

Creating profiles creates empty nodes that do not contain an administrative console or server. After federating these nodes, use the Deployment Manager to create a cluster of servers that use these nodes.

Creating WebSphere profiles

Once you have installed WebSphere Network Deployment software in one of the ways listed in ModesofinstallingtheWebSphereNetworkDeploymentsoftware, you can create different type of WebSphere profiles. Create WebSphere profiles for your WebSphere Deployment Manager and for your WebSphere Application Server instances.

If you selected the **Cell (Deployment Manager and a Managed Node)** option (on the WebSphere Application Server environments screen) when you installed WebSphere Application Server Network Deployment software, the Deployment Manager and managed application server profiles were created automatically for you.

Creating WebSphere profiles for 64-bit WebSphere Application Server

Use the WebSphere `manageprofiles` script (`manageprofiles.bat` on Windows and `manageprofiles.sh` on Linux or UNIX) to create profiles on a 64-bit WebSphere Application Server.

Create a Deployment Manager profile on the node that you selected to host the WebSphere Deployment Manager. This profile contains the WebSphere Administrative Console and also hosts the cell to which the nodes of your cluster will be federated.

You must also create profiles for each of the WebSphere Application Server instances that will comprise your cluster.

(Only for JDK 7) Configure WebSphere and WebSphere profile to use JDK 1.7

If you are using JDK 7, before creating a profile, perform the following steps to ensure that WebSphere server and newly created profile uses JDK 1.7. If you are using JDK 8, this procedure is not required:

Execute the following commands from the <*WAS_HOME*>\AppServer\bin directory:

1) List available SDKs:

   managesdk -listAvailable

2) Change the default SDK to SDK 7.0:

   managesdk -setCommandDefault -sdkname 1.7_64

3) Set the New Profile to use SDK 7.0:

   managesdk -setNewProfileDefault -sdkname 1.7_64

If you have already created a profile, only then run the commands listed below:

```
managesdk -listAvailable [-verbose]
managesdk -listEnabledProfile -profileName AppSrv01 [-verbose]
managesdk -listEnabledProfileAll [-verbose]
managesdk -enableProfile -profileName AppSrv01 -sdkname 1.7_64
-enableServers
managesdk -enableProfileAll -sdkname 1.7_64 -enableServers
managesdk -getNewProfileDefault [-verbose]
managesdk -setNewProfileDefault -sdkname 1.7_64
managesdk -getCommandDefault [-verbose]
managesdk -setCommandDefault -sdkname 1.7_64
```

To create a WebSphere profile with the manageprofiles script:

1) On the computer that you will create the profile for, open a command prompt and navigate to the *[appserver root]*/bin/ directory.
2) Start the WebSphere Profile Management Tool by entering the following command:
   – (Windows) `manageprofiles.bat`
   – (Linux/UNIX) `./manageprofiles.sh`
3) Type a command with the appropriate options to create a profile with the `manageprofiles` script. For example, type the following text:
   – (Windows):

     [appserver root]\bin>manageprofiles.bat -create -templatePath "*[appserver root]*\profileTemplates\default" -profileName DS_AppSrv01 -profilePath "*[appserver root]*\profiles\DS_AppSrv01" -isDefault

   – (Linux/UNIX):

     [appserver root]/bin>./manageprofiles.sh -create -templatePath "*[appserver root]*/profileTemplates/default" -profileName DS_AppSrv01 -profilePath "*[appserver root]*/profiles/DS_AppSrv01" -isDefault

     Creating Deployment Manager Profile

```
[appserver root]\bin>manageprofiles.bat -create -profileName
LC_Dmgr01 -profilePath "[appserver root]\profiles\LC_Dmgr01"
-templatePath "[appserver root]\profileTemplates\management"
```

Creating Managed Node Profile

```
[appserver root]\bin>manageprofiles.bat -create -profileName
LC_AppSrv01 -profilePath "[appserver root]\profiles\LC_AppSrv01"
-templatePath "[appserver root]\profileTemplates\managed"
```

NOTE: Above mentioned commands are using minimum parameters required to create a profile. Addiionaly, you can specify the `nodename`, `cellname`, and `hostname`*by setting the following arguments:*

```
-nodeName
-cellName
-hostName
```

For more information about parameters that you can use with this command, refer to this articlehttp://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.express.iseries.doc/info/iseriesexp/ae/rxml_manageprofiles.html in the WebSphere Application Server documentation.

NOTE: You can view a list of the allowable options for the `manageprofiles` script by typing `manageprofiles.sh help create`—*from a command line. You should typically specify the following options:*

- The template path, which is the path where profile templates reside. The profile path is usually *[appserver root]*/profileTemplates. `default`, `cell`, `dmgr`, `managed`, `management`, and`secureproxy` are examples of profile templates.
- The profile path. For more information about the profile path, see Conventionsusedinthis document.
- The profile name. Specify a profile name that readily identifies the WebSphere Application Server that the profile applies to (for example, include the identifier DS for AEM Forms).
- If the profile is the default profile for the WebSphere Application Server. The `-isDefault` option specifies that the profile is the default profile. On a cluster that uses Network Deployment, the `dmgr01` profile typically exists as the default profile.

  NOTE: Depending on the option that you select on the **WebSphere Application Server Environments** screen, you may need to execute `managedprofiles.bat` or`managedprofiles.sh` after installation for creating profiles. For example, if you select **None** on the **WebSphere Application Server Environments**screen, you need to execute the appropriate command twice—once for the Deployment Manager and then for the application server node.

Configuring WebSphere Application Server if global security is enabled

If your installation uses global security, you must run WebSphere Application Server as a user with the appropriate roles. You can employ one of the following options to configure WebSphere Application Server to run if WebSphere global security is enabled:

- Create a new user with the necessary roles, and run WebSphere Application Server as that user. If a user already exists to run WebSphere Application Server, assign the necessary roles to that user.

  IMPORTANT: *Ensure that you start WebSphere Application Server as this user. Some WebSphere processes may fail if you start WebSphere Application Server as a different user while global security is enabled.*

  In a secure environment, it is recommended that you employ this option.
- Configure the EVERYONE group with the necessary roles.

To create a new WebSphere Application Server user:

1) In the WebSphere Administrative Console navigation tree, click **Environment** > **Naming** > **CORBA Naming Service Users**, and then in the right pane, click **Add**.
2) In **Roles**, select all the roles.
3) Under Search and Select Users, select the User Realm.
4) In the search box, type the search string and click **Search**. ***NOTE:*** *To retrieve all users, type an asterisk (*).*
5) From the Available text box, select the required users and click the right arrow to add them to the Mapped to role box.
6) Click **Save directly to master configuration**.

To configure an existing WebSphere Application Server user:

1) In the WebSphere Administrative Console navigation tree, click **Environment** > **Naming**> **CORBA Naming Service Users**, and then in the right pane, select the user.
2) In **Roles**, select the required roles.
3) Click **OK**or **Apply**.
4) Click **Save directly to master configuration**.

To configure the EVERYONE group

1) In the WebSphere Administrative Console navigation tree, click **Environment** > **Naming** > **CORBA Naming Service Groups**.
2) In **Roles**, select the required roles.
3) Enable **Select from special subjects**, and then from the Special subjects list, select the **EVERYONE** group.

NOTE: If the EVERYONE group is already configured, the group will not be shown in the Special subjects list. You only need to assign the required roles to this group if not already done so.

1) Click **OK**or **Apply**.
2) Click **Save directly to master configuration**.

Configure CSIv2 inbound transport

On the default Global Security enabled installation of IBM WebSphere, CSIv2 inbound transport option is set to SSL-required. This configuration causes Output and Forms components to fail. Ensure that you change CSIv2 inbound transport option to SSL-Supported: To change the option:

1) Log in to IBM WebSphere administration console.
2) Expand **Security**, and then click **Global security**.
3) In the Authentication section, expand **RMI/IIOP security**, and then click **CSIv2 inbound communications**.
4) In CSIv2 Transport Layer section, set value of **Transport** to **SSL-Supported**.
5) Click **Apply**.

NOTE: After enabling global security and configuring appropriate roles for Application server, additional configurations are required to enable OSGi functionality built within the JEE stack. These configurations are performed after installing and configuring AEM Forms on JEE on WebSphere application server. For detailed steps, see Enable Websphere Global Administrative Security.

Federating WebSphere Application Server profiles

You must now federate individual servers by adding the profiles that you created for each WebSphere Application Server instance into the Deployment Manager profile. (See Addingprofiles.)

You can also remove a WebSphere Application Server instance from an existing WebSphere cell by removing its profile from the Deployment Manager profile. (See Removinganddeletingprofiles.)

Adding profiles

Before you add WebSphere Application Server profiles, ensure that the Deployment Manager is running. Also ensure that you can connect to the Deployment Manager from the WebSphere Application Server instance by using the name of the Deployment Manager as well as the IP address.

IMPORTANT: Before you add WebSphere Application Server profiles, ensure that the system clocks of all WebSphere Application Server instances are synchronized.

To add a custom profile to the Deployment Manager:

1) If the Deployment Manager is not running, navigate to the bin directory of the Deployment Manager Profile and run the appropriate script:
   - (Windows) `startManager.bat`
   - (Linux, UNIX) `./startManager.sh`

   *If you installed WebSphere Application Server using the **Cell (deployment manager and a managed node)** option, navigate to the directory [appserver root]/profiles/<profile_name>/bin and start the node agent by running the appropriate command:*
   - (Windows) `startNode.bat`
   - (Linux, UNIX) `./startNode.sh`

NOTE: You do not need to execute `startNode.bat` or `startNode.sh` for the application server node profile unless the node is added to the cell . After this node is added to the cell, you can start the node by executing the appropriate `startNode` command. For information on adding nodes to a cell, refer to step 3. Run`startNode.bat`or `startNode.sh` only for the managed node installed with the Deployment Manager.

2) From a command prompt, navigate to the*[profiles root]/<profile name>*/bin directory of the WebSphere Application Server instance you want to add.

3) Run the `addNode` script by using the computer name as a parameter; for example, type this text:
   – (Windows) `addNode.bat [dmgr_host] [dmgr_port]`
   – (UNIX/Linux) `./addNode.sh [dmgr_host] [dmgr_port]`

   NOTE: The `dmgr_host` argument is required. All of the other arguments are optional. The default port number is 8879 for the default SOAP port of the deployment manager. For more information, see this articlehttp://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.iseries.doc/info/iseriesnd/ae/rxml_addnode.html*in the WebSphere Application Server documentation.*

   In addition to federating the node to the cell, `addNode` also starts the node agent process. After the node is federated to a cell, the node agent is started with the `startNode` command, which is also located in the bin directory of the WebSphere Application Server profile. During this process, the node being federated communicates to the Deployment Manager by using port 8879 by default.

   It is a good practice to add the node agent as an operating system daemon process in UNIX. You can add the node agent as a service in Windows by using `WASService`, which is available in the bin directory of the base application server installation.

Removing and deleting profiles

You can remove a WebSphere Application Server profile from the cell by removing its profile from the WebSphere Deployment Manager. You can execute this task by using either a pair of script files or the Deployment Manager Administrative Console.

NOTE: Removing a profile from the cell only removes the server from the cluster; it does not delete the profile. The profile remains (and can be added back to the cell later, if needed). To completely remove a profile, delete the profile as a separate task.

You can delete profiles that you no longer need on your Deployment Manager and servers.

To remove a WebSphere Application Server using script files:

1) If the Deployment Manager is not running, navigate to the bin directory of the Deployment Manager Profile and run the appropriate script:
   – (Windows) `startManager.bat`
   – (Linux, UNIX) `./startManager.sh`

2) On each WebSphere Application Server that you want to remove, navigate to the bin directory of the profile that is running the node agent and run the appropriate `removeNode` script:
   – (Windows) `removeNode.bat`

– (Linux, UNIX) `./removeNode.sh`

3) Navigate to the bin directory of the Deployment Manager profile and run the appropriate `cleanup` script:
   – (Windows) `cleanupNode.bat <node name> [deploymgr host] [deploymgr port] [options]`
   – (Linux, UNIX) `./cleanupNode.sh <node name> [deploymgr host] [deploymgr port] [options]`

   For more information, refer to this articlein the WebSphere Application Server documentation.

To remove a WebSphere Application Server using the Deployment Manager:

1) Verify that the Deployment Manager is running.
2) In a web browser, type the URL to the Deployment Manager; for example, type `http://<servername>:<port>/ibm/console`

   NOTE: By default, the Deployment Manager Administrative Console web application listens on port 9060.
3) In the left pane, select **System Administration**and click **Nodes**.
4) Select the node to remove and click **Remove Node**.
5) To verify that the node is removed, navigate to **System Administration** > **Nodes** and confirm that the node is not listed.

To delete a profile:

1) Open a command prompt and navigate to the *[appserver root]*/bin directory.
2) Run the following command from the console:
   – (Windows) `manageprofiles.bat -delete -profileName`*[profileName]*
   – (UNIX/Linux) ./`manageprofiles.sh -delete -profileName`*[profileName]*

   NOTE: The profile directory and log files are not deleted. You must manually delete the profile directory. Any attempt to create a profile by using the same name as the deleted profile without first deleting the directory causes an error.

Creating the WebSphere cluster

You must now create the WebSphere cluster by perform the following tasks:

- Creating the cluster by using the Deployment Manager.
- Configuring the distributed environment settings for the cluster.
- Add ports and host aliases for WebSphere Application Server instances of the cluster.

By default, the WebSphere Administrative Console web application listens on port 9060.

To create a cluster using the Deployment Manager:

1) Log in to the WebSphere Administrative Console of the computer hosting Deployment Manager.
2) In a web browser, enter the URL to the Deployment Manager; for example, type `http://<servername>:<port>/ibm/console`

   NOTE: By default, the Deployment Manager Administrative Console web application listens on port 9060.
3) In the WebSphere Administrative Console navigation tree, click**Servers > Clusters > WebSphere application server clusters**, and then click **New**.
4) In the **Enter Basic Cluster Information** box, enter the name of the cluster; for example, type `ds_cluster`.
5) In the **Member name** box in the right pane, enter a member name. This name is for the first in the cluster.
6) In the **Select Node** list, select the node that this cluster member will reside on.
7) Select **Create the member using an application server template**, select **default** from the list, and then click **Next**.
8) In the **Member Name** box, enter the name of another member to add to the cluster.
9) In the **Select Node** list, select the node that this cluster member will reside on.
10) Select **Generate unique HTTP ports** and click **Add Member**.
11) Repeat steps 8 to 11 to add WebSphere Application Servers to the cluster, entering the new member name.
12) After you add all members, click **Next**.
13) Click **Finish** and then click **Save**.
14) Click **System Administration** > **Save Changes to Master Repository**, select **Synchronize changes with Nodes**, and then click **Save**.

To configure distributed environment settings for the cluster:

1) In the WebSphere Administrative Console navigation tree, click **System administration**>**Nodes**, and ensure that the nodes are listed, that their status is **Synchronized**, and that all WebSphere Application Server instances of the cluster are started.
2) Click **Servers > Server Types > WebSphere application servers** and, in the right pane, click the server name.
3) Click the **Configuration** tab and, under **Container Settings**, click**Session management**.
4) Under Additional Properties, click **Distributed environment settings**.
5) Under General Properties, click **None**and then **OK.**
6) Click **Save directly to the master configuration.**
7) On the next screen, under Additional Properties, click **Distributed Environment Settings**and Click **custom tuning parameters.**
8) Select **Low (optimize for failover)** and then click **OK**.
9) In the navigation tree, click **Servers**>**Application servers**and, in the right pane, click the server name.

10) Under Performance, select **Performance Monitoring Infrastructure (PMI)**.
11) On the next screen, select **Enable Performance Monitoring Infrastructure (PMI)**.
12) Under Currently Monitored Statistics Set, select **Basic** and then click **OK**.
13) Repeat steps 2 to 13 for each server in your cluster.
14) In the **Messages** box, click **Save directly to the master configuration**.

To configure WebSphere Application Server ports and aliases:

1) In a web browser, type the URL to the Deployment Manager; for example, type `http://<servername>:<port>/ibm/console`
   NOTE: By default, the WebSphere Administrative Console listens on port 9060.
2) In the navigation tree, click **Servers**>**Application servers**and, in the right pane, click the server name.
3) On the next screen, under Communications, click **Ports**.
4) In the table, click **WC_defaulthost** and assign a port address. ***NOTE:*** *For horizontal clusters, each server can have unique or identical address.*
5) Repeat steps 2 to 4 for each server in the cluster.
6) Click **Save directly to the master configuration**.
7) In the navigation tree, click **Environment**>**Virtual Hosts**and, in the right pane, click **default_host**.
8) Under Additional Properties, click **Host Aliases**.
9) On the next screen, click **New** and add the port you assigned for a server in the cluster.
10) In the **Host Name** box, enter an asterisk (*).
11) Repeat step 9 and 10 for each port that is assigned in step 4.
12) Click **OK** and then click **Save directly to master configuration**.
13) Restart the server. Click **Servers > Server Types > WebSphere application servers**, select the check box beside the server name, and then click **Restart**.

Modifying the SOAP connection time-out settings

Modify the SOAP connection time-out settings for each WebSphere Application Server in the cluster and for Deployment Manager.

To modify SOAP connection time-out settings

1) Log in to the WebSphere Administrative Console and, in the navigation tree, click **Servers > Cluster > WebSphere application server clusters.**
2) In the right pane, stop all clusters.
3) Navigate to *[appserver root]*\profiles\<profile name>\properties and open the soap.client.props file in a text editor.
4) Configure the `com.ibm.SOAP.requestTimeout` property to `1800`.
5) Save the edited file.
6) Repeat steps 3 to 5 for each application server and Deployment Manager in the cluster.

7) Restart the deployment manager, node management and cluster.

Adding a new node to an existing cluster

Do the following to add a new node to a cluster:

1) Install WebSphere Network Deployment software. See InstallingWebSphereNetworkDeployment-software for details.
2) If you have not selected application server option while installing WebSphere Network Deployment software, then create a WebSphere profile now. See CreatingWebSphereprofiles for details.
3) Install Fix Packs and Feature Packs. See Supported Platform Combinations
4) Configure time-out settings. See ModifyingtheSOAPconnectiontime-outsettings
5) Federate the profile you created. See FederatingWebSphereApplicationServerprofiles for details.
6) Add New Node to the Cluster
   - Click **Servers > Clusters > WebSphere application server clusters**.
   - In the right pane, click the name of the cluster to which you want to add a node.
   - Click **Additional Properties > Cluster members** in the right pane.
   - Click **New.**
   - On the **Create additional cluster members** screen, specify a name for the new member and then select the node that you want to add to the cluster.
   - Click **Add Member** and then click **Next**.
   - Review the summary screen and click **Finish.**
   - Click **Save directly to the master configuration**.
7) Before starting new node, ensure that:
   - All required software are installed and environment variables are created.
   - Temporary directory location is available for new node.
   - GDS(shared) location is available for new node.
   - Adobe Fonts, customer font and system font directories are available for new node.
   - PDFG configurations are complete. See ConfiguringPDFGenerator for details.
   - Custom properties, JVM arguments and heap arguments are configured for the new node. You may copy these settings from existing nodes.
   - Database jar file is available on new node at the same location as on exisiting nodes. You should not create Data Source for the new node, it is already available for the cluster.
   -
8) Start new node.

   NOTE: Ensure that all the directories (local and shared) are available on the new node at the same location as on existing nodes.

3.5. Testing the WebSphere Application Server cluster

You can test the WebSphere Application Server cluster to ensure that all members are active and that the cluster operates according to your design. You should ensure that the WebSphere Application Server cluster functions correctly before you proceed to install and configure AEM Forms.

To test the WebSphere Application Server cluster:

1) Ensure that all WebSphere Application Server instances of the cluster are started.
2) View the server.log file located in *[appserver root]*/profiles/*[profile name]*/logs/*[application server name]*/SystemOut.log. Messages such as the following one confirm the active members of the cluster:

```
[1/22/08 13:50:09:643 PDT] 00000018 PtpConnectedC I DCSV1031I: DCS Stack
DefaultCoreGroup.lc9_cluster at Member LCcell\Node01\Node01Server1:
Received a connection from an undefined member LCcell\Node02\
Node02Server1. Source address is /11.11.11.11.
[1/22/08 13:50:09:696 PDT] 0000001f RoleMember I DCSV8051I: DCS Stack
DefaultCoreGroup.lc9_cluster at Member LCcell\Node01\Node01Server1: Core
group membership set changed. Added: [LCcell\Node02\Node02Server1].
[1/22/08 13:50:09:704 PDT] 0000001d RecoveryDirec I CWRLS0012I: All
persistent services have been directed to perform recovery processing for
this WebSphere server (LCcell\Node01\Node01Server1).
[1/22/08 13:50:09:712 PDT] 00000018 MbuRmmAdapter I DCSV1032I: DCS Stack
DefaultCoreGroup.lc9_cluster at Member LCcell\Node01\Node01Server1:
Connected a defined member LCcell\Node02\Node02Server1.
[1/22/08 13:50:09:839 PDT] 00000020 RecoveryManag A WTRN0028I:
Transaction service recovering 0 transactions.
[1/22/08 13:50:26:744 PDT] 0000001f RoleMergeLead I DCSV8054I: DCS Stack
DefaultCoreGroup.lc9_cluster at Member LCcell\Node01\Node01Server1: View
change in process.
[1/22/08 13:50:26:764 PDT] 00000018 VSyncAlgo1 I DCSV2004I: DCS Stack
DefaultCoreGroup.lc9_cluster at Member LCcell\Node01\Node01Server1: View
synchronization completed successfully. The View Identifier is
(1:0.LCcell\Node01\Node01Server1). The internal details are None.
```

3.6. Next steps

You must now install the AEM Forms solution component files. (See InstallingAEMForms.)

4. Installing AEM Forms modules

4.1. Before you begin

Checking the installer

Observe the following best practices with the installer files before you begin the installation process.

Check the downloaded files

If you downloaded the installer from the Adobe website, verify the integrity of the installer file using the MD5 checksum. Do one of the following to calculate and compare the MD5 checksum of the downloaded file with the checksum published on the Adobe licensing website:

- **Linux:** Use the `md5sum` command
- **Solaris:** Use the `digest` command
- **Windows:** Use a tool such as WinMD5
- **AIX:** Use the `md5sum` command

Expand the downloaded archive files

If you downloaded the ESD from the Adobe website, extract the entire aemforms_server_6_3_0_websphere_all_win.zip (Windows) or aemforms_server_6_3_0_websphere_all_unix.tar.gz (AIX, Linux, or Solaris) archive file to your computer. For non-Windows, use the `gunzip` command to extract the .gz file.

NOTE: Be sure to keep the directory hierarchy unchanged from the original ESD file.

4.2. Installation considerations

Installation paths

To successfully install, you need read, write, and execute permissions on the installation directory. The following also apply to the installation paths:

- When installing AEM Forms on JEE, do not use double-byte or extended Latin characters (such as àâçéèêëîïôùûÄÖßÜ) in the installation path.

- On Windows, the AEM Forms on JEE installation directory path must not contain any non-ASCII characters (for example, international characters such as é or ñ).
- On UNIX-based systems, you must be logged in as the root user to successfully install the modules. If you are logged in as a non-root user, change the installation directory to one on which you have permissions (read-write-execute privileges).
- On Windows, you must have administrator privileges to install AEM Forms on JEE.
- When you run the AEM Forms on JEE installer, you should run it as the same user that installed WebSphere Application Server.

Temporary directories

Temporary files are generated in the temp directory. In certain instances, the generated temporary files may remain after the installer is closed. You can remove these files manually.

When installing on Linux, the installation program uses the logged-in user's home directory as a temporary directory for storing files. As a result, messages such as the following may appear in the console:

```
WARNING: could not delete temporary file /home/<username>/ismp001/1556006
```

When you complete the installation, you must manually delete the temporary files from the following directories:

- (Windows) TMP or TEMP path as set in the environment variables
- (AIX, Linux, or Solaris) Logged-in user’s home directory

On UNIX-based systems, a non-root user can use the following directory as the temporary directory:

- (Linux) /var/tmp or /usr/tmp
- (AIX) /tmp or /usr/tmp
- (Solaris) /var/tmp or /usr/tmp

Installing on a Windows staging platform for Linux or UNIX

AEM Forms on JEE can be installed and configured on Windows for deployment on a Linux or UNIX platform. You can use this functionality for installing on a locked-down Linux or UNIX environment. A locked-down environment does not have a graphical user interface installed. For the Linux or UNIX platform, the installation program installs binaries that are used by Configuration Manager to configure the product.

The computer running Windows can then be used as a staging location for the deployable objects, which can be copied to a Linux or UNIX computer for deployment to the application server. The application server on the Windows-based computer, and the Linux or UNIX target computer on which you want to install AEM forms on JEE must be the same.

General installation notes

- On Windows, improve the speed of installation by disabling any on-access virus scanning software during installation. For details, see Using an antivirus on server running AEMForms.

- If you are installing on UNIX-based systems and are not installing directly from a release DVD, set executable permissions on the installation file.
- To avoid permission issues during deployment, ensure that you run the AEM Forms on JEE installer and Configuration Manager as the same user who will run the application server.
- If you are installing on UNIX-based computers, the installation directory you specify should not contain any spaces.
- Ensure that the JAVA_HOME environment variable points to *[appserver root]*/java/.
- When configuring WebSphere on Windows, make sure that Configuration Manager is running using the appropriate JDK. WebSphere installations typically use the IBM JDK. If WebSphere is not using the IBM JDK, re-launch Configuration Manager using the *[aem-forms root]*/configurationManager/bin/ConfigurationManager.bat script.
- If errors occur during installation, the installation program creates the install.log file, which contains the error messages. This log file is created in the *[aem-forms root]*/log directory.

4.3. Installing AEM Forms on JEE

1) Start the installation program:
   - (Windows) Navigate to the \server\Disk1\InstData\Windows_64\VM directory on the installation media or folder on your hard disk where you copied the installer. Right-click the `install.exe` file and select Run as administrator.
   - (Non-Windows) Navigate to the appropriate directory, and from a command prompt, type `./install.bin`.
     - (AIX) /server/Disk1/InstData/AIX/NoVM
     - (Linux) /server/Disk1/InstData/Linux/NoVM
     - (Solaris) /server/Disk1/InstData/Solaris/NoVM
2) When prompted, select the language for the installation to use and click **OK**.
3) On the Introduction screen, click **Next**.
4) On the Choose Install Folder screen, accept the default directory or click **Choose** and navigate to the directory where you intend to install AEM Forms on JEE, and then click **Next**. If you type the name of a directory that does not exist, it is created for you.

   Click Restore Default Folder to restore the default directory path.
5) **(Windows only)** On the Manual Installation Options screen, select the target deployment option and click **Next**:
   - **Windows (Local):** Select this option if you are installing and deploying AEM Forms on JEE on the local server.
   - **Staged (Installed on Windows, targeting remote systems):** Select this option if you plan to use Windows as a staging platform for your deployment and then select the target operating system on the remote server. You can select a UNIX operating system as the target for deployment even if you are installing on Windows. (See *Installing on a Windows staging platform for Linux or UNIX*.)

6) Read the AEM Forms on JEE License Agreement, select **I accept** to accept the terms of the license agreement, and then click **Next**. If you do not accept the license agreement, you cannot continue.
7) On the Pre-Installation Summary screen, review the details and click **Install**. The installation program displays the progress of the installation.
8) Review the Release Notes information and click **Next**.
9) Review the details on the Install Complete screen.
10) The **Start Configuration Manager** checkbox is selected by default. Click **Done** to run the Configuration Manager.

    NOTE: (PDF Generator for Windows only) If Acrobat is not installed on all nodes in the cluster, install it now. Then complete the steps in Configuring PDF Generator listed in the post-deployment section.

4.4. Configuring the caching locators in clusters (caching using TCP only)

If you implement caching for your AEM Forms cluster by using TCP, configure the TCP locators to find other members of the AEM Forms cluster.

NOTE: This section does not apply if you implement caching for your AEM Forms cluster by using UDP. (See ModifyingtheJVMpropertiesto configure caching for your AEM Forms cluster using UDP.)

Do the following to enable AEM Forms cluster caching using TCP:

- Ensure that the TCP locators are installed and configured. TCP locators are installed in the *[aem_forms root]*/lib/caching directory, with a default configuration, when you install AEM Forms. You can change the default configuration. (See ModifyingtheTCPlocators.)
- Configure each node in the AEM Forms cluster to use the locators. (See ModifyingtheJVMproperties.)
- Ensure that TCP locators are running.

Modifying TCP locators

The AEM Forms installer creates a default configuration of the TCP locators that is ready to use without modification. You can move the locators to any computer on your network and run them on that computer. The locators do not have to reside on a computer that is a member of the AEM Forms cluster. You can also create additional failover locators to support high availability in your cluster. (See InstallTCPlocators)

You can also modify the TCP locators to use a port other than the default port (22345). (See Modifythedefaultlocatorport(Windows): or Modifythedefaultlocatorport(UNIX):.)

Install TCP locators

1) Log on to the computer where you installed AEM Forms and navigate to the [aem_-forms]\lib\caching\bin caching directory.
2) Copy the caching directory and its contents to the computer on which you want to run the locators.

   You can start TCP locator from default location. You should copy the caching directory to another location, only if:

   – You want to run TCP locator on a machine that does not have AEM Forms.
   – You do not want to start TCP locator from default location.

   ***NOTE:** Do not run TCP locators on all the nodes of the AEM Forms Cluster. It is good practice to run minimum two locators. One TCP locator serves as a primary locator and other TCP locator serves as a secondary locator to handle failover issues. You can add more than two TCP locators as backup locators but it is not mandatory.*

Modify the default locator port (Windows)

1) Open the startlocator.bat file in a text editor. The *startlocator* file for a default installation is on the computer where you installed AEM Forms, in the *[aem_forms root]*/lib/caching directory.
2) Change the default port number (22345) to your preferred port number in the following properties:

   `set port=22345`

   The port number can be any available port between 1025 and 65535. ***NOTE:** Ensure that the port number that is configured here matches the port number that is configured in the JVM argument of each node of the AEM Forms cluster.The port number can be any available port between 1025 and 65535.*
3) If you are using more than one locator for failover, assign all of such locators to JVM argument `-Dlocators` listed at the end of the startlocator.bat file.

   `-Dlocators=localhost[22345]`
4) (Computers with multiple network cards only) If the computer hosting the locator has multiple network cards, set the following properties in the script:

   `set bindaddr=<bind IP address>`

   Where `<bind IP address>` is the IP address that the locator will listen on. You must specify the `<bind IP address>` for the JVM argument `adobe.cache.cluster-locators` on each node in your AEM Forms cluster.

   NOTE: If you do not specify the bind address and the bind port in the `startlocator` script, you will be prompted to input these values when you execute the script. However, for IPv6, you must specify the bind address and the bind port in the `startlocator` *script itself.*
5) Save the edited file.
6) Repeat steps 1 to 4 on any additional locators for your AEM Forms cluster.

Create the properties file

1) Create a GemFire.properties file.
2) Pass the parameters required in the GemFire.properties file:
   – name=`TCPLocator1`
   – locators=`10.131.96.64[22345],10.131.96.217[22345]`
3) Pass the file using the `-DgemfirePropertyFile` by starting the locator as following:

```
java -cp .\gemfire.jar com.gemstone.gemfire.internal.SystemAdmin
start-locator -port=%port% -address=%bindaddr%
-DgemfirePropertyFile=gemfire.properties -Djava.io.tmpdir=%TEMPDIR%
-Dgemfire.log-file=GFLocator.log -Dgemfire.license-type=production
-Dgemfire.license-file=gemfireLicense.zip
```

RELATED LINKS:

Modify the default locator port (UNIX)

1) Open the startlocator.sh file in a text editor. The *startlocator* file for a default installation is located on the computer where you installed AEM Forms, in the *[aem_forms root]*/lib/caching directory.
2) Change the default port number (22345) to your preferred port number in the following properties:

   `GF_PORT=22345`

   The port number can be any available port between 1025 and 65535.

   IMPORTANT: Ensure that the port number that is configured here matches the port number that is configured in the JVM argument of each node of the AEM Forms cluster.
3) If you are using more than one locator for failover, assign all of such locators to JVM argument `-Dlocators` listed at the end of the startlocator.sh file.

   `-Dlocators=localhost[22345]`
4) (*Computers with multiple network cards only*) If the computer hosting the locators has multiple network cards, modify the following argument:

   `GF_BIND_ADDRESS="<bind IP address>"`

   Where `<bind IP address>` is the IP address that the locator will listen on. You must specify the `<bind IP address>` for the JVM argument `adobe.cache.cluster-locators` on each node in your AEM Forms cluster.

   NOTE: For IPv6, it is recommended that you specify the bind address and the bind port in the `startlocator` *script itself.*
5) Save the edited file.
6) Repeat steps on any additional locators for your AEM Forms cluster.

Start the TCP locators

To use TCP-based caching for AEM Forms Cluster using TCP locator, you must start the TCP locators before you start your cluster. If the TCP locators are not running when you start the members of the AEM Forms cluster, the AEM Forms cluster will not function.

1) On the computer where the TCP locators are installed, navigate to the caching directory. For a default installation, the TCP locators are installed on the computer where you installed AEM Forms, in the [aem_forms]\lib\caching\bin\ directory.
2) *(IPv6 only)* Modify `gfsh.bat`(Windows) or `gfsh.sh`(UNIX) and add the following JVM arguments:

   ```
   -Djava.net.preferIPv6Stack=true
   -Djava.net.preferIPv6Addresses=true
   ```
3) Run the appropriate file:
   - (Windows) `gfsh.bat`
   - (UNIX) `gfsh.sh.sh`
4) Run the following command:

   start locator --name=<locator name> --port=<port number>

   NOTE: It is recommended to start the locator process as a background process. For example, in UNIX use the `nphup` command to start the background locator process: `nohup ./gfsh.sh start locator -name=<locator_name> -port=<port_number> &`
5) Repeat above steps on any additional locators for your AEM Forms cluster.

NOTE: (Windows Only)On running startlocator script, you would be prompted to change the default value. You can choose to keep the default values provided in the script or you can provide new values.

Stop TCP locators

1) On the computer where the TCP locators are installed, navigate to the caching directory. For a default installation, the TCP locators are installed on the computer where you installed AEM Forms, in the [aem_forms]\lib\caching\bin directory.
2) Run the following command:

   stop locator --name=<locator name>
3) Repeat steps 1to 2 on any additional locators for your AEM Forms cluster.

NOTE: If you are not using the default values in the `startlocator` script and mentioned specific IP address and port values, specify the same values in the `stoplocator` script. Otherwise, the `stoplocator` script may fail to stop the locators.

Install gfsh tcp locator as windows service

To install TCP locator as windows service, complete the following steps:

1) Download YAJSW from http://sourceforge.net/projects/yajsw/files/
2) Unpack the zip file to a folder: **yajsw**.

   NOTE: Do not remove or copy files from this folder to any another folder. Do not rename any folders within **yajsw**.
3) Call java -version and ensure that your default java installation is 1.5 or higher.
4) Run the following command:

   start locator --name=<locator name> --port=<port number>
5) Check the process id of the TCP Locator Java process. We need the pid of the Java process not of the batch file which started TCP Locator.
6) Go to yajsw/bat and execute genConfig.bat <pid>.

   This generates the file yajsw/conf/wrapper.conf which is the configuration file for wrapping TCP Locator.
7) Create a file gemfire.properties. Add the following parameter to the file.
8) `locators= [host][[port]]`

   The parameter specifies hostname and port of the second locator. For example, *locators=10.42.86.25[22345]*
9) Open conf/wrapper.conf with a text editor and make the following changes.
   - wrapper.ntservice.name=TCPLocatorServiceForLiveCycle
   - wrapper.ntservice.displayname=TCP Locator Service For LiveCycle
   - wrapper.ntservice.description=Starts TCP Locator
   - wrapper.java.additional.2 = -DgemfirePropertyFile=[path of the gemfire.properties file]
10) Run the following command to stop the TCP Locator:

    stop locator --locator=<locator name>
11) Go to yajsw/bat and execute installService.bat to install the Windows service for TCP Locator.
12) To uninstall the Windows service execute uninstallService.bat.
13) Before performing next steps, perform step 1-10 on all the nodes that contain TCP Locator.

4.5. Global Document Storage Directory (GDS)

On cluster configurations, create a shared file system for GDS directory accessible to each node on the AEM Forms cluster. This shared file system can be a local storage on a computer or a share on the dedicated network storage system. Ensure that all the nodes of the cluster have read and write permissions on the shared storage. The GDS directory should have low access time, high up time, and should be accessible as UNC style path. For example, \\storagename\shared\GDS.

4.6. Installing the font directories in cluster nodes

You must install the font directories for each node in the cluster, including the AEM forms fonts that are installed in the *[aem_forms root]*\fonts directory.

The fonts must exist in the same path on each node, and the directory must have identical contents on all nodes in the cluster. To ensure this, use one of the following options:

- Use a shared directory that all nodes in the cluster can access. Copy fonts from [*aem_forms root]*\fonts to the shared directory. Using shared fonts directories can slow down the access to the fonts and induces performance issues.
- Copy the *[aem_forms root]*\fonts directory to each node in the cluster in an identical path.

Record the location where you create these shared directories for later use when you configure AEM Forms using Configuration Manager.

NOTE: The font directories must be distinct from the GDS directory. However, they may be distinct sibling subdirectories of a single shared parent directory. The requirements and steps mentioned above are applicable to the custom font directories.

4.7. Next steps

You must now configure AEM Forms on JEE for deployment. You can also choose to run Configuration Manager later by using the ConfigurationManager.bat or ConfigurationManager.sh file located in *[aem-forms root]*\configurationManager\bin.

5. Configuring AEM Forms for deployment

5.1. Considerations when configuring and deploying AEM Forms on JEE

General Considerations

- While configuring, you must provide the location of the JDBC drivers for your database. Oracle and SQL Server drivers are in the*[aem-forms root]*/lib/db/*[database]* directory. You can download IBM DB2 driver from IBM website. For the complete list of Supported Driver Versions and download locations, see Supported Platform Combination
- .
- Temporary directory: It is recommended to use local directory as a temporary directory. The temporary directory should exist on every node of the cluster and the path of the temporary directory must be same for every node in the cluster.
- Global Document Storage (GDS) directory: Specify the GDS directory that meets the requirements outlined in the Preparing to Install (Single Server or Server Cluster). For latest documentation, see http://www.adobe.com/go/learn_aemforms_tutorials_63_en
- .
- On cluster environments, several steps need to be performed manually in addition to the automatic configuration that Configuration Manager performs.

Considerations for WebSphere application server

- Configuration Manager does not support deployment or undeployment of EAR files with custom file names. If your EAR files use a custom file name, you must manually deploy and undeploy them to the application server.
- If you are deploying components to WebSphere on a localized instance of Windows operating system, Configuration Manager deployment process reaches approximately 7% completion and then adobe-livecycle-websphere.ear fails to deploy. You must perform additional steps described in the Miscellaneous Errors section of the adobe-livecycle-websphere.ear fails to deploy
- article.
- If you are installing in a distributed environment to a secured server, you will encounter SSL handshake exceptions when running Configuration Manager. To avoid this error, run the following executable file before running Configuration Manager: *[appserver root]*/bin/retrieveSigners.bat. The retrieveSigners utility retrieves the certificates from the WebSphere Deployment Manager

server and adds them to the local server's trust store. See Retrieving signers using the retrieve Signersutilityatthe client

- on IBM Information Center.
- Some Configuration Manager screens require you to provide the SOAP port of the application server or the deployment manager. For more information on how to determine SOAP ports of your WebSphere application server, see blog
- http://blogs.adobe.com/livecycledocs/?p=243
- .
- If you are configuring a remote application server, ensure that an application server is also installed on the computer where you run Configuration Manager so that it can use the application server library files. In an environment where a remote application server is installed on Linux, AIX, or Solaris, and AEM Forms on JEE is installed on Windows environment, copy the appropriate database driver from [aem-forms root]\lib to the [appserver root]/universalDriver/lib folder of the remote server.
- You can determine the JNDI port number by logging in to WebSphere Administrative Console and navigate to Servers > Server Types > WebSphere application servers > [server name] > Communications > Ports. You will need to provide a value for BOOTSTRAP_ADDRESS when you configure the application server using Configuration Manager.

Considerations while configuring AEM Forms on JEE Server Clusters

- You cannot configure settings for IPv6-based clusters using Configuration Manager.
- It is recommended to have local server fonts and customer fonts directories at the same path on each node in the cluster. Shared fonts directories instead of local fonts directories may cause performance issues.

5.2. AEM Forms on JEE pre-configuration tasks

NOTE: Press **F1** in Configuration Manager to view Help information for the screen you are viewing. You can view the configuration progress at any time by clicking View Progress Log.

1) If you did not start Configuration Manager automatically from the installation program, navigate to the *[aem-forms root]*/configurationManager/bin directory and run the ConfigurationManager.bat/ConfigurationManager.sh script.
2) If prompted, select a language for Configuration Manager to use and click **OK.**
3) On the Welcome screen, click **Next**.
4) Do not select any option on the Upgrade Task Selection screen and click **Next**.
5) On the Modules screen, select AEM Forms on JEE modules you wish to configure and click **Next**.

   NOTE: Some modules have technical dependencies on other modules for proper configuration and functioning. Configuration Manager displays a dialog and does not allow to proceed further if mutually dependent modules are not selected. For example, you must select Content Repository modules if you are configuring Forms Workflow

– In AEM Forms, Adaptive Forms, Correspondence Management, HTML5 Forms , Forms Portal, HTML Workspace, Process Reporting, Forms centric workflows on OSGi, capabilities use crx-repository. If you plan to use AEM Forms for these capabilities, then crx-repository is required.
– You do not require crx-repository for AEM Forms Document Security.

.

6) On the Task Selection screen, select all the tasks you want to perform and click **Next**.

NOTE: If you are using Oracle RAC, do not select the Package JDBC modules into Adobe Experience Manager Forms EAR files (secure datasources) option.

5.3. Configuring and deploying AEM Forms on JEE

Configuring AEM Forms

On the Configure Adobe Experience Manager Forms (2 of 5) screen, click **Next** to accept the default directory locations, or click **Browse** to navigate to and change the directories that Adobe Experience Manager Forms will use to access fonts, and then click **Next**.

TIP: *Click **Edit configuration** to change any values on this screen. This button is not available when the Configuration Manager is run for the first time, but is available on the second and subsequent runs of the Configuration Manager.*

- (Optional) To change the default location of the **Adobe server fonts directory**, type the path or browse to the directory.
- To change the default location of the **Customer fonts directory,**click **Browse** or specify a new location for your customer fonts.

  NOTE: Your right to use fonts provided by parties other than Adobe is governed by the license agreements provided to you by such parties with those fonts, and is not covered under your license to use Adobe software. Adobe recommends that you review and ensure that you are in compliance with all applicable non-Adobe license agreements before using non-Adobe fonts with Adobe software, particularly with respect to use of fonts in a server environment.
- (Optional) To change the default location of the **System fonts directory**, type the path or browse to the directory. To add more directories to the list, click **Add**.
- (Optional) To enable FIPS, ensure that **Enable Federal Information Processing Standards (FIPS) 140-2 cryptography** is selected. Select this option only if you require the Federal Information Processing Standards (FIPS) to be enforced.

1) On the Configure Adobe Experience Manager forms(1 of 5) screen, click **Configure** and click **Next** when done.
2) On the Configure Adobe Experience Manager Forms (2 of 5) screen, click **Next** to accept the default directory locations, or click **Browse** to navigate to and change the directories that AEM Forms will use to access fonts, and then click **Next**.

TIP: *Click* ***Edit configuration*** *to change any values on this screen. This button is not available when the Configuration Manager is run for the first time, but is available on the second and subsequent runs of the Configuration Manager.*

- (Optional) To change the default location of the **Adobe server fonts directory**, type the path or browse to the directory.
- To change the default location of the **Customer fonts directory,**click **Browse** or specify a new location for your customer fonts.

  NOTE: Your right to use fonts provided by parties other than Adobe is governed by the license agreements provided to you by such parties with those fonts, and is not covered under your license to use Adobe software. Adobe recommends that you review and ensure that you are in compliance with all applicable non-Adobe license agreements before using non-Adobe fonts with Adobe software, particularly with respect to use of fonts in a server environment.
- (Optional) To change the default location of the **System fonts directory**, type the path or browse to the directory. To add more directories to the list, click **Add**.
- (Optional) To enable FIPS, ensure that Enable **FIPS** is selected. Select this option only if you require the Federal Information Processing Standards (FIPS) to be enforced.

3) Click **Browse** on the Configure Adobe Experience Manager forms (3 of 5) screen to specify the**Location of the temporary directory**, and then click **Next**.

   NOTE: Ensure that the temporary directory is on the local file system. AEM Forms does not support a temporary directory at a remote location.

   NOTE: If you do not specify the temporary directory, the default system-configured temp location is used. The temporary directory must exist on every node of the cluster and path of the temporary directory must be same on every node of the cluster.

4) On the Configure Adobe Experience Manager Forms (4 of 5) screen, click **Browse** to specify the path for the Global Document Storage (GDS) directory, and then click **Next**.. ***NOTE:*** *If you leave the GDS directory field empty, AEM Forms will create the directory in a default location in the application server directory tree. After you finish the configuration steps, you can access the location from administration console > Settings > Core System Settings > Configurations.* ***NOTE:*** *Ensure that GDS directory is accessible from all the nodes of the cluster. For Cluster, do not leave the directory field empty..*

   - **Use GDS**: Use the file system-based GDS for all persistent document storage. This option provides the best performance, and a single location for GDS.
   - **Use database**: Use the AEM Forms database for storing the persistent documents and long-lived artifacts. However, the file-system based GDS is also required. Using the database simplifies backup and restore procedures.

   Click ***Configure*** *to configure the AEM Forms EARs with this directory information and, after the configuration is complete, click* ***Next****.*

Configure CRX

1) The CRX Configuration screen allows you to configure the CRX repository and install it into the adobe-livecycle-cq-author.ear EAR file.
   a) Specify the path to the repository. The default location is *[aem-forms root]*/crx-repository.

      NOTE: Ensure that the CRX repository path does not contain spaces and the content repository is available on all the nodes of the cluster. After the configuration is complete, copy the content repository from local node to all the nodes on the same location (as specified on the CRX configuration screen) .
   b) Select the repository type, as appropriate and keep a note of the following points:
      - CRX3 TAR is not supported in clustered deployments.
      - If selecting CRX3 Mongo DB, specify the Mongo database name and URL to the database. The format of the URL is: `mongodb://<HOST>:<Port>`.

        HOST: IP address of the machine running MongoDB.

        Port: Port number used for the MongoDB. The default port number is 27017.
      - CRX3 RDB is supported only with Oracle 12c or IBM DB2 10.5 databases. Selecting this option sets the CRX repository persistence to RDB MK (document MK) .
   c) Click **Configure** to create the required repository files at the specified location.

   NOTE: *If your AEM Forms on JEE server is running remotely, select* ***Server is running on remote host****, and specify the path to the repository on the remote host.*

   Click ***Next*** *to continue.*

   NOTE: Once the packages are configured, you cannot remove them by re-running the Configuration Manager. For clean uninstallation of deployed packages, you need to uninstall and delete the packages using Package Manager.

(Remote host only) CRX Configuration Summary

1) For a remote deployment, copy the content from the [*aem-forms root*]/configurationManager/export/crx-quickstart/ directory to the location on the remote host you specified on the CRX Configuration screen.

   NOTE: In case of clustered deployment, you must copy the content from the [aem-forms root]/configurationManager/export/crx-quickstart/ directory to the specified location on all cluster node hosts.

Configuring Acrobat for PDF Generator

1) **(Windows only)**On the Configure Acrobat For PDF Generator screen, click **Configure** to run the script that will configure Adobe Acrobat and required environment settings. Click **Next** when complete. ***NOTE:*** *This screen will perform the desired configuration only when Configuration Manager is running locally. You must have Adobe Acrobat DC Pro already installed or this step will*

fail. ***NOTE:*** *You should manually configure Acrobat for PDF generator on all the other nodes of the cluster. See Configuring PDF Generator in the Post Deployment chapter.*

Configuration Summary

1) On the Configure Adobe Experience Manager forms Summary screen, click **Next**. Configured archives are placed in the *[aem-forms root]*/configurationManager/export directory.

Configuring your application server and database

1) On the Application Server Configuration Details screen, provide the information for the fields (all fields are mandatory) and then click **Verify Server Connection**. When the verification has completed successfully, click **Next**.

   NOTE: If you are using WebSphere application server with Microsoft SQL Server database and Java 7, use the JDBC driver located at [aem-forms root]/lib/db/mssql/java7.

   NOTE: If WebSphere Administrative Security is off, Admin User ID and Password fields can be left blank.

   NOTE: When using WebSphere Cluster or WebSphere Network Deployment server to configure a standalone WebSphere Application server, enter the port number of the deployment manager in the SOAP Port field.

   NOTE: If you are using non-default WebSphere profile, ensure that you provide the complete path, including the profile name, in the Local Application Server Root Directory field.

2) On the Application Server Configuration Selection screen, select the tasks for Configuration Manager to perform, and click **Next**.

   If you prefer to configure the application server cluster manually, ensure that all the tasks are deselected, then click ***Next****.*

3) On the Server Settings Configuration screen *(appears only if Configure Server Settings was selected)*, provide the information for the fields, and then click **Next**.

   NOTE: *: If you are using UDP then multicast port can be any available port between 1025 and 65535. The multicast port must be unique to the AEM Forms on JEE cluster (that is, the port must not be used by any other cluster on the same network, any attempt to use the same port by any other cluster on the same network would result in bootstrap failure).*

   NOTE: *LCM does not configure* `-Dadobe.cache.multicast-address` *and* `-Dadobe.cache.bind-address` *jvm arguments. You may need to configure these arguments manually. See Modifying the JVM properties section for more details.*

4) On the Datasource Configuration screen *(appears only if Configure Datasource option is selected)*, provide the information for the fields and then click **Test Database Connection**. When the connection is tested successfully, click **Next**.

   You can choose to manually configure data sources rather than allowing Configuration Manager to configure them for you. To override automatic data source configuration, select ***Manually configure data source in the WebSphere Administrative Console before continuing****, at the bottom of the screen.*

Without exiting Configuration Manager, go to the application server administration console, and configure data sources as described in Configuring the AEM Forms database connectivity in Installing AEM forms on JEE for WebSphere Server Guide.

5) On the Application Server Configuration screen, click **Configure**. When the process is completed, click **Next**.

6) If you have enabled SSL, perform the following steps. These steps change "http" to "https" in the integration URL:

   a) Open Webspehere console. The default URL is [host]:<ibm_admin_port>/ibm/console.

   b) Navigate to Servers > Server Types > Websphere Application Server and select server. For example Server1.

   c) In Server Infrastructure, select Java and Process Management . Click Process Definition. In Additional Properties, select Java Virtual Machine

7) On the Application Server Configuration Validation screen, select the tasks for validating and then click **Validate** and select Yes on prompt to deploy adobe-lcm-lcvalidator.ear. When the process is completed, click **Next**.

Copy CRX Content

Copy all the content of the [*aem_forms root*]/configurationManager/export/crx-quickstart/ directory to the location specified on the C'RX Configuration screen on all the cluster nodes.

Deploying AEM Forms on JEE EARs

1) You must deploy the EAR only on the master node and keep other nodes in the shutdown status.

   In the WebSphere administration console, stop all servers running on slave nodes and keep only the server of the master node running.

   NOTE: After you have completed all configurations and have quit the Configuration Manager, ensure that you run one of the stopped servers, wait for it to start completely, and then run other stopped servers, one by one.

2) On the Deploy Adobe Experience Manager Forms EARs screen, select the EAR files to deploy, and then click **Deploy**. This operation may take several minutes to complete. When the deployment has completed successfully, click **Next**.

   NOTE: If the deployment of EARs fails with the error – The system failed to make the SOAP RPC call: invoke – increase the SOAP timeout value as described in Modifying the WebSphere time-out settings section and then deploy the EARs.

   NOTE: *When Configuration Manager has started the execution of the IBM WebSphere® JACL deployment scripts, you cannot stop the deployment even if you exit or cancel Configuration Manager prior to deployment completion. No user action is required because the product EARs will be successfully deployed.*

   By default, Configuration Manager deploys the EAR files to the WebSphere default virtual host, `default_host`*. To deploy the EAR files to a different virtual host, select the target host from the Virtual Host list.*

To connect to the application server using a secure port while running Configuration Manager, do the following tasks:

a) Copy the [appserver root]\java_<version>\jre\lib\security\java.security file to another folder on the same machine.

b) Open the copied java.security file for editing.

c) Uncomment the following lines:

```
ssl.SocketFactory.provider=com.ibm.jsse2.SSLSocketFactoryImpl
ssl.ServerSocketFactory.provider=com.ibm.jsse2.SSLServerSocketFactoryImpl
```

d) Comment the following lines:

```
ssl.SocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLSocketFactory
ssl.ServerSocketFactory.provider=com.ibm.websphere.ssl.protocol.SSLServerSocketFactory
```

e) Save and close the file.

f) Exit the Configuration Manager.

g) Open the [aem-forms root]\Adobe_Experience_Manager_Forms\configurationManager\bin\ConfigurationManager.bat for editing.

h) Add the following argument to the JAVA_OPTS property:

```
-Djava.security.properties=<path of the copied java.security file>
```

i) Run the Configuration Manager using the ConfigurationManager.bat file and continue from the Adobe Experience Manager Forms Database Initialization screen.

NOTE: Whenever an application is deployed for the first time, the application name is retained. Subsequent deployments of the application on a different cluster within the same cell append the name of the cluster to the application name.

NOTE: You have to manually deploy adobe-livecycle-author.ear after configuring AEM Forms and upgrading the repository.

Initializing AEM Forms on JEE database

1) On the Adobe Experience Manager forms Database Initialization screen, verify that the hostname and port number provided for your application server is correct and then click **Initialize**. The database initialization task creates tables in the database, adds default data to the tables, and creates basic roles in the database. When the initialization has completed successfully, click **Next**.

NOTE: *Before continuing with the next steps, wait until the ServiceEvent REGISTERED and ServiceEvent UNREGISTERED messages stop appearing in the <crx-repository>/error.log file. Depending on network and database response speed, it might take a few hours for RDBMK to be up and running.*

NOTE: *Initialize the database only on one node of the cluster. Subsequent steps are performed only on initialized server.*

Restart the application server manually if you are prompted to do so.

2) On the Adobe Experience Manager forms Information screen, enter **Adobe Experience Manager forms User ID** and **Password** whose default values are *administrator* and *password* respectively.

   NOTE: Before verifying the connection to the server, verify that AEM is up and running. If AEM is not up and running and the server is restarted, it may lead to the corruption of repository data. Perform the following steps to verify that AEM is up and running:

   a) Watch the error.log file for activity. Ensure that it is stable and no more action is performed. The default path of the error.log file is <aem-forms_root>/crx-repository/logs/error.log.

   b) In the browser window, open URL http://[host]:[port]/lc/system/console/bundles, and ensure that only one bundle is in the installed state.

   *Click **Verify Server Connection**, and when complete, click **Next**.*

   NOTE: The server information that appears on this screen represents default values for the deployment.

   Verifying the server connection helps narrow troubleshooting in case failures occur in the deployment or validation. If the connection test passes but deployment or validation fails in the next few steps, connectivity issues can be eliminated from the troubleshooting process.

Deploying Central Migration Bridge Service

1) On the Central Migration Bridge Service Deployment Configuration screen, if applicable, select the **Include Central Migration Bridge Service** in deployment option and then click **Next**.

Deploying AEM Forms on JEE components

1) On the Adobe Experience Manager forms Component Deployment screen, click **Deploy**. The components that are deployed at this time are Java archive files that plug into the service container that is part of AEM Forms on JEE for purposes of deploying, orchestrating, and executing services. When the deployment has completed successfully, click **Next**.

2) On the Adobe Experience Manager forms Component Deployment Validation screen, click **Validate**. Click **View Progress Log** to view the validation progress and, when the validation has completed successfully, click **Next**.

Configuring AEM Forms components

1) On the Configure Adobe Experience Manager Forms Components screen, select the tasks to run with Configuration Manager, and click **Next**.

Configure Connector for EMC Documentum®

NOTE: In case of a remote AEM Forms on JEE deployment, you cannot configure the Connector for EMC Documentum using Configuration Manager.

1) On the Specify Client for EMC Documentum screen, select **Configure Connector for EMC Documentum Content Server**, and specify the following settings. Enter the details, click **Verify**, and when complete, click **Next** to continue.
   - **Choose EMC Documentum Client Version:**Select the client version to use with the EMC Documentum Content Server.
   - **EMC Documentum Client Installation Directory Path:**Click **Browse** to select the directory path.
2) On the Specify EMC Documentum Content Server Settings screen, enter the EMC Documentum Server details, and then click**Next**. Press F1 for information about the details you need to enter.
3) On the Configure Connector for EMC Documentum screen, click **Configure Documentum Connector**. When completed, click **Next**.
4) On the Required Manual Configurations for Connector for EMC Documentum screen, review and perform the manual steps listed on all the nodes of the cluster and then click **Next**.

Configure Connector for IBM® Content Manager

NOTE: In case of a remote AEM Forms on JEE deployment, you cannot configure the Connector for IBM Content Manager using Configuration Manager.

1) On the Specify Client for IBM Content Manager screen, select **Configure Connector for IBM Content Manager**, and enter a value for the IBM Content Manager Client Installation Directory Path. Click **Verify** and when complete, click **Next** to continue.
2) On the Specify IBM Content Manager Server Settings screen, enter the details of the IBM Content Manager Server, and click **Next**.
3) On the Configure Connector for IBM Content Manager screen, click **Configure IBM Content Manager Connector**. When complete, click **Next**.
4) On the Required Manual Configurations for Connector for IBM Content Manager screen, review and perform the manual steps listed on all the nodes of the cluster and then click **Next**.

Configure Connector for IBM® FileNet

NOTE: In case of a remote AEM Forms on JEE deployment, you cannot configure the Connector for IBM FileNet using Configuration Manager.

1) On the Specify Client for IBM FileNet screen, select **Configure Client for IBM FileNet Content Manager**, and specify the following settings.
   - **Choose IBM FileNet Client Version:**Select the client version that you want to use with the IBM FileNet Content Server.
   - **IBM FileNet Client Installation Directory Path:** Click **Browse** to select the directory path.

     NOTE: The validation of IBM FIleNet may fail if there are special characters, such as hyphen (-), underscore (_), comma (,), or dot (.) in the directory name containing the IBM FileNet client.

   *Click **Verify**, and when complete, click **Next** to continue.*
2) On the Specify IBM FileNet Content Server Settings screen, enter the required details, and click **Next**. Press F1 for more information.
3) On the Specify Client for IBM FileNet Process Engine screen, enter the required details, and click **Verify**. When complete, click **Next**.
4) On the Specify IBM FileNet Process Engine Server Settings screen, enter the required details and click **Next**. Press F1 for more information.
5) On the Configure Connector for IBM FileNet screen, click **Configure FileNet Connector**. When complete, click **Next**.
6) On the Required Manual Configurations for Connector for IBM FileNet screen, review and perform the manual steps listed on all the nodes of the cluster and then click **Next**.

Configure Connector for Microsoft® SharePoint®

NOTE: In case of a remote AEM Forms on JEE deployment, you cannot configure the Connector for Microsoft SharePoint using Configuration Manager.

On the Configure Adobe Adobe Experience Manager Forms Connector for Microsoft SharePoint screen, do one of the following tasks:

- Deselect the **Configure Adobe Experience Manager Forms Connector for Microsoft SharePoint** option to manually configure Microsoft Sharepoint later, and then click **Next**.
- Leave the **Configure Adobe Experience Manager forms Connector for Microsoft SharePoint** option selected. Enter the required values, and then click Configure SharePoint Connector. When complete, click **Next**.

  NOTE: You can skip this step if you want to configure the Connector for Microsoft SharePoint later using administration console.

Configuring forms server for native file conversions

1) **(PDF Generator only)**On the **Admin user credentials for native PDF conversions**screen, enter the user name and password of a user with administrative privileges on the server computer, and then click**Add user.**

   NOTE: You must add at least one administrative user for Windows 2008 Server. On Windows 2008 Server, User Account Control (UAC) must be disabled for the users you add. To disable UAC, click **Control Panel**> **User Accounts** > **Turn User Account Control on or off**and deselect Use User Account Control (UAC) to help protect your computer, then click **OK**. Restart the computer to apply these changes.

System readiness test for PDF Generator

1) On the **Document Services PDF Generator System Readiness Test** screen, click **Start** to validate if the system has been appropriately configured for PDF Generator. Review the System Readiness Tool Report and click **Next.**Note that the system readiness test fails if AEM Forms on JEE is deployed on a remote machine.

Configuring Acrobat Reader DC extensions

1) On the Acrobat Reader DC extensions Credential Configuration screen, specify the details that are associated with the Acrobat Reader DC extensions credential that activates the module services.

   NOTE: You can skip this step at this time by selecting **Configure later using administration console**. You can configure the Acrobat Reader DC extensions credential by using Administration Console after you complete the deployment. (After logging in to administration console, click **Home** > **Settings** >**Trust Store Management** > **Local Credentials** .*)*

   *Click **Configure**and then click **Next**.*

Summary, and Next Steps

1) Review the Configuration Manager task summary list and choose the appropriate options:
   – Select Launch Next Steps to view information about AEM Forms on JEE users and administrative interfaces to launch an html page containing step-by-step instructions to start and use AEM Forms.

   ***NOTE:** You will see a message on the screen to restart the server. However, do not immediately restart. Ensure that [crx-repository]/logs/error.log is stable and all bundles (except signatures) are in active mode before you restart the server.Click **Finish** to exit the Configuration Manager.*

6. Manually Configuring a WebSphere Cluster

This chapter describes how to manually configure a WebSphere Application Server cluster to prepare for the manual deployment of AEM Forms in the clustered environment. This chapter applies only if you chose not to configure your WebSphere Application Server cluster automatically. For information about how to automatically configure your application server, see “ConfiguringAEMformsforDeployment” .

At this point in the installation process, you have already installed AEM Forms files and run Configuration Manager to configure the AEM Forms deployable archives. Now, you must perform the following tasks manually:

- Configure the WebSphere Application Servers. (See ConfiguringtheWebSphereApplicationServer-instances.)
- Configure JDBC connectivity. (See ConfiguringtheAEMformsdatabaseconnectivity.

6.1. Directory permissions

The AEM Forms application will extract files to the *[appserver root]*/installedApps directory. Therefore, it is important that writable permissions be given to that directory. If writable permissions cannot be given, the section below describes how to modify the location for the extracted files.

NOTE: It is recommended that you modify the location of the extracted files.

Modify the location for the extracted files

1) Log in to the WebSphere Administrative Console.
2) Do one of the following:
   – Click **Servers** > **Server Types** > **WebSphere Application servers** and click your server name, such as **server1**.
3) Under Server Infrastructure, click **Java and forms workflow**>**Process Definition**.
4) Under Additional Properties, click **Java Virtual Machine** and then click **Custom Properties**.
5) Click **New** and create a custom property named **adobeidp.RootDirectory**.
6) Set the value of adobeidp.RootDirectory to the path where Adobe native files should be extracted, such as *[appserver root]*/profiles/<*profile_name*>/installedApps.
7) Click **OK** or **Apply**.
8) In the Messages box, click **Save directly to master configuration**, and then restart the application server.

6.2. Configuring the WebSphere Application Server instances

You must configure the WebSphere Application Server instances that you installed in the cluster by performing the following tasks:

- Modify the WebSphere time-out settings. (See ModifyingtheWebSpheretime-outsettings.)
- Modify the JVM properties. (See ModifyingtheJVMproperties.)
- Create a J2C authentication alias for the database. (See CreatingaJ2Cauthenticationaliasfortheda-tabase.)

Modifying the WebSphere time-out settings

You must modify the WebSphere time-out settings on each WebSphere Application Server in the cluster.

To modify WebSphere time-out settings:

1) In the WebSphere Administrative Console navigation tree, click **Servers** > **Application servers** and, in the right pane, click the server name.
2) Under Container Settings, click **Container services** > **Transaction Service**.
3) In the **Total transaction lifetime timeout** box, type `600` and then click **OK**.
4) Under Container Settings, click **Container Services** > **ORB Service**.
5) In the**Request timeout** box, type `360` and, in the **Locate Request Timeout** box, type `600`, and then click **OK**.
6) Under Server Infrastructure, click **Administration** > **Administration Services**.
7) On the next screen, click **JMX Connectors** and, in the table, click **SOAPConnector**.
8) On the next screen, click**Custom properties** and, in the table, click **requestTimeout**.
9) In the Value box, type `1800`.
10) Click **OK** and then click **Save directly to the master configuration**.

Modifying the JVM properties

You must modify the Java Virtual Machine (JVM) properties of each WebSphere Application Server instance in the AEM Forms cluster to add AEM Forms options.

NOTE: You must restart each node of the application server after you modify the JVM parameters.

Before starting this procedure, you must know if your cluster uses a 32-bit or 64-bit JVM. See Preparing to Install AEM Forms (Server Cluster) to determine the JVM required for your cluster configuration.

Before starting this procedure, you must determine how your AEM Forms cluster implements cluster caching so that you can correctly configure a JVM argument for cluster caching. You may implement cluster caching by using UDP or TCP but not both. The following factors may affect your choice:

- UDP can be used only if your cluster is based on IPv4.
- Use TCP if your cluster is either IPv4-based or IPv6-based. On an IPv6-based cluster, you must use TCP to be IPv6-compliant.

  If you implement cluster caching by using TCP, you must also ensure that you configure the TCP locators correctly (see "Configuringthecachinglocators(cachingusingTCPonly)").

TIP: It is recommended to use TCP instead of UDP multicasting for production systems because of the inherent reliability of the TCP protocol.

To modify JVM properties:

1) Log in to the WebSphere Administrative Console and, in the navigation tree, click **Servers** > **Application servers** and then, in the right pane, click the server name.
2) Under Server Infrastructure, click **Java and forms workflow** > **Process Definition**.
3) Under Additional Properties, click **Java Virtual Machine** and add or configure the following properties:
   - In the **Initial Heap Size** box, type `512`
   - In the **Maximum Heap Size** box, set one of the following values:
     - (32-bit JVM only) Type `1024`
     - (64-bit JVM only) Type `4096`
   - In the **Generic JVM arguments** box, add the following arguments:

     `-Xgcpolicy:gencon`

     `-Dfile.encoding=utf8`
   - In the **Generic JVM arguments** box, set one of the following values:
     - (32-bit JVM only) Type `-XX:MaxPermSize=256m`
     - (64-bit JVM only) Type `-XX:MaxPermSize=512m`
4) On the same screen, in the **Generic JVM arguments** box, add the following caching arguments depending on the configured cluster cache mechanism (UDP or TCP):
   - **Caching using UDP discovery**
     - Configure the multicast port argument in the following format:

       `-Dadobe.cache.multicast-port=<port number>`

       NOTE: The value for `<port number>` can be any available port between 1025 and 65535. The multicast port must be unique to the AEM Forms cluster (that is, the port must not be used by any other cluster on the same network, any attempt to use the same port by any other cluster on the same network would result in bootstrap failure). It is recommended that you configure the same `<port number>`*on all nodes in the AEM Forms cluster, as in this example:*

       `-Dadobe.cache.multicast-port=33456`
     - Setting multicast address argument is optional. Default muticast addresses for IPv4 and IPv6 are as following:

       `IPv6 - FF38::1234`
       `IPv4 - 239.192.81.1`

       If you have restriction on multicast addresses in your network, use following argument to set multicast addresses:

       `-Dadobe.cache.multicast-address=<ip address>`

       NOTE: The value for `<ip address>` is the IP address used for multicast networking. The IP address is ignored if `adobe.cache.multicast-port` *is zero.*

       NOTE: The multicast address must be unique to the AEM Forms cluster and must not be used by any other cluster on the same network. It is recommended that you configure the same `<ip address>`*on all nodes in the AEM Forms cluster. For example:*

```
-Dadobe.cache.multicast-address=239.192.81.1
```

– **Caching using TCP only**

• For IPv4, configure the cluster locators argument in the following format:

```
-Dadobe.cache.cluster-locators=<IPaddress>[<port number>],<IPaddress>[<port number>]
```

For IPv6, configure the cluster locators argument in the following format:

```
-Dadobe.cache.cluster-locators=<hostname>@<IPv6 address>[<port number>], <hostname>@<IPv6 address>[<port number>]
```

NOTE: Configure, as a comma-separated list, the locators for all nodes of the cluster. The value for `<IPaddress>` is the IP address of the computer running the locator, and the value for `<port number>` is any unused port between 1025 and 65535. It is recommended that you configure the same `<port number>` *for all locators, as in this example:*

```
-Dadobe.cache.cluster-locators=10.20.30.5[22345],10.20.30.6[22345]
```

NOTE: Do not run TCP locator for all the nodes. Configure only two TCP locators. Enable one TCP locator to serve as a primary locator and another TCP locator to serve as a secondary/backup locator. For information on configuring TCP locators, see Configuringthecachinglocatorsinclusters(cachingusingTCPonly).

– For machines with multiple Network Interfaces

Some machines may be connected to multiple networks via multiple Network Interface Cards (NICs). For such machines, set the JVM property `-Dadobe.cache.bind-address` *to the IP address of the network interface card that you are using for forms server.*

```
-Dadobe.cache.bind-address=<IP Address>
```

NOTE: *It is recommended to set JVM property -Dadobe.cache.bind-address for machines with one Network Interface Card, also.*

5) To prevent application server from Denial of Service attacks configure the following JVM argument:

```
-DentityExpansionLimit=10000
```

6) Click **Apply** and click **Custom Properties**.

7) *(IPv4 only)* On the next screen, click **New**, add or configure the following properties, and then click **OK**:

– In the **Name** box, type `java.net.preferIPv4Stack`.

– In the **Value** box, type `true`.

8) *(IPv6 only)* On the next screen, click **New**, add or configure the following properties, and then click **OK**:

– In the **Name** box, type `java.net.preferIPv6Stack`.

– In the **Value** box, type `true`.

– In the **Name** box, type `java.net.preferIPv6Addresses`.

– In the **Value** box, type `true`.

9) Click **OK** and then click **Save directly to the master configuration**.

10) Restart the server.
11) Repeat steps 11 to 19 for each server in the cluster.

Creating a J2C authentication alias for the database

You must create a J2C authentication alias for the database.

To create a J2C authentication configuration for the data source:

1) In the WebSphere Administrative Console navigation tree, click **Security > Global security.**
2) In the right pane, under Authentication, click **Java Authentication and Authorization Service > J2C authentication data**, and then click **New**.
3) Set the following properties:
   - In the **Alias** box, type an alias name appropriate to the database user, such as `IDP_DS/db2-db2user`.
   - In the **User ID**box, type a name, such as `db2user`. This ID is the login credential used to access the database that will be used with the IDP_DS data source.
   - In the **Password**box, type a password for this user.

   NOTE: In this guide, IDP_DS identifies the AEM Forms data source.
4) Click **OK** and then click **Save directly to master configuration**.
5) Repeat steps 3 and 4 for RM_DS and AEM_DS. Use `EDC_DS/db2-db2user` as the alias name.

   NOTE: EDC_DS is JNDI name of the RM_DS datasource.

6.3. Configuring the AEM Forms database connectivity

To enable WebSphere and your AEM Forms deployment to connect to the AEM Forms database, you must create a database connection for AEM Forms by installing the database drivers and then setting up a data source.

You must install drivers for the type of database that you use for the AEM Forms database. The drivers should be placed in the installation directories of the application server.

You must configure the data source to connect to the database. For WebSphere, you can configure a DB2, an Oracle, SQL Server data source.

You will need the following information from tasks you did in Preparing to Install AEM Forms (Server Cluster):

- Database name
- Server name
- Port number
- User name
- Password

Refer to the following section that applies to your database:

- ConfiguringtheDB2datasource
- ConfiguringtheOracledatasource
- ConfiguringtheSQLServerdatasource

Configuring the DB2 data source

Configuring the DB2 data source requires you to install the DB2 database drivers, create a DB2 JDBC provider on WebSphere, create the data source on WebSphere, and then configure the corresponding connection pool.

To install the DB2 database driver:

1) On a WebSphere Application Server instance, in the *[appserver root]* directory, create a directory named db2libs.
2) Download the driver from IBM Website and place the db2jcc4.jar file to the *[appserver root]*\db2libs directory:
3) Repeat steps 1 to 2 for each WebSphere Application Server in the cluster.

To create a DB2 JDBC provider:

1) On a WebSphere Application Server instance, in the WebSphere Administrative Console navigation tree, click **Environment** > **WebSphere Variables** and, in right pane, click **DB2UNIVERSAL_JDBC_DRIVER_PATH**.
2) In the **Value** box on the next screen, type the path to the db2libs directory.
3) Repeat steps 1 to 2 for each node scope as well as for the Cell Manager scope, inserting the path to the db2libs directory on the relevant node.
4) Click **OK** or **Apply** and in the **Messages** box, click **Save directly to master configuration**.
5) In the navigation tree, click **Resources**>**JDBC**>**JDBC Providers**.
6) In the drop-down list above the table, select **Cluster=<cluster name>**as the scope, and then click **New**.
7) In the Step 1 pane, set the following configuration and then click **Next**:
   - In the **Database type**list, select **DB2**.
   - In the **Provider type** list, select **DB2 Universal JDBC Driver Provider**.
   - In the**Implementation type** list, select **Connection pool data source**. Take note that for each Configuration Manager configuration script, the field implementation class name is com.ibm.db2.jcc.DB2ConnectionPoolDataSource.
   - In the **Name** box, keep the name **DB2 Universal JDBC Driver Provider**.
8) In the Step 2 pane, enter the path to the db2libs directory (for example, *[appserver root]*/db2libs), and then click **Next**.
9) In the Step 3 pane, click **Finish** and then click **Save directly to master configuration**.

Create AEM_DS datasource

1) In the navigation tree, click **Resources** > **JDBC**> **JDBC Providers** and, in the right pane, click the provider.
2) Under Additional Properties, click **Data sources** and then click **New**.
3) In the Step 1 pane, set the following configuration and then click **Next**.
   – In the **Data source name** box, type **Livecycle - DB2 - AEM_DS**.
   – In the **JNDI name** box, type **AEM_DS**.
4) In the Step 2 pane, type a database name and server name.

   NOTE: If the port used by the database is not the default port (50000), also specify your alternative port in the **Port number** box.
5) Ensure that **Use this data source in container managed persistence (CMP)** is selected.
6) Click **Next** and set the following configurations in the Step 3 pane:
   – In the list under **Component-managed authentication alias**, select the authentication alias created for thisdata source in *CreatingaJ2Cauthenticationaliasfor the database*.
   – In the **Mapping-configuration alias** list, select **DefaultPrincipalMapping**.
   – In the **Container-managed authentication alias** list, select the authentication alias created for this data source in *Creating a J2C authentication alias for the database*.
7) Click **Next** and, in the Step 4 pane, click **Finish**.
8) Click **Save directly to the master configuration**.

Create and configure an Oracle pluggable database

Oracle pluggable database on AEM Forms on JEE can be configured manually only and not through Configuration Manager. For introduction to pluggable database and multi-tenant architecture, see Introduction to the Multitenant Architecture.

To create and configure an Oracle pluggable data source, complete the following steps:

1) Create a container database using non-interactive/silent mode of Database Configuration Assistant (DBCA).
   a) Go to your oracle home. For example, on Windows you can run *cd%Oracle_HOME%\bin* to go to your Oracle home.
   b) Pass the following command to create the container database in non-interactive/silent mode using Database Configuration Assistant (DBCA). Replace the database name in the command with your database name.

```
dbca -silent -createDatabase -templateName General_Purpose.dbc
-gdbname ordb.corp.adobe.com -sid ordb -createAsContainerDatabase
true -responseFile NO_VALUE -characterSet AL32UTF8 -memoryPercentage
30 -emConfiguration LOCAL
```

2) Using SQL*Plus®, connect to the new container database as the DBA:

```
sqlplus system/password@localhost:1521/ordb.corp.adobe.com as sysdba
```

3) In SQL*Plus®, to create pluggable database with the appropriate name (here mynewpdb) and user name and password (here mynewadm/password), pass the following command:

```
SQL> CREATE PLUGGABLE DATABASE mynewpdb ADMIN USER mynewadm IDENTIFIED BY
passwordFILE_NAME_CONVERT=('D:\app\oracle\oradata\ordb\pdbseed','D:\app\
oracle\oradata\ordb\mynewpdb');
```

4) Alter the database by running the following command in SQL*Plus® to open the database in the read-write mode:

```
SQL> alter pluggable database mynewpdb open;
```

5) Grant the required access to the admin users of the pluggable database. The minimum access that the admin users require to work with the database are to:
   - Create sessions,
   - Create tables,
   - Create views,
   - Create sequences, and
   - Access unlimited tablespace.

   *Following is the sample command for achieving this in SQL*Plus®:*

```
sqlplus mynewadm/password@localhost:1521/mynewpdb.corp.adobe.com as
sysdbaSQL> grant CREATE SESSION to mynewadm;SQL> grant CREATE TABLE to
mynewadm;SQL> grant CREATE VIEW to mynewadm;SQL> grant CREATE SEQUENCE to
mynewadm;SQL> grant UNLIMITED TABLESPACE to mynewadm;
```

6) Configure JDBC connectivity manually. For more information on connecting to JDBC, see Configuring Adobe Experience Manager Forms OnJEEOnWebLogicCluster.
   a) Before clicking Test Configuration, update the JDBC URL for both RM_DS, IDP_DS, and AEM_DS. Replace : (colon) in the URL with a / (forward slash). For example:

      ```
      jdbc:oracle:thin:@localhost:1521/mynewpdb.corp.adobe.com
      ```

   b) Click Test Configuration to verify the pluggable database connectivity.

Configure LiveCycle - DB2 - AEM_DS connection pools

1) In the navigation tree, click **Resources** > **JDBC** >**JDBC Providers** and, in the right pane, click the **DB2 Universal JDBC Driver Provider**. See *To create a DB2 JDBC provider*..
2) Under Additional Properties, click **Data sources** and, in the right pane, click **Livecycle - DB2 - AEM_DS**.
3) On the next screen, under Additional Properties, click **Connection Pool Properties** and set the properties asfollows:
   - In the **Maximum connections** box, type **30**.
   - In the **Minimum connections** box, type **1**.
4) Click **OK** or **Apply**, and then click **Save directly to master configuration**.

Configure the custom property for DB2

1) In the navigation tree, click **Resources** > **JDBC** >**Data sources** and, in the right pane, click the data source that youcreated in *To create the Oracle JDBC data source* section.
2) Under Additional Properties, click **Custom properties** and then click **New**.
3)

Configure LiveCycle - DB2 - AEM_DS connection pools

Configure the custom property for DB2

1) In the navigation tree, click **Resources** > **JDBC** > **Data sources** and, in the right pane, click the data source. See *To create the DB2 JDBC data source*.
2) Under Additional Properties, click **Custom properties** and then click **New**.
3) In the **Name** box, type **useRRASetEquals** and in the **Value** box, type **true**.
4) Click **OK** or **Apply** and then click **Save directly to master configuration**.

To create AEM_DS datasource

1) In the navigation tree, click **Resources** > **JDBC**> **JDBC Providers** and, in the right pane, click the provider.
2) Under Additional Properties, click **Data sources** and then click **New**.
3) In the Step 1 pane, set the following configuration and then click **Next**.
   – In the **Data source name** box, type `Livecycle - DB2 - IDP_DS`.
   – In the the **JNDI name** box, type `IDP_DS`.
4) In the Step 2 pane, type a database name and server name.

   NOTE: If the port used by the database is not the default port (50000), also specify your alternative port in the **Port number***box.*
5) Ensure that **Use this data source in container managed persistence (CMP)** is selected.
6) Click **Next** and set the following configurations in the Step 3 pane:
   – In the list under **Component-managed authentication alias**, select the authentication alias created for this data source in CreatingaJ2Cauthenticationaliasforthedatabase.
   – In the **Mapping-configuration alias** list, select **DefaultPrincipalMapping**.
   – In the **Container-managed authentication alias** list, select the authentication alias created for this data source in CreatingaJ2Cauthenticationaliasforthedatabase.
7) Click **Next** and, in the Step 4 pane, click **Finish**.
8) Click **Save directly to the master configuration.**

Configure LiveCycle - DB2 - IDP_DS connection pools

1) In the navigation tree, click **Resources**>**JDBC**>**JDBC Providers** and, in the right pane, click the DB2 Universal JDBC Driver Provider. See *To create a DB2 JDBC provider*.
2) Under Additional Properties, click **Data sources** and, in the right pane, click **Livecycle - DB2 - IDP_DS**.
3) On the next screen, under Additional Properties, click **Connection Pool Properties** and set the properties as follows:
   – In the **Maximum connections**box, type `30`.
   – In the **Minimum connections**box, type `1`.
4) Click **OK** or **Apply**, and then click **Save directly to master configuration**.

Configure the custom property for DB2

1) In the navigation tree, click **Resources** > **JDBC**>**Data sources**and, in the right pane, click the data source. See *To create the DB2 JDBC data source*.
2) Under Additional Properties, click **Custom properties**and then click **New**.
3) In the **Name** box, type `useRRASetEquals` and in the **Value** box, type `true`.
4) Click **OK** or **Apply** and then click **Save directly to master configuration**.

Create the DB2 JDBC data source for Document Security

NOTE: This procedure applies only if you have Document Security installed.

1) In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and click the provider you created in *To create a DB2 JDBC provider* section.
2) Under Additional Properties, click **Data sources** and then click **New**.
3) In the Step 1 pane, set the following configurations and then click **Next**:
   – In the **Data source name** box, type `Livecycle - DB2 - RM_DS`.
   – In the **JNDI name** box, type `EDC_DS`.
   – In the list under Component-Managed Authentication and XA Recovery Authentication Alias, select the authentication alias created for this data source in CreatingaJ2Cauthenticationaliasforthedatabase.
4) In the Step 2 pane, type the database name and server name of the database you created.

   NOTE: If the port used by the database is not the default port (50000), also specify your alternative port in the **Port number***box.*
5) Click **Next** and, in the Step 3 pane, click **Finish**.
6) Select the data source you just created to modify additional parameters and set the following configuration:
   – In the **Container-managed authentication alias** list, select the authentication alias created for this data source in CreatingaJ2CauthenticationaliasforthedatabaseIn the **Mapping-configuration alias** list, select **DefaultPrincipalMapping**.
7) Click **OK** or **Apply**, and then click **Save directly to master configuration**.

Configure LiveCycle - DB2 - RM_DS connection pools for Document Security

NOTE: This section applies only if you have Document Security installed.

1) In the navigation tree, click **Resources**>**JDBC**>**JDBC Providers** and, in the right pane, click the **DB2 Universal JDBC Driver Provider** you created in *To create a DB2 JDBC provider* section.
2) Under Additional Properties, click **Data sources** and, in the right pane, click **LiveCycle - DB2 - RM_DS**.
3) On the next screen, under Additional Properties, click **Connection Pool Properties** and set the properties as follows:
   – In the **Maximum connections**box, enter 20.
   – In the **Minimum connections**box, enter 5.
4) Click **OK** or **Apply**, and then click **Save directly to master configuration**.

Configure the custom property for DB2:

1) In the navigation tree, click **Resources** > **JDBC**>**Data sources**and, in the right pane, click the data source you created in *To create the DB2 JDBC data source for Document Security* section.
2) Under Additional Properties, click **Custom properties**and then click **New**.
3) In the **Name** box, type `useRRASetEquals` and in the **Value** box, type `true`.
4) Click **OK** or **Apply** and then click **Save directly to master configuration**.

Set default isolation level

1) Log in to WebSphere Integrated Solutions Console.
2) In the WebSphere Administrative Console navigation tree, click **Resources** > **JDBC** > **Data Sources**.
3) From the drop-down list in the right pane, for Cluster,select **Cluster=[appropriate cluster name]**. All data sources under the cluster is displayed.
4) Click**LiveCycle - DB2 - IDP_DS** with JNDI name **IDP_DS**.
5) Click **Custom Properties**.
6) Search for **webSphereDefaultIsolationLevel** property, and click to open it for edit.
7) Set value as **2**. The value 2 denotes Read Committed.
8) Click **Apply** and then click **OK**.
9) Repeat steps 5-8 for **LiveCycle - DB2 - RM_DS** with JNDI name **EDC_DS**.
10) In the Messages box at the top of the page, click **Save directly to master configuration**.
11) Restart WebSphere.

Configuring the Oracle data source

Configuring the Oracle data source requires you to install the Oracle database drivers, create an Oracle JDBC provider on WebSphere, create the data source on WebSphere, and then configure the corresponding connection pool.

Install the Oracle database driver

1) For each WebSphere Application Server instance, in the *[appserver root]* directory, create a directory named *db_driver*.
2) Copy the ojdbc6.jar for JDK 1.6 driver file from the *[DVD_root]*/third_party/db/oracle directory to the directory created in step 1.

Create the Oracle JDBC provider

1) On a WebSphere Application Server instance, in the WebSphere Administrative Console navigation tree, click **Environment**>**WebSphere Variables** and, in the right pane, click **ORACLE_JDBC_DRIVER_PATH**.
2) Under General Properties, in the **Value** box, type the path to the ojdbc6.jar file you created in Configuring the Oracle data source and then click **OK**.
3) Repeat steps 1 to 2 for each WebSphere Application Server instance, inserting the appropriate path to the db_driver directory for the node on which the WebSphere Application Server instance resides.
4) Click **Save directly to master configuration**.
5) In the navigation tree, click **Resources**>**JDBC**>**JDBC Providers**.
6) In the drop-down list above the table, select **Cluster=<cluster_name>**as the scope and then click **New**.
7) In the Step 1 pane, set the following configuration and then click **Next**:
   - In the **Database type** list, select **Oracle**.
   - In the **Provider type** list, select **Oracle JDBC Driver**.
   - In the **Implementation type** list, select **Connection pool data source**.
8) In the Step 2 pane, accept the default database class path and then click **Next**.
9) In the Step 3 pane, click **Finish** and then click **Save directly to master configuration**.

Create the Oracle JDBC data source

1) In the navigation tree, click **Resources**>**JDBC**>**JDBC Providers** and, in the right pane, click the provider you created in Configuring the Oracle data source section.
2) Under Additional Properties, click **Data sources** and then click **New**.
3) In the Step 1 pane, set the following configurations and then click **Next**:
   - In the **Data source name**box, type `Livecycle - oracle - IDP_DS`.
   - In the **JNDI name** box, type `IDP_DS`.
   - In the list, under Component-Managed Authentication and XA Recovery Authentication, select the authentication alias created for this data source in CreatingaJ2Cauthenticationaliasforthedatabase
4) In the Step 2 pane, type the following line in the **URL** box and then click **Next**:

   `jdbc:oracle:thin:@<server_host>:<port>:<SID>`

where <server_host> is the IP address of the database server, <port> is the port on which the database is listening (default 1521), and <SID> is the service ID of the database.

5) In the Step 3 pane, click **Finish** and then click **Save directly to master configuration**.
6) Select the data source you just created to modify additional parameters and set the following configuration options:
   – In the **Container-managed authentication alias** list, select the authentication alias created for this data source in CreatingaJ2Cauthenticationaliasforthedatabase.
   – In the **Mapping-configuration alias** list, select **DefaultPrincipalMapping**.
7) Click **OK** or **Apply**, and then click **Save directly to master configuration**.

Configure LiveCycle - oracle - IDP_DS connection pools

1) In the navigation tree, click **Resources**>**JDBC** >**JDBC Providers** and, in the right pane, click the Oracle JDBC driverdata source. See,*create the Oracle JDBC provider*.
2) Under Additional Properties, click **Data sources** and, in the right pane, click **Livecycle - oracle - IDP_DS**.
3) On the next screen, under Additional Properties, click **Connection Pool Properties** and, in the **Maximum connections** box, type `30`.
4) Click **OK** or **Apply**, and then click **Save directly to master configuration**.

Configure the custom property for Oracle

1) In the navigation tree, click **Resources** > **JDBC**>**Data sources**and, in the right pane, click the data source that you created in *To create the Oracle JDBC data source*section.
2) Under Additional Properties, click **Custom properties**and then click **New**.
3) In the **Name** box, type `useRRASetEquals` and in the **Value** box, type `true`.
4) Click **OK** or **Apply** and then click **Save directly to master configuration**.

Create the Oracle JDBC data source for Document Security

NOTE: This section applies only if you have Document Security installed.

1) In the navigation tree, click **Resources**>**JDBC**>**JDBC Providers** and, in the right pane, click the provider you created in *create the Oracle JDBC provider* section.
2) Under Additional Properties, click **Data sources** and then click **New**.
3) In the Step 1 pane, set the following configurations and then click **Next**:
   – In the **Data source name** box, type `Livecycle - oracle - RM_DS`.
   – In the **JNDI name** box, type `EDC_DS`.
   – In the list under Component-Managed Authentication and XA Recovery Authentication Alias, select the authentication alias created for this data source in CreatingaJ2Cauthenticationa-liasforthedatabase.
4) In Step 2 pane, type the following line in the **URL** box and then click **Next**:

   `jdbc:oracle:thin:@<server_host>:<port>:<SID>`

where <server_host> is the IP address of the database server, <port> is the port on which the database is listening (default 1521), and <SID> is the service ID of the database.

5) In the Step 3 pane, click **Finish** and then click **Save directly to master configuration**.
6) Select the data source you just created to modify additional parameters and set the following configuration options:
   – In the **Container-managed authentication alias** list, select the authentication alias created for this data source in CreatingaJ2Cauthenticationaliasforthedatabase.
   – In the **Mapping-configuration alias** list, select **DefaultPrincipalMapping**.
7) Click **OK** and then click **Save directly to master configuration**.

Configure LiveCycle - oracle - RM_DS connection pools for Document Security

NOTE: This section applies only if you have Document Security installed.

1) In the navigation tree, click **Resources**> **JDBC**>**JDBC Providers** and, in the right pane, click the Oracle JDBC driver provider created in *To create the Oracle JDBC provider* section.
2) Under Additional Properties, click **Data sources** and, in the right pane, click **Livecycle - oracle - RM_DS**.
3) On the next screen, under Additional Properties, click **Connection Pool Properties** and set the properties as follows:
   – In the **Maximum connections**box, enter 20.
   – In the **Minimum connections**box, enter 1.
4) Click **OK** or **Apply**, and then click **Save directly to master configuration**.

Configure the custom property for Oracle:

1) In the navigation tree, click **Resources** > **JDBC**>**Data sources**and, in the right pane, click the data source that you created in *To create the Oracle JDBC data source for Document Security*section.
2) Under Additional Properties, click **Custom properties**and then click **New**.
3) In the **Name** box, type `useRRASetEquals` and in the **Value** box, type `true`.
4) Click **OK** or **Apply** and then click **Save directly to master configuration**.

Configuring the SQL Server data source

Configuring the SQL Server data source requires you to install the SQL Server database drivers, create a SQL Server JDBC provider on WebSphere, create the data source on WebSphere, and then configure the corresponding connection pool.

Install the SQL Server database driver

- (for IBM JDK 6) If you have not done so already, copy the SQL Server JDBC Driver from [*aem-forms root*]\lib\db\mssql\java6 to the [*appserver root*]\lib\ directory.

  (for IBM JDK 7) If you have not done so already, copy the SQL Server JDBC Driver from [aem-forms root]\lib\db\mssql to the [appserver root]\lib\ directory.

NOTE: Make note of the directory location where you install the driver on your system.

Create the SQL Server JDBC provider

1) In the WebSphere Administrative Console navigation tree, click **Environment** > **WebSphere Variables** and, in the right pane, click MICROSOFT_JDBC_DRIVER_PATH..
2) Under **General Properties**, in the **Value** box, type the path to the sqljdbc.jar file that you created and then click **OK**.
3) In the **Messages** box, click **Save directly to master configuration**.
4) In the navigation tree, click **Resources**>**JDBC**>**JDBC Providers**.
5) In the **Scope** drop-down list in the right pane, select **Cluster=<cluster name>**as the level, and then click **New**.
6) In the **Create new JDBC provider** pane, set the following configurations and then click **Next**:
   - In the **Database type** list, select `SQL Server`.
   - In the **Provider Type** list, select `Microsoft SQL Server JDBC Driver`.
   - In the **Implementation type**list, select `Connection Pool Data Source`.
   - In the **Name** box, type `Microsoft SQL Server JDBC Driver`, or accept the default value.
7) In the **Enter database class path information** pane, replace the existing entry with one of the following, and then click **Next**:
   - `${MICROSOFT_JDBC_DRIVER_PATH}/sqljdbc.jar`

   NOTE: If you have set the WebSphere variable MICROSOFT_JDBC_DRIVER_PATH, the database class path information is populated automatically.
8) In the **Summary** pane, click **Finish** and then click **Save directly to master configuration**.

Create the SQL Server data source for LiveCycle

Follow the steps below to create the SQL Server data source for your application server version.

1) In the navigation tree, click **Resources**>**JDBC > JDBC Providers** and, in the right pane, click the provider that you created in *Create the SQL Server JDBC provider* section.
2) Under **Additional Properties**, click **Data sources** and then click **New**.
3) In the **Enter basic data source information pane**, set the following configurations and then click **Next**:
   - In the **Data source name** box, type`Livecycle - SQLServer - IDP_DS`.
   - In the **JNDI name** box, type `IDP_DS`.
4) In the**Enter database specific properties for the data source** pane, enter the database name, server name, and port.
5) In the **Setup security aliases** pane, set the following, and click **Next**.
   - In the **Component managed authentication alias** list, select the authentication alias that you created for this data source in *To create a J2C authentication configuration for the data source* section.
   - In the **Mapping-configuration alias** list, select **DefaultPrincipalMapping**.

- In the **Container managed authentication alias** list, select the authentication alias that you created for this data source in *To create a J2C authentication configuration for the data source* section.

6) In the**Summary** pane, click **Finish**, and then click **Save directly to master configuration**.
7) Set the data store helper class for the data source. Do the following tasks:
   - In the navigation tree, click **Resources** > **JDBC** > **Data sources**and, in the right pane, click the data source that you created.
   - In the next screen, under **Data store helper class name**, select **Specify a user-defined data store helper**, and replace the existing entry with the following text:

     `com.ibm.websphere.rsadapter.GenericDataStoreHelper`
8) Change the statement cache size. Do the following tasks:
   - In WebSphere Administrative Console, click **JDBC > Data sources**.
   - Click the data source you just created and under**Additional Properties**, click **WebSphere Application Server data source properties**.
   - Change the value of the **Statement cache size** field to `80`.
   - Click **OK** or **Apply** and the click **Save directly to master configuration**.

Configure LiveCycle - SQLServer - IDP_DS connection pools

1) In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the provider that you created earlier
   - **Microsoft SQL Server JDBC Driver**.
2) Under **Additional Properties**, click**Data sources** and then select **Livecycle - SQLServer - IDP_DS**.
3) On the next screen, under **Additional Properties**, click **Connection Pool Properties** and, in the **Maximum connections** box, type`30`.
4) 9. Click **OK** or **Apply** and then click **Save directly to master configuration**.

Configure the custom property for SQL Server

1) In the navigation tree, click **Resources** > **JDBC** > **Data** sources and, in the right pane, click the data source that you created in *Create the SQL Server data source for LiveCycle* section.
2) Under **Additional Properties**, click **Custom properties** and then click **New**.
3) In the **Name** box, type `useRRASetEquals` and in the **Value** box, type `true`.
4) Click **OK** or **Apply** and then click **Save directly to master configuration**.

To create AEM_DS datasource

1) In the navigation tree, click **Resources** > **JDBC**> **JDBC Providers** and, in the right pane, click the provider that you created in *Create the SQL Server JDBC provider section*.
2) Under Additional Properties, click **Data sources** and then click **New**.
3) In the **Enter basic data source information** pane, set the following configuration and then click **Next**.

- In the **Data source name** box, type `Livecycle - SQLServer - AEM_DS`.
- In the the **JNDI name** box, type `AEM_DS`.

4) In the **Enter database specific properties for the data source** pane, type a database name, server name, and port.
5) In the **Setup security aliases** pane, set the following, and click **Next**.
   - In the list under **Component-managed authentication alias**, select the authentication alias created for this data source in CreatingaJ2Cauthenticationaliasforthedatabase.
   - In the **Mapping-configuration alias** list, select **DefaultPrincipalMapping**.
   - In the **Container-managed authentication alias** list, select the authentication alias created for this data source in CreatingaJ2Cauthenticationaliasforthedatabase.
6) In the **Summary** pane, click **Finish**, and then click **Save directly to master configuration**.
7) Set the data store helper class for the data source. Do the following tasks:
   - In the navigation tree, click **Resources** > **JDBC** > **Data sources** and, in the right pane, click the data sourcethat you created.
   - In the next screen, under **Data store helper class name**, select **Specify a user-defined data store helper**, andreplace the existing entry with the following text:**com.ibm.websphere.rsadapter.GenericDataStoreHelper**
8) Change the statement cache size. Do the following tasks:
   - In WebSphere Administrative Console, click **JDBC** > **Data sources**.
   - Click the data source you just created and under **Additional Properties**, click **WebSphere Application Serverdata source properties**.
   - Change the value of the **Statement cache size** field to **80**.
   - Click **OK** or **Apply** and the click **Save directly to master configuration**.

Configure LiveCycle - SQLServer - AEM_DS connection pools

1) In the navigation tree, click **Resources**>**JDBC**>**JDBC Providers** and, in the right pane, click the provider that you created earlier **Microsoft SQL Server JDBC Driver**..
2) Under Additional Properties, click **Data sources** and, in the right pane, click **Livecycle - SQLServer - AEM_DS**.
3) On the next screen, under **Additional Properties**, click **Connection Pool Properties** and, in the **Maximumconnections** box, type **30**.
4) Click **OK** or **Apply**, and then click **Save directly to master configuration**.

Configure the custom property for SQL Server

1) In the navigation tree, click **Resources** > **JDBC**>**Data sources**and, in the right pane, click the data source that you created in *Create the SQL Server data source for LiveCycle section*.
2) Under Additional Properties, click **Custom properties**and then click **New**.
3) In the **Name** box, type `useRRASetEquals` and in the **Value** box, type `true`.
4) Click **OK** or **Apply** and then click **Save directly to master configuration**.

Create SQL Server data source for Document Security

Follow the steps below to create the SQL Server data source for your application server version.

1) In the navigation tree, click **Resources**>**JDBC > JDBC Providers** and, in the right pane, click the provider that you created in *Create the SQL Server JDBC provider* section.
2) Under **Additional Properties**, click **Data sources** and then click **New**.
3) In the **Enter basic data source information pane**, set the following configurations and then click **Next**:
   - In the **Data source name** box, type`Livecycle - SQLServer - RM_DS`.
   - In the **JNDI name** box, type `EDC_DS`.
4) In the**Enter database specific properties for the data source** pane, in the **Data store helper class name** box, replace the existing entry with the following:
   `com.ibm.websphere.rsadapter.GenericDataStoreHelper`
5) In the **Setup security aliases** pane, set the following, and click **Next**.
   - In the **Component managed authentication alias** list, select the authentication alias that you created for this data source in *To create a J2C authentication configuration for the data source* section.
   - In the **Mapping-configuration alias** list, select **DefaultPrincipalMapping**.
   - In the **Container managed authentication alias** list, select the authentication alias that you created for this data source in *To create a J2C authentication configuration for the data source* section.
6) In the**Summary** pane, click **Finish**, and then click **Save directly to master configuration**.
7) Change the statement cache size. Do the following tasks:
   - In WebSphere Administrative Console, click **JDBC > Data sources**.
   - Click the data source you just created and under**Additional Properties**, click **WebSphere Application Server data source properties**.
   - Change the value of the **Statement cache size** field to `80`.
   - Click **OK** or **Apply** and the click **Save directly to master configuration**.

Configure LiveCycle - SQLServer - RM_DS connection pools

1) In the navigation tree, click **Resources** > **JDBC** > **JDBC Providers** and, in the right pane, click the provider that you created earlier
   - **SQL Server Provider**.
2) Under **Additional Properties**, click**Data sources** and then select **Livecycle - SQLServer - RM_DS**.
3) On the next screen, under **Additional Properties**, click **Connection Pool Properties** and, in the **Maximum connections** box, type`20`.
4) Click **OK** or **Apply** and then click **Save directly to master configuration**.

Configure the custom property for SQL Server

1) In the navigation tree, click **Resources** > **JDBC** > **Data sources** and, in the right pane, click the data source that you created.
2) Under **Additional Properties**, click **Custom properties** and then click **New**.
3) In the **Name** box, type `useRRASetEquals` and in the **Value** box, type `true`.
4) Click **OK** or **Apply** and then click **Save directly to master configuration**.

Configure integrated security on Windows

1) In the navigation tree, click **Resources**>**JDBC**>**Data Sources** and, in the right pane, click **IDP_DS**.
2) In the right pane, under Additional Properties, click **Custom Properties**, and on the next screen, click **integratedSecurity**.
3) On the next screen, under General Properties, type `true` in the**Value** box.
4) In the navigation tree, click **Resources**>**JDBC**>**Data Sources** and, in the right pane, click **Livecycle - SQLServer - RM_DS**.
5) In the right pane, under Additional Properties, click **Custom Properties**, and on the next screen, click **integratedSecurity**.
6) On the next screen, under General Properties, type `true` in the**Value** box.
7) Click **Apply** and then click **Save directly to master configuration**.
8) On the computer where WebSphere is installed, add the sqljdbc_auth.dll file to the Windows systems path (C:\Windows). The sqljdbc_auth.dll file is in the same location as the Microsoft SQL JDBC 4.0 driver installation (default is *[InstallDir]*/sqljdbc_3.0/enu/auth/x86).
9) Modify the *Log On As* property of the Windows service that starts the WebSphere Application Server *[node name]* by doing the following tasks:
   – Click **Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Services**.
   – Right click **[node name]** and select **Properties**.
   – On the **Log On** tab, select **This account** and select a valid user account other than Local System, then click **OK**.
10) Change SQL Server's Security from **Mixed mode** to **Windows Authentication only**.

6.4. Next steps

After you configure your WebSphere Application Server cluster, do the following tasks:

- Configure the LiveCycle EAR files by using Configuration Manager. (See "ConfiguringLiveCyclefor-Deployment".)
- Choose one of these ways to deploy the LiveCycle EAR files to your WebSphere Application Server cluster:
  – **Automatically:** Use Configuration Manager. (See "ConfiguringLiveCycleforDeployment".)
  – **Manually:** See "Appendix-ManuallyDeployingtoWebSphere".

7. Manually Deploying to WebSphere

7.1. About deploying AEM Forms on JEE modules

Before you deploy AEM Forms on JEE, ensure that you completed these tasks:

- Run Configuration Manager to configure AEM Forms on JEE modules according to your system and application server requirements. To add a module to your deployment, you can run Configuration Manager to make the changes and then redeploy the updated EAR file.

  If you are deploying AEM Forms on JEE for the first time, initialize the database by using Configuration Manager after you deploy the EAR files.

  If you are using an external web server, see your web server documentation for information about the configuration that is required to allow access to the application server.

Summary of deployable components

During the deployment process, you need to deploy the following components for AEM Forms on JEE:

- adobe-livecycle-native-websphere-*[OS]*.ear
- adobe-livecycle-websphere.ear
- adobe-workspace-client.ear

After AEM Forms on JEE is configured using Configuration Manager, these files are located in the *[aem-forms root]*/configurationManager/export/ directory.

7.2. Deploying to WebSphere

Deploy AEM Forms on JEE modules to WebSphere by deploying the component EAR files to the application server using the WebSphere Administrative Console.

Before deploying to WebSphere, start the application server or the cluster. After you deploy the required components, stop and restart the application server or cluster before you start any services.

To deploy the EAR files:

1) *(WebSphere 8.x or 9.x)* In the WebSphere Administrative Console navigation tree, click **Applications** > **Install New Application**.

   *In the WebSphere Administrative Console navigation tree, click **Applications > New Application.***

2) *(WebSphere 8.x or 9.x)*In the right pane, select **Remote file system** or **Local File System.**

*In the right pane, click **New Enterprise Application** and then select **Remote file system** or **Local File System.***

3) Click **Browse**, navigate to one of the EAR files in Summaryofdeployablecomponents, and select the EAR file.
4) Select **Show all installation options and parameters**and expand **Choose to generate default bindings and mappings**.
5) Select **Generate Default Bindings** and click **Next**.
6) In the left column of the Summary pane on the right, select the last step and click **Finish**.
7) When the EAR file is installed successfully, in the **Messages** box, click **Save directly to Master Configuration**.
8) Repeat these steps for each of the EAR files in Summaryofdeployablecomponents.

7.3. Starting the application

After deploying the module, you need to start the applications. When the red "X" beside the name of the application changes to a green arrow, the application has been deployed and started successfully. WebSphere displays an error message if it cannot start the application.

For information about WebSphere error messages, see your WebSphere Application Server documentation.

To start an application in WebSphere:

1) (WebSphere 8.x or 9.x) In the WebSphere Administrative Console navigation tree, click **Applications** > **Enterprise Applications**.

   *In the WebSphere Administrative Console navigation tree, click **Applications > Application Types > WebSphere Enterprise applications.***
2) Select any or all of the AEM Forms on JEE applications that you want to start and click **Start**. The red "X" beside the status of each application changes to a green arrow, indicating that the application is running.

7.4. Launch configuration manager to configure AEM Forms for deployment

Further, you need to do the following:

- Initialize AEM Forms database
- Deploy AEM Forms components
- Validate AEM Forms component deployment
- Configure AEM Forms components

Launch the configuration manager to configure AEM Forms for deployment. For more information, see the chapter Configuring AEM Forms for deployment.

8. Post-deployment tasks

8.1. General tasks

Install Microsoft Visual C++ redistributable library

AEM Forms Configuration Manager installs Microsoft Visual C++ redistributable library only on the master node of the cluster. You have to manually install the library on all slave nodes. Perform the following steps on all slave nodes of the cluster:

1) Open the command prompt.
2) Navigate to the [Appserver_DVD]\third_party\msvcredist_2010_SP1 folder.
3) Run the following command to install Microsoft Visual C++ redistributable library:
   (For English Language) `vcredist_x86.exe /q /lang 1033`
   (For French Language) `vcredist_x86.exe /q /lang 1036`
   (For German Language) `vcredist_x86.exe /q /lang 1031`
   (For Japanese Language) `vcredist_x86.exe /q /lang 1041`

Configure Allowed Referrers

When you run Configuration Manager, the default host, IPv4 address, IPv6 address, loopback address, and localhost address are added to the Allowed Referrer list. These addresses are added only for the machine where Configuration Manager is run. For AEM Forms on JEE cluster, manually add all other cluster nodes to the list:

1) In administration console, click **Settings** > **User Management** > **Configuration** > **Configure Allowed Referrer URL's**. The Allowed Referrer list appears at the bottom of the page. The default URL of administration console is http://[server]:[host]/adminui.
2) To add an allowed referrer:
   a) Type a host name or IP address in the Allowed Referrers box. To add more than one allowed referrer at a time, type each host name or IP address on a new line. Provide hostName and IP address of all cluster nodes/load balancer.
   b) In the HTTP Port and HTTPS Ports boxes, specify the ports to allow for HTTP, HTTPS, or both. If you leave those boxes empty, the default ports (port 80 for HTTP and port 443 for HTTPS) are used. If you enter `0` (zero) in the boxes, all ports on that server are enabled. You can also enter a specific port number to enable only that port.
   c) Click Add.

3) Click **Save**.

   If the Allowed Referrer List is empty, the CSRF feature stops working and the system becomes insecure.

4) After changing the Allowed Referrer list, restart the AEM Forms JEE cluster.

Configure the serialization agent

AEM Forms requires the `sun.util.calendar` package to be whitelisted. Perform the following steps to add the package to the whitelist:

1) Open the Web Console in a browser window. The default URL is http://[server]:[port]/system/console/configMgr.
2) Search and open Deserialization Firewall Configuration.
3) In the whitelist field, add the `sun.util.calendar` package and click Save.

Setting the correct date, time, and time zone

Setting the correct date, time, and time zone on all servers connected to your AEM Forms on JEE environment will ensure that time-dependent modules, such as Digital Signatures and Acrobat Reader DC extensions function correctly. For example, if a signature appears to have been created in the future, it will not validate.

Servers that require synchronization are database servers, LDAP servers, HTTP servers, and J2EE servers.

Configure URL and port number for client SDK

Perform the following section, only if you have installed CRX repository:

The default URL of AEM Forms client SDK (CSDK) is http://localhost:8080. Change the default URL to the current URL of your AEM Forms environment. The current URL is required to enable and configure authentication between AEM configuration manager and CRX-repository:

1) Open the configuration manager URL, http://<server>:<port>/lc/system/console/configMgr, in a browser window.
2) Search and open the Adobe LiveCycle Client SDK Configuration service for editing.
3) In the Server URL field, specify current URL of your AEM Forms environment, and click Save.

Boot delegate RSA and BouncyCastle libraries

Perform the following section, only if you have installed CRX repository:

AEM Forms requires RSA and BouncyCastle libraries to be installed with AEM Forms add-on package. Perform the following steps to boot delegate these libraries:

1) Stop the AEM instance.
2) Navigate to the [AEM installation directory]\crx-repository\launchpad\ folder and open the sling.properties file for editing.

3) Add the following properties to the sling.properties file:

```
sling.bootdelegation.class.com.rsa.jsafe.provider.JsafeJCE=com.rsa.*sling.bootdelegation.class.org.bouncycastle.jce.provider.BouncyCastleProvider=org.bouncycastle.*
```

4) Save and close the file. Restart the AEM instance.

NOTE: Before restarting the AEM Forms server, wait until the ServiceEvent REGISTERED and ServiceEvent UNREGISTERED messages stop appearing in the <crx-repository>/error.log file and the log is stable.

Restart the application server

When you first deploy AEM Forms on JEE, the server is in a deployment mode in which most modules are in memory. As a result, the memory consumption is high and the server is not in typical production state. You must restart the application server to get the server back into a clean state.

NOTE: You may skip to restart the AEM Forms on JEE server, if you have restarted the server after configuring CRX clustering or after updating Allowed Referrer list

Verify the deployment

You can verify the deployment by logging in to Administration Console. If you log in successfully, it means AEM Forms on JEE is running on the application server and the default user is created in the database. To verify the CRX repository deployment, access the CRX welcome page.

You can review the application server log files to ensure that components were deployed correctly or to determine the cause of any deployment issues you may encounter.

Accessing administration console

1) Type the following URL in a web browser:

   `http://[hostname]:[port]/adminui`

   For example: `http://localhost:9080/adminui`

2) If you have upgraded to AEM Forms on JEE, enter the same administrator username and password as that of your previous installation. In case of a fresh installation, enter the default username and password.

3) After you log in, click **Services** to access the service administration pages or click **Settings** to access the pages on which you can administer settings for different modules.

Accessing OSGi Management Console

OSGi console provides a way to manage OSGi bundles and services configurations. To, access the OSGi Management console:

1) Type the following URL in a web browser:

   `http://[hostname]:[port]/lc/system/console`

2) Enter the CRX Administrator username and password. The default username and password for logging in is admin and admin (same as CRX Administrator).

NOTE: You cannot log into OSGi Management Console using the credentials of AEM Forms on JEE Administrator or AEM Super Administrator.

3) After you log in, you can access various components, services, bundles, and other configurations.

View the log files

Events, such as run-time or startup errors, are recorded to the application server log files. If you have problems deploying to the application server, you can use the log files to find the problem. You can open the log files using any text editor.

The following log files are located in the *[appserver root]*/profiles/*[profilename]*/logs/*[server name]* directory:

- SystemErr.log
- SystemOut.log
- startServer.log

Following CRX log files are located at [*CRX_home*]/logs

- error.log
- audit.log
- access.log
- request.log
- update.log

NOTE: Each time AEM Forms on JEE starts, the following error appears in the log:

```
FacesConfigur E org.apache.myfaces.config.FacesConfigurator
configureRenderKits failed to configure class
com.adobe.framework.jsf.renderkit.SecureInputRenderer
java.lang.ClassCastException
```

This error occurs due to a different version of the IBM JSF engine expected by WebSphere. This is a known issue and this error can be safely ignored.

Configure Author and Publish instance

Perform the following tasks to configure Author and Publish instance only if you have installed and configured the CRX repository:

Configure the Author instance

Author instance is embedded within the AEM Forms on JEE server. It implies that you do not need to make any configuration updates to the Author instance. The instance inherits all configuration settings from the AEM Forms on JEE instance.

Configure the Publish instance

You must run separate author and publish instances.You can configure the instances on different machines.

NOTE: The cluster topology is not recommended for the publish instance. Use a single publish instance or configure a farm of publish instances.

NOTE: By default, the publish instance is configured to run the mode similar to corresponding author instance. The mode can be TarMK, MongoMK, or RDBMK. Run the publish instance on TarMK mode.

Configure the Publish Node

1) Create a new appserver profile for the publish instance on the same or on a different machine.
2) On the author instance, navigate to the [*aem-forms root*]/configurationManager/export/ directory.
3) Copy the adobe-livecycle-cq-publish.ear file and deploy it to the appserver profile created in step 1.
4) Copy the content of the [*aem-forms root*]/configurationManager/export/crx-quickstart directory to the file server for the publish instance.
5) **(If author instance is configured to run RDBMK)** Delete the following files from the install directory copied to the publish instance:
   – org.apache.jackrabbit.oak.plugins.document.DocumentNodeStoreService.cfg
   – org.apache.sling.datasource.JNDIDataSourceFactory-oak.cfg
6) Start the publish server with `-Dcom.adobe.livecycle.crx.home=<location for crx-repository>` parameter, where `<location for crx-repository>` is the location where you copied the crx-repository directory for the publish instance. For example, if the content of the cq-quickstart directory are copied to the C:\CM-publish\crx-repository directory, then the <location for crx-repository> parameter will be Dcom.adobe.livecycle.crx.home=C:\CM-publish\crx-repository.

NOTE: If author and publish instances are on the same machine, ensure that you start the publish instance using a different port.

IMPORTANT: Ensure that the CRX repository path does not contain spaces.

Communicating between the Author and Publish instances

Enable two-way communication between Author and Publish instances:

Define Publish instance URL

1) Go to http://<*authorHost*>:<*authorPort*>/lc/etc/replication/agents.author/publish.html.
2) Click **Edit**. The Agent Settings dialog opens.
3) Click the **Transport** tab and specify the URL to the publish server in the URI field.
   http://<publishHost>:<publishPort>/lc/bin/receive?sling:authRequestLogin=1
   NOTE: If there are multiple publish instances managed by a Load Balancer, specify the URL to the load balancer in the URI field.
4) Click **OK**.

NOTE: For author clusters, these steps need to be performed on one author instance (preferably a master instance).

Define publish instance URL for ActivationManagerImpl

1) Go to http://<*authorHost*>:<*authorPort*>/lc/system/console/configMgr. The default username and password for logging in are admin and admin (same as CRX Administrator).
2) Find and click the Edit icon next to the `com.adobe.livecycle.content.activate.impl.ActivationManagerImpl.name` setting.
3) In the ActivationManager Publish URL field, specify the URL for the corresponding publish instance.
4) Click **Save**.

Configure reverse replication queue

1) Go to http://<*authorHost*>:<*authorPort*>/lc/etc/replication/agents.author/publish_reverse.html.
2) Click **Edit**. The Agent Settings dialog opens.
3) Click the **Transport** tab and specify the URL to the corresponding publish server in the URI field.

   NOTE: If there are multiple publish instances managed by a Load Balancer, specify the URL to the load balancer in the URI field.
4) Click **OK**.

Define author instance URL

1) Go to http://<*publishHost*>:<*publishPort*>/lc/system/console/configMgr. The default username and password for logging in are admin and admin (same as CRX Administrator).
2) Find and click the Edit icon next to the `com.adobe.livecycle.content.activate.impl.VersionRestoreManagerImpl.name` setting.
3) In the VersionRestoreManager Author URL field, specify the URL for the corresponding author instance.

   NOTE: If there are multiple author instances managed by a Load Balancer, specify the URL to the load balancer in the VersionRestoreManager Author URL field.
4) Click **Save**.

Configure IPv6 implementation

NOTE: Perform these steps only if the machine/server is using an IPv6 address.

To map the IPv6 address to a hostname on the server and client machines:

1) Navigate to the C:\Windows\System32\drivers\etc directory.
2) Open the `hosts` file in a text editor.
3) Add a mapping for the IPv6 address to a host name. For example:
   `2001:1890:110b:712b:d1d:9c99:37ef:7281 <ipv6_hostname>`
4) Save and close the file.

Ensure that you use the mapped host name instead of the IPv6 address to access the machine.

Install Japanese fonts for Adobe Reader

If your document fragments use Japanese fonts, you must install the Japanese Language Support Package for Adobe Reader. Otherwise, your letters and forms will not render and function properly. For installing language packs, visit the downloads page for Adobe Reader.

Upgrading to Workbench

Once you have completed your AEM Forms on JEE server upgrade and verified that it is working properly, install the new version of Workbench in order to continue creating and modifying your AEM Forms on JEE applications.

Configure CSIv2 inbound transport

On the default Global Security enabled installation of IBM WebSphere, CSIv2 inbound transport option is set to SSL-required. This configuration causes Output and Forms components to fail. Ensure that you change CSIv2 inbound transport option to SSL-Supported: To change the option:

1) Log in to IBM WebSphere administration console.
2) Expand **Security**, and then click **Global security**.
3) In the Authentication section, expand **RMI/IIOP security**, and then click **CSIv2 inbound communications**
4) In CSIv2 Transport Layer section, set value of **Transport** to **SSL-Supported**.
5) Click **Apply**.

Isolating JBoss Clusters

There are a lot of JBoss services that create multiple JGroup channels services. These channels should only communicate with specific channels. Isolate JGroups clusters from other clusters on the network to ensure that the communication happens only with specific channels. See application server documentation for steps to isolate JBoss clusters.

Enabling JMS for JBoss

JMS services are disabled, by default. Perform the following steps to enable JMS services:

1) Copy the following tags from standalone_full.xml to the lc_turnkey.xml.

```
<extension module="org.jboss.as.messaging">....</extension>
<subsystem xmlns="urn:jboss:domain:messaging:1.4">  </subsystem>
```

2) Run the add-user.bat script to create an application user. Add the application user to the Guest group.

   NOTE: The JMS DSC component requires a connection username and password. Ensure that the newly added application user has permissions to use JMS Queue/Topic for Send/Receive operation.

NOTE: By default, the lc_turnkey.xml file the `security-setting match="#">.....</security-settings>` snippet has a guest role with ready JMS Send/Receive privileges. You must create an application user.

3) Change the JMS DSC configuration to include the newly created application user.
4) In the JMS Service configuration, change the org.jnp.interfaces.NamingContextFactory to org.jboss.as.naming.InitialContextFactory.

Migrate adaptive forms and Correspondence Management assets

The migration utility makes assets of earlier versions compatible with AEM 6.3 forms. You can download the utility from AEM package share. For detailed steps, see https://helpx.adobe.com/aem-forms/6-3/migration-utility.html

.

Reconfigure analytics and reports

In AEM 6.3 Forms, traffic variable for source and success event for impression are not available. So, when you upgrade to AEM 6.3 Forms, AEM Forms stops sending data to Adobe Analytics server and analytics reports for adaptive forms and adaptive document are not available. Moreover, AEM 6.3 Forms introduces traffic variable for the version of form analytics and success event for the amount of time spent on a field. So, reconfigure analytics and reports for your AEM Forms environment. For detailed steps, see https://helpx.adobe.com/content/help/en/aem-forms/6-3/configure-analytics-forms-documents.html.

Methods to calculate average fill time for forms and average read time for adaptive documents have changed. So, when you upgrade to AEM 6.3 forms, the old data from previous AEM Forms release for these metrics is available only in Adobe Analytics. It is not visible in AEM Forms analytics reports. For these metrics, AEM Forms analytics reports display data which is captured after performing the upgrade.

Configure the ContentRepositoryConnector service

By default, the ContentRepositoryConnector service is configured to use URL http://localhost:8080/lc/crx/server/. Perform the following steps to configure the service for your environment:

1) Log in to AEM Forms Admin UI using credentials administrator/password. The default URL of Admin UI is http://[IP]:[Port]/adminui.
2) Navigate to Services > Application and Services > Service Management.
3) Search and open the ContentRepositoryConnector service for editing.
4) Open the Configuration tab and replace the default URL in the Experience Management Server field with the URL of your environment.

IP

IP address of the machine on which application server is running.

Port

Port number which AEM Forms is using. The default port number for JBoss, WebLogic, and WebSphere 8080, 8001, and 9080, respectively.

8.2. Verify the AEM Forms cluster

1) View the Gemfire.log file, located in the directory appropriate to your application server:
   – *WebSphere: [lc_temp_dir]*/adobews_*/Caching.
   where adobe_temp_dir is the temporary directory during EAR configuration using Configuration Manager.
2) Messages such as the following confirm that the cache is connected to all servers of the cluster:

```
[info 2008/01/22 14:24:31.109 EST GemfireCacheAdapter <UDP mcast
receiver> nid=0x5b611c24] Membership: received new view
[server-0:2916|1] [server-0:2916/2913, server-1:3168/3165]
[info 2008/01/22 14:24:31.125 EST GemfireCacheAdapter <View Message
Processor> nid=0x7574d1dc] DMMembership: admitting member
<server-1:3168/3165>; now there are 2 non-admin member(s)
```

NOTE: Ensure that the number of non-admin members (two in the example log entry above) matches the number of members in your cluster. A discrepancy indicates that some members of the cluster are not connected to the cache.

8.3. Verify the CRX Cluster

1) Go to http://<authorHost>:<authorPort>/lc/. Login with OSGi Management Console user credentials. The default credentials are administrator/password.
2) Create an asset on one node and verify it on the other node.

8.4. Configure Author and Publish instance

Perform the following tasks to configure Author and Publish instance only if you have installed and configured the CRX repository:

Configure the Author instance

Author instance is embedded within the AEM Forms on JEE server. It implies that you do not need to make any configuration updates to the Author instance. The instance inherits all configuration settings from the AEM Forms on JEE instance.

Configure the Publish instance

You must run separate author and publish instances.You can configure the instances on different machines.

NOTE: The cluster topology is not recommended for the publish instance. Use a single publish instance or configure a farm of publish instances.

NOTE: By default, the publish instance is configured to run the mode similar to corresponding author instance. The mode can be TarMK, MongoMK, or RDBMK. Run the publish instance on TarMK mode.

Configure the Publish Node

1) Create a new appserver profile for the publish instance on the same or on a different machine.
2) On the author instance, navigate to the [*aem-forms root*]/configurationManager/export/ directory.
3) Copy the adobe-livecycle-cq-publish.ear file and deploy it to the appserver profile created in step 1.
4) Copy the content of the [*aem-forms root*]/configurationManager/export/crx-quickstart directory to the file server for the publish instance.
5) **(If author instance is configured to run RDBMK)** Delete the following files from the install directory copied to the publish instance:
   – org.apache.jackrabbit.oak.plugins.document.DocumentNodeStoreService.cfg
   – org.apache.sling.datasource.JNDIDataSourceFactory-oak.cfg
6) Start the publish server with `-Dcom.adobe.livecycle.crx.home=<location for crx-repository>` parameter, where `<location for crx-repository>` is the location where you copied the crx-repository directory for the publish instance. For example, if the content of the cq-quickstart directory are copied to the C:\CM-publish\crx-repository directory, then the <location for crx-repository> parameter will be Dcom.adobe.livecycle.crx.home=C:\CM-publish\crx-repository.

NOTE: If author and publish instances are on the same machine, ensure that you start the publish instance using a different port.

IMPORTANT: Ensure that the CRX repository path does not contain spaces.

Communicating between the Author and Publish instances

Enable two-way communication between Author and Publish instances:

Define Publish instance URL

1) Go to http://<*authorHost*>:<*authorPort*>/lc/etc/replication/agents.author/publish.html.
2) Click **Edit**. The Agent Settings dialog opens.
3) Click the **Transport** tab and specify the URL to the publish server in the URI field.
   http://<publishHost>:<publishPort>/lc/bin/receive?sling:authRequestLogin=1
   NOTE: If there are multiple publish instances managed by a Load Balancer, specify the URL to the load balancer in the URI field.

4) Click **OK**.

NOTE: For author clusters, these steps need to be performed on one author instance (preferably a master instance).

Define publish instance URL for ActivationManagerImpl

1) Go to http://<*authorHost*>:<*authorPort*>/lc/system/console/configMgr. The default username and password for logging in are admin and admin (same as CRX Administrator).
2) Find and click the Edit icon next to the `com.adobe.livecycle.content.activate.impl.ActivationManagerImpl.name` setting.
3) In the ActivationManager Publish URL field, specify the URL for the corresponding publish instance.
4) Click **Save**.

Configure reverse replication queue

1) Go to http://<*authorHost*>:<*authorPort*>/lc/etc/replication/agents.author/publish_reverse.html.
2) Click **Edit**. The Agent Settings dialog opens.
3) Click the **Transport** tab and specify the URL to the corresponding publish server in the URI field.

   NOTE: If there are multiple publish instances managed by a Load Balancer, specify the URL to the load balancer in the URI field.
4) Click **OK**.

Define author instance URL

1) Go to http://<*publishHost*>:<*publishPort*>/lc/system/console/configMgr. The default username and password for logging in are admin and admin (same as CRX Administrator).
2) Find and click the Edit icon next to the `com.adobe.livecycle.content.activate.impl.VersionRestoreManagerImpl.name` setting.
3) In the VersionRestoreManager Author URL field, specify the URL for the corresponding author instance.

   NOTE: If there are multiple author instances managed by a Load Balancer, specify the URL to the load balancer in the VersionRestoreManager Author URL field.
4) Click **Save**.

Configure IPv6 implementation

NOTE: Perform these steps only if the machine/server is using an IPv6 address.

To map the IPv6 address to a hostname on the server and client machines:

1) Navigate to the C:\Windows\System32\drivers\etc directory.
2) Open the `hosts` file in a text editor.
3) Add a mapping for the IPv6 address to a host name. For example:

```
2001:1890:110b:712b:d1d:9c99:37ef:7281 <ipv6_hostname>
```

4) Save and close the file.

Ensure that you use the mapped host name instead of the IPv6 address to access the machine.

Install Japanese fonts for Adobe Reader

If your document fragments use Japanese fonts, you must install the Japanese Language Support Package for Adobe Reader. Otherwise, your letters and forms will not render and function properly. For installing language packs, visit the downloads page for Adobe Reader.

8.5. Configuring PDF Generator

If you installed PDF Generator, complete the following tasks:

Environment variables

If you configured PDF Generator to convert files to PDF, for some file formats, you must manually set environment variables that contain the absolute path of the executable that is used to start the corresponding application. The table below lists the environment variables for the native applications.

NOTE: Ensure that the required applications are installed on all nodes in the cluster.

NOTE: All environment variables and respective paths are case-sensitive.

Application	Environment variable	Example
Adobe Acrobat	`Acrobat_PATH`	`C:\Program Files (x86)\Adobe\Acrobat 2015\Acrobat\Acrobat.exe`
Notepad	`Notepad_PATH`	`C:\WINDOWS\notepad.exe` You can leave the `Notepad_PATH` variable blank.
OpenOffice	`OpenOffice_PATH`	`C:\Program Files (x86)\OpenOffice 4`

NOTE: These environment variables must be set for all nodes in the cluster.

NOTE: The environment variable `OpenOffice_PATH` is set to the installation folder instead of the path to the executable.

Configuring the application server to use HTTP proxy server

If the computer that AEM Forms on JEE is running on uses proxy settings to access external web sites, the application server should be started with the following values set as Java virtual machine (JVM) arguments:

```
-Dhttp.proxyHost=[server host]
-Dhttp.proxyPort=[server port]
```

Complete the following procedure to start your application server with HTTP proxy host setting.

1) In the WebSphere Administrative Console navigation tree, log in to WebSphere Administrative Console, click Servers > Server Types > WebSphere application servers, and then click the name of the server instance to configure (for example, server1).
2) Under Server Infrastructure, click **Java and Process Management** > **Process Definition.**
3) Under Additional Properties, click **Java Virtual Machine** > **Custom Properties**.
4) Click **New** and, in the **Name** box, type `http.proxyHost`.
5) In the **Value** box, type the host name or IP address of your HTTP proxy server and then click **OK**.
6) Click **New** and, in the **Name** box, type `http.proxyPort`.
7) In the **Value** box, type the port number of your HTTP proxy server and then click **OK**.
8) In the **Messages** box, click **Save directly to master configuration**.
9) Restart all WebSphere server instances.

Setting the Adobe PDF Printer as the default printer

You must set the Adobe PDF Printer to be the default printer on the server. If the Adobe PDF Printer is not set as the default, PDF Generator cannot convert files successfully.

For clusters, you must set Adobe PDF Printer as the default printer on all nodes.

Set the default printer

1) Select **Start** > **Printers and Faxes**.
2) In the Printers and Faxes window, right-click **Adobe PDF** and select **Set as Default Printer**.

Configuring Acrobat Professional (Windows-based Computers Only)

NOTE: This procedure is required only if you upgraded to or installed Acrobat after you completed the AEM Forms on JEE installation. Upgrading Acrobat can be completed after you run Configuration Manager and deploy AEM Forms on JEE to the application server. Acrobat Professional root directory is designated as *[Acrobat root]*. Typically, the root directory is *C:\Program Files (x86)\Adobe\Acrobat 2015\Acrobat*.

Configure Acrobat for use with PDF Generator

1) If an earlier version of Acrobat is installed, uninstall it by using Add or Remove Programs in the Windows Control Panel.
2) Install Acrobat DC Pro by running the installer.
3) Navigate to the additional\scripts folder on the AEM Forms on JEE installation media.
4) Run the following batch file.

```
Acrobat_for_PDFG_Configuration.bat [aem_forms root]/pdfg_config
```

NOTE: On clusters, you must run the command on the cluster node where AEM forms on JEE is installed.

5) On other cluster nodes on which you do not run AEM Forms on JEE Configuration Manager, do the following:
   – Add a new registry DWORD entry named SplWOW64TimeOut at HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Print. Set its value to 60000.
   – Copy `PDFGen.api` from the [*aem-forms root*]/plugins/x86_win32 directory on the node where AEM Forms on JEE is installed to the [*Acrobat root*]/plug_ins directory on the node being currently configured.
6) Open Acrobat and select **Help** > **Check for updates** > **Preferences**.
7) De-select **Automatically check for Adobe updates**.

Validate the Acrobat installation

1) Navigate to a PDF file on your system and double-click it to open it in Acrobat. If the PDF file opens successfully, Acrobat is installed correctly.
2) If the PDF file does not open correctly, uninstall Acrobat and reinstall it.

NOTE: Ensure that you dismiss all Acrobat dialog boxes that are displayed after Acrobat installation is complete and disable the automatic updates for Acrobat. Set the `Acrobat_PATH` environment variable to point to Acrobat.exe. For example, C:\Program Files (x86)\Adobe\Acrobat 2015\Acrobat\Acrobat.exe.

Add temporary directories to trusted directories list in Acrobat

The `OptimizePDF` service uses Adobe Acrobat and mandates that AEM Forms on JEE temporary directory and PDF Generator temporary directory are listed in the trusted directories list of Acrobat.

If AEM Forms on JEE temporary directory and PDF Generator temporary directory are not listed in the trusted directories list, the `OptimizePDF` service fails to run. Perform the following steps to add directories to the temporary directory list:

1) Open Acrobat, Choose Edit > Preferences.
2) From the Categories on the left, select Security (Enhanced), and then select the Enable Enhanced Security option.
3) To add AEM Forms on JEE temporary directory and PDF Generator temporary directory to the trusted directories list, click **Add Folder Path**, select directories, and click **OK.**

Installing East Asian characters in Windows Server 2003

When HTML files are converted to PDF using PDF Generator, some East Asian languages, such as Japanese, Korean, and Chinese, and also right-to-left languages, such as Arabic, Armenian, Georgian, Hebrew, Indic, Thai, and Vietnamese, may not be displayed in the PDF file.

To ensure that these languages are displayed in Windows Server 2003, appropriate fonts must be present on the client and server.

Install East Asian characters in Windows Server 2003

1) Select **Start** > **Control Panel** and open **Regional and Language Options**.
2) Click the **Languages** tab and select **Install Files for East Asian Languages**.
3) Click the **Advanced** tab and select all options under Code Page Conversion Tables.

If converted PDF files are still missing fonts, verify that the Arial Unicode MS (TrueType) font (ARIALUNI.TTF) is present in the C:\WINDOWS\Fonts directory.

Adding fonts to PDF Generator

AEM Forms on JEE provides a central repository of fonts, which is accessible to all AEM Forms on JEE modules. Make any extra fonts available to non-AEM Forms on JEE applications on the server so that PDF Generator can use these fonts to create PDF documents created with these applications.

NOTE: *Restart the application server after adding new fonts to the specified fonts folder.*

Non-AEM Forms on JEE applications

The following list contains non-AEM Forms on JEE applications that PDF Generator can use for PDF generation on the server side:

Windows-only Applications

- Microsoft Office Word
- Microsoft Office Excel
- Microsoft Office PowerPoint
- Microsoft Office Project
- Microsoft Office Publisher
- Adobe FrameMaker
- Adobe PageMaker
- Adobe Acrobat Professional

Multi-platform applications

- OpenOffice Writer
- OpenOffice Calc
- OpenOffice Draw
- OpenOffice Impress

NOTE: In addition to these applications, your list may include additional applications that you added.

Of the above applications, the OpenOffice Suite (which includes Writer, Calc, Draw, and Impress) is available on Windows, Solaris, and Linux platforms, whereas other applications are available on Windows only.

Adding new fonts to Windows applications only

All Windows-only applications that are mentioned above can access all the fonts available in the C:\Windows\Fonts (or equivalent) folder. In addition to C:\Windows\Fonts, each of these applications may have its own private fonts folders.

Therefore, if you plan to add any custom fonts to the AEM Forms on JEE fonts repository, ensure that the same fonts are available to the Windows-only applications also by copying these fonts to either C:\Windows\Fonts or to an equivalent folder.

Your custom fonts must be licensed under an agreement that allows you to use them with the applications that have access to these fonts.

Adding new fonts to other applications

If you added support for PDF creation in other applications, see the Help for these applications to add new fonts. In Windows, copying your custom fonts to the C:\Windows\Fonts (or equivalent) folder should be sufficient.

Adding new fonts to OpenOffice Suite

Adding custom fonts to OpenOffice Suite is explained on the OpenOffice *Fonts-FAQ* page at http://wiki.services.openoffice.org.

Configuring HTML to PDF conversions

The HTML-to-PDF conversion process is designed to use the settings from Acrobat DC Pro that override the settings from PDF Generator.

NOTE: This configuration is required to enable the HTML-to-PDF conversion process, otherwise this conversion type will fail.

Configure the HTML-to-PDF conversion

1) Install and validate Acrobat as described in ConfiguringAcrobatProfessional.
2) Locate the pdfgen.api file in the *[aem-forms root]*\plugins\x86_win32 directory and copy it to *[Acrobat root]*\Acrobat\plug_ins directory.

Enable support for Unicode fonts in HTML to PDF conversions

IMPORTANT: The HTML-to-PDF conversion fails if the zipped input file contains HTML files with double-byte characters in filenames. To avoid this problem, do not use double-byte characters when naming HTML files.

1) Copy the Unicode font to any of the following directories as appropriate for your system:
   - Windows
     *[Windows root]**Windows**fonts*
     *[Windows root]**WINNT**fonts*
   - UNIX

/usr/lib/X11/fonts/TrueType
/usr/openwin/lib/X11/fonts/TrueType
/usr/share/fonts/default/TrueType
/usr/X11R6/lib/X11/fonts/ttf
/usr/X11R6/lib/X11/fonts/truetype
/usr/X11R6/lib/X11/fonts/TrueType
/usr/X11R6/lib/X11/fonts/TTF
/Users/cfqauser/Library/Fonts
/System/Library/Fonts
/Library/Fonts
/Users/ + System.getProperty(<username>, root) + /Library/Fonts
System.getProperty(JAVA_HOME) + /lib/fonts
/usr/share/fonts (Solaris)

NOTE: Ensure that the directory /usr/lib/X11/fonts exists. If it does not exist, create a symbolic link from /usr/share/X11/fonts to /usr/lib/X11/fonts using the `ln` command.

NOTE: Ensure that the fonts are present in either /usr/share/fonts or /usr/share/X11/fonts directory.

2) Unzip the IBM type1 courier font to the /usr/share/X11/fonts/font-ibm-type1-1.0.3 folder.
3) Create a symbolic link from /usr/share/fonts to /usr/share/X11/fonts.
4) Modify the font-name mapping in the cffont.properties file located in the *[aem-forms root]*/deploy/adobe-generatepdf-dsc.jar file:
   - Extract the archive file, and locate the cffont.properties file and open it in an editor.
   - In the comma-separated list of Java font names, add a map to your Unicode system font for each font type. In the example below, kochi mincho is the name of your Unicode system font.

     ```
     dialog=Arial, Helvetica, kochi mincho
     dialog.bold=Arial Bold, Helvetica-Bold, kochi mincho ...
     ```

   - Save and close the properties file, and then repackage and redeploy the `adobe-generatepdf-dsc.jar` file.

NOTE: On a Japanese operating system, specify the font mapping in the cffont.properties.ja file as well, which takes precedence over the standard cffont.properties file.

TIP: Fonts in the list are searched from left to right, using the first font found. HTML-to-PDF conversion logs return a list of all the font names that are found in the system. To determine the font name you need to map, add the font to one of the directories above, restart the server, and run a conversion. You can determine from the log files the font name to use for mapping.

To embed the font in the generated PDF files, set the `embedFonts` property in the cffont.properties file to `true` (the default is `false`).

Installing the Network Printer Client

PDF Generator includes an executable file to install the PDF Generator network printer on a client computer. After the installation is complete, a PDF Generator printer is added to the list of existing printers on the client computer. This printer can then be used to send documents for conversion to PDF.

NOTE: The Network Printer Client installation wizard available in the administration console is supported only on Windows operating system. Ensure that you use a 32-bit JVM to launch the Network Printer Client installation wizard. You will encounter an error if you use a 64-bit JVM.

If the PDFG Network Printer fails to install on Windows or if you want to install the printer on UNIX or Linux platforms, use the operating system's native Add Printer utility and configure it as described in ConfigurePDFGNetworkPrinteronWindowsusingthenativeAddPrinterwizard

Install the PDF Generator Network Printer Client

NOTE: Before installing the PDF Generator network printer client on Windows Server 2012, ensure that you have the Internet Printing Client feature installed on your Windows Server 2012. For installing the feature, see Windows Server 2012 Help.

1) Ensure that you have successfully installed PDF Generator on your server.
2) Do one of the following:
   - From a Windows client computer, open the following URL in your web browser, where *[host]* is the name of the server where you installed PDF Generator and *[port]* is the application server port used.

     `http://[host]:[port]/pdfg-ipp/install`
   - In administration console, click **Home > Services > PDF Generator > PDFG Network Printer**. In the **PDFG Network Printer Installation** section, click **Click here** to launch the PDFG Network Printer Installation.
3) On the Configure Internet Port screen, select **Use the specified user account** option, and provide the credentials of a AEM Forms on JEE user who has the PDFG Administrator/User role. This user must also have an email address that can be used to receive the converted files. To have this security setting apply to all users on the client computer, select**Use the same security options for all users**, and then click **OK**.

   NOTE: *If the user's password changes, then users will need to reinstall the PDFG Network Printer on their computers. You cannot update the password from administration console.*

   Upon successful installation, a dialog box appears, indicating that the printer is successfully installed.
4) Click **OK**. You will now have a PDF Generator printer available in your list of printers.

Configure PDFG Network Printer on Windows using the native Add Printer wizard

1) Click **Start** >**Printers and Faxes** and double-click **Add Printer**.
2) Click **Next**, select **A network printer, or a printer attached to another computer**, and then click **Next**.

3) Select **Connect to a printer on the Internet or on a home or office network** and type the following URL for the PDFG printer, where *[host]* is the server name and *[port]* is the port number where the server is running:

   `http://[host]:[port]/pdfg-ipp/printer`

4) On the Configure Internet Port screen, select **Use the specified user account** and provide valid User credentials.
5) In the **Printer Driver Select** box, choose any standard PostScript-based printer driver (for example, HP Color LaserJet PS).
6) Complete the installation by choosing appropriate options (for example, setting this printer as default).

   NOTE: The user credentials used while adding the printer must have a valid email ID configured in User Management to receive the response.
7) Configure the email service's sendmail service. Provide a valid SMTP server and authentication information in the service's configuration options.

Install and configure the PDF Generator Network Printer Client using Proxy server port forwarding

1) Configure port forwarding on the CC Proxy server on a particular port to the AEM forms on JEE Server, and disable the authentication at proxy server level (because AEM Forms on JEE uses its own authentication). If a client connects to this Proxy server on the forwarded port, then all the requests will be forwarded to the AEM Forms on JEE Server.
2) Install PDFG Network Printer using the following URL:

   `http://[proxy server]:[forwarded port]/pdfg-ipp/install.`
3) Provide the necessary credentials for authentication of the PDFG Network Printer.
4) The PDFG Network Printer will be installed on the client machine which you can use for PDF conversion using the firewall protected AEM Forms on JEE Server.

Changing File Block Settings

Change Microsoft Office trust center settings to enable PDFG to convert older versions of Microsoft office documents.

1) Click the **File tab** in any Office 2013 application. Under **File**, click **Options**; the Options dialog box appears
2) Click **Trust Center**, and then click **Trust Center Settings**.
3) In the **Trust Center settings**, click **File Block Settings**.
4) In the File Type list, uncheck open for the file type that you want PDF Generator to convert.

Watched folder performance parameters

To avoid `java.io.IOException` error messages indicating that not enough disk space is available to perform PDF conversions by using a watched folder, you can modify the settings for PDF Generator in administration console.

You must ensure that for WebSphere application server, the maximum transaction time-out and ORB service have proper values.

Configure transaction time-out

1) Do the following:
   – Log in to WebSphere Administrative Console, click **Servers** > **Server Types** > **WebSphere application servers**, and then click the name of the server instance to configure (for example, *server1*).
2) Under Container Settings, click **Container Services > Transaction Service**.
3) Under General Properties, in the **Total transaction lifetime timeout** box, type `300` (or higher).
4) Ensure that the value in the **Maximum transaction timeout** box is greater than or equal to the **Total transaction lifetime timeout**.
5) Click **OK** or **Apply** and then click **Save directly to master configuration**.

Increase the CORBA time-out value

1) Do the following:
   – Log in to WebSphere Administrative Console, click **Servers** > **Server Types** > **WebSphere application servers**, and then click the name of the server instance to configure (for example, *server1*).
2) Under Container Settings, click **Container Services > ORB Service**.
3) Under General Properties, in the **Request timeout** box, type `360` and, in the **Locate Request Timeout** box, type `300`.
4) Click **OK** or **Apply** and then click **Save directly to master configuration**.

Set performance parameters for PDF Generator

1) Log in to administration console and click **Services** >**Applications and Services**> **Service Management**.
2) In the list of services, navigate to and click **PDFGConfigService**, and then set the following values:
   – **PDFG Cleanup Scan Seconds**: 1800
   – **Job Expiration Seconds**: 6000
   – **Server Conversion Timeout**: Change the default of 270 to a higher value, such as 450.
3) Click **Save** and restart the server.

Enable PDF Conversion for Microsoft Word document containing protected fields

PDF Generator supports Microsoft Word documents containing protected fields. To enable PDF Conversion for Microsoft Word document containing protected fields, change the file type settings:

1) In the **administration console**, navigate to **Services** > **PDF Generator** > **File Type Settings**, and open your file type settings profile.
2) Expand the **Microsoft Word** option and select the **Preserve document markup in Adobe PDF (for Microsoft Office 2003 or later)** option.
3) Click **Save As**, specify name of the file type setting, and click **OK**.

8.6. Configure SSL for Document Security

Document Security requires the application server to be configured to use SSL. See administrationhelp

.

8.7. Enable FIPS mode

NOTE: If you have configured it in the previous version, skip the following section:

AEM Forms on JEE provides a FIPS mode to restrict data protection to Federal Information Processing Standard (FIPS) 140-2 approved algorithms using the RSA BSAFE Crypto-C 2.1 encryption module.

If you did not enable this option by using Configuration Manager during AEM Forms on JEE configuration or if you enabled it but want to turn it off, you can change this setting through Administration Console.

Modifying FIPS mode requires you to restart the server.

FIPS mode does not support Acrobat versions earlier than 7.0. If FIPS mode is enabled and the Encrypt With Password and Remove Password processes include the Acrobat 5 setting, the process fails.

In general, when FIPS is enabled, the Assembler service does not apply password encryption to any document. If this is attempted, a `FIPSModeException` is thrown, indicating that “Password encryption is not permitted in FIPS mode.” Additionally, the `PDFsFromBookmarks` element is not supported in FIPS mode when the base document is password-encrypted.

Turn FIPS mode on or off

1) Log in to administration console.
2) Click **Settings** > **Core System Settings**> **Configurations**.
3) Select **Enable FIPS** to enable FIPS mode or deselect to disable FIPS mode.
4) Click **OK** and restart the application server.

NOTE: AEM forms on JEE software does not validate code to ensure FIPS compatibility. It provides a FIPS operation mode so that FIPS-approved algorithms are used for cryptographic services from the FIPS-approved libraries (RSA).

8.8. Enable WebSphere Global Administrative Security

NOTE: If you did not select the Content Repository option on the Modules screen of the configuration manager, do not perform the following steps.

WebSphere Global Administrative Security administrative security helps in hardening environment for AEM Forms. It is recommended to enable Global Administrative Security on both author and publish instances.

By default, AEM internally uses the token **j_security_check**. Using the j_security_check token can cause a conflict with WebSphere's Global Administrative Security, as the token j_security_check is also used as the default for form-based authentication. To resolve this conflict, complete the following steps to switch over AEM to use the token **j_sling_security_check**.

NOTE: *These configuration changes are performed each time an AEM (OSGi) patch is applied that updates bundle.jar.*

Enable Administrative Security on the author instance

Perform the following steps to WebSphere Global Administrative Security on an author instance of AEM Forms:

1) Turn off global security
   a) Open administrative console of WebSphere application server
   b) Click Security > Global security. In Administrative Security, uncheck the Enable Administrative Security option, click Apply, and click Save. It saves directly to the master configuration
   c) Restart the WebSphere application server.
2) Log in to CRX DE Lite as an administrator. The default URL is http://[server]:[port]/lc/crx/de/index.jsp
3) Open the /libs/Livecycle/core/content/login/login.js file for editing
4) Search the term `j_security_check` and replace it with `j_sling_security_check` and click Save All.
5) Log out of CRX DE Lite.
6) Open AEM Configuration Manager. The default URL is http://server:port/lc/system/console/configMgr/.
7) Locate and open the Day CRX Token Authentication Handler configuration.
8) Set value of the Alternate Authentication URL to `j_sling_security_check` and click Save.
9) Log out of the Configuration Manager.
10) Refresh browser cache.
11) Turn on the Global security
    a) Open administrative console of WebSphere application server
    b) Click Security > Global security. In Administrative Security, select the Enable Administrative Security option, click Apply, and click Save. It saves directly to the master configuration
    c) Restart the WebSphere application server.

Enable WebSphere Global Administrative Security on the publish instance

Perform the following steps to WebSphere Global Administrative Security on an publish instance of AEM Forms:

1) Locate and extract the bundle.jar file for the CRXDE Lite bundle. Locate the file docroot/js/CRX/util/Util.js within that JAR, and search and replace**j_security_check** with **j_sling_security_check**. Use the following steps to locate and extract the CRXDE Lite JAR file:

   NOTE: Use a tool, such as WinRAR, that allows you to extract, edit, and re-inject the file without expanding the entire archive.

   a) Open your CRX Console to the Bundles page at **http://[server]:[port]/lc/system/console/bundles** and search for **Adobe Granite CRXDE Lite** and expand it. Note down the number (the bundle ID under the heading ID) on the left side of **Adobe Granite CRXDE Lite**.

   b) Go to the CRX Repository on disk. Within the crx-repository directory, go to \launchpad\felix\bundle###\version0.0 - where ### is the number of the bundle from the **http://[server]:[port]/lc/system/console/bundles** page.

   c) Copy the bundle.jar file.

2) In Config Manager, **http://host:port/lc/system/console/configMgr**, go to **Day CRX Token Authentication Handler** and set **Alternate Authentication URL** to **j_sling_security_check**.

3) In Config Manager, go to **Apache Sling Authentication Service** and set the **Authentication URI Suffices** to **/j_sling_security_check**.

4) Using CRXDE Lite, **http://[host]:[port]/crx/de/index.jsp**, copy the below files from their current location under /libs/** to new /apps/** locations. The paths under /libs/, such as /cq/core/components/login, should be created if they do not exist such that the copied files reside in the same structure under /apps.

Copy the file	To the location
/libs/granite/core/components/login/login.jsp	/apps/granite/core/components/login/login.jsp
/libs/social/connect/components/sociallogin/sociallogin.jsp	/apps/social/connect/components/sociallogin/sociallogin.jsp
/libs/social/connect/components/sociallogin/cqlogin.jsp	/apps/social/connect/components/sociallogin/cqlogin.jsp
/libs/social/connect/components/socialconnect/socialconnect.jsp	/apps/social/connect/components/socialconnect/socialconnect.jsp
/libs/foundation/components/login/login.jsp	/apps/foundation/components/login/login.jsp

5) Open each of the new copied files under /apps/ and search/replace **j_security_check** with **j_sling_security_check**. Ensure that you save the changes.

6) In CRXDE Lite, go to **/etc/clientlibs/social/commons/scf/session.js** and search/replace **j_security_check** with **j_sling_security _check**.

7) Optionally, if you are using GeoMetrixx Outdoors, modify the following files in the same manner as in step 4. The GeoMetrixx Outdoors website already overlays some of the files.
   – /apps/community-components/components/basepage/clientlibs/basepage.js
   – /apps/geometrixx-outdoors/components/social/sociallogin/cqlogin.jsp
   – /apps/geometrixx-outdoors/components/social/connect/components/socialconnect/socialconnect.jsp
8) Restart AEM.

8.9.

8.10.

8.11. Configure CSIv2 inbound transport

On the default Global Security enabled installation of IBM WebSphere, CSIv2 inbound transport option is set to SSL-required. This configuration causes Output and Forms components to fail. Ensure that you change CSIv2 inbound transport option to SSL-Supported: To change the option:

1) Log in to IBM WebSphere administration console.
2) Expand **Security**, and then click **Global security**.
3) In the Authentication section, expand **RMI/IIOP security**, and then click **CSIv2 inbound communications**
4) In CSIv2 Transport Layer section, set value of **Transport** to **SSL-Supported**.
5) Click **Apply**.

8.12. Configuring Connector for EMC Documentum

NOTE: AEM Forms on JEE supports EMC Documentum 6.7 SP1 and 7.0 with minor updates only. Make sure your ECM is upgraded accordingly.

NOTE: Ensure that installing client for the connectors, copying the JAR file, and configuration changes tasks are performed on all the nodes of the cluster.

If you installed Connector for EMC Documentum as part of your AEM Forms on JEE, complete the following procedure to configure the service to connect to the Documentum repository.

Configure Connector for EMC Documentum

1) Locate the adobe-component-ext.properties file in the *[appserver root]*/profiles/[profile name] folder (if the file does not exist, create it).
2) Add a new system property that provides the following Documentum Foundation Classes JAR files:

- dfc.jar
- aspectjrt.jar
- log4j.jar
- jaxb-api.jar
- configservice-impl.jar
- configservice-api.jar
- commons-codec-1.3.jar
- commons-lang-2.4.jar

The new system property should take on this form:

```
[component id].ext=[JAR files and/or folders]
```

For example, using default Content Server and Documentum Foundation Classes installations, add to the file one of the following system properties on a new line, with no line breaks, and end the line with a carriage return:

- Connector for EMC Documentum 6.7 SP1 and 7.0 only:

```
com.adobe.livecycle.ConnectorforEMCDocumentum.ext=
C:/Program Files/Documentum/Shared/dfc.jar,
C:/ProgramFiles/Documentum/Shared/aspectjrt.jar,
C:/Program Files/Documentum/Shared/log4j.jar,
C:/Program Files/Documentum/Shared/jaxb-api.jar,
C:/Program Files/Documentum/Shared/configservice-impl.jar,
C:/Program Files/Documentum/Shared/configservice-api.jar
C:/Program Files/Documentum/Shared/commons-codec-1.3.jar
C:/Program Files/Documentum/Shared/commons-lang-2.4.jar
```

NOTE: The above text contains formatting characters for line breaks. If you copy and paste this text, you must remove the formatting characters.

3) Repeat previous steps on each application server instance of the cluster.
4) Open a web browser and enter this URL:

```
http://[host]:[port]/adminui
```

5) Log in using the default user name and password:

***User name**: administrator*

***Password**: password*

6) Navigate to **Services** > **Connector for EMC Documentum** > **Configuration Settings** and perform these tasks:
   - Type all the required Documentum repository information.
   - To use Documentum as your repository provider, under Repository Service Provider Information, select **EMC Documentum Repository Provider**, and then click **Save**. For more information, click the Help link in the upper-right corner of the page in the Administration Help.
7) (Optional) Navigate to **Services** > **Connector for EMC Documentum** > **Repository Credentials Settings**, click **Add**, specify the Docbase information, and then click **Save**. (For more information, click **Help** in the upper-right corner.)

8) If the application server is not currently running, start the server. Otherwise, stop and then restart the server.

9) Open a web browser and enter this URL.

   `http://[host]:[port]/adminui`

10) Log in using the default user name and password:

    ***User name**: administrator*

    ***Password**: password*

11) Navigate to **Services** > **Applications and Services** > **Service Management** and select these services:
    - EMCDocumentumAuthProviderService
    - EMCDocumentumContentRepositoryConnector
    - EMCDocumentumRepositoryProvider
    - EMCDocumentumECMUpgradeService

12) Click **Start**. If any of the services do not start correctly, check the settings you completed earlier.

13) Do one of the following tasks:
    - To use the Documentum Authorization service (EMCDocumentumAuthProviderService) to display content from a Documentum repository in the Resources view of Workbench, continue with this procedure. Using the Documentum Authorization service overrides the default AEM Forms on JEE authorization and must be configured to log in to Workbench using Documentum credentials.
    - To use the AEM Forms on JEE repository, log in to Workbench by using the AEM Forms on JEE super administrator credentials (by default, *administrator* and *password*).

    You have now completed the required steps for this procedure. Use the credentials provided in this step for accessing the default repository in this case and use the default AEM Forms on JEE authorization service.

14) Restart the application server.

15) Log in to administration console and click **Settings** > **User Management** > **Domain Management**.

16) Click **New Enterprise Domain**, and type a domain ID and name. The domain ID is the unique identifier for the domain. The name is a descriptive name for the domain.

    ***NOTE: (WebLogic and WebSphere only)** When using DB2 for your AEM Forms on JEE database, the maximum permitted length of the ID is 100 single-byte (ASCII) characters or 50 double-byte characters or 25 four-byte characters. (See "Adding enterprise domains" in administration help.)*

17) Add a custom authentication provider:
    - Click **Add Authentication**.
    - In the Authentication Provider list, select **Custom**.
    - Select **EMCDocumentumAuthProvider** and then click **OK**.

18) Add an LDAP authentication provider:
    - Click **Add Authentication**.
    - In the Authentication Provider list, select **LDAP**, and then click **OK**.

19) Add an LDAP directory:

- Click **Add Directory**.
- In the Profile Name box, type a unique name, and then click **Next**.
- Specify values for the **Server**, **Port**, **SSL**, **Binding**, and **Populate page with** options. If you select User for the Binding option, you must also specify values for the **Name** and **Password** fields.
- (Optional) Select **Retrieve Base DN** to retrieve base domain names, as required.
- Click **Next**, configure the user settings, click **Next**, configure group settings, as required, and then click **Next**.

  *For details about the settings, click **User Management Help** in the upper-right corner of the page.*

20) Click **OK** to exit the Add Directory page and then click OK again.
21) Select the new enterprise domain and click **Sync Now**. Depending on the number of users and groups in your LDAP network and the speed on your connection, the synchronization process may take several minutes.

    *(Optional) To verify the status of the synchronization, click **Refresh** and view the status in the Current Sync State column.*
22) Navigate to **Settings > User Management > Users and Groups**.
23) Search for users that were synchronized from LDAP and perform these tasks:
    - Select one or more users and click **Assign Role**.
    - Select one or more AEM Forms on JEE roles and click **OK**.
    - Click **OK** a second time to confirm the role assignment.

      *Repeat this step for all users that you assign roles to. For more information, click **User Management Help** in the upper-right corner of the page.*
24) Start Workbench and log in by using the credentials for the Documentum repository:

    ***Username**: [username]@[repository_name]*

    ***Password**: [password]*

    After you log in, the Documentum repository appears in the Resources view within Workbench. If you do not log in using the username@repository_name, Workbench attempts to log in to the default repository.
25) (Optional) To install the AEM Forms on JEE Samples for Connector for EMC Documentum, create a Documentum repository named Samples, and then install the samples in that repository.

After you configure the Connector for EMC Documentum service, see *AEM Forms on JEE administration help* for information about configuring Workbench with your Documentum repository.

Creating the XDP MIME format in a Documentum repository

Before users can store and retrieve XDP files from a Documentum repository, you must do one of these tasks:

- Create a corresponding XDP format in each repository where users will access XDP files.

- Configure the Connector for EMC Documentum service to use a Documentum Administrator account when accessing the Documentum repository. In this case, the Connector for EMC Documentum service uses the XDP format whenever it is required.

Create the XDP format on Documentum Content Server using Documentum Administrator

1) Log in to Documentum Administrator.
2) Click **Formats** and then select **File** > **New** > **Format**.
3) Type the following information in the corresponding fields:
   Name: `xdp`
   Default File Extension: `xdp`
   Mime Type: `application/xdp`
4) Repeat steps 1 to 3 for all other Documentum repositories where users will store XDP files.

Configure the Connector for EMC Documentum service to use a Documentum Administrator

1) Open a web browser and enter this URL:
   http://[host]:[port]/adminui
2) Log in using the default user name and password:
   User name*: administrator*
   Password*: password*
3) Click **Services** > **Connector for EMC Documentum** > **Configuration Settings**.
4) Under Documentum Principal Credentials Information, update the following information and then click **Save**:
   User Name: *[Documentum Administrator user name]*
   Password: *[Documentum Administrator password]*
5) Click **Repository Credentials Settings**, select a repository from the list or, if none exist, click **Add**.
6) Provide the appropriate information in the corresponding fields and then click **Save**:
   Repository Name: *[Repository Name]*
   Repository Credentials User Name: *[Documentum Administrator user name]*
   Repository Credentials Password: *[Documentum Administrator password]*
7) Repeat steps 5 and 6 for all repositories where users will store XDP files.

Add support for multiple connection brokers

AEM Forms on JEE Configuration Manager supports configuring only one connection broker. Use AEM Forms on JEE Administrator Console to add support for multiple connection brokers:

1) Open AEM Forms on JEE Administrator Console.
2) Navigate to Home > Services > Connector for EMC Documentum > Configuration Settings.
3) In the **Connection broker Host Name or IP Address,** enter comma seperated list of hostnames of different connection brokers. For example, host1, host2, host3.

4) In the **Port Number of Connection broker**, enter comma seperated list of the ports of corresponding connection brokers. For example, 1489, 1491, 1489.
5) Click **Save**.

8.13. Configuring the Connector for IBM Content Manager

NOTE: AEM forms supports IBM Content Manager. See the Supported Platform Combinations document and make sure your ECM is upgraded to the supported version.

NOTE: Ensure that installing client for the connectors, copying the JAR file, and configuration changes tasks are performed on all the nodes of the cluster.

If you installed the Connector for IBM Content Manager as part of your AEM Forms installation, complete the following procedure to configure the service to connect to the IBM Content Manager datastore.

Configure Connector for IBM Content Manager

1) Locate the adobe-component-ext.properties file in the *[appserver root]*/profiles/[profile name] folder. If the file does not exist, create it.
2) Add a new system property that provides the location of the following IBM II4C JAR files:
   - cmb81.jar
   - cmbcm81.jar
   - cmbicm81.jar
   - cmblog4j81.jar
   - cmbsdk81.jar
   - cmbutil81.jar
   - cmbutilicm81.jar
   - cmbview81.jar
   - cmbwas81.jar
   - cmbwcm81.jar
   - cmgmt

   NOTE: cmgmt is not a JAR file. On Windows, by default, this folder is at `C:/Program Files/IBM/db2cmv8/`.
   - common.jar
   - db2jcc.jar
   - db2jcc_license_cisuz.jar
   - db2jcc_license_cu.jar
   - ecore.jar
   - ibmjgssprovider.jar
   - ibmjsseprovider2.jar
   - ibmpkcs.jar

- icmrm81.jar
- jcache.jar
- log4j-1.2.8.jar
- xerces.jar
- xml.jar
- xsd.jar

The new system property looks similar to the following:

```
[component id].ext=[JAR files and/or folders]
```

For example, using a default DB2 Universal Database Client and II4C installation, in the file, add the following system property on a new line, with no line breaks, and end the line with a carriage return:

```
C:/Program Files/IBM/db2cmv8/cmgmt,
C:/Program Files/IBM/db2cmv8/java/jre/lib/ibmjsseprovider2.jar,
C:/Program Files/IBM/db2cmv8/java/jre/lib/ibmjgssprovider.jar,
C:/Program Files/IBM/db2cmv8/java/jre/lib/ibmpkcs.jar,
C:/Program Files/IBM/db2cmv8/java/jre/lib/xml.jar,
C:/Program Files/IBM/db2cmv8/lib/cmbview81.jar,
C:/Program Files/IBM/db2cmv8/lib/cmb81.jar,
C:/Program Files/IBM/db2cmv8/lib/cmbcm81.jar,
C:/Program Files/IBM/db2cmv8/lib/xsd.jar,
C:/Program Files/IBM/db2cmv8/lib/common.jar,
C:/Program Files/IBM/db2cmv8/lib/ecore.jar,
C:/Program Files/IBM/db2cmv8/lib/cmbicm81.jar,
C:/Program Files/IBM/db2cmv8/lib/cmbwcm81.jar,
C:/Program Files/IBM/db2cmv8/lib/jcache.jar,
C:/Program Files/IBM/db2cmv8/lib/cmbutil81.jar,
C:/Program Files/IBM/db2cmv8/lib/cmbutilicm81.jar,
C:/Program Files/IBM/db2cmv8/lib/icmrm81.jar,
C:/Program Files/IBM/db2cmv8/lib/db2jcc.jar,
C:/Program Files/IBM/db2cmv8/lib/db2jcc_license_cu.jar,
C:/Program Files/IBM/db2cmv8/lib/db2jcc_license_cisuz.jar,
C:/Program Files/IBM/db2cmv8/lib/xerces.jar,
C:/Program Files/IBM/db2cmv8/lib/cmblog4j81.jar,
C:/Program Files/IBM/db2cmv8/lib/log4j-1.2.8.jar,
C:/Program Files/IBM/db2cmv8/lib/cmbsdk81.jar,
C:/Program Files/IBM/db2cmv8/lib/cmbwas81.jar
```

3) If the application server is not currently running, start the server; otherwise, stop and then restart the server.

You can now connect to the IBM Content Manager datastore from the IBMCMConnectorService Property Sheets by using the Use User Credentials as the login mode.

You have now completed the required steps for this procedure.

(Optional) If you want to connect to IBM Content Manager datastore from IBMCMConnectorService Property Sheets by using the Use Credentials From Process Context as the login mode, complete the following procedure.

Connect using Use Credentials from process context login mode

1) Open a web browser and enter this URL:
   http://[host]:[port]/adminui
2) Log in using the super administrator credentials. Default values set during installation are:
   User name: *administrator*
   Password: *password*
3) Click **Services** > **Connector for IBM Content Manager**
4) Type all of the required repository information and click **Save**. For more information about the IBM Content Manager repository information, click the **Help** link in the upper-right corner of the page.
5) Do one of these tasks:
   – To use the IBM Content Manager Authorization service IBMCMAuthProvider to use content from an IBM Content Manager datastore, in the Processes view of Workbench, continue with this procedure. Using the IBM Content Manager Authorization service overrides the default AEM Forms authorization and must be configured to log in to Workbench by using IBM Content Manager credentials.
   – To use the System Credentials provided in step 4 to use content from an IBM Content Manager datastore, in the Processes view of Workbench, log in to Workbench by using the AEM Forms super administrator credentials (by default, *administrator* and *password*). You have now completed the required steps for this procedure. The System Credentials that are provided in step 4 use the default AEM Forms authorization service for accessing the default repository in this case.
6) Log in to the administration console, and click **Settings** > **User Management** > **Domain Management**.
7) Click **New Enterprise Domain** and type a domain ID and name. The domain ID is the unique identifier for the domain. The name is a descriptive name for the domain. ***NOTE:*** *When using DB2 for your AEM Forms database, the maximum permitted length of the ID is 100 single-byte (ASCII) characters or 50 double-byte characters or 25 four-byte characters. (See "Adding enterprise domains" in administration help.)*
8) Add a custom authentication provider:
   – Click **Add Authentication**.
   – In the **Authentication Provider** list, select **Custom**, and then select **IBMCMAuthProviderService**and click **OK**.
9) Add an LDAP authentication provider:
   – Click **Add Authentication**.
   – In the **Authentication Provider** list, select **LDAP** and then click **OK**.

10) Add an LDAP directory:
    - Click**Add Directory**.
    - In the **Profile Name** box, type a unique name, and then click **Next**.
    - Specify values for the **Server**, **Port**, **SSL**, **Binding**, and **Populate page with** options. If you select **User** for the **Binding** option, you must also specify values for the **Name** and **Password** fields. (Optional) Select **Retrieve Base DN** to retrieve base domain names, as required. When finished, click **Next**.
    - Configure the user settings, click **Next**, configure group settings as required, and then click **Next**.

    *For details about the above settings, click the **Help** link in the upper-right corner of the page.*
11) Click **OK** to exit the Add Directory page and click **OK** again.
12) Select the new enterprise domain and click **Sync Now**. Depending on the number of users and groups in your LDAP network and the speed on your connection, the synchronization process may take several minutes.
13) To verify the status of the synchronization, click **Refresh** and view the status in the **Current Sync State** column.
14) Navigate to **Settings** > **User Management** > **Users and Groups**.
15) Search for users that were synchronized from LDAP and do these tasks:
    - Select one or more users and click **Assign Role**.
    - Select one or more AEM Forms roles and click **OK**.
    - Click **OK** a second time to confirm the role assignment.

    *Repeat this step for all users that you want to assign roles to. For more information, click the **Help** link in the upper-right corner of the page.*
16) Start Workbench and log in using the following credentials for IBM Content Manager datastore:

    ***Username:** [username]@[repository_name]*

    ***Password:** [password]*

    *The IBM Content Manager datastore can now be used in the Processes view within Workbench when the login mode for IBMCMConnectorService orchestrable components is selected as**Use Credentials from process context.***

8.14. Configuring the Connector for IBM FileNet

AEM forms supports IBM FileNet 5.0 and 5.2 only. Make sure your ECM is upgraded accordingly.

NOTE: AEM Forms supports FileNet 5.2 Content Engine; FileNet 5.2 Process Engine is not supported.

If you installed Connector for IBM FileNet as part of your AEM Forms, you must configure the service to connect to the FileNet object store.

NOTE: Ensure that installing client for the connectors, copying of JAR file, and configuration changes tasks are performed on all the nodes of the cluster.

Complete the following procedure to configure Connector for IBM FileNet.

1) Log in to WebSphere Administrative Console, click **Servers > Server Types > WebSphere application servers**, and then click the name of the server instance to configure (for example, server1).
2) Under Server Infrastructure, click **Java and forms workflow** > **Process Definition**.
3) Under Additional Properties, click **Java Virtual Machine**.
4) Click **Apply** and then click **Save to Master Configuration**.
5) Locate the adobe-component-ext.properties file in the*[appserver root]*/profiles/[profile name] folder (if the file does not exist, create it).
6) Add a new system property that provides the location of these FileNet Application Engine JAR files:

   For FileNet 5.x add following JAR files

   – Jace.jar
   – javaapi.jar
   – log4j.jar
   – pe.jar
   – stax-api.jar
   – xlxpScanner.jar
   – xlxpScannerUtils.jar

   NOTE: Add the pe.jar file only if your deployment uses the IBMFileNetProcessEngineConnector service. The new system property should reflect this structure:

   ```
   [component id].ext=[JAR files and/or folders]
   ```

   For example, using a default FileNet Application Engine installation on a Windows operating system, add the following system property on a new line with no line breaks and end the line with a carriage return:

   NOTE: The following text contains formatting characters for line breaks. If you copy this text to a location outside this document, remove the formatting characters when you paste it to the new location.

   ```
   com.adobe.livecycle.ConnectorforIBMFileNet.ext=
   C:/Program Files/FileNet/AE/CE_API/lib2/javaapi.jar,
   C:/Program Files/FileNet/AE/CE_API/lib2/log4j-1.2.13.jar
   ```

7) (FileNet Process Engine Connector only) Configure the connection properties for the process engine as follows:

   – Using a text editor, create a file with the following content as a single line and end the line with a carriage return:

     (FileNet 5.0 only)

     ```
     RemoteServerUrl =
     cemp:http://[contentserver_IP]:[contentengine_port]/wsi/FNCEWS40DIME
     /
     ```

     (FileNet 5.2 only)

     ```
     RemoteServerUrl =
     cemp:http://[contentserver_IP]:[contentengine_port]/wsi/FNCEWS40MTOM
     /
     ```

– Save the file as WcmApiConfig.properties in a separate folder, and add the location of the folder that contains the WcmApiConfig.properties file to the adobe-component-ext.properties file.

For example, if you save the file as c:/pe_config/WcmApiConfig.properties, add the path c:/pe_config to the adobe-component-ext.properties file.

NOTE: The filename is case-sensitive.

8) Locate the file wsjaas.conf and add the following lines:

```
FileNetP8 {com.filenet.api.util.WSILoginModule required;};
FileNetP8WSI {com.filenet.api.util.WSILoginModule required;};
FileNetP8Engine
{com.ibm.ws.security.common.auth.module.proxy.WSLoginModuleProxy
required delegate=com.ibm.ws.security.common.auth.module.
WSLoginModuleImpl;};
FileNetP8Server
{com.ibm.ws.security.common.auth.module.proxy.WSLoginModuleProxy
required delegate=com.ibm.ws.security.common.auth.module.
WSLoginModuleImpl;};
FileNetP8KerberosService
{com.ibm.ws.security.common.auth.module.proxy.WSLoginModuleProxy
required delegate=com.filenet.engine.authentication.kerberos.login.
KrbServiceLoginModule;
com.ibm.ws.security.common.auth.module.proxy.WSLoginModuleProxy required
delegate=com.ibm.ws.security.server.lm.ltpaLoginModule;
com.ibm.ws.security.common.auth.module.proxy.WSLoginModuleProxy required
delegate=com.ibm.ws.security.server.lm.
wsMapDefaultInboundLoginModule;};
```

NOTE: By default, the wsjaas.conf file is located in the folder *[appserver root]*/profiles/*[profile name]/properties/.*

9) If the application server is not currently running, start the server. Otherwise, stop and then restart the server.

10) (*Applicable only if IBM FileNet and AEM Forms are installed on the same WebSphere application server*) Verify that these settings have been implemented correctly in the WebSphere Administrative Console by doing the following:

– In the WebSphere Administrative Console navigation tree, click **Security > Global security.**

– Under Authentication, click **Java Authentication and Authorization Service > Application logins**.

– Click the **FileNetP8** application login, and then click **JAAS login modules**.

If the values on this page do not match the following, modify them:

***Module class name**: "com.filenet.api.util.WSILoginModule"*

***Authentication Strategy**: REQUIRED*

***Module Order**: 1*

*Click **OK** or **Apply**, and then click **Save directly to master configuration**.*

11) Open a web browser and enter this URL:

http://[host]:[port]/adminui

12) Log in using the default user name and password:

***User name**: administrator*

***Password**: password*

13) Click **Services** > **Connector for IBM FileNet**.

14) Provide the Content Engine URL. For example, `cemp:http://ContentEngineHostNameorIP:port/wsi/FNCEWS40MTOM?jaasConfigurationName=FileNetP8WSI`

15) Provide all the required FileNet repository information and, under Repository Service Provider Information, select **IBM FileNet Repository Provider**.

*If your deployment uses the optional process engine service, under Process Engine Settings, select **Use Process Engine Connector Service** and specify the process engine settings. For more information, click the **Help** link in the upper-right corner of the page.*

NOTE: The credentials that you provide in this step are validated later when you start the IBM FileNet repository services. If the credentials are not valid, an error is thrown and the services will not start.

16) Click **Save** and navigate to **Services** > **Applications and Services** > **Service Management**.

17)

18) Select the check box next to each of these services and click **Start**:

- IBMFileNetAuthProviderService
- IBMFileNetContentRepositoryConnector
- IBMFileNetRepositoryProvider
- IBMFileNetProcessEngineConnector (if configured)

If any of the services do not start correctly, verify the Process Engine settings.

19) Do one of the following tasks:

- To use the FileNet Authorization service (IBMFileNetAuthProviderService) to display content from a FileNet object store in the Resources view of Workbench, continue with this procedure. Using the FileNet Authorization service overrides the default AEM Forms authorization and must be configured to log in to Workbench by using FileNet credentials.
- To use the AEM forms repository, log in to Workbench by using the super administrator credentials (by default, *administrator* and *password*). The credentials provided in step 16 use the default AEM Forms authorization service for accessing the default repository in this case.

20) Restart your application server.

21) Log in to administration console and click **Settings** > **User Management** > **Domain Management**.

22) Click **New Enterprise Domain** and then type a domain ID and name. The domain ID is the unique identifier for the domain. The name is a descriptive name for the domain.

When using DB2 for your AEM Forms database, the maximum permitted length of the ID is 100 single-byte (ASCII) characters or 50 double-byte characters or 25 four-byte characters. (See "Adding enterprise domains" in Administration Help.)

23) Add a custom authentication provider:

- Click **Add Authentication**.
- In the **Authentication Provider** list, select **Custom**.
- Select **IBMFileNetAuthProviderService** and then click **OK**.

24) Add an LDAP authentication provider:
- Click **Add Authentication**.
- In the **Authentication Provider** list, select **LDAP** and then click **OK**.

25) Add an LDAP directory:
- Click**Add Directory** and, in the **Profile Name** box, type a unique name, and then click **Next**.
- Specify values for the **Server**, **Port**, **SSL**, **Binding**, and **Populate page with** options. If you select **User** for the **Binding** option, you must also specify values for the **Name** and **Password** fields.
- (Optional) Select **Retrieve Base DN** to retrieve base domain names, as required. When finished, click **Next**.
- Configure the user settings, click **Next**, configure group settings as required, and then click **Next**.

  *For details about the settings, click **Help** link in the upper-right corner of the page.*

26) Click **OK** to exit the Add Directory page, and then click **OK** again.

27) Select the new enterprise domain and click **Sync Now**. Depending on the number of users and groups in your LDAP network and the speed on your connection, the synchronization process may take several minutes.

  *(Optional) To verify the status of the synchronization, click **Refresh** and view the status in the **Current Sync State** column.*

28) Navigate to **Settings** > **User Management** > **Users and Groups**.

29) Search for users that were synchronized from LDAP and perform these tasks:
- Select one or more users and click **Assign Role**.
- Select one or more AEM Forms roles and click **OK**.
- Click **OK** a second time to confirm the role assignment.

  *Repeat this step for all users you want to assign roles to. For more information, click the **Help** link in the upper-right corner of the page.*

30) Start Workbench and log in using the following credentials for the IBM FileNet repository:

  ***User name:** [username]@[repository_name]*

  ***Password:** [password]*

  The FileNet object store should now be visible in the Resources view within Workbench. If you do not log in using the username@repository name, Workbench attempts to log in to the default repository specified in step 16.

31) (Optional) If you intend to install the AEM Forms Samples for Connector for IBM FileNet, create a FileNet object store named *Samples* and install the samples in that object store.

  After you configure Connector for IBM FileNet, it is recommended that you see administration help for information about configuring Workbench functions properly with your FileNet repository.

8.15. Configure the ContentRepositoryConnector service

By default, the ContentRepositoryConnector service is configured to use URL http://local-host:8080/lc/crx/server/. Perform the following steps to configure the service for your environment:

1) Log in to AEM Forms Admin UI using credentials administrator/password. The default URL of Admin UI is http://[IP]:[Port]/adminui.
2) Navigate to Services > Application and Services > Service Management.
3) Search and open the ContentRepositoryConnector service for editing.
4) Open the Configuration tab and replace the default URL in the Experience Management Server field with the URL of your environment.

IP

IP address of the machine on which application server is running.

Port

Port number which AEM Forms is using. The default port number for JBoss, WebLogic, and WebSphere 8080, 8001, and 9080, respectively.

9. Configuring Load Balancing

You can configure your WebSphere cluster to provide load-balancing functionality. Use the IBM HTTP server that ships with the WebSphere Application Server to perform the following tasks:

- Preparatory tasks. (Preparingforinstallation)
- Install IBM HTTP Server. (Installingtheweb server)
- Install the web server plug-in. (Installingtheweb server plug-in)

NOTE: AEM Forms in a cluster environment supports only sticky sessions for load balancing. IBM HTTP server supports sticky sessions by default.

NOTE: Session affinity associates all the requests coming from an end-user with a specific node of the application server cluster. It is required to keep the session affinity enabled for cluster environments. For detailed instructions to configure session affinity, see documentation of corresponding application server.

9.1. Preparing for installation

Before you install the web server, perform the following configuration tasks:

Server domain: If you are using a domain architecture, ensure that the server is not a member of any domain other than the same domain as the LDAP server.

Create local user: In Microsoft Windows, if you plan to run IBM HTTP Server as a service, you can create a local account and make this account a part of the local administrators group.

9.2. Installing the web server

The following steps describe how to install IBM HTTP Server on a separate node from the WebSphere Network Deployment or WebSphere basic application servers. For information about installing and configuring other IBM supported web servers, such as Apache, Microsoft IIS, and Sun Java System Web Server, see the IBM web page Editing Web Server ConfigurationFile.

NOTE: *Ensure that you have WebSphere Application Server Network Deployment and supplement installation files are available locally.*

You must first insert the installation media or copy the files to a local directory.

NOTE: This procedure can be used to upgrade the current version of IBM HTTP Server by replacing the existing installation.

1) To start the installation, go to the directory that contains the WebSphere Application Server Network Deployment installer and type the appropriate command:
   - (Linux/UNIX) `./launchpad.sh`
   - (Windows) `launchpad.bat`

2) From the Launch Pad, select **Launch the installation wizard for IBM HTTP Server** and provide location of first part of the extracted installation files of the supplement.
3) On the Welcome screen, click **Next**.
4) Select **I accept both the IBM and the non-IBM terms** and click **Next**.
5) Specify the location of the installation directory and click **Next**.
6) Specify the HTTP port and HTTP Administration port and click **Next**.
7) (Windows) Select**Run IBM HTTP Server as a Windows Service**, **Run IBM HTTP Administration as a Windows Service**, and **Log on as local system account**.

   NOTE: A user name and password is not required for this selection. To run this service using a specific user account and password combination, select**Log on as a specified user account***and specify your user ID and password information.*
8) Under Startup Type, select **Automatic** and then click **Next**.
9) Provide User ID and Password to create HTTP Administration server and click Next.
10) Uncheck**Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server Web server definition** option and click Next.
11) Review the Installation Summary panel to verify your selections, click **Back** to change any of your specifications, and click **Next** to begin installing IBM HTTP Server.

    After displaying the installation status, the wizard displays the Completion status panel that indicates a successful installation.
12) Click **Finish**.

9.3. Installing the web server plug-in

After the application server is installed and the applications are deployed, install the web server plug-in on the HTTP server. This procedure assumes that the HTTP server is on a node that is not in the cluster.

1) On the web server computer (the remote system that has HTTP server installed),go to the WebSphere Network Deployment installer directory and run Launch Pad by typing the appropriate command:
   – (Linux/UNIX) `./launchpad.sh`
   – (Windows) `launchpad.bat`
2) From Launch Pad, select **Launch the installation wizard for Web server plug-ins**.
3) Deselect **Installation roadmap** and **Plug-ins section of the Getting Started guide**, and then click **Next**.
4) Select **I accept both the IBM and the non-IBM terms** and click **Next**. The installer will now check your system.
5) On the System Prerequisites Check screen, click **Next**.
6) If your system passes the prerequisites check, click **Next**.

   NOTE: If your system does not pass the prerequisites check, stop the installation, correct any problems, and restart the installation.
7) Select **IBM HTTP Server V7** and click **Next**.

8) Select **Web server machine (remote)**and click **Next**.
9) Specify the *[plugins_root]*directory and the location where the web server plug-ins should be installed, and click **Next**.
10) In **Select the existing IBM HTTP Server httpd.conf file**, click **Browse** and select the httpd.conf file from the *[webserver root]*/conf directory, where *[webserver root]* specifies the directory where IBM HTTP Server is installed.
11) In the **Specify the Web server port** box, keep the default port value of 80 and click **Next**.
12) In the **Specify a unique Web server definition name** box, enter a unique identifier for this definition and then click **Next**.
13) In the **Web server plugin-cfg.xml file** box, accept the default settings and then click **Next**.
14) In the **Host name or IP address for the Application Server** box, type the host name or IP address of the ND node and then click **Next**.
15) In the confirmation pane, click **Next** and, in the summary information pane, click **Next**.
16) After the the web server plug-in is installed and copied, click **Next** and then click **Finish**.
17) Copy the appropriate file from IBM HTTP Server <plugin_dir>/bin to the WebSphere Network Deployment *[appserver root]*\bin folder:
    – (Windows) configure*[webserver definition name]*.bat. For example, configureserver1.bat
    – (Linux/UNIX) configure*[webserver definition name]*.sh
18) Ensure that Deployment Manager is running and then run configure*<webserver definition name>*.bat for Windows or configure*<webserver definition name>*.sh for Linux or UNIX on the WebSphere Network Deployment computer to create an unmanaged node on the WebSphere Network Deployment computer and add the web server to it.
19) Log in to the WebSphere Administrative Console and, in the navigation tree, click **Servers > Web servers** and then, click web server name. Under **Additional Properties**click **Remote Web server management**. Ensure that Port, Username and Password details are the same as provided for IBM HTTP Administration server.
20) Click **Servers > Web servers**and then, in the right pane, Select check box beside the web server name. Click **Start**.Before performing above step, ***NOTE:*** *ensure that IBM HTTP Administration Server is running on the remote machine (IBM HTTP Server machine)*
21) Open a web browser and access the administrative console for the web server computer (http://*[web server name]*:80/adminui) to verify whether the plug-in generated and propagated successfully. The following response indicates that you must generate and propagate the plug-in as described in steps 21 to 24:

    `/[application name] not defined`

    NOTE: The plug-in generates and propagates automatically only if your system previously enabled automatic synchronization, which is disabled by default.
22) Log in to the WebSphere Administrative Console and, in the navigation tree, click **Servers** > **Web servers** and then, in the right pane, select the **Select** check box beside the HTTP server name.
23) Click **Generate Plug-in**. A message confirms successful generation of the Plugin-cfg.xml file.
24) Click **Propagate Plug-in**. A message confirms successful propagation of the Plugin-cfg.xml file.
25) Restart the web server.

10. Advanced Production Configuration

This section describes advanced tuning for Output, Forms Standard, and PDF Generator modules. This section should be completed only on a production system by an advanced application server administrator.

10.1. Configuring pool size for Output and Forms

The current default value for PoolMax is 4. The actual value to set depends on the hardware configuration and the expected usage in your environment.

For optimal use, we recommend that the lower limit of PoolMax not be less than the number of CPU cores that are available. The upper limit must be determined by the load pattern on your server. Generally, the upper limit should be set to twice the number of CPUs cores on your server.

Modify the existing PoolMax value

1) Log in to the WebSphere Administrative Console.
2) In the navigation tree, click **Servers** >**Application Servers**>*[server name]*>**Java and Process Management** >**Process Definition** > **Java Virtual Machine**> **Custom Properties**.
3) Add the following properties for ConvertPdf:
   - `com.adobe.convertpdf.bmc.POOL_MAX=[new value]`
   - `com.adobe.convertpdf.bmc.MAXIMUM_REUSE_COUNT=5000`
   - `com.adobe.convertpdf.bmc.REPORT_TIMING_INFORMATION=true`
   - `com.adobe.convertpdf.bmc.CT_ALLOW_SYSTEM_FONTS=true`
4) Add the following properties for XMLFM:
   - `com.adobe.xmlform.bmc.POOL_MAX=[new value]`
   - `com.adobe.xmlform.bmc.MAXIMUM_REUSE_COUNT=5000`
   - `com.adobe.xmlform.bmc.REPORT_TIMING_INFORMATION=true`
   - `com.adobe.xmlform.bmc.CT_ALLOW_SYSTEM_FONTS=true`
5) (*Cluster only*) Repeat steps 2 to 4 for each server in the cluster.

10.2. PDF Generator

PDF Generator is capable of doing multiple PDF conversions simultaneously for some types of input files. This is enforced through the use of stateless session beans.

Configuring EJB Pool Size

Four different stateless session beans exist for enforcing independent pool sizes for the following types of input files:

- Adobe PostScript® and Encapsulated PostScript (EPS) files
- Image files, such as BMP, TIFF, PNG, and JPEG files
- OpenOffice files
- All other file types (except HTML files), such as Microsoft Office, PageMaker®, and FrameMaker® files

The pool size for HTML-to-PDF conversions is not managed through the use of stateless session beans.

The default pool size for PostScript and EPS files and for image files is set to 3, and the default pool size for OpenOffice and other file types (except HTML) is set to 1.

You can configure the PS/EPS and image pool size to a different value based on your server hardware configuration, such as the number of CPUs, the number of cores within each CPU, and so on. However, it is mandatory that the pool size for the OpenOffice and other file types be left unchanged at 1 for proper functioning of PDF Generator.

This section describes how the pool size for PS2PDF and Image2PDF can be configured for each of the supported application servers.

The text that follows assumes that the following two AEM Forms on JEE application EARs are deployed on the application server:

- adobe-livecycle-websphere.ear
- adobe-livecycle-native-websphere-*[platform]*.ear

  where [platform] should be replaced with one of the following strings, depending on your operating system:
- (Windows) x86_win32
- (Linux) x86_linux
- (SunOS™) sparc_sunos
- (AIX) powerpc_aix

Configure the pool size for PS2PDF and Image2PDF

10.3. Enabling CIFS on Windows

You will need to manually configure the Windows Server machine that host AEM Forms on JEE.

NOTE: Ensure that the server has a static IP address.

On Windows machines, you need to do the following:

Enable NetBIOS over TCP/IP

You need to enable NetBIOS over TCP/IP so that clients connecting to the AEM Forms on JEE Server can have their requests revolved for the server host name.

1) In the **Local Area Connection Properties** dialog box, on the**General** tab, select **Internet Protocol**, and then click **Properties**.
2) In the **General** tab of the**Internet Protocol (TCP/IP) Properties** dialog box, ensure that the server has a static IP address. Click **Advanced**.
3) In the **Advanced TCP/IP Settings** dialog box, select the **WINS** tab and select **Enable NetBIOS over TCP/IP**.

Add additional IP addresses

1) In the **Local Area Connection Properties** dialog box, on the**General** tab, select **Internet Protocol**, and then click **Properties**.
2) In the **General** tab of the**Internet Protocol (TCP/IP) Properties** dialog box, ensure that the server has a static IP address. Click **Advanced**.
3) In the **Advanced TCP/IP Settings** dialog box, select the **IP Settings**tab and click **Add**.
4) Specify a static IP address and click **Add.**

Disable SMB over NetBIOS registry (Windows Server 2003 only)

You must disable SMB over NetBIOS by editing the Windows registry.

1) In the Windows Registry Editor, navigate to **HKEY_LOCAL_MACHINE** > **SYSTEM** > **CurrentControlSet** > **Services** > **NetBT** > **Parameters**.
2) Set the DWORD **SMBDeviceEnabled** to 0. If it is not present, add a new DWORD value with name SMBDeviceEnabled and set it to 0.

Disable File and Printer Sharing on Windows Server 2008

- Go to **Network Settings**, deselect **File and Printer Sharing for Microsoft Clients,** and c lick **Apply**.

Disable File and Printer Sharing on Windows Server 2012 only)

- Go to **Control Panel > Network and Internet >Network and Sharing Center > Advanced sharing settings**, and turn off **File and Printer Sharing**.

11. Appendix - Install using the Command Line Interface

11.1. Overview

AEM Forms on JEE provides a command line interface (CLI) for the installation program. The CLI is intended to be used by advanced users of AEM Forms on JEE or in server environments which do not support the use of the Graphical User Interface (GUI) of the installation program. The CLI runs in console mode with one interactive session for all install operations.

After you start the installation process, follow the on-screen instructions to choose your installation options. Respond to each prompt to proceed to the next step in the installation.

NOTE: If you want to change a choice that you made on a previous step, type `back`. You can cancel the installation at any time by typing `quit`.

11.2. Install AEM Forms on JEE

1) Open a command prompt and navigate to the folder in the installation media or your hard disk that contains the installer executable:
   - (Windows) server\Disk1\InstData\Windows_64\NoVM
   - (Linux) server/Disk1/InstData/Linux/NoVM
   - (Solaris) server/Disk1/InstData/Solaris/NoVM
   - (AIX) server/Disk1/InstData/AIX/VM
2) Open a command prompt and run the following command:
   - (Windows) `install.exe -i console`
   - (Non-Windows) `./install.bin -i console`

     NOTE: Entering the command without the `-i console` option launches the GUI-based installer.
3) Respond to the prompts as described in the following table:

Prompt	Description
Choose Locale	Select the locale for the installation to use by entering a value between 1 and 3. You can select the default value by pressing **Enter**. The options are Deutsch, English, and Français. English is the default locale.
Choose Install Folder	On the Destination screen, press **Enter** to accept the default directory or type the new installation directory location. Do not use accented characters in the directory name. Otherwise, the CLI will ignore the accents and create a directory after modifying the accented characters.
AEM forms on JEE Server License Agreement	Press **Enter** to read through the pages of the license agreement. If you agree to the agreement, type `Y` and press **Enter**.
Pre-Installation Summary	Press **Enter** to continue installation with the choices you have made. Type `back` to go back to previous steps and change any of the settings.
Ready To Install	Press **Enter** to start the installation process.
Installing	During the installation process, the progress bar advances to indicate the progress of installation.
Configuration Manager	Press **Enter** to complete the installation of AEM Forms on JEE. You can run the Configuration Manager in GUI mode by invoking the following script: (Windows): C:\Adobe\Adobe_Experience_Manager_Forms\configurationManager\bin\ConfigurationManager.bat (Non-Windows): `/opt/adobe/Adobe_Experience_Manager_Forms/configurationManager/bin/ConfigurationManager.sh`
Installation Complete	Press **Enter** to exit the installer.

11.3. Error logs

If an error occurs, you can review the install.log in the log directory of your installation:

- (Windows) *[aem-forms root]*\log
- (non-Windows) *[aem-forms root]*/log

12. Appendix - Configuration Manager Command Line Interface

The CLI is intended to be used in server environments that do not support the use of the Graphical User Interface (GUI) of the Configuration Manager.

12.1. Order of operations

The Configuration Manager CLI must follow the same order of operations as the GUI version of the Configuration Manager. Ensure that you use the CLI operations in this order:

1) Configure AEM Forms on JEE.
2) Configure CRX.
3) Migrate existing turnkey database. (Upgrade Turnkey only)
4) Validate application server topology.
5) Validate database connectivity.
6) Configure the application server.
7) Validate application server configurations.
8) Deploy AEM Forms on JEE.
9) Initialize AEM forms on JEE.
10) Validate AEM Forms on JEE.
11) Deploy the AEM Forms on JEE modules.
12) Validate the AEM Forms on JEE module deployment.
13) Check system readiness for PDF Generator.
14) Add administrator user for PDF Generator.
15) Configure Connector for IBM Content Manager.
16) Configure Connector for IBM FileNet.
17) Configure Connector for EMC Documentum.
18) Configure Connector for SharePoint.

IMPORTANT: You must restart each of your cluster nodes after you complete Configuration Manager CLI operations.

12.2. Command Line Interface property file

- Use the property file cli_propertyFile_template.txt file as a template and edit the values based on the Configuration Manager operations you intend to use.

- Use the GUI of the Configuration Manager and then use the property file created by the GUI version as the CLI version property file. When you run the *[aem-forms root]*/configurationManager/bin/ConfigurationManager.bat/sh file, the userValuesForCLI.properties file is created in the *[aem-forms root]*/configurationManager/config directory. You can use this file as input for the Configuration Manager CLI.

  NOTE: The file does not contain the properties listed below, which are optional. If required, you can manually add these properties to the file:

  – `ApplicationServerRestartRequired`
  – `lcGdsLocation`
  – `lcPrevGdsLocation`

  NOTE: In the CLI properties file, you must use the escape character (\) for Windows paths directory separator (\). For example, if the Fonts folder to be mentioned is C:\Windows\Fonts, in the Configuration Manager CLI script, you should enter it as `C:\\Windows\\Fonts`.

  NOTE: The following modules depend on ALC-LFS-ContentRepository. If you are using the cli_propertyFile_template.txt as template then either remove the ALC-LFS-ContentRepository from excludedSolutionComponents list or add the following LFS in excludedSolutionComponents list:

  – *ALC-LFS-ProcessManagement*
  – *ALC-LFS-CorrespondenceManagement*
  – *ALC-LFS-ContentRepository*
  – *ALC-LFS-MobileForms*
  – ALC-LFS_FormsManager

12.3. General configuration properties

Common properties

Common properties are:

WebLogic and WebSphere specific properties: Required for the Configure Application Server, Deploy AEM Forms on JEE, Validate Application Server Topology and Validate Application Server Configurations operations.

AEM Forms on JEE Server specific properties: Required for the Initialize AEM Forms on JEE and Deploy AEM Forms on JEE Components operations.

These properties are required for the following operations:

- Initialize AEM Forms on JEE
- Deploy AEM Forms on JEE components.

Property	Values	Description
targetServer.topologyType	server or cluster	The type of application server topology for which you are deploying AEM forms on JEE.
targetServer.name	String	The name assigned to the application server/admin server node or cluster.
targetServer.adminHost	String Default is *localhost*	The hostname of the server where the application server is installed.
targetServer.adminPort	Integer	The port number the admin server uses to listen for SOAP requests.
targetServer.adminUserID	String	The administrative user ID to use when accessing the application server.
localServer.appServerRootDir	Default: (Windows) C:\Program Files\IBM\ WebSphere\AppServer (Linux, Solaris) /opt/IBM/WebSphere/AppServer (AIX) /usr/IBM/WebSphere/AppServer	The root directory of the application server instance that you are configuring locally (on which you plan to deploy AEM Forms on JEE or that you will use to communicate with a remote server on which you plan to deploy AEM Forms on JEE).
AEM Forms on JEE Server specific properties		
LCHost	String	The hostname of the server where AEM Forms on JEE will be deployed. For cluster deployments, hostname of any one of the cluster nodes where the application server is running.
LCPort	Integer	The web port number where AEM Forms on JEE will be deployed.

Property	Values	Description
excludedSolutionComponents	String. Values include: ALC-LFS-Forms, ALC-LFS-ConnectorEMCDocumentum, ALC-LFS-ConnectorIBMFileNet, ALC-LFS-ConnectorIBMContentManager, ALC-LFS-DigitalSignatures, ALC-LFS-DataCapture, ALC-LFS-Output, ALC-LFS-PDFGenerator, ALC-LFS-ProcessManagement, ALC-LFS-ReaderExtensions, ALC-LFS-RightsManagement ALC-LFS-CorrespondenceManagement, ALC-LFS-ContentRepository, ALC-LFS-MobileForms, ALC-LFS_FormsManager	(Optional) List the AEM Forms on JEE modules you do not want to configure. Specify the excluded modules in a comma separated list.
includeCentralMigrationService	true: to include service false: to exclude servcie	The property to include or exclude Central Migration Bridge Service.
CRX Content repository The following properties are specified in the `cli_propertyFile_crx_template.txt`file.	true: false:	
contentRepository.rootDir		Path of the CRX repository.
use.crx3.mongo	true: false:	If you have performed a fresh installation, to use Mongo DB with CRX3 set value to true. If the value is false CRX3 TAR is configured.
mongo.db.uri	<URI of Mongo DB>	If you are using Mongo DB, set URI of Mongo DB
mongo.db.name	<name of Mongo DB>	If you are using Mongo DB, provide name of Mongo DB instance

Property	Values	Description
use.crx3.rdb.mk	true: false:	When the value of this property is true, the CRX repository is configured with RDB MK. The default value is false where the repository is configured as CRX3 TAR.

Configure AEM Forms on JEE properties

These properties only apply to the configure AEM Forms on JEE operation.

Property	Values	Description
AdobeFontsDir	String	Location of the Adobe server fonts directory. This path must be accessible from all cluster nodes being deployed to.
customerFontsDir	String	Location of the customer fonts directory. This path must be accessible from all cluster nodes being deployed to.
systemFontsDir	String	Location of the system fonts directory. This path must be accessible from all cluster nodes being deployed to.
LCTempDir	String	Location of the temporary directory. This path must be accessible from all cluster nodes being deployed to.

Property	Values	Description
LCGlobalDocStorageDir	String	The global document storage root directory. Specify a path to an NFS shared directory used to store long-lived documents and to share them among all cluster nodes. This path must be accessible from all cluster nodes being deployed to.
EnableDocumentDBStorage	true or false Default: false	Enables or disables document storage in database for persistent documents. Even if you enable document storage in database, you will need the file system directory for GDS.

Configure or validate application server properties

Configure or Validate WebSphere properties

The Configuration Manager can configure or validate your WebSphere application server as required by AEM Forms on JEE.

These properties apply to the following operations:

- Configure Application Server
- Validate Application Server Topology
- Validate Application Server Configurations
- Validate Database Connectivity

Application server properties

Property	Values	Description
You must configure the application server-specific properties section. For more information see Commonproperties		

Property	Values	Description
jvm.initialHeapSize	Default: 256	The initial heap size, in MB, for the JVM.
jvm.maxHeapSize	Default: 4096	The maximum heap size, in MB, for the JVM.
WebLogic and WebSphere Cluster only		
cache.useUDP	true	Set the value to `true` if AEM Forms on JEE uses UDP to implement caching. Set to `false` if AEM Forms on JEE uses TCP to implement caching.
cache.udp.port	Default: 33456	The port number that the primary computer uses for UDP-based caching communication. Configure only if cache.useUDP=true.
cache.tcpip.primaryhost	String	The host name of the computer where the primary application server is installed. Configure only if cache.useUDP!=true.
cache.tcpip.primaryport	Default: 22345	The port number that the primary application server computer uses for TCP-based caching communication. Configure only if cache.useUDP!=true.
cache.tcpip.secondaryhost	String	The host name of the computer where the secondary application server is installed. Configure only if cache.useUDP!=true.
cache.tcpip.secondaryport	Default: 22345	The port number that the secondary application server computer uses for TCP-based caching communication. Configure only if cache.useUDP!=true.

Property	Values	Description
Datasource configuration		
datasource.dbType	Choose: • oracle *db2* *sqlserver*	The type of database configured to use with AEM Forms on JEE.
datasource.dbName	String	The name of the database.
datasource.dbHost	String	The host name or IP address of the server where the database is located.
datasource.dbPort	Integer	The database port AEM Forms on JEE will use when communicating with the database.
datasource.dbUser	String	The user ID AEM Forms on JEE will use when accessing the database.
datasource.dbPassword	String	The password associated with the database user ID.
datasource.target.driverPath	String	JDBC driver in the application server lib directory. This path must be valid and accessible from all cluster nodes being configured.
datasource.local.driverPath	String	Local JDBC driver. This value is used for testing direct database connection.

Deploy AEM Forms on JEE properties

These Deploy AEM Forms on JEE properties only apply to the deploy AEM Forms on JEE operation.

Property	Values	Description
For more information, see Common properties.		

Property	Values	Description
deployment.includeIVS	false	Specifies whether IVS EAR files are included in the deployment. It is recommended not to include IVS EAR files in a production environment.
targetServer.virtualHost	String	Virtual host of your WebSphere application server. The default values are admin_host, default_host, proxy_host.

Initialize AEM Forms on JEE properties

These initialize AEM Forms on JEE properties only apply to the initialize AEM Forms on JEE operation.

Property	Values	Description
For more information, see Common properties.		

Deploy AEM Forms on JEE Components properties

These properties apply to the following operations:

- Deploy AEM Forms on JEE Components
- Validate AEM Forms on JEE Component Deployment
- Validate AEM Forms on JEE Server.

Property	Values	Description
You must configure the AEM Forms on JEE Server Information section. For more information, see Common properties		
LCAdminUserID	String	The user ID to assign to the AEM Forms on JEE Administrator user. This User ID is used to login to the Administrator Console.
LCAdminPassword	String	The password to assign to the AEM Forms on JEE Administrator user. This password is used to login to the Administrator Console.

Add administrator user for PDF Generator

These properties apply only to the adding administrator user for PDF Generator operation. These properties are present in cli_propertyFile_pdfg_template.txt

Property	Values	Description
LCHost	String	Hostname where AEM Forms on JEE Server is installed.
LCPort	Integer	Port number where AEM Forms on JEE application server is configured
LCAdminUserID	String	The user ID to assign to the AEM Forms on JEE Administrator user. This User ID is used to login to the Administrator Console.
LCAdminPassword	String	The password to assign to the AEM Forms on JEE Administrator user. This password is used to login to the Administrator Console.
LCServerMachineAdminUser	String	The user ID of the Administrator user of the Operation System hosting AEM forms on JEE
LCServerMachineAdminUserPasswd	String	The password of the Administrator user of the Operation System hosting AEM forms on JEE

Configure Connector for IBM Content Manager

Property	Values	Description
LCHost	String	Hostname where AEM Forms on JEE Server is installed.
LCPort	Integer	Port number where AEM Forms on JEE application server is configured

Property	Values	Description
LCAdminUserID	String	The user ID to assign to the AEM Forms on JEE Administrator user. This User ID is used to login to the Administrator Console.
LCAdminPassword	String	The password to assign to the AEM Forms on JEE Administrator user. This password is used to login to the Administrator Console.
CDVTopology.appserverrootdir	String	The root directory of the application server instance that you are configuring on a remote server (on which you plan to deploy AEM Forms on JEE)
ConfigureIBMCM	true or false	Specify true to configure Connector for IBM Content Manager
IBMCMClientPathDirectory	String	Location of IBM Content Manager client installation directory.
DataStoreName	String	Name of the DataStore of IBM Content Manager Server that you want to connect to
IBMCMUsername	String	The user name assign to the IBM Content Manager Administrator user. This User ID is used to login to the IBM Content Manager.
IBMCMPassword	String	The password to assign to the IBM Content Manager Administrator user. This password is used to login to the IBM Content Manager.
ConnectionString	String	Additional arguments used in the connection string to connect to IBM Content Manager(Optional).

Configure Connector for IBM FileNet

Property	Values	Description
LCHost	String	Host name of the machine where AEM Forms on JEE Server is installed.
LCPort	Integer	Port number where AEM Forms on JEE application server is configured
LCAdminUserID	String	The user ID to assign to the AEM Forms on JEE Administrator user. This User ID is used to login to the Administrator Console.
LCAdminPassword	String	The password to assign to the AEM Forms on JEE Administrator user. This password is used to login to the Administrator Console.
CDVTopology.appserverrootdir	String	The root directory of the application server instance that you are configuring on a remote server (on which you plan to deploy AEM Forms on JEE)
ConfigureFilenetCE	true or false	Specify true to configure Connector for IBM Filenet
FilenetConfigureCEVersion	String	The FileNet client version to configure. Specify FilenetClientVersion5.0 or FilenetClientVersion5.2
FilenetCEClientPathDirectory	String	Location of IBM Filenet Content Manager client installation directory.
ContentEngineName	String	Host name or IP address of the machine where IBM Filenet Content Engine is installed
ContentEnginePort	String	The port number used by IBM Filenet Content Engine
CredentialProtectionSchema	CLEAR or SYMMETRIC	Specify the level of protection.

Property	Values	Description
EncryptionFileLocation	String	Location of the encryption file. This is required only when you select SYMMETRIC option for CredentialProtectionSchema attribute. Use a forward slash (/) or double backward slashes (\\) as a path seperator.
DefaultObjectStore	String	Name of the ObjectStore for the Connector for IBM Filenet Content Server.
FilenetContentEngineUsername	String	The user ID to connect to the IBM FileNet Content server. The user ID with read-access privileges would be allowed to connect to the Default object Store.
FilenetContentEnginePassword	String	The password to assigned to the IBM FileNet user. This password is used to connect to Default object Store.
ConfigureFilenetPE	true or false	Specify true to configure Connector for IBM FileNet
FilenetPEClientPathDirectory	String	Location of IBM FIleNet client installation directory
FilenetProcessEngineHostname	String	Host name or IP address of the process router.
FilenetProcessEnginePortNumber	Integer	Port number for IBM FileNet Content Server
FilenetPERouterURLConnectionPoint	String	Name of the process router.
FilenetProcessEngineUsername	String	The user ID to connect to the IBM FileNet Content Server
FilenetProcessEnginePassword	String	The password to connect to the IBM FileNet Content Server

Configure Connector for EMC Documentum

Property	Values	Description
LCHost	String	Host name where AEM Forms on JEE Server is installed.
LCPort	Integer	Port number where AEM Forms on JEE application server is configured
LCAdminUserID	String	The user ID to assign to the AEM Forms on JEE Administrator user. This User ID is used to login to the Administrator Console.
LCAdminPassword	String	The password to assign to the AEM Forms on JEE Administrator user. This password is used to login to the Administrator Console.
CDVTopology.appserverrootdir	String	The root directory of the application server instance that you are configuring on a remote server (on which you plan to deploy AEM Forms on JEE)
ConfigureDocumentum	true or false	Specify true to configure Connector for EMC Documentum
DocumentumClientVersion	String	The EMC Documentum client version to configure. Specify DocumentumClientVersion6.7 or DocumentumClientVersion7.0
DocumentumClientPathDirectory	String	Location of EMC Documentum client installation directory
ConnectionBrokerHostName	String	Host name or IP address of the EMC Documentum Content Server.
ConnectionBrokerPortNumber	String	Port number for EMC Documentum Content Server

Property	Values	Description
DocumentumUsername	String	The user ID to connect to the EMC Documentum Content Server.
DocumentumPassword	String	The password ID to connect to the EMC Documentum Content Server.
DocumentumDefaultRepositoryName	String	Name of the default repository of MC Documentum Content Server

Configure Connector for Microsoft SharePoint

Property	Values	Description
LCHost	String	Host name where AEM Forms on JEE Server is installed.
LCPort	Integer	Port number where AEM Forms on JEE application server is configured
LCAdminUserID	String	The user ID to assign to the AEM Forms on JEE Administrator user. This User ID is used to login to the Administrator Console.
LCAdminPassword	String	The password to assign to the AEM Forms on JEE Administrator user. This password is used to login to the Administrator Console.
CDVTopology.appserverrootdir	String	The root directory of the application server instance that you are configuring on a remote server (on which you plan to deploy AEM Forms on JEE)
ConfigureSharePoint	true or false	Specify true to configure Connector for Microsoft SharePoint
SharePointServerAddress	String	Host name or IP address of the Sharepoint Server

Property	Values	Description
SharePointUsername	String	The user ID to connect to the Sharepoint Server
SharePointPassword	String	The password to connect to the Sharepoint Server
SharePointDomain	String	The Domain Name of the Sharepoint Server
ConnectionString	String	Additional arguments used in the connection string to connect to the Sharepoint Server(optional

Command Line Interface Usage

Once you have configured your property file, you must navigate to the *[AEM Forms on JEE root]*/configurationManager/bin folder.

To view a complete description of the Configuration Manager CLI commands, type: `ConfigurationManagerCLI help <command name>`.

Configure AEM Forms on JEE CLI Usage

The Configure AEM Forms on JEE operation requires the following syntax:

configureLiveCycle -f *<propertyFile>*

Where:

- -f *<propertyFile>:* A property file containing the required arguments. For more information on creating a property file, see *Command Line Interface property file*.

Configure CRX CLI Usage

The Configure CRX Repository requires the following syntax:

configureCRXRepository -f *<propertyFile>*

Validate Application Server Topology CLI Usage

The Validate Application Server Topology operation is optional and requires the following syntax:

validateApplicationServerTopology -f *<propertyFile> -targetServer_AdminPassword <password>*

Where:

- -targetServer_AdminPassword <password>: Allows you to set the Admin password on the command line. If this argument is present, it will override the targetServer.adminPassword property in the property file.

Validate database connectivity CLI Usage

The validate Database Connectivity operation is optional and requires the following syntax:

validateDBConnectivity -f *<propertyFile> -datasource_dbPasssword <password>*

Where:

- -datasource_dbPassword <password>: Allows you to set the database user password on the command line. If this argument is present, it will override the datasource.dbPassword property in the property file.

Configure the Application Server CLI Usage

The Configure Application Server operation requires the following syntax:

configureApplicationServer *-targetServer_AdminPassword <password>*-f *<propertyFile>* [-skip *<configurationsToSkipList>*]

Where:

- -targetServer_AdminPassword <password>: Allows you to set the Administrator password on the command line. If this argument is present, it will override the targetServer_AdminPassword property in the property file.
- -skip *<configurationsToSkipList>*: This is an optional parameter which allows you to list the application server components you do not want to configure. Specify the excluded components in a comma separated list. Valid options are Datasource or Core.

Validate Application Server Configurations CLI Usage

The Validate Application Server Configurations operation is optional and requires the following syntax:

validateApplicationServerConfigurations -f *<propertyFile> -targetServer_AdminPassword <password>*

Where:

- -targetServer_AdminPassword <password>: Allows you to set the Admin password on the command line. If this argument is present, it will override the targetServer.adminPassword property in the property file.

(WebSphere and Weblogic Only) Deploy AEM Forms on JEE CLI Usage

The Deploy AEM Forms on JEE operation requires the following syntax:

deployLiveCycle -f *<propertyFile>*

IMPORTANT: You must restart your application server after you complete Deploy AEM Forms on JEE operation.

Initialize AEM Forms on JEE CLI Usage

The initialize AEM Forms on JEE operation requires the following syntax:

initializeLiveCycle -f *<propertyFile>*

Validate AEM Forms on JEE Server CLI Usage

The Validate AEM Forms on JEE Server operation is optional and requires the following syntax:

validateLiveCycleServer -f *<propertyFile> -LCAdminPassword <password>*

Where:

- -LCAdminPassword <password>: Allows you to set the Admin password on the command line. If this argument is present, it will override the targetServer.adminPassword property in the property file.

Deploy AEM Forms on JEE Components CLI Usage

The Deploy AEM Forms on JEE Components operation requires the following syntax:

deployLiveCycleComponents -f *<propertyFile> -LCAdminPassword <password>*

Validate AEM Forms on JEE Component Deployment CLI Usage

The Validate AEM Forms on JEE Component Deployment operation is optional and requires the following syntax:

validateLiveCycleComponentDeployment -f *<propertyFile> -LCAdminPassword <password>*

Check system readiness for PDF Generator

The Checking system readiness for PDF Generator operation requires the following syntax:

pdfg-checkSystemReadiness

Adding administrator user for PDF Generator

The adding administrator user for PDF Generator operation requires the following syntax:

pdfg-addAdminUser -f *<propertyFile>*

Where:

- -f *<propertyFile>:* A property file containing the required arguments. For more information on creating a property file, see *Command Line Interface property file*.

Configure Connector for IBM Content Manager

The Configure Connector for IBM Content Manager operation is optional and requires the following syntax:

IBMCM-configurationCLI -f <propertyFile>

IMPORTANT: Modify the <propertyFile> called cli_propertyFile_ecm_ibmcm_template.txt located in the *[aem-forms root]*\configurationManager\bin\ directory.

Perform the following steps manually to complete the configuration for Connector for IBM Content Manager.

1) Copy the *adobe-component-ext.properties* file from *[aem-forms root]*/configurationManager/configure-ecm/websphere to the following [appserver root]/profiles/[profile_name] directory.
2) Restart the Application Server.
3) Start the following services from administration console
   - IBMCMAuthProviderService
   - IBMCMConnectorService

Configure Connector for IBM FileNet

The Configure Connector for IBM FileNet operation is optional and requires the following syntax:

filenet-configurationCLI -f <propertyFile>

IMPORTANT: Modify the <propertyFile> called cli_propertyFile_ecm_filenet_template.txt located in the *[aem-forms root]*\configurationManager\bin\ directory.

Perform the following steps manually to complete the configuration for Connector for IBM Content Manager.

1) Copy the *adobe-component-ext.properties* file from *[aem-forms root]*/configurationManager/configure-ecm/websphere to the following [appserver root]/profiles/[profile_name] directory.
2) Locate the wsjass.conf file in the [appserver root]/profiles/[profile name]/properties directory and add to it contents of wsjass.conf file available in [aem-forms root]/configurationManager/configure-ecm/websphere directory.
3) Restart the Application Server.
4) Start the following services from administration console
   - IBMFileNetAuthProviderService
   - IBMFileNetContentRepositoryConnector
   - IBMFileNetRepositoryProvider
   - IBMFileNetProcessEngineConnector(If configured)

Configure Connector for EMC Documentum

The Configure Connector for EMC Documentum operation is optional and requires the following syntax:

documentum-configurationCLI -f <propertyFile>

IMPORTANT: Modify the <propertyFile> called cli_propertyFile_ecm_documentum_template.txt located in the *[aem-forms root]*\configurationManager\bin\ directory.

Perform the following steps manually to complete the configuration for Connector for EMC Documentum.

1) Copy the *adobe-component-ext.properties* file from *[aem-forms root]*/configurationManager/configure-ecm/websphere to the following [appserver root]/profiles/[profile_name] directory.
2) Restart the Application Server.
3) Start the following services from administration console
   - EMCDocumentumAuthProviderService
   - EMCDocumentumRepositoryProvider
   - EMCDocumentumContentRepositoryConnector

Configure Connector for Microsoft SharePoint

The Configure Connector for Microsoft SharePoint operation is optional and requires the following syntax:

sharepoint-configurationCLI -f <propertyFile>

Where:

IMPORTANT: Modify the <propertyFile> called cli_propertyFile_ecm_sharepoint_template.txt located in the *[aem-forms root]*\configurationManager\bin\ directory.

12.4. Examples Usage

From the C:\Adobe\Adobe_Experience_Manager_Forms\configurationManager\bin, type:

```
ConfigurationManagerCLI configureLiveCycle -f cli_propertyFile.txt
```

Where *cli_propertyFile.txt* is the name of the property file you created.

12.5. Configuration Manager CLI Logs

If an error occurs, you can review the CLI logs located here in the *[aem-forms root]*\configurationManager\log folder. The log file generated will have a naming convention such as lcmCLI.0.log where the number in the filename (0) will increment when the log files are rolled over.

12.6. Next steps

If you used Configuration Manager CLI to configure and deploy AEM Forms on JEE, then do the following tasks now:

- Perform post deployment configurations

13. Appendix - Increasing the Deployer heap size for WebSphere

You must increase the heap size in the `ejbdeploy.bat/sh` script to avoid time-out errors.

13.1. AIX, Linux, Soloaris

1) Go to the *[appserver root]*/deploytool/itp/ directory and open `ejbdeploy.sh` for editing.
2) **(Solaris only)**In the `SunOS` section, find the `EJBDEPLOY_JVM_OPTIONS` attribute and change the value of the `-XX:PermSize` option to `256m`, and ensure that the value of the `-Xverify` option is `none`.
3) Change the heap size in the $JAVA_CMD\ section to the following value:
   `-Xms256m Xmx4096m`
4) Save and close the file.
   Windows

13.2. Windows

1) Go to *[appserver root]*\deploytool\itp and open the `ejbdeploy.bat` file in a text editor.
2) Find the line beginning with %JAVA_HOME% and then find the argument `-Xmx`.
3) Change the argument to `-Xmx4096M`.
4) Save and close the file.

13.3. Increase MaxPermSize (WebSphere on Solaris)

1) Log in to the WebSphere Administrative Console.
2) In the navigation tree of the WebSphere Administrative Console, do one of the following:
   – Click **Servers** > **Server Types** > **WebSphere Application servers** and, in the right pane, click the server name.
3) Under Server Infrastructure, click **Java and forms workflow**>**Process Definition**.
4) Under Additional Properties, click **Java Virtual Machine**.
5) In the **Generic JVM Arguments,**enter the MaxPermSize parameter as follows:
   `-XX:MaxPermSize=1024m`
6) Click **OK** or **Apply**.
7) In the Messages box, click **Save**directly to master configuration, and then restart the application server.