ADOBE DRIVE CC

ADMINISTRATOR’S GUIDE

revision 3

Adobe®

Adobe Drive CC Administrator’s Guide

The information in this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Adobe Systems Inc. Adobe Systems Inc. assumes no responsibility or liability for any errors or inaccuracies that may appear in this document. The software described in this document is furnished under license and may only be used or copied in accordance with the terms of such license.

Adobe Systems Inc., 345 Park Avenue, San Jose, California 95110, USA.

Adobe Drive CC Administrator’s Guide

Overview

This document is intended for server administrators. For information about how to use Adobe® Drive CC to connect to an AEM Assets server, see the *Adobe Drive 5 User Guide* and other documentation at helpx.adobe.com/drive.html.

Adobe Drive CC is the name of the version 5 release. The product is referred to in the documentation and in the user interface as Adobe Drive 5.

- If your site uses a custom connector provided by a third party, you may want to ensure that the connector is installed correctly for all configurations. For more details, see “Custom connectors” on page 3.
- As server administrator, you are responsible for configuring Adobe Drive 5 to simplify user experience when a user connects to your server through the Adobe Drive 5 Connect UI. You do this using a server presets configuration file. See “Configuring server presets for Adobe Drive 5” on page 4.
- To connect to an AEM Assets server through Adobe Drive 5, each client should ensure that the certificates in the server’s certificate chain are trusted. If any certificate is not trusted, a user fails to connect to the server in the first attempt. An error is displayed asking the user to contact the administrator. If you are the administrator, see “Adding a non-trusted certificate to a client” on page 5 for details around resolving the issue.
- You can use the Adobe Application Manager Enterprise Edition (AAMEE) to package Adobe Drive 5 in a platform-specific format suitable for enterprise deployment. See “> cd C:\Program Files\Common Files\Adobe\Adobe Drive 5\jre\bin > keytool -import -keystore > cd C:\Program Files\Common Files\Adobe\Adobe Drive 5\jre\lib\security > cacerts -file cqnewpubliccert.cert -alias cqse” on page 6.

Custom connectors

Adobe Drive 5 is extensible. If you are a third-party asset-management vendor, the Adobe Drive 5 SDK lets you provide integrated access to your AEM Assets system from selected Adobe Creative Suite® 6 and Creative Cloud™ desktop applications. Use the SDK to customize Adobe Drive 5 to enable it to seamlessly represent the contents of your remote AEM Assets system as a network drive on the end user’s file system.

Adobe Drive 5 provides access to “hidden” user functions within integrated applications, such as viewing version history or adding a check-in comment when saving a file. These features are automatically activated in the integrated desktop application when the user installs Adobe Drive 5 along with your custom connector.

Using third-party custom connectors

If your site uses a third party custom connector, the addition of 64-bit Windows support in Adobe Drive 5 might affect your installation. When you install this patch release, check that your custom connector is installed correctly.

- A custom connector must be installed in the Adobe Service Manager plug-ins folder:

```
C:\Program Files\Common Files\Adobe\AD4ServiceManager\plugins
```

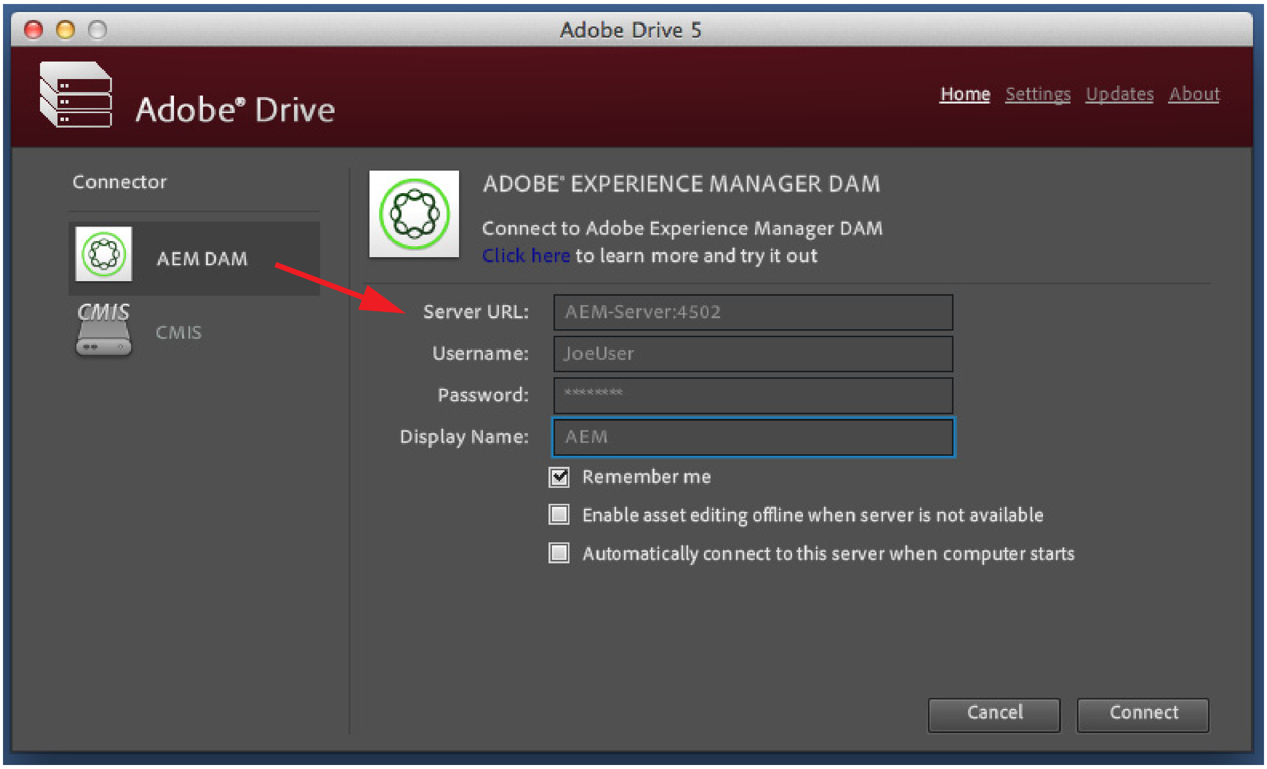
▶ In previous releases, plug-ins for 64-bit Windows systems were installed in the 32-bit compatibility location, under `C:\Program Files (x86)`:

```
C:\Program Files (x86)\Common Files\Adobe\AD4ServiceManager\plugins
```

It is not necessary to remove a plug-in that is installed in the `(x86)` folder, but to work with a 64-bit Windows system, a copy must also be present in the default location. Check with your provider to determine whether you need to alter the default installation procedure for the connector.

Configuring server presets for Adobe Drive 5

The Adobe Drive 5 Connect UI can be customized to offer easy access to your servers. When you bring up the Adobe Drive 5 Connect UI on a client system, it offers a list of Preset Servers for each connector in the left panel; when you select one, the URL for that server is automatically filled in as the Server URL.



ADOBE® EXPERIENCE MANAGER DAM

Connect to Adobe Experience Manager DAM

Click here to learn more and try it out

Server URL: AEM-Server:4502

Username: JoeUser

Password: ********

Display Name: AEM

☑ Remember me

□ Enable asset editing offline when server is not available

□ Automatically connect to this server when computer starts

The Preset Servers shown in this list are taken from a configuration file named `serverPresets.xml`. This an editable text file. As administrator, you can configure this file and deploy it along with Adobe Drive 5 on each client system.

Adobe Drive 5 looks for the configuration file on the client system at this location:

In Windows	`C:\Program Files\Common Files\Adobe\Adobe Drive 4`
In Mac OS	`/Library/Application Support/Adobe/Adobe Drive 4`

Configuring the presets file

The `ServerPresets.xml` file is a UTF8-encoded XML file that associates a list of server names with their URLs. It contains a single `<serverpresets>` element, which in turn contains a set of `<server>` elements with this syntax:

```
<server name="display name" url="server URL">
```

Each element corresponds to one list item in the Preset Servers panel of the Adobe Drive 5 Connect UI.

The `ServerPresets.xml` file that is installed as part of the default configuration contains no `<server>` elements, but has comments describing how to configure the file. Here is an example of the configured file, edited to configure for two CMIS servers and two AEM Assets servers:

```
<?xml version="1.0" encoding="UTF-8"?>
<serverpresets version="1.0" defaultScheme="cmis">
    <server name="My CMIS Server A"
        url="cmis://myservera.mycompany.com:8080/alfresco/service/cmis"/>
    <server name="My CMIS Server B"
        url="cmis://myserverb.mycompany.com:8080/alfresco/service/cmis"/>
    <server name="My DAM Server A"
        url="cq://myservera.mycompany.com:4502"/>
    <server name="My DAM Server B"
        url="cq://myserverb.mycompany.com:4502"/>
</serverpresets>
```

Deploying your configuration

There are three paths to deploying your configuration file with Adobe Drive 5:

- As an Adobe partner, you can customize the Adobe Drive 5 installer to install your configured `ServerPresets.xml` file along with Adobe Drive 5. For information about how to do this, see the *Adobe Drive 5 SDK Programmer's Guide*.
- As an IT administrator, you can update the servers available to Adobe Drive 5 users by pushing your configured `ServerPresets.xml` file to user systems on which Adobe Drive 5 has already been installed.
- As a local system administrator, you can edit the default `ServerPresets.xml` file in a text editor on the local system. You may need to copy the file to edit it.

Adding a non-trusted certificate to a client

In any deployment environment, each client must make sure that all certificates in the certificate chain for an AEM Assets server are trusted; that is, included in the Java `cacerts keystore`. If any certificate in the chain is not trusted, the user's first attempt to connect to the AEM Assets server through Adobe Drive 5 fails with this error:

> *Unable to connect because the server certificate is not trusted. To connect to this server, check with your system administrator or refer to the Adobe Drive support documentation.*

If your users encounter this problem, you must add the non-trusted certificate to the client's trusted store, according to platform. For both platforms:

- The `cacerts` file is part of the Java installation. You must have write access to this file in order to add a certificate.

- The default password for the `cacerts keystore` is 'changeit'. Use this password when prompted while adding the certificate.

In Mac OS In Mac OS, the `cacerts` file is part of the standard Java installation. If you upgrade Java, you might lose the entry for a certificate that you previously added to the `keystore`. If this happens, you must add it again.

Add a non-trusted certificate to the Java `cacerts keystore` using the following commands in a command shell:

1. Change the permission of `cacerts` in the installed Java location using the `chmod` command. The permission for the file should be: `lrwxr-xr-x`

2. Add the non-trusted certificate to the `cacerts keystore` with commands like this:

```
/Library/Java/Home/bin/keytool -keystore
/Library/Java/Home/lib/security/cacerts -import -alias cqse
    -file cqnewpubliccert.cert
```

In Windows In Windows, the `cacerts` file is part of Java in the Adobe Drive 5 installation. If you uninstall Adobe Drive 5 and reinstall it, add the certificate back to the trusted store after reinstalling.

To add a certificate, open a command shell as Administrator with full privileges:

1. From the Start menu, right-click Command Shell and choose Run as > Administrator, or use Run to enter the command:

```
runas /user:<admin> "cmd.exe"
```

2. Change the permission of `cacerts` to allow "Read and Write". The file that Adobe Drive uses is here:

```
C:\Program Files\Common Files\Adobe\Adobe Drive 5\jre\lib\security\cacerts
```

3. Add the non-trusted certificate to the `cacerts keystore` with the following commands:

```
> cd C:\Program Files\Common Files\Adobe\Adobe Drive 5\jre\bin
> keytool -import -keystore
> cd C:\Program Files\Common Files\Adobe\Adobe Drive 5\jre\lib\security
> cacerts -file cqnewpubliccert.cert -alias cqse
```