ColdFusion (2016 release) Lockdown Guide

Written by Pete Freitag, Foundeo Inc.

Adobe Systems Incorporated

Version 1.0
02 Feb 2016

Adobe ColdFusion (2016 release) Lockdown Guide

The content of this guide is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Adobe Systems Incorporated. Adobe Systems Incorporated assumes no responsibility or liability for any errors or inaccuracies that may appear in the informational content contained in this guide.

Please remember that existing artwork or images that you may want to include in your project may be protected under copyright law. The unauthorized incorporation of such material into your new work could be a violation of the rights of the copyright owner. Please be sure to obtain any permission required from the copyright owner.
Any references to company names in sample templates are for demonstration purposes only and are not intended to refer to any actual organization.

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

Notice to U.S. Government End Users. The Software and Documentation are "Commercial Items," as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation," as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §§227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

For U.S. Government End Users, Adobe agrees to comply with all applicable equal opportunity laws including, if appropriate, the provisions of Executive Order 11246, as amended, Section 402 of the Vietnam Era Veterans Readjustment Assistance Act of 1974 (38 USC 4212), and Section 503 of the Rehabilitation Act of 1973, as amended, and the regulations at 41 CFR Parts 60-1 through 60-60, 60-250, and 60-741. The affirmative action clause and regulations contained in the preceding sentence shall be incorporated by reference.

Table of Contents

Section 1: Introduction

The *ColdFusion (2016 release) Lockdown Guide* is written to help server administrators secure their ColdFusion (2016 release) installations. In this document you will find several tips and suggestions intended to improve the security of your ColdFusion server.

IMPORTANT: The reader is strongly encouraged to test all recommendations on an isolated test environment before deploying into production.

1.1 Default File Paths and Usernames

This guide will provide example file system paths for installation, you should not use the same example installation paths provided in this guide.

1.2 Operating Systems and Web Servers

This guide focuses on Windows 2012 R2 / IIS 8.5, and Red Hat Enterprise Linux (RHEL) 7 / Apache 2.4. Many of the suggestions presented in this document can be extrapolated to apply to similar Operating Systems and Web Servers.

1.3 ColdFusion Version

This guide was written for ColdFusion (2016 Release) Enterprise Edition.

1.4 Scope of Document

This document does not detail security settings for the Operating System, the Web Server, or Network Firewalls. It is focused on security settings for the ColdFusion server only.

All suggestions in this document should be tested and validated on a non-production environment before deploying to production.

1.5 Applying to Existing Installations

This guide is written from the perspective of a fresh installation. When possible consider performing a fresh installation of the operating system, web server and the ColdFusion server. If an attacker has compromised the existing server in any way you should start with a fresh operating system installation on new hardware.

1.6 Naming Conventions

In this guide we will refer to the ColdFusion installation root directory as `{cf.root}` it corresponds to the directory that you select when installing ColdFusion. The ColdFusion instance root is referred to as `{cf.instance.root}` in this guide, enterprise installations may have multiple instances, but the default instance is `{cf.root}/cfusion/`

Section 2: ColdFusion on Windows

This section covers the installation and configuration of ColdFusion (2016 release) on a Windows 2012 R2 server. If you are running Linux, please start at section 5.

In this section we will perform the following:

- Installation Prerequisites
- Install ColdFusion
- Check for, and install any ColdFusion hotfixes.
- Create dedicated user account(s) for ColdFusion to run as.
- Create dedicated user account(s) for IIS Application Pool Identities.
- Configure file system permissions.
- Run the web server configuration tool to connect ColdFusion to IIS
- Configure IIS
- Update the JVM

2.1 Installation Prerequisites

Before you begin the installation process perform the following steps:

- Configure a network firewall (and / or configure Windows firewall) to block all incoming public traffic during installation.
- Read the Microsoft Windows Security Compliance Manager guidelines and documentation: http://www.microsoft.com/en-us/download/details.aspx?id=16776
- Create separate partitions and / or drives for ColdFusion Installation, website assets, and log files. This may reduce what can be compromised by a path traversal attack. It can also mitigate a denial of service attack that attempts to fill the main system drive.
- Remove or disable any software on the server that is not required.
- Run Windows Update and ensure all software running on the server is fully patched.
- Ensure that all partitions use NTFS to allow for fine grained access control and auditing.
- Download ColdFusion from adobe.com
- Verify that the MD5 checksum listed on adobe.com download page matches the file you downloaded. To use the Microsoft File Checksum Integrity Verifier (FCIV) utility, download http://support.microsoft.com/kb/841290 and run the following in a Command Prompt: `FCIV -md5 installer-file-name.exe`

2.2 Install IIS Roles and Features

Open the Windows *Server Manager* application, under the *Manage* menu select *Add Roles and Features*. If IIS is not already installed check *Web Server (IIS)*.

The following represents a common minimal set of IIS Role Services:

- Common HTTP Features: Default Document
- Common HTTP Features: HTTP Errors
- Common HTTP Features: Static Content
- Health and Diagnostics: HTTP Logging
- Security: Request Filtering
- Security: IP and Domain Restrictions
- Application Development: .NET Extensibility 4.5 (or latest version)
- Application Development: ASP.NET 4.5 (or latest version)
- Application Development: CGI
- Application Development: ISAPI Extensions
- Application Development: ISAPI Filters
- Management Tools: IIS Management Console

If you use WebSockets you should also install:

- *Application Development: WebSocket Protocol*.

If you wish to add web server level authentication to any sites you should also install:

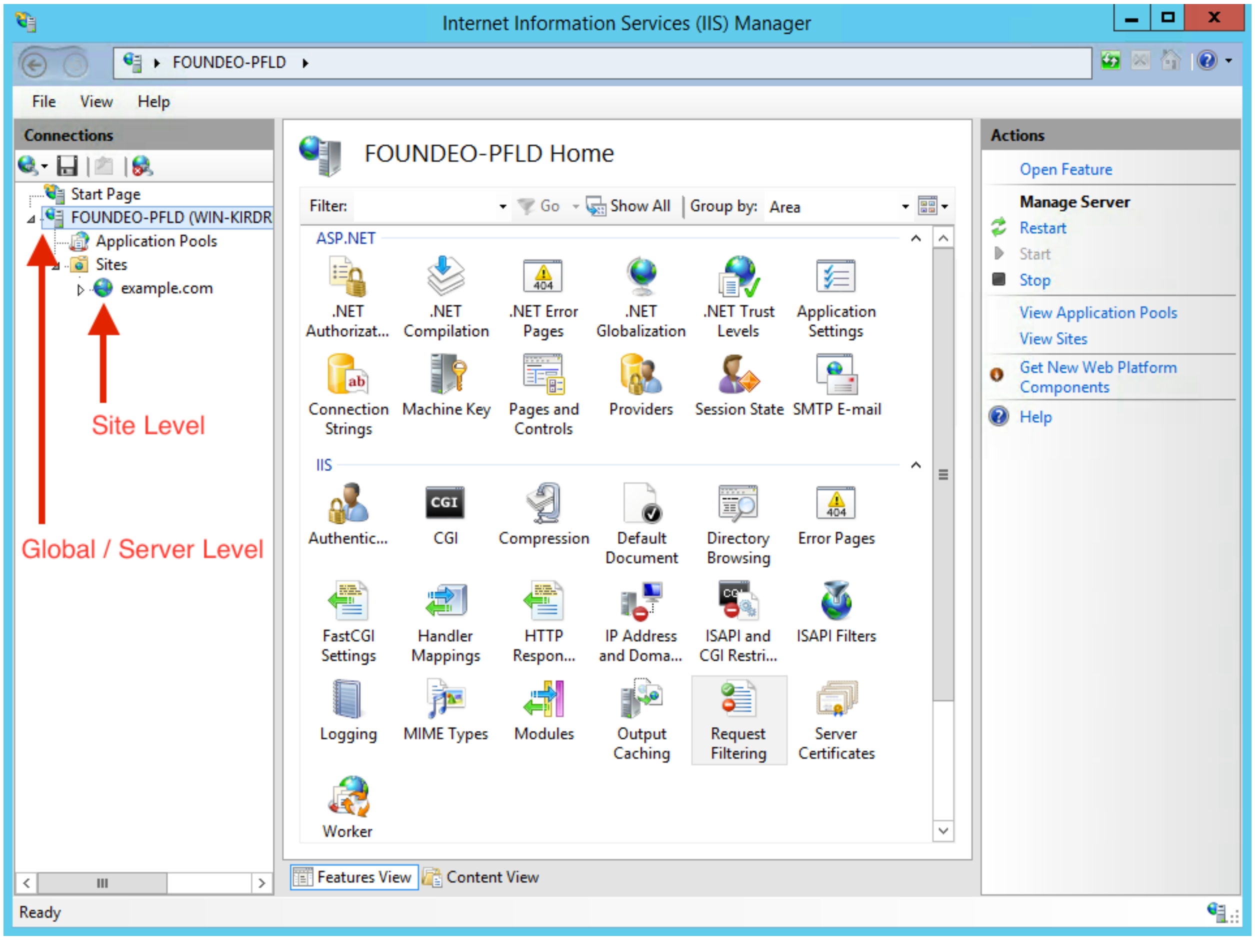
- Security: Windows Authentication

Select any additional IIS role services or features that your web applications require. You can always go back and add additional role services later if necessary.

2.3 Configure IIS Request Filtering

2.3.1 Configure Deny URL Sequences

Open the *Internet Information Services (IIS) Manager* application and click on the global server level (the parent node above Sites and Application Pools).



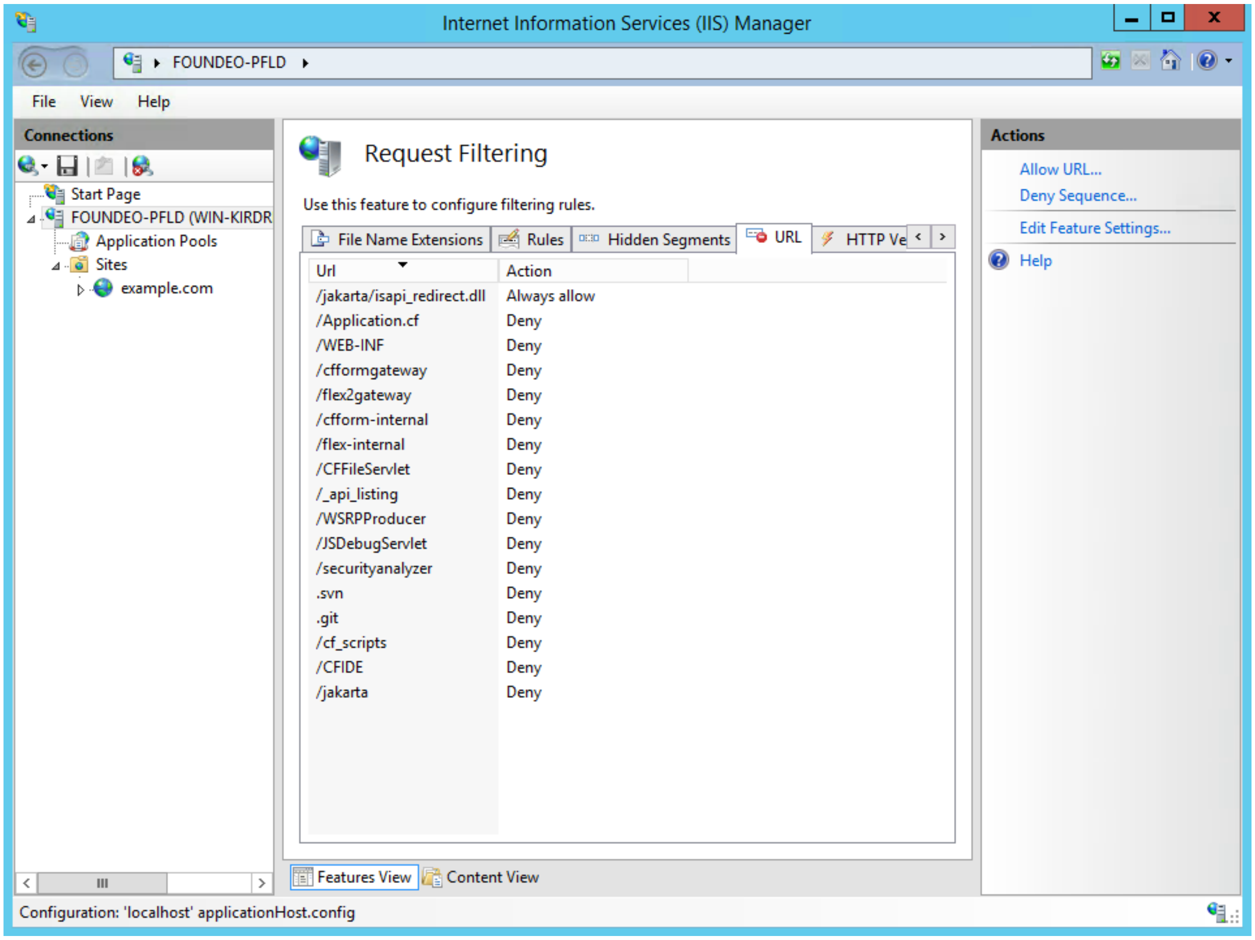
Click on *Request Filtering* and the select the *URL* tab. Click on *Deny Sequence* and enter `/CFIDE/` to block access to it.

You should be able to block `/CFIDE` globally for all public websites in ColdFusion (2016 release) without breaking any features. Consult Appendix B - Table B.1 (located at the end of this guide) to review what URIs exist under `/CFIDE` and their purpose.

As of ColdFusion (2016 release), the `/CFIDE` virtual directory is no longer created by the web server connector tools. In addition the `/CFIDE/scripts` directory has been moved out of `/CFIDE` and into a new directory called `/cf_scripts`.

Next review Table 2.3.1 and block all URIs that are not required by your application.

Note: Request Filtering was added to IIS 7.0, the user interface in the IIS manager to configure request filtering was added in IIS 7.5. If you are using IIS 7.0 request filtering can be configured in the `applicationHost.config` and `web.config` files.



Use this feature to configure filtering rules.

Url	Action
/jakarta/isapi_redirect.dll	Always allow
/Application.cf	Deny
/WEB-INF	Deny
/cfformgateway	Deny
/flex2gateway	Deny
/cfform-internal	Deny
/flex-internal	Deny
/CFFileServlet	Deny
/_api_listing	Deny
/WSRPProducer	Deny
/JSDebugServlet	Deny
/securityanalyzer	Deny
.svn	Deny
.git	Deny
/cf_scripts	Deny
/CFIDE	Deny
/jakarta	Deny

Configuration: 'localhost' applicationHost.config

Table 2.3.1: Additional URIs to consider blocking:

URI	Purpose	Safe to Block
/Application.cf	Block Application.cfc and Application.cfm requests which result in an error when accessed directly.	Yes
/WEB-INF	WEB-INF contains configuration data used by the java application server. The Tomcat connector will block this already, but you can block it at the web server level as well.	Yes

URI	Purpose	Safe to Block
/cfformgateway	Used for <cfform format=flash>	Only if Flash Forms are not used. Flash Forms have been deprecated since CF11.
/flex2gateway	Flex Remoting	Only if Flex Remoting is not used.
/cfform-internal	Used for <cfform format=flash>	Only if Flash Forms are not used. Flash Forms have been deprecated since CF11.
/flex-internal	Flex Remoting	Only if Flex Remoting is not used.
/CFFileServlet	Serves dynamically generated assets. It supports the cfreport, cfpresentation, cfchart, and cfimage (with action=captcha and action=writeToBrowser) tags	Only if cfreport, cfpresentation, cfchart and cfimage are not used.
/rest/	Used for Rest web services support.	Only if CF REST web services are not used.
/*rest*/_api_listing /api/_api_listing	Used for the API Manager to retrieve a list of REST services on the server. This endpoint requires ColdFusion Administrator credentials and the administrator setting: *Allow REST Discovery* to be checked.	Only if not using API Manager with CF REST Service Discovery.
/api/	Identical to /rest/ used for CF Rest web services.	Only if you are not using this endpoint for CF Rest services **and** do not have a /api/ folder on your server.
/WSRPProducer	Web Services Endpoint for WSRP.	Usually, unless WSRP is used.

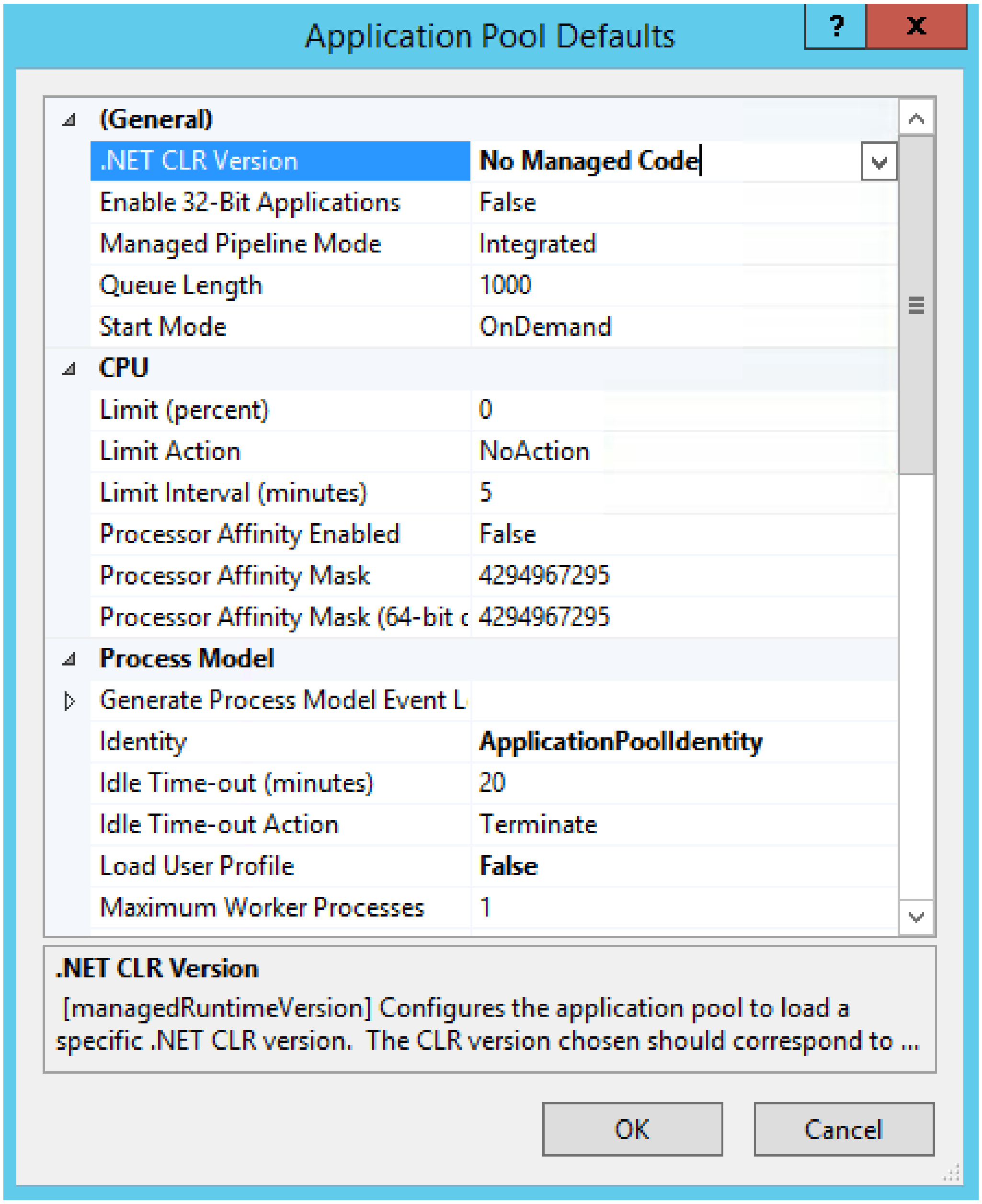
URI	Purpose	Safe to Block
/JSDebugServlet	Used for JavaScript debugging / cfclient	Yes, this should only be used on development servers.
/securityanalyzer	Used for CFBuilder Security Analyzer	Yes, this should only be used on development servers.
.svn	If you use subversion to deploy your ColdFusion applications you can block the .svn folders, which may allow source code disclosure.	Yes
.git	If you use git version control to deploy source code you may have hidden .git folders.	Yes
/cf_scripts/scripts	This holds scripts and client side assets that are used for cfform, cfajaxproxy, etc.	Block if you do not use the tags OR if you setup a new Default Script Src location in ColdFusion Administrator.
/cf_scripts/cfclient	Provides assets used by the cfclient tag.	If not using cfclient.
/cf_scripts/classes	Assets used by java applets for tags: cfgrid, cftree, cfslider and cftextinput (deprecated)	If not using java applet tags.

URI	Purpose	Safe to Block
/cf_scripts	Holds the scripts, cfclient and classes folders described above.	If you can block the scripts, cfclient and classes subfolders then simply block this URI.

2.4 Configure Application Pool Defaults

In the IIS Manager click on *Application Pools*, remove any unused or unnecessary Application Pools that may exist. The *Applications* column shows how many sites are using an application pool.

In the Actions menu click on *Set Application Pool Defaults*. This defines the default Application Pool settings used when creating a new site. You can override the defaults for a specific Application Pool by clicking on an Application Pool and then clicking on *Advanced Settings*.



(General)	
.NET CLR Version	**No Managed Code**
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Queue Length	1000
Start Mode	OnDemand
CPU	
Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295
Process Model	
Generate Process Model Event L	
Identity	**ApplicationPoolIdentity**
Idle Time-out (minutes)	20
Idle Time-out Action	Terminate
Load User Profile	**False**
Maximum Worker Processes	1

.NET CLR Version

[managedRuntimeVersion] Configures the application pool to load a specific .NET CLR version. The CLR version chosen should correspond to ...

2.4.1 .NET Framework Version

If your sites do not require the .NET Framework (you do not use ColdFusion WebSockets, ASP.NET or related technologies), change *.NET Framework Version* to *No Managed Code*.

2.4.2 Process Model > Identity

In the *Set Application Pool Defaults* dialog look *Process Model* and locate the *Identity* setting.

The *Identity* may be left at the default value: `ApplicationPoolIdentity.` With the default `ApplicationPoolIdentity` IIS automatically creates an isolated SID for each application pool that is created on the server with this option. This provides isolation between each application pool (or website) in IIS.

You may instead create new Windows user accounts to use for Application pool identities. If you have multiple sites create a new user for each site. Ensure that each user has minimal permission. The custom user approach may be useful if you are accessing other network resources and do not want to grant entire machine access (The `ApplicationPoolIdentity` will act as the machine identity when attempting to access resources on a network).

In some cases it may be necessary to modify your security policy when custom users are used. Please see https://support.microsoft.com/en-us/kb/981949 for more information.

2.5 Configure Anonymous Authentication

Open the *Internet Information Services (IIS) Manager* application and click on the global server level (the parent node above Sites and Application Pools). Next double click on *Authentication*, then click on Anonymous Authentication.

If all your sites require authentication (for example for an Intranet using Windows Authentication) you can click *Disable*. Any public facing website will require Anonymous Authentication to be enabled.

By default IIS is configured to use the built-in `IUSR` account as the Anonymous Authentication identity. The `IUSR` account may be acceptable for a server with a single website, or websites that do not require isolation.

The `IUSR` account is a member of the `Users` group. When attempting to access resources over the network it will act anonymously (it does not have permission to authenticate as the machine).

You can switch the Anonymous user identity to the Application pool identity by clicking on *Edit* in the Actions menu and then selecting the corresponding radio box.

As of IIS 7.5 when the default `ApplicationPoolIdentity` is used as the Application Pool Account, a virtual identity is automatically created for each application pool, allowing for isolation. You can isolate access using `IIS AppPool\AppPoolName` as the principal when setting NTFS file system permissions.

The third option is to use a custom Windows user account for the Anonymous Authentication User. If you have multiple sites you can create multiple users and configure the Anonymous Authentication User at the site level to provide isolation.

More information about IIS authentication and identities:

http://www.iis.net/learn/get-started/planning-for-security/understanding-built-in-user-and-group-accounts-in-iis

http://www.iis.net/learn/get-started/planning-for-security/secure-content-in-iis-through-file-system-acls

2.6 Remove X-Powered-By Response Header

Double click on *HTTP Response Headers* under the global server level in IIS. Click on *X-Powered-By* and select *Remove* if present.

2.7 Remove ASP.NET ISAPI Filters and Handler Mappings

If you do not require ASP.NET functionality, in the IIS global server level click on *ISAPI Filters* and remove all ASP.NET ISAPI filters. Next click on *ISAPI and CGI Restrictions* click on each ASP.NET ISAPI filter and click *Deny*.

Next click on Handler Mappings in the IIS global root node. Remove all unnecessary Handler Mappings. Do not remove the *StaticFile* handler unless your application does not serve static files (js, css, images, etc). Do not remove the *ISAPI-dll* handler, this will be required for the ColdFusion web server connector to function.

2.8 Create ColdFusion User Accounts

Create a windows user account (in Computer Management) for ColdFusion to run as. In this guide we use *cfuser*, but you should select a unique user name.

If you are setting up multiple instances of ColdFusion you may consider creating dedicated user accounts for each instance to isolate instances from each other.

For each user created in this section right click and select Properties. In the *Remote Desktop Services Profile* tab check the box that says *Deny this user permission to log on to Remote Desktop Session Host server*.

If the new users were added to any default groups (such as Users) remove them from that group.

2.9 Setup Web Root Folder Structure

Create a directory to contain your web sites, for example `d:\web-sites\` and then create a sub directory to hold each web site. If possible, use a dedicated partition and drive letter to decrease the success of directory traversal attacks.

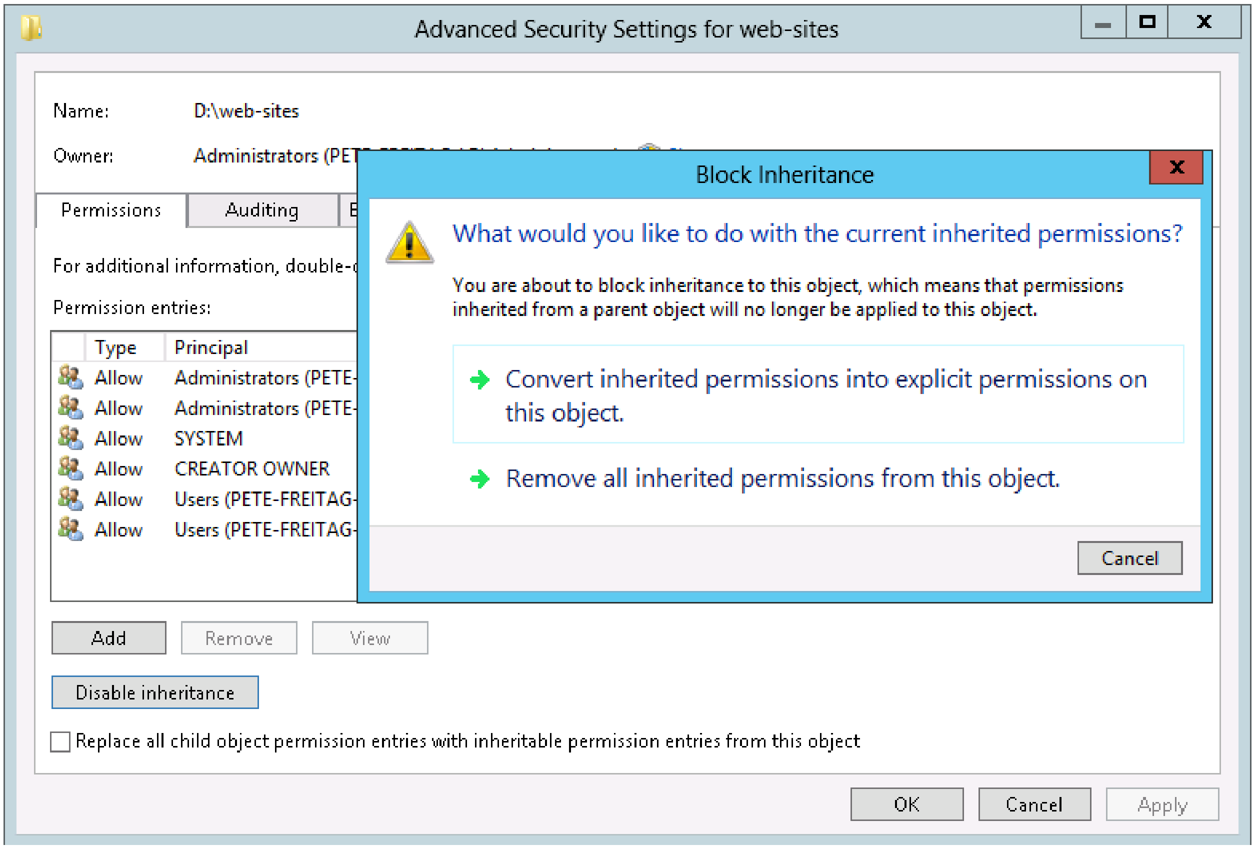
2.10 Add Sites to IIS

Add your website(s) to IIS so they can be configured by the web server configuration tool.

Important: It is important to note that because ColdFusion has not been connected to IIS yet, requests to cfm, cfc, etc files could allow your source code to be downloaded. You should make sure that your network firewall is blocking access to the ports IIS listens on to prevent serving of your CFML source over IIS.

2.11 Setup Web Root Permissions

Right click on the web site folder (for example `d:\web-sites\`), and select *Properties*. Select the *Security* tab and click the *Advanced* button. In the *Permissions* tab click the *Disable inheritance* button, then select *Remove all inherited permissions from this object*.



Advanced Security Settings for web-sites

Name: D:\web-sites

Owner: Administrators (PET

For additional information, double-c

Permission entries:

Type	Principal
Allow	Administrators (PETE-
Allow	Administrators (PETE-
Allow	SYSTEM
Allow	CREATOR OWNER
Allow	Users (PETE-FREITAG-
Allow	Users (PETE-FREITAG-

□ Replace all child object permission entries with inheritable permission entries from this object

Block Inheritance

What would you like to do with the current inherited permissions?

You are about to block inheritance to this object, which means that permissions inherited from a parent object will no longer be applied to this object.

→ Convert inherited permissions into explicit permissions on this object.

→ Remove all inherited permissions from this object.

Click *Add*, then click *Select a principal* and use table 2.11.1 to select the appropriate permissions for each Principal listed.

Check *Replace all child object permission entries with inheritable permission entries from this object* and click *OK*.

Table 2.11.1 Web Root Content Security Permissions

Principal (User / Group)	Permissions
Administrators (or equivalent users and groups)	Full Control
Your Application Pool Account (`IIS_IUSRS` or `IIS AppPool\YourAppPoolName` or *custom user*)	Read & execute List folder contents Read

Principal (User / Group)	Permissions
Anonymous Authentication Account (omit anonymous access is allowed for the site. Set to `IUSR` or `IIS_IUSRS` or `IIS AppPool\YourAppPoolName` or custom user).	Read & execute List folder contents Read
cfuser (Your ColdFusion Instance Service Identity)	Read & execute List folder contents Read (*Add additional permissions as needed, for example if CFFILE is used to write image files in an images folder under the webroot, grant write permission to the images folder*).

Selecting the Application Pool Account

Refer to section 2.4.2 where you configured your Application Pool Process Model Identity.

If your Application Pool is running as `ApplicationPoolIdentity` you can use `IIS_IUSRS` to represent all application pools or you can use `IIS AppPool\YourAppPoolName to` represent a single Application Pool.

Using `IIS AppPool\YourAppPoolName` allows you to isolate each web root from other sites in IIS.

If you created a new user for your application pool identity, select this user.

Selecting the Anonymous Authentication Account

Refer to section 2.5 Configure Anonymous Authentication. If you are using `IUSR` for anonymous authenticate select `IUSR` as the principal. If you are using the Application Pool Identity you can use `IIS_IUSRS` or `IIS AppPool\YourAppPoolName` - these users should already be selected since they are also your *Application Pool Account*.

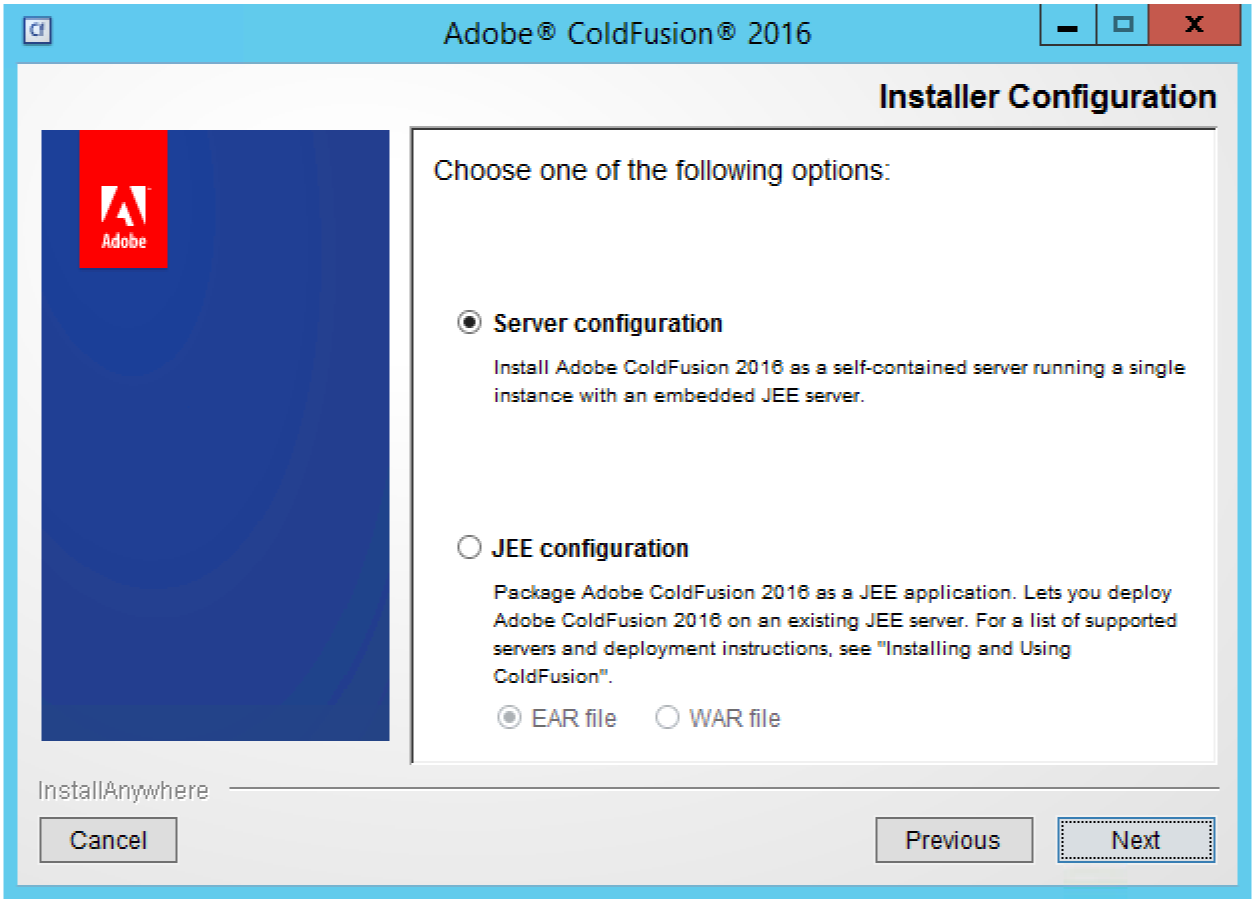
If you created a new user for Anonymous Authentication, select this user as the principal.

Important: Try requesting a static files (an image or txt file) to confirm that your permission are setup correctly before moving forward.

2.14 Run the ColdFusion Installer

Run the installer exe.

On the *Installer Configuration* view select *Server configuration* unless you are deploying to an external JEE server (such as JBoss, WebLogic or WebSphere).



Adobe® ColdFusion® 2016

Installer Configuration

Choose one of the following options:

● Server configuration

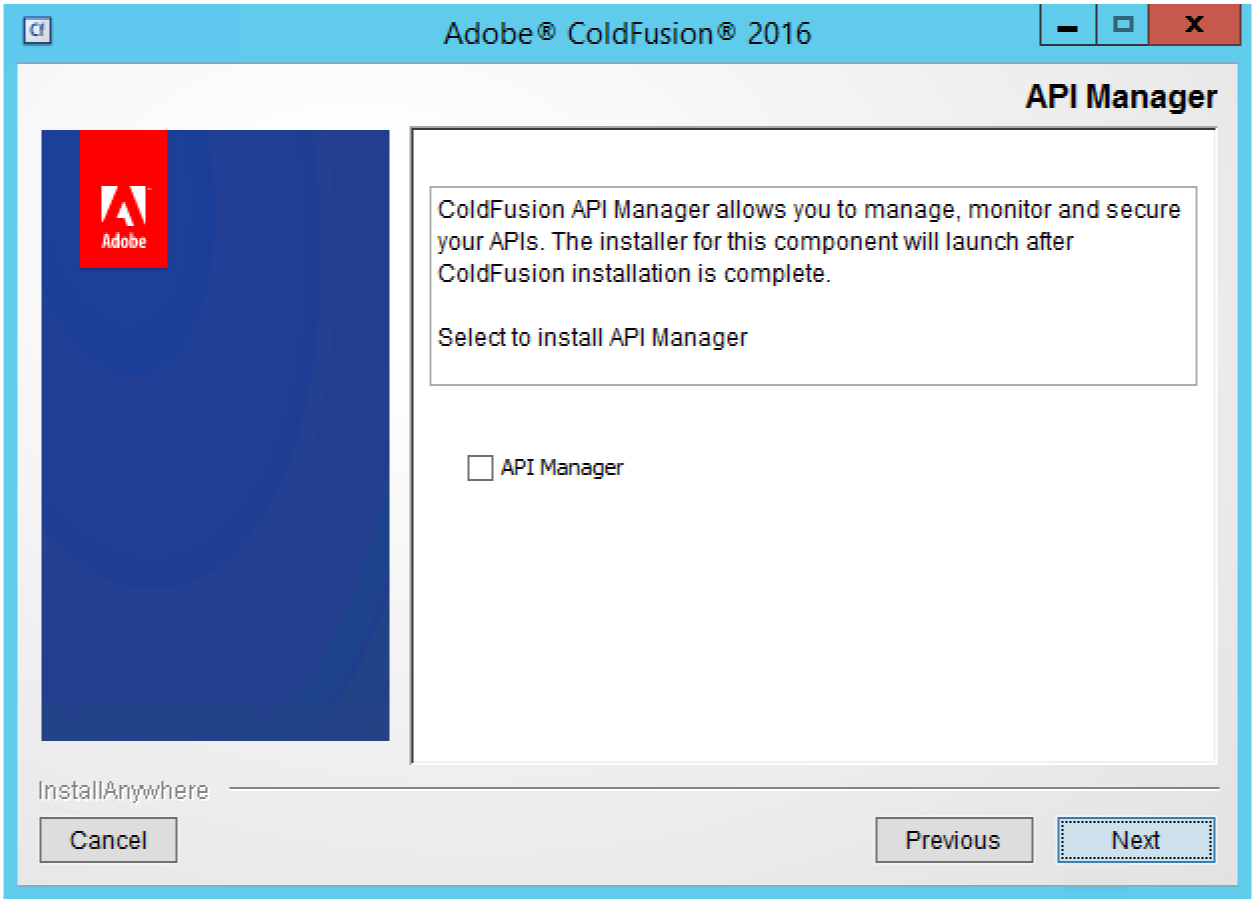
Install Adobe ColdFusion 2016 as a self-contained server running a single instance with an embedded JEE server.

○ JEE configuration

Package Adobe ColdFusion 2016 as a JEE application. Lets you deploy Adobe ColdFusion 2016 on an existing JEE server. For a list of supported servers and deployment instructions, see "Installing and Using ColdFusion".

● EAR file ○ WAR file

Keep the checkbox for the API Manager unchecked, an exe for the API Manager installer will be placed in your {cf.root} installation directory that you can install later.



Adobe® ColdFusion® 2016

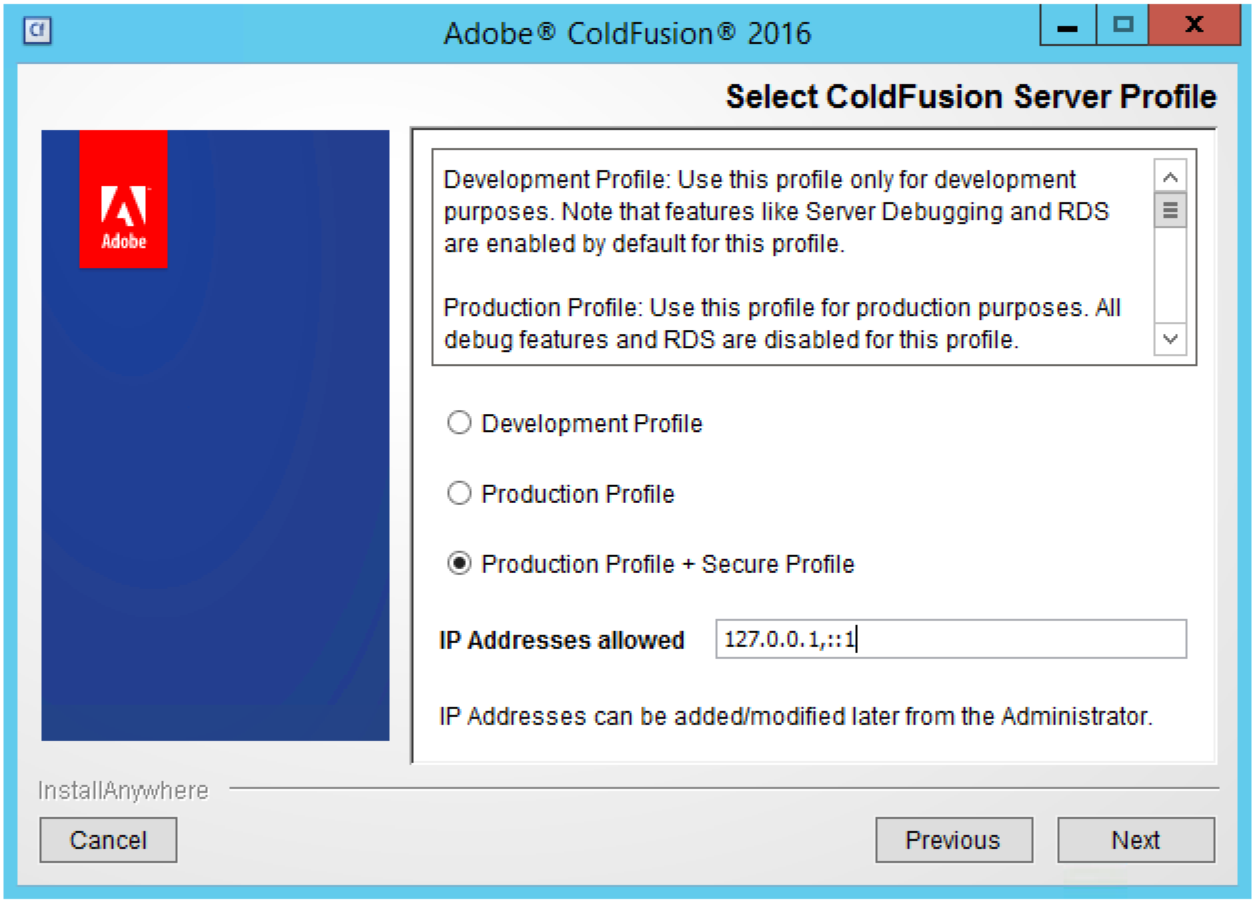
API Manager

ColdFusion API Manager allows you to manage, monitor and secure your APIs. The installer for this component will launch after ColdFusion installation is complete.

Select to install API Manager

□ API Manager

Select *Production Profile* + *Secure Profile*, and specify IP addresses which may access ColdFusion Administrator.



Select ColdFusion Server Profile

Development Profile: Use this profile only for development purposes. Note that features like Server Debugging and RDS are enabled by default for this profile.

Production Profile: Use this profile for production purposes. All debug features and RDS are disabled for this profile.

○ Development Profile

○ Production Profile

● Production Profile + Secure Profile

IP Addresses allowed 127.0.0.1,::1

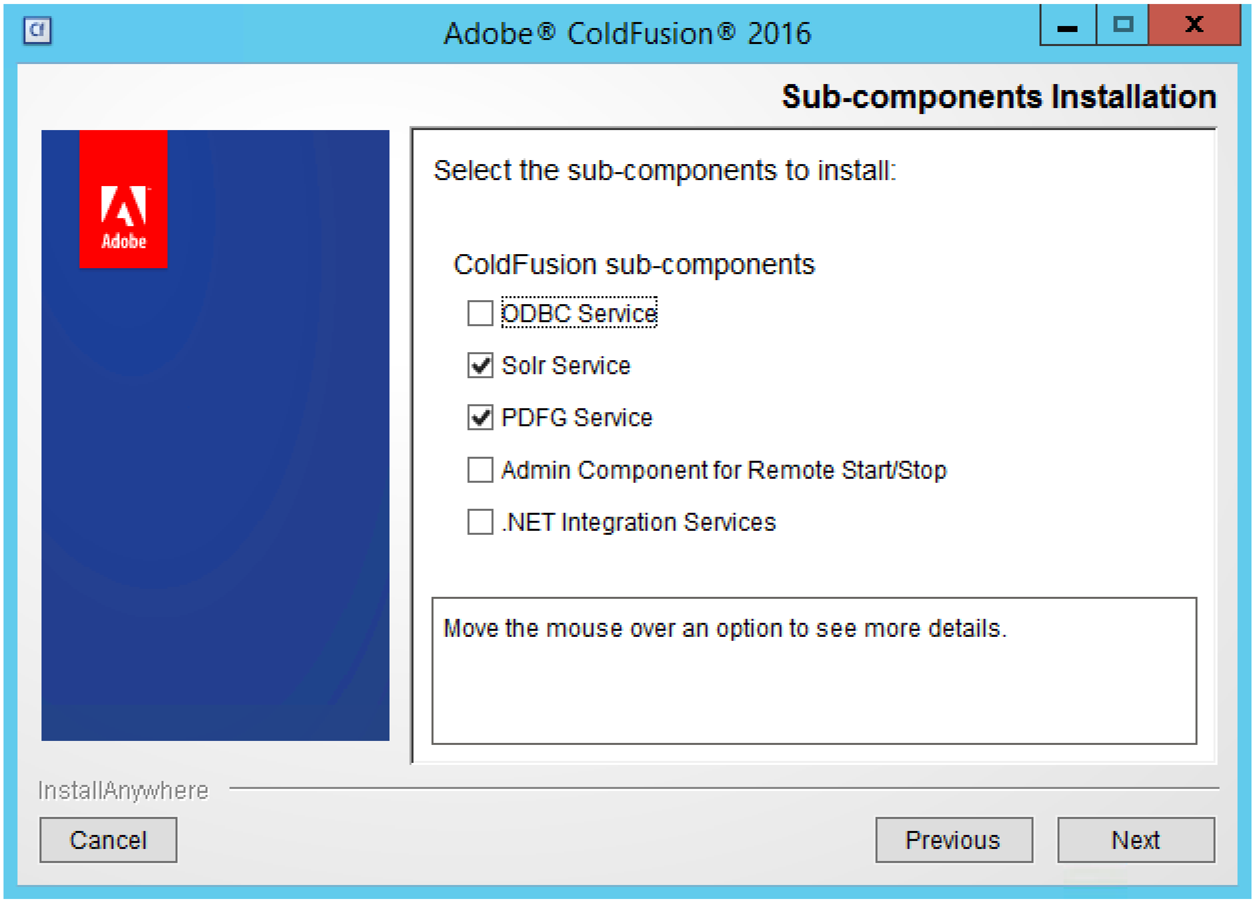
IP Addresses can be added/modified later from the Administrator.

The Secure Profile option provides a more secure foundation of default settings. You can review the settings it toggles here: https://helpx.adobe.com/coldfusion/configuring-administering/administering-coldfusion-security.html

Some of the settings that the Secure Profile toggles may cause application compatibility issues. Just as you should with each step in this guide, ensure that you have tested your application for such issues.

As of ColdFusion 11+ the Secure Profile settings can also be toggled from the ColdFusion Administrator.

Next select only the Sub-components which are required for your application(s).



Adobe® ColdFusion® 2016

Sub-components Installation

Select the sub-components to install:

ColdFusion sub-components

☐ ODBC Service

☑ Solr Service

☑ PDFG Service

☐ Admin Component for Remote Start/Stop

☐ .NET Integration Services

Move the mouse over an option to see more details.

ODBC Service - Required when connecting to Access Databases, not required for SQL Server.

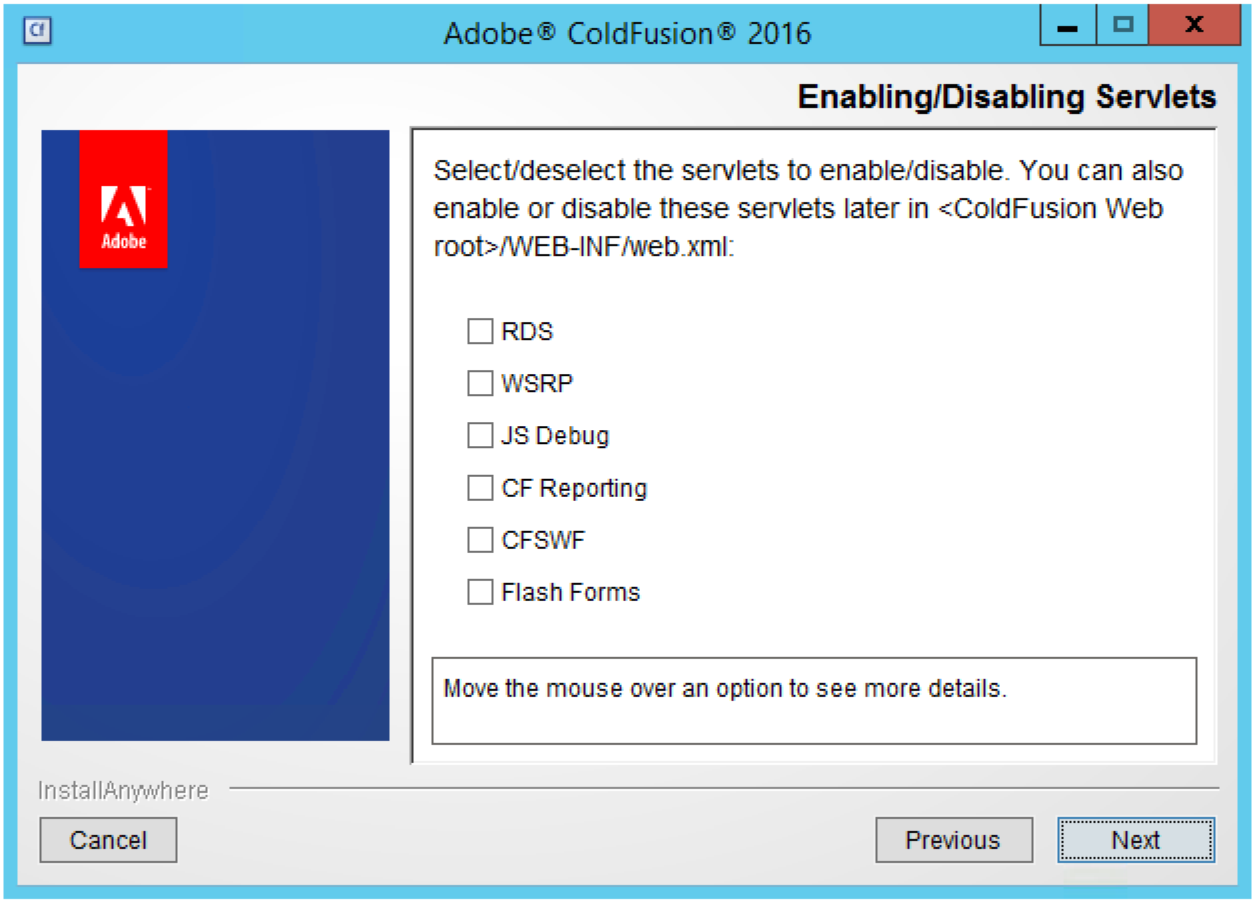
Solr Service - Full text search engine used by `cfindex`, `cfsearch` and `cfcollection` tags.

PDFG Service - Webkit based PDF Rendering engine used by the `cfhtmltopdf` tag. You can still use `cfdocument` without installing this service.

Admin Component for Remote Start/Stop - Allows ColdFusion Builder or Server Manager AIR app to start or stop ColdFusion.

.NET Integration Services - Allows createObject and cfobject to create instances of .NET objects and assemblies.

Check each servlet that is not needed to disable it. See Section 4 for more info.



Enabling/Disabling Servlets

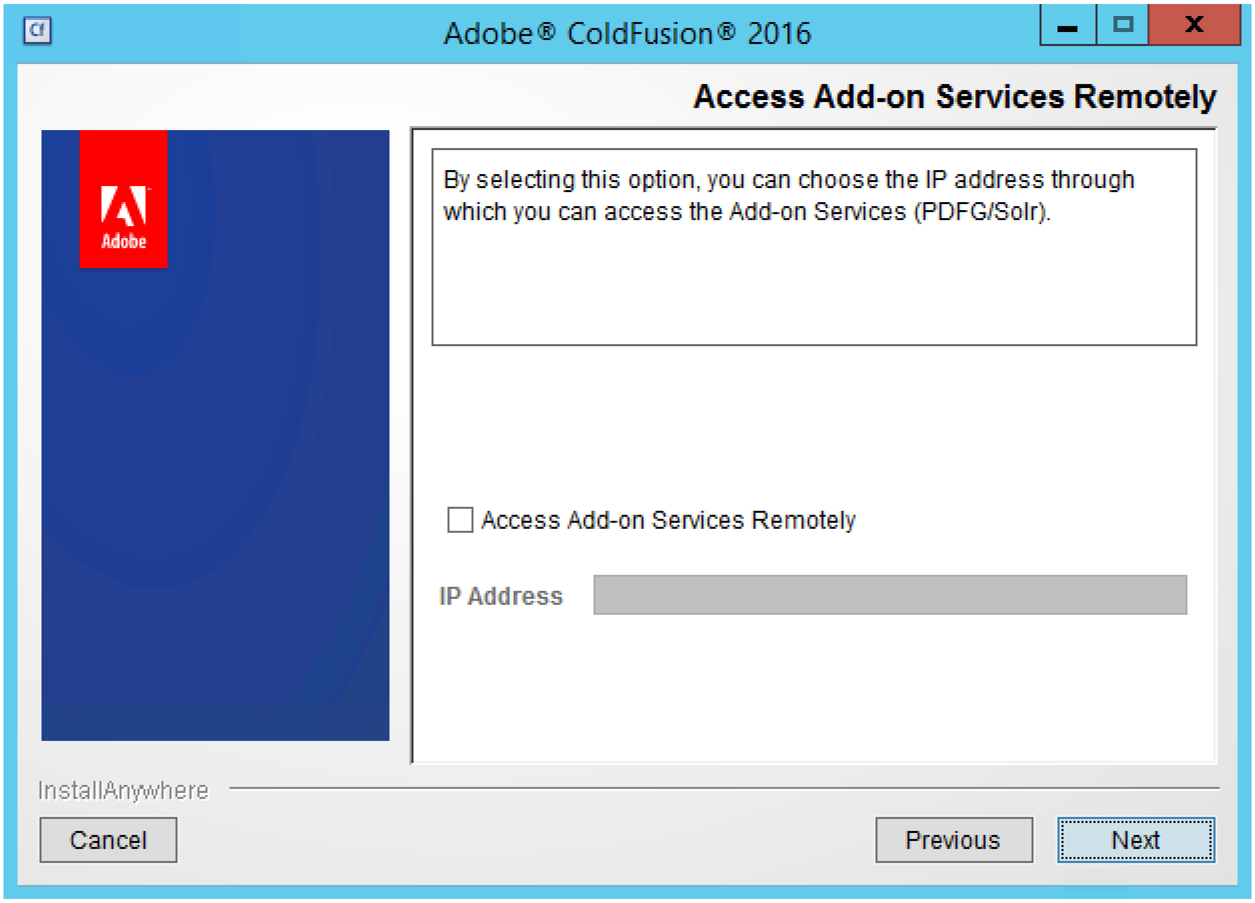
Select/deselect the servlets to enable/disable. You can also enable or disable these servlets later in <ColdFusion Web root>/WEB-INF/web.xml:

□ RDS
□ WSRP
□ JS Debug
□ CF Reporting
□ CFSWF
□ Flash Forms

Move the mouse over an option to see more details.

If you selected the PDFG (`cfhtmltopdf` tag) or Solr (`cfsearch`, `cfindex`, `cfcollection` tags) sub-components the *ColdFusion (2016 release) Add-on Services* windows service will be installed.

When the *Access Add-on Services Remotely* checkbox is unchecked, the Add-on Services are only accessible from the local machine (localhost). If you want to allow access to the services from multiple ColdFusion servers (other than localhost), check the checkbox and specify the IP addresses of the remote ColdFusion servers.


Adobe® ColdFusion® 2016

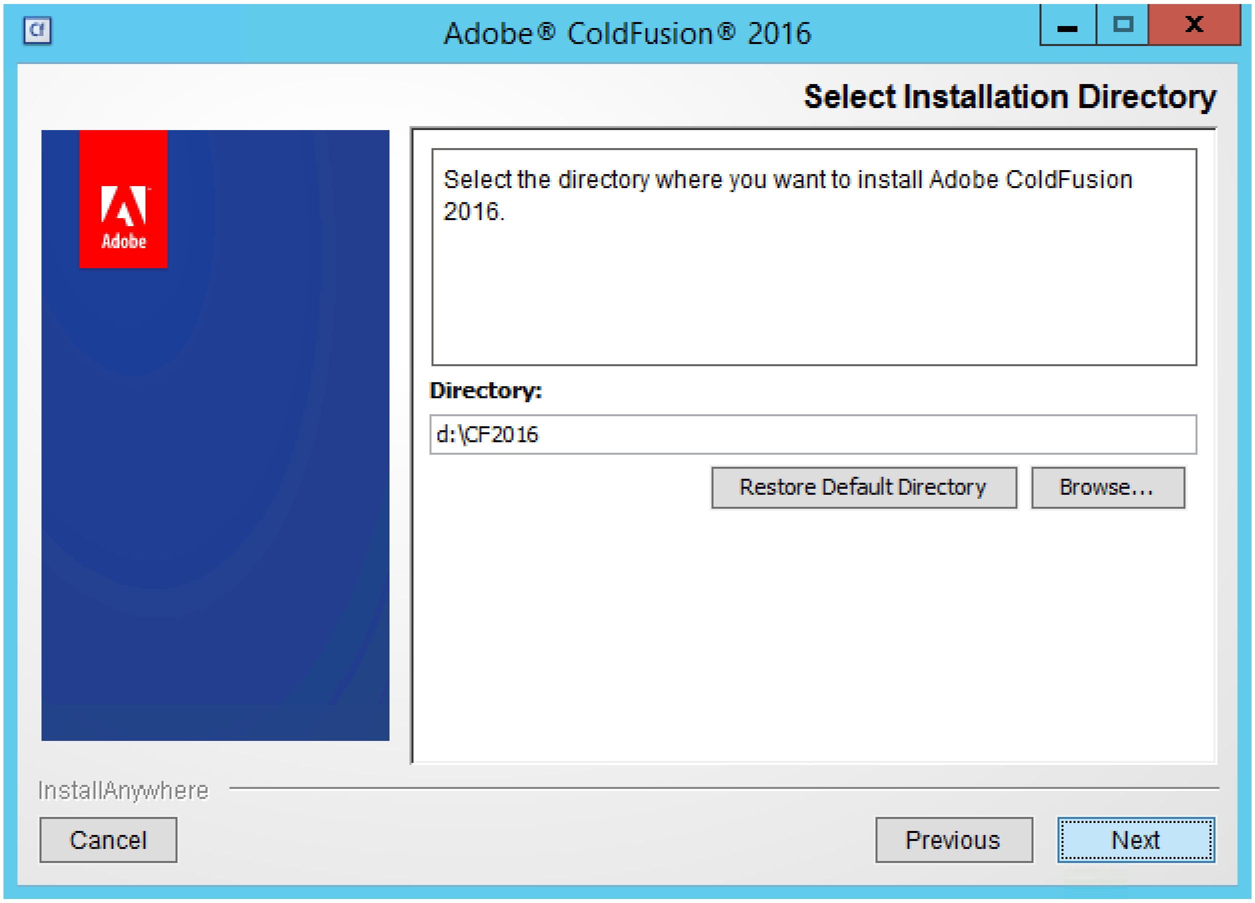
Access Add-on Services Remotely

By selecting this option, you can choose the IP address through which you can access the Add-on Services (PDFG/Solr).

□ Access Add-on Services Remotely

IP Address

Select a non-standard installation directory, ideally on a dedicated drive/partition. This path is referred to as `{cf.root}` throughout the rest of the guide.



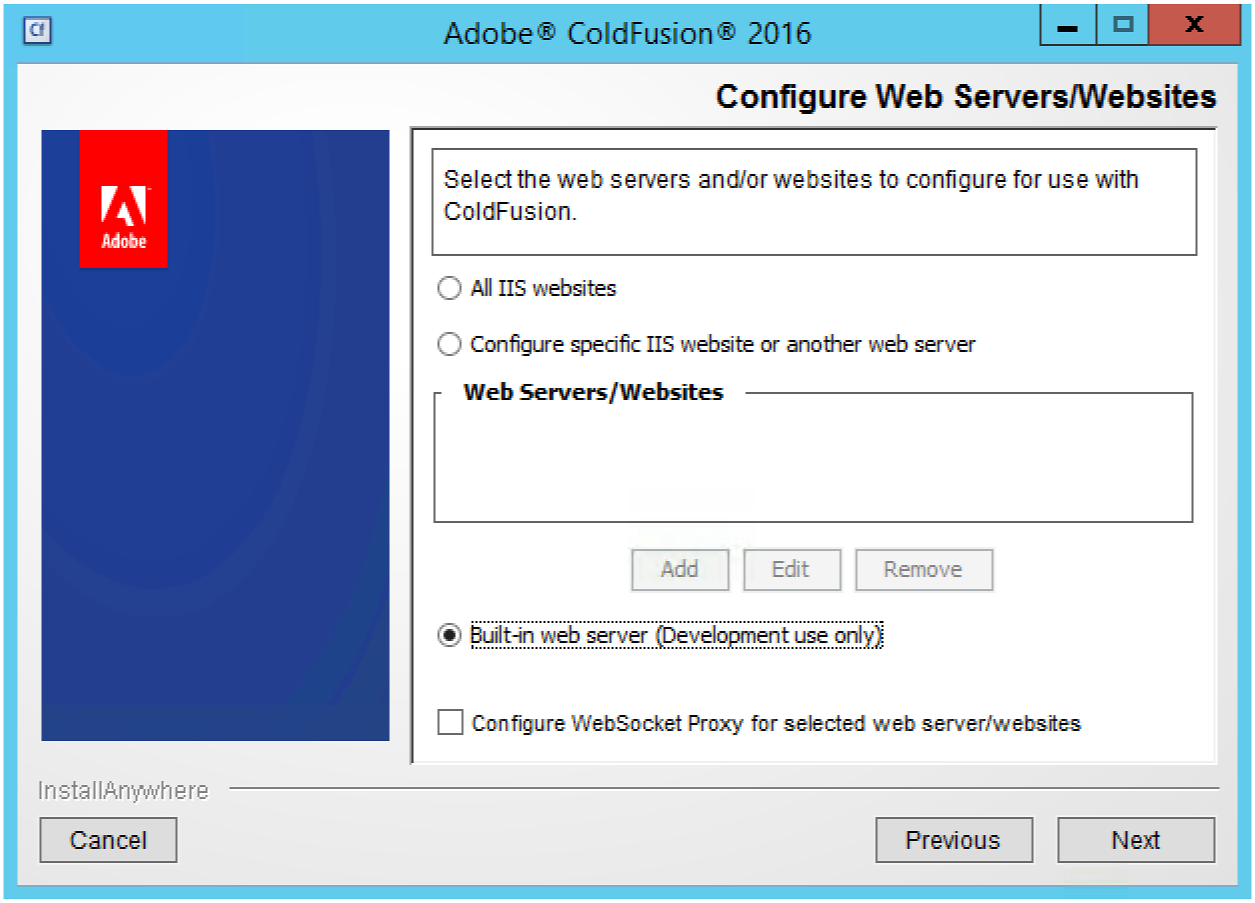
Adobe® ColdFusion® 2016

Select Installation Directory

Select the directory where you want to install Adobe ColdFusion 2016.

Directory: d:\CF2016

Select the Built-in web server, we will run the web server configuration utility later in this guide to connect ColdFusion to IIS. Keep the WebSocket Proxy checkbox unchecked as well, you can install that manually as well.



Adobe® ColdFusion® 2016

Configure Web Servers/Websites

Select the web servers and/or websites to configure for use with ColdFusion.

○ All IIS websites

○ Configure specific IIS website or another web server

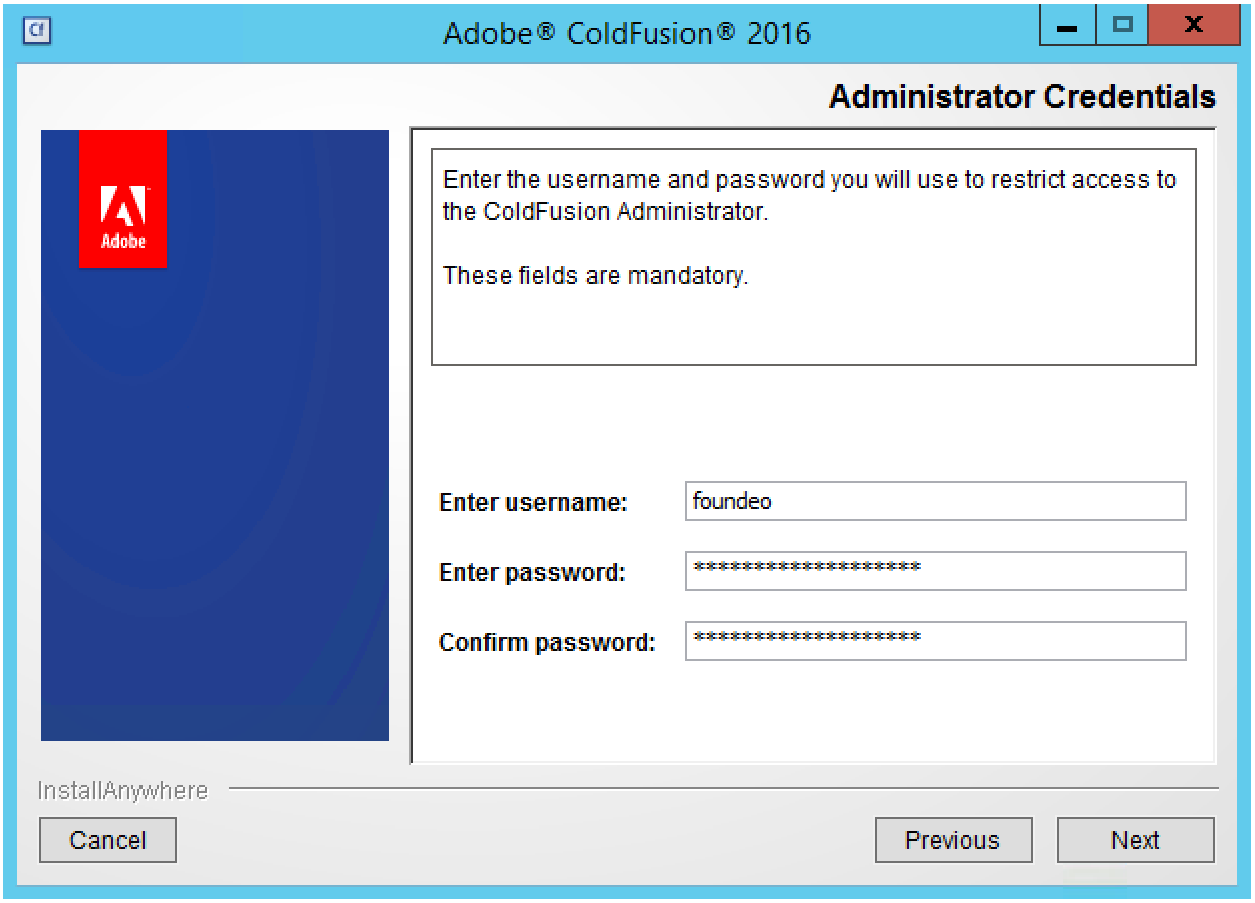
Web Servers/Websites

● Built-in web server (Development use only)

□ Configure WebSocket Proxy for selected web server/websites

When the built-in web server is selected you will be prompted for a port to run the Built-in web server, select a port number other than the default 8500.

For *Administrator Credentials*, select a unique username (not *admin*) and a strong password.



Administrator Credentials

Enter the username and password you will use to restrict access to the ColdFusion Administrator.

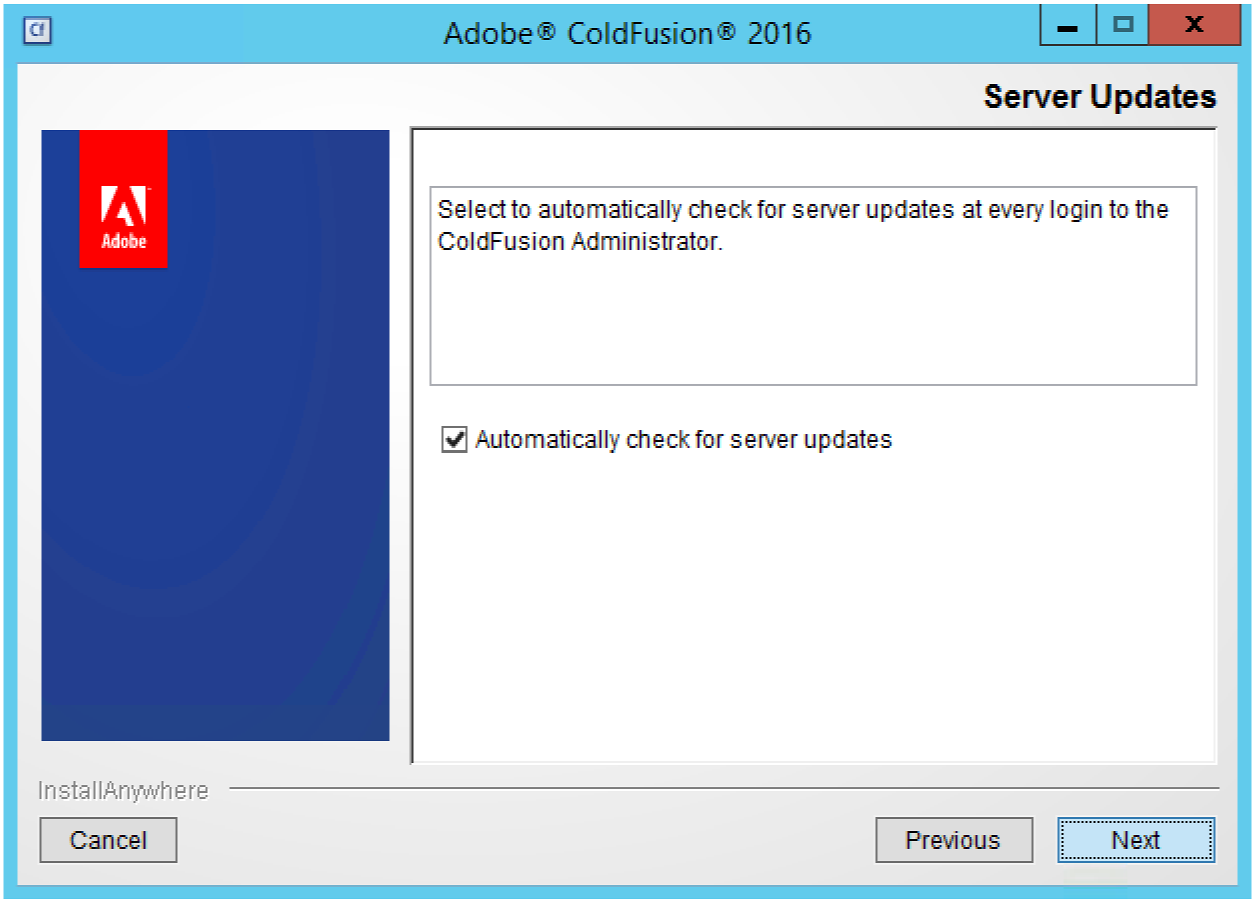
These fields are mandatory.

Enter username: foundeo

Enter password: ********************

Confirm password: ********************

Keep the *Automatically check for server updates* checkbox checked unless you are on a server that does not have a public internet connection.



Adobe® ColdFusion® 2016

Server Updates

Select to automatically check for server updates at every login to the ColdFusion Administrator.

☑ Automatically check for server updates

Click *Next* and then *Install* to complete the installation.

2.15 Install ColdFusion Hotfixes and Updates

Login to the ColdFusion administrator via the built-in web server. For example: http://127.0.0.1:8500/CFIDE/administrator/ (replace 8500 with your port you selected during installation).

Click on *Server Updates* > *Updates* if any hotfixes are available select the latest hotfix, and click *Download*.

Verify the integrity of the download by running `FCIV -md5` on the `hotfix_XXX.jar` file, see that the checksum matches the value found in Adobe ColdFusion update feed: https://www.adobe.com/go/coldfusion-updates

If your server does not have a public internet connection you can locate the hotfix_XXX.jar file url using the ColdFusion update feed. Download the hotfix_XXX.jar file on a computer with internet access, verify the checksum, and then transfer it to the server.

If your server requires a proxy server to connect to the internet you may need to add the following *JVM Arguments* (in ColdFusion Administrator under *Server Settings* > *Java and JVM*) and then restart ColdFusion to use your proxy server:

```
-Dhttp.proxyHost=proxy.example.com -Dhttp.proxyPort=12345 -
Dhttp.proxyUser=u -Dhttp.proxyPassword=p
```

If the md5 checksum matches, install the hotfix from an elevated (Run as Administrator) Command Prompt or PowerShell terminal:

```
x:\cf2016\jre\bin\java -jar x:\cf2016\cfusion\hf-
updates\hotfix_XXX.jar
```

Replace `hotfix_XXX.jar` with the filename of the hotfix jar you are installing, replace `c:\cf2016` with the directory you selected for ColdFusion installation, `{cf.root}`, follow the prompts. The installer will typically attempt to restart ColdFusion when complete. After ColdFusion restarts login to ColdFusion administrator again to verify that the hotfix was installed.

Visit: http://www.adobe.com/support/security/ and read any pertinent ColdFusion Security Bulletins. Confirm that all required security patches have been applied.

Some hot fixes or updates may require you to run the ColdFusion Web Server Configuration Tool to *Upgrade* the connector. Carefully review the hotfix release notes to determine if the connector needs to be updated. If you are following this guide on a fresh install the connector will be installed in the next step.

Consult the ColdFusion hotfix installation guide for more info: http://blogs.coldfusion.com/post.cfm/coldfusion-hotfix-installation-guide

2.16 Run the ColdFusion Web Server Configuration Tool

Right click on `wsconfig.exe`, located in `{cf.instance.root}/runtime/bin/` and select ***Run as Administrator***. Click the Add... button.

Next to *Web Server* make sure Internet Information Server (IIS) is selected. For *IIS Web Site*, you can either install the connector for *All* sites on IIS or install it for sites one at a time. Select individual sites to isolate application pools or to run dedicated instances of ColdFusion for each site.

It may be necessary to tune some of the web server connector configuration variables, especially if you have more than one website. See http://blogs.coldfusion.com/post.cfm/coldfusion-11-iis-connector-tuning for more information.

2.17 Run the ColdFusion WebSocket Proxy Configuration Tool

If you do not use WebSockets skip this section.

ColdFusion 11+ has support for proxying WebSocket traffic directly in IIS via the IIS 8+ WebSocket Protocol role service (installed in section 2.2).

Right click on `wsproxyconfig.exe` in `{cf.instance.root}/bin/` and select *Run As Administrator*.   Click Add and select the appropriate options for your required configuration and click Ok.

Sites that use the ColdFusion WebSocket proxy must change the .NET Framework Version in Application Pool Settings from No Managed Code to a version of .NET that supports WebSockets (v4+).

2.18 Setup File System Permissions

Grant the user you created for ColdFusion to run as (*cfuser* in our example) and the Administrators group full control over the ColdFusion installation directory. Remove all other user and group permission from this directory.

Right click on your `{cf.root}` directory in Windows Explorer and select *Properties*. Click on the *Security* tab then click *Advanced*. In the *Permissions* tab click the *Disable inheritance* button and select *Remove all inherited permissions from this object*. This clears all permissions from the parent folder and allows you to define a new set of permissions on this folder and all subfolders.

Click the *Add* button, in the Permission Entry dialog click *Select a principal*. Enter the *cfuser* as the principal. Check *Full control* and click *OK*. Click *Add* again, and grant Full control to the *Administrators* group.

Check the checkbox to *Replace all child object permission entries with inheritable permission entries from this object*. Click *OK* to apply these permissions.

For maximum security consider a more restrictive permission structure for the ColdFusion installation directory to prevent runtime changes to certain resources or configuration. Restrictive permissions may however break features like security hotfix installation from within ColdFusion administrator. If you run the ColdFusion Hotfix installer as described in section 2.14, the installer will execute under your Administrative user account instead of the user account that ColdFusion runs as (`cfuser`), allowing for more restrictive file system permissions.

Table 2.18.1

Folder	Principal	Permission
{cf.root}	Administrators	Full Control
{cf.root}	cfuser	Full Control
{cf.root}/config/wsconfig/	*Application Pool Identity*	Read & execute List folder contents Read
{cf.root}/config/wsconfig/*n*/isapi_redirect.log	*Application Pool Identity*	Read Write
{cf.root}/config/wsconfig/*n*/isapi_redirect.dll	*Application Pool Identity* and *Anonymous Authentication Identity*	Read & execute List folder contents Read
{cf.root}/config/wsproxy/	*Application Pool Identity*	Read & execute List folder contents Read
{cf.instance.root}/wwwroot/cf_scripts	*Application Pool Identity* and *Anonymous Authentication Identity*	Read & execute List folder contents Read

The *Application Pool Identity* principal will be set to one of the following: a user account you created, the `IIS_IUSRS` group (if you selected *All* sites during the *ColdFusion Web Server Configuration Tool* installation), or a single application pool if you connected ColdFusion to only one site, for example `IIS AppPool\ExampleAppPoolName` (replace `ExampleAppPoolName` with the name of an Application Pool in IIS). Review section 2.4 and 2.11 to select the appropriate principal.

The Anonymous Authentication Identity (`IUSR` or *Application Pool Identity* or a Custom User Account) needs read permission to the `isapi_redirect.dll` file in order to serve anonymous HTTP requests. Review section 2.5 and 2.11 to select the appropriate principal.

The ColdFusion IIS connector writes logs to a file named `isapi_redirect.log` by default. The IIS *Application Pool Identity* needs write permission to this file. You may consider changing the location of this file, which is defined in the `isapi_redirect.properties` file, to a non default directory (ideally on a drive/partition dedicated to logging). Any changes made to `isapi_redirect.properties` may be overwritten when reinstalling a connector.

Note: if you are setting up multiple instances of ColdFusion or multiple connectors you will need to repeat this step for each connector. Each connector instance is placed in a subdirectory of `{cf.root}/config/wsconfig/n/` where *n* is a number (starting with 1 by default).

The `{cf.root}/config/wsproxy/` is used for the WebSocket proxy if you did not install the WebSocket Proxy Connector (section 2.15) then you would not have this directory.

2.19 Registry Permissions

Open `regedit.exe` and navigate to the registry key `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\` and locate each key matching a ColdFusion service, for example `ColdFusion (2016 release) Application Server`. Right click on each key and select Permissions and grant the ColdFusion instance user account read permission.

If your application makes use of Client variables and uses the registry for storage (not recommended) the ColdFusion user will need Full Permission to the `HKEY_LOCAL_MACHINE\SOFTWARE\Macromedia\ColdFusion\CurrentVersion\Clients` key (this key will not exist until client variables have been used).

Restart ColdFusion and test your application.

2.20 Specify Log On User for ColdFusion Services

Open the Services Manager and change the user the service runs as to be the user you created (`cfuser` in the guide example). The installation creates a service named *ColdFusion (2016 release) Application Server* which runs the initial ColdFusion instance named *cfusion*. Right click the service, click Properties and select the *Log On* tab to specify the username and password for the account you created. Restart the ColdFusion (2016 release) Application Server Service.

If you installed any optional subcomponents (such as Solr, .NET or the PDF Generation Service) ensure that their respective Windows Service is configured to run as a dedicated user account as well. If you installed a subcomponent but are not using it, change the service Startup type to *Disabled* and stop the service.

After restarting services ensure that ColdFusion and your web sites are working properly.

2.21 Remove Unused Handler Mappings

In IIS under the root/global configuration node double click Handler Mappings. You will see several handler mappings defined the ColdFusion Web Server Configuration Tool. You can remove all the handler mappings that your web applications do not require.

The ColdFusion Web Server Server Configuration Tool defines several handler mappings, which are used for serving default documents and custom error handlers. A minimal configuration is keeping only `StaticFile, ISAPI-DLL,` and `cfmHandler`.

Restart IIS and test your websites.

Note that if you rerun the Web Server Configuration Tool to update a connector you may need to repeat this step again.

2.22 Configure uriworkermap.properties

Additional mappings are specified in the `{cf.root}/config/wsconfig/`*`n`*`/uriworkermap.properties` file. Any unnecessary URI patterns could be removed from this file or excluded by prefixing them with a `!`

You will also find that as of ColdFusion (2016 release) the URI pattern `/CFIDE/*` is blocked by the following line in `uriworkermap.properties`:

```
!/CFIDE/* = cfusion
```

Do not remove that pattern.

Restart IIS and test your web sites.

For more information see: https://tomcat.apache.org/connectors-doc/reference/uriworkermap.html

2.23 ColdFusion Administrator Web Site

If possible use the built-in web server to access the ColdFusion Administrator via localhost, and skip this step. Using the built-in server allows you to keep `/CFIDE` blocked globally for all sites on IIS.

If you plan on accessing the ColdFusion Administrator from IP addresses other than localhost (not recommended) then using IIS for the ColdFusion Administrator access will allow you to easily configure IP restrictions, HTTPS, and additional authentication layers.

First create a self signed certificate (or preferably utilize a certificate from a trusted certificate authority) by clicking on the **Server Certificates** icon under the IIS root. Click on the link to **Create Self-Signed Certificate** on the right under Actions.

Create an **empty directory** for the web site root of the ColdFusion administrator web site (eg `d:\web-sites\cfadmin\`). It is important to use an empty directory, **do not** use the wwwroot directory of the ColdFusion instance.

Next click on **Sites** and **Add Web Site** to create a new website for ColdFusion Administrator, point the web root or *content directory* to the directory you just created. Bind the new site to 127.0.0.1 (or another IP address only accessible to system administrators). Select HTTPS for the protocol, and select the self signed certificate.

Click the *Test Settings…* button to verify that permissions are setup correctly.

Consider disabling anonymous access to this site and require web server authentication for an additional layer of protection and auditing.

Next Require SSL for this website by double clicking on the *SSL Settings* icon for the *cfadmin* site and check the *Require SSL* checkbox.

Visit https://127.0.0.1/ and ensure that it requires SSL and authentication. If you choose a self signed certificate you will receive a SSL warning.

Remove Request Filtering Rule for ColdFusion Administrator Site

Because we have specified that the URI `/CFIDE` is blocked on a global level (using IIS Request Filtering, configured in section 2.3.1), we need to enable that URI only on our *cfadmin* web site. To do this click on the *cfadmin* website under sites, and click on Request Filtering. Select the URL tab and click on the rule matching `/CFIDE` and click the Remove button.

Next refer to section 2.3.1, add request filtering rules to block all the `/CFIDE` uri's except `/CFIDE/administrator` (see table 2.3.1).

Run the ColdFusion Web Server Configuration Tool

As discussed in section 2.22 *Configure uriworkermap.properties* the connector blocks /CFIDE/* by default. You can run wsconfig.exe again (right click to Run as Administrator) to create a unique connection to the IIS cfadmin website you created. Click Add, and select your ColdFusion administrator website under *IIS Web Site*.

Refer to section 2.18 to apply appropriate permissions to your new `{cf.root}/config/wsconfig/2/` directory (the directory number may be higher than two if you configured multiple sites).

Configure uriworkermap.properties for ColdFusion Administrator access

Edit the file: `{cf.root}/config/wsconfig/`*n*`/uriworkermap.properties` make sure that *n* refers to your ColdFusion administrator web site connector. Remove the line:

```
!/CFIDE/* = cfusion
```

Create a /CFIDE Virtual Directory for CFAdmin Site

In IIS right click on your *cfadmin* site and click Add Virtual Directory. Set the *Alias* to CFIDE and the physical path to `{cf.root}/{cf.instance}/wwwroot/CFIDE`

Test and Verify

Test that you can access: `/CFIDE/administrator/index.cfm` via your IIS website.

Verify that public access to this website is denied.

Verify that all your public websites do not allow access to `/CFIDE/administrator/index.cfm`

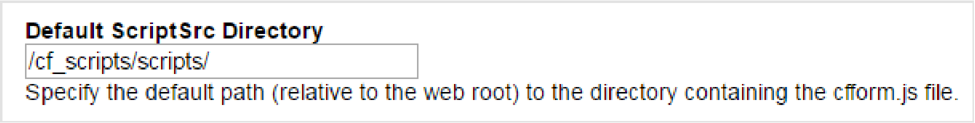
2.23 Create alias for /cf_scripts/scripts

In a prior section we blocked the URI `/cf_scripts/scripts` with request filtering. If your web sites leverage certain tags or features you can change this URI to a non default URI.

Some CFML tags or features may require assets in `/cf_scripts/scripts`: See Appendix B table B.2 for a full listing. If you do not use any of these tags you can continue to the next section. If you are not sure if your applications use these tags review the web server logs for requests containing `/cf_scripts/scripts/` in the URI (look for `/CFIDE/scripts` on servers running ColdFusion 11 or lower).

In IIS right click on each website that uses the tags listed above and select *Add Virtual Directory*. For alias, specify a new name for this folder, for example /cfscripts-*random* and set the physical path to `{cf.instance.root}/wwwroot/cf_scripts/scripts`.

Once the virtual directory is in place you can update the ColdFusion administrator to specify the new URI for `/cf_scripts/scripts` under the Server setting page:



Default ScriptSrc Directory

/cf_scripts/scripts/

Specify the default path (relative to the web root) to the directory containing the cfform.js file.

Replace `/cf_scripts/scripts/` with the new virtual directory URI, eg: `/cfscripts-1216/`

If your server has a lot of virtual directories you can use `appcmd.exe` from Command Prompt:

```
appcmd list app /path:"/" /xml | appcmd add vdir -in /path:/cfscripts-
1216 /physicalPath:x:\cf2016\cfusion\wwwroot\cf_scripts\scripts
```

Note that the ColdFusion Administrator does use these scripts. So if you changed the default script src you will need to configure an alias in the built-in web server if you use it for accessing the ColdFusion Administrator. See section 4.1 for instructions on creating an alias in the built-in web server.

2.24 Remove the /cf_scripts Virtual Directories

The ColdFusion Web Server Configuration Tool adds a `/cf_scripts` virtual directory to each website that is configured, in most cases you will not need this defined on every web site. See Appendix B table B.2 for a full listing of tags that use `/cf_scripts`

If your server has a lot of sites configured it can be tedious to remove each manually, you can use `appcmd.exe` to remove all `cf_scripts` virtual directories by running this following:

```
appcmd list vdir /path:"/cf_scripts" -xml | appcmd delete vdir -in
```

2.25 Update the JVM to the latest supported version

The Java Virtual Machine (JVM) included with the ColdFusion installer may not contain the latest java security hotfixes. You must periodically check with Oracle for JVM security hotfixes. Oracle typically releases security hotfixes for Java on a quarterly basis.

Visit java.oracle.com and download the latest Java Runtime Environment (JRE) supported by ColdFusion (2016 release).

Before editing, create a backup of the `jvm.config` file located in the `{cf.instance.root}/bin/` directory. Open the file with a text editor to locate the line beginning with `java.home=` for example:

```
java.home=C:\\CF2016\\jre
```

Change that line to the path of the new JRE, for example:

```
java.home=C:/java/jdk1.8.0_XX/jre
```

Note: the path must use forward slashes `/` or escaped backslashes `\\` otherwise ColdFusion will not start.

Restart ColdFusion. Visit the System Information page of ColdFusion administrator to confirm that the JVM has been updated.

If you need to revert your changes and go back to the default JVM, replace `jvm.config` with your backup and restart/start ColdFusion.

Repeat for each ColdFusion instance.

Test your sites again.

To update the JVM for ColdFusion (2016 release) Add-on Services

If you installed the *ColdFusion (2016 release) Add-on Services* for Solr (`cfsearch`, `cfcollection`, `cfindex`) or the PDF Service (`cfhtmltopdf`) they run in a separate process and will use the `{cf.root}/jre` by default.

Locate the file `{cf.root}/cfusion/jetty/jetty.lax` and make a backup of it. Next right click on `jetty.lax` and open it with Notepad or any plain text editor. Look for a line that defines the property `lax.nl.current.vm` for example:

```
lax.nl.current.vm=C:\\ColdFusion2016\\jre\\bin\\javaw.exe
```

Change it to point to `javaw.exe` on your new JVM. Ensure that you use two backslashes `\\` to separate folders. For example:

```
lax.nl.current.vm=C:\\java\\jdk1.8.0_XX\\jre\\bin\\javaw.exe
```

Restart the *ColdFusion (2016 release) Add-on Services* service.

Test your sites again.

For additional information on updating the JVM please see:

http://blogs.coldfusion.com/post.cfm/how-to-change-upgrade-jdk-version-of-coldfusion-server

http://www.carehart.org/blog/client/index.cfm/2014/12/11/help_I_updated_CFs_JVM_and_it_wont_start

https://www.youtube.com/watch?v=zzC31EAlZ8Y

2.26 Lockdown the /jakarta Virtual Directory

The ColdFusion connector for IIS will create a virtual directory `/jakarta` which points to `{cf.root}/config/wsconfig/n/` where *n* is some integer for each connector instance. This virtual directory is used to execute the `isapi_redirect.dll` file.
The `isapi_redirect.dll` file is the only file that needs to be publicly accessible in the `/jarkarta` virtual directory.

Open the *Internet Information Services (IIS) Manager* application and click on the global server level (the parent node above Sites and Application Pools). Click on *Request Filtering* and the select the *URL* tab. Click Allow URL and specify `/jakarta/isapi_redirect.dll` to allow requests to the DLL. Next click on *Deny Sequence* and enter `/jakarta` to block access to the rest of the folder.

Test your sites again.

Section 3: ColdFusion Administrator Settings

In this section several recommendations are made for ColdFusion server settings. It is important to understand that changes to some of these settings may affect how your website functions, and performs. Be sure to understand the implications of all settings before making any changes.

3.1 Server Settings > Settings

Setting	Default	Recommendation	Description
Timeout Requests after	Checked / 60 Sec.	Checked / 5 Sec.	Set this value as low as possible. Any templates (such as scheduled tasks) that might take longer, should use the `cfsetting` tag. For example: `<cfsetting requesttimeout="60">`
Use UUID for cftoken	Unchecked	Checked	The default cftoken values are sequential and make it fairly easy to hijack sessions by guessing a valid CFID / CFTOKEN pair. This setting is not necessarily required if J2EE session are enabled, however it doesn't hurt to turn it on anyways.
Disable CFC Type check	Unchecked	Unchecked	Developers may rely on the argument types, enabling this setting might allow attackers to cause new exceptions in the application. This setting may be enabled if the developer(s) have built the application to account for this.
Disable access to internal ColdFusion Java components	Unchecked	Checked	The internal ColdFusion Java components may allow administrative duties to be performed. Some developers may write code that relies on these components. This practice should be avoided as these components are not documented.

Setting	Default	Recommendation	Description
Prefix serialized JSON with	Unchecked: //	Checked: //	This setting helps prevent JSON hijacking, and should be turned on. ColdFusion AJAX tags and functions automatically remove the prefix. If developers have written CFC functions with returnformat="json" or use the SerializeJSON function, the prefix will be applied, and should be removed in the client code before processing. Developers can override this setting at the application level.
Maximum Output Buffer size	1024KB	Lower	A lower output buffer size may reduce the memory footprint in some applications. Keep in mind that once the output buffer is flushed tags that modify the response headers will throw an exception.
Enable In-Memory File System	Checked	Unchecked if not used	If your applications do not require in memory file system uncheck this checkbox.
Memory Limit for In-Memory Virtual File System	100MB	Tuned based on JVM heap size and feature usage	Ensure that you have allocated sufficient JVM heap space to accommodate the memory limit.
Memory Limit per Application for In-Memory Virtual File System	20MB	Tuned based on JVM heap size and feature usage	Ensure that you have sufficient JVM heap space to accommodate the memory limit.
Watch configuration files for changes (check every N seconds)	Unchecked	Unchecked	If your configuration requires this setting to be enabled (if using WebSphere ND vertical cluster for example), increase the time to be as large as possible. If an attacker is able to modify the configuration of your ColdFusion server, their changes can become active within a short period of time when this setting is enabled.

Setting	Default	Recommendation	Description
Enable Global Script Protection	Unchecked	**Understand limitations**, Checked	This setting provides **very limited protection** against certain Cross Site Scripting attack vectors. It is important to understand that enabling **this setting does not protect your site from all possible Cross Site Scripting attacks**. When this setting is turned on it uses a regular expression defined in the file `neo-security.xml` to replace input variables containing following tags: `object`, `embed`, `script`, `applet`, `meta` with `InvalidTag`. This setting does not restrict any javascript strings that may be injected and executed, iframe tags, or any XSS obfuscation techniques.
Disable creation of unnamed applications	Unchecked	Checked	Applications should have a name so they can be isolated from each other.
Allow adding application variables to Servlet Context	Unchecked	Unchecked	Keep unchecked to improve application isolation.
Default ScriptSrc Directory	/cf_scripts/scripts/	/*somewhere-else*/	See section 2.16 (Windows) or 5.4 (Linux). Because the scripts directory also contains CFML source code (such as FCKeditor), you should move this directory to a non-default location.
Allowed file extensions for CFInclude tag	*	cfm	This setting restricts the file extensions which get compiled (executed) by a cfinclude tag. Any file file extensions not matching this list are statically included, any CFML source code would not be executed. Take care to ensure that you have specified any file extensions of files that contain CFML code and are included with cfinclude. This setting can be defined at an application level as well.

Setting	Default	Recommendation	Description
Missing Template Handler	Blank or /CFIDE/administrator/templates/missing_temp late_error.cfm	Specified	The missing template handler HTML should be equivalent to the 404 error handler specified on your web server. When blank, the missing template handler is not specified a potential attacker may get a rough idea of the ColdFusion version in use.
Site-wide Error Handler	Blank or /CFIDE/administrator/templates/secure_profile_error.cfm	Specified	When blank, the site-wide error handler may expose information about the cause of exceptions. Specify a custom site-wide error handler that discloses the same generic message to the user for all exceptions. Be sure to log and monitor the actual exceptions thrown.
Maximum number of POST request parameters	100	As low as your application allows.	Set this to the maximum number of form fields you have on any given page. Allowing too many form fields may allow for a DOS attack known as HashDOS. See http://www.petefreitag.com/item/808.cfm
Maximum size of post data	100MB	As low as possible	If your application does not deal with large HTTP POST operations (such as file uploads, or large web service requests), reduce this size to 1MB. If the application does allow uploads of files set this to the maximum size you want to allow. You should also be able to specify a HTTP Request size limit on your web server.
Request Throttle Threshold	4MB	1MB	ColdFusion will throttle any request larger than this value. If your application requires a large number of concurrent file uploads to take place, you may need to increase this setting.
Request Throttle Memory	200MB	100MB on 32 bit installations.	On a 32 bit installation the default value would be close to 20% of the heap. 64 bit servers allow for much larger heap sizes. Aim for 10% of the maximum heap size as an upper limit for this setting.

Setting	Default	Recommendation	Description
Allow REST Discovery	Unchecked	Unchecked if not used.	This setting enables the end point `/rest/_api_listing` or `/api/_api_listing` to allow the ColdFusion API manager to get a listing of REST apis. ColdFusion Administrator authentication is required.

3.2 Server Settings > Request Tuning

The Request Tuning settings can help mitigate the ability to perform a successful Denial of Service (DOS) attack on your server.

Setting	Default	Recommendation	Description
Maximum number of simultaneous Template requests	25	Tuned based on hardware capabilities, and application characteristics.	When this setting is too high or too low the ability to perform a denial of service attack increases. When too low requests will be queued when the server is placed under load. When too high requests may not be queued under load causing the CPU time of all requests to increase significantly (known as context switching). Find a good medium by performing load tests against your production environment, use the value that has the ability to serve the most requests per second.
Maximum number of simultaneous Flash Remoting requests	5	1 if not using Flash Remoting, otherwise tuned.	If your applications do not use flash remoting set this value to 1. If you do use flash remoting use a load testing approach to find the optimal value for this setting. Note that the Server Monitor feature in Enterprise makes use of flash remoting.
Maximum number of simultaneous Web Service requests	5	1 if not publishing SOAP web services, otherwise tuned	If your applications do not publish SOAP web services set this value to 1. Otherwise tune this setting using load tests.
Maximum number of simultaneous CFC function requests	15	1 if not using Remote CFC function requests, otherwise tuned.	This setting applies only to CFC functions that have access=remote specified, when they are invoked via a HTTP request, for example: /example.cfc?method=MethodName. The ColdFusion AJAX proxy uses this method to invoke CFCs. If your applications do not make use of this feature set to 1. Otherwise use load testing to find the optimal value for this setting.
Maximum number of simultaneous Report threads	1	1	Keep this value at 1 unless you are using cfreport heavily.

Setting	Default	Recommendation	Description
Maximum number of threads available for CFTHREAD	10	1 if not using cfthread, tuned otherwise.	Set this value to 1 if you are not using cfthread. If you do use cfthread setting a value too high can lead to context switching.
Timeout requests waiting in queue after	60 seconds	5 seconds (Match Request Timeout)	This setting can generally be set equivalent to the *Timeout Requests After* value specified in the Settings section. A lower setting here can mitigate the effectiveness of DOS attacks.
Request Queue Timeout Page	Blank or /CFIDE/administrator/templates/request_timeout_error.cfm	Specified	Specify a HTML file giving the user a message to wait and retry their request again. The message should not disclose the fact that the queue timed out.

3.3 Server Settings > Caching

Setting	Default	Recommendation	Description
Trusted Cache	Unchecked	Checked - *Understand that code changes will not appear until cache is flushed*.	Enabling trusted cache improves performance by caching CFML code for the duration of the server process (unless manually cleared). This may also mitigate a situation where an attacker attempts to change a file on the server, the new code would not execute until the server is restarted or the cache is cleared.

3.4 Server Settings > Client Variables

Setting	Default	Recommendation	Description
Default Storage Mechanism for Client Sessions	Cookie	None / Cookie	If applications have client management enabled a large amount of data can accumulate on the server. This can lead to a storage failure if disks become full. Because the registry is typically located on the system partition it is not recommended to use the Registry.

3.5 Server Settings > Memory Variables

Setting	Default	Recommendation	Description
Use J2EE session variables	Unchecked	Checked if J2EE interoperability required.	When checked ColdFusion will use the session management of the underlying JEE container (eg Tomcat) instead of it's own CFID/CFTOKEN. When J2EE sessions are enabled certain features such as application specific session cookie settings (`this.sessionCookie` in Application.cfc) do not apply. The functions `SessionRotate` and `SessionInvalidate` do operate on J2EE sessions.
Enable Session Variables	Checked	Unchecked only if not using sessions	Most applications require session variables but if none of the applications on the server require them uncheck this box.
Session Storage	In Memory	In Memory or Redis	When using Redis to store sessions take extreme care to ensure that the datastore is protected by network firewalls and a strong password.
Maximum Timeout: Session Variables	2 Days	Lower	Two days is generally too long for sessions to persist. Lower session timeouts reduce the window of risk of session hijacking.
Default Timeout: Session Variables	20 Minutes	Lower	Twenty minutes is a good default value, but high security applications will require a lower timeout value.
Cookie Timeout	1440 Minutes	-1	By setting to -1 ColdFusion will set the session cookie as a browser session cookies, which is valid as long as the users browser window is open.
HTTPOnly	Checked	Checked	Session cookies should always be marked as HTTPOnly to prevent JavaScript or other client side technologies from accessing their values (on supported clients).
Secure	Unchecked	Checked if all sites require SSL.	A client will only transmit a *secure* cookie over a secured connection (eg SSL).

Setting	Default	Recommendation	Description
Disable updating ColdFusion internal cookies using ColdFusion tags/functions.	Checked on Secure Profile	Checked if all sites require SSL.	You can use this feature to prevent a developer from overriding your global session cookie security settings. Check this only if all applications will use the same settings.

3.6 Server Settings > Mappings

Remove any mappings your applications do not require, such as `/gateway`

3.7 Server Settings > Mail

Setting	Default	Recommendation	Description
Enable SSL socket connections to mail server	Unchecked	Checked if supported	Consider enabling SSL or TLS encryption for sending mail with ColdFusion.
Enable TLS connection to mail server	Unchecked	Checked if supported	Consider enabling SSL or TLS encryption for sending mail with ColdFusion.

3.8 Server Settings > WebSocket

Setting	Default	Recommendation	Description
Enable WebSocket Service	Unchecked	Unchecked if not needed.	Disable the WebSocket Service if not required by your applications.

3.9 Server Settings > Charting

Setting	Default	Recommendation	Description
Disk cache location	{cf.instance}/tmpCache/CFFileServlet/_cf_chart	Non default location.	Consider changing the disk cache location to a non default path. The ColdFusion user will require read and write permission to the path specified if cfchart is used.

3.10 Data & Services > Data Sources

Remove the example data sources, `cfartgallery`, `cfbookclub`, `cfcodeexplorer`, `cfdocexamples`.

Setting	Default	Recommendation	Description
Login Timeout (sec)	30 Seconds	5 Seconds	Decrease this value to be less than the *Timeout Requests after* setting.
Query Timeout (seconds)	0 (*no timeout)*	Specified	Specify an upper limit to mitigate DOS attacks.
Allowed SQL	SELECT, INSERT, UPDATE , DELETE, CREATE, DROP, ALTER, GRANT, REVOKE, Stored Procedures	Enable only what your application requires.	The CREATE, DROP, ALTER, GRANT, and REVOKE operations are not commonly used in web applications. Ensure that the database user that ColdFusion connects as, also has limited permissions to only what is necessary.

3.11 Data & Services > ColdFusion Collections

Remove the example collection: `bookclub` if it exists.

3.12 Data & Services > Solr Server

Consider using a HTTPS connection to the Solr server, especially if it is located on another server.

3.13 Data & Services > Flex Integration

Setting	Default	Recommendation	Description
Enable Flash Remoting support	Checked	Unchecked if not used.	Disable Flash Remoting if it is not being used. Note Flash Remoting is used by the Server Monitoring feature in the Enterprise edition.
Enable Remote Adobe LiveCycle Data Management access	Unchecked	Unchecked if not used.	Disable if not used.
Enable RMI over SSL for Data Management	Unchecked	Checked if using LiveCycle Data Services ES	Enable and specify a keystore and password if using LiveCycle Data Services ES with Flex.

3.14 Data & Services > PDF Service

If the PDF Service is used to generate PDFs containing sensitive data ensure that HTTPS is enabled.

3.12 Debugging & Logging > Debug Output Settings

Setting	Default	Recommendation	Description
Enable Robust Exception Information	Unchecked	Unchecked	When robust exception information is enabled sensitive information may be disclosed when exceptions occur.
Enable AJAX Debug Log Window	Unchecked	Unchecked	Debugging should not be enabled on a production server.
Enable Request Debugging Output	Unchecked	Unchecked	Debugging should not be enabled on a production server.

3.13 Debugging & Logging > Debugger Settings

Setting	Default	Recommendation	Description
Allow Line Debugging	Unchecked	Unchecked	Debugging should not be enabled on a production server.

3.14 Debugging & Logging > Logging Settings

Setting	Default	Recommendation	Description
Log directory	{cf.instance.root}/logs	Non Default	Ensure that the location of this directory has sufficient storage space to hold Maximum File Size multiplied by the Maximum number of archives multiplied by the number of log files (6 or more).
Maximum number of archives	10	Larger	When a log file reaches the Maximum File Size (5000KB by default), it is archived. When the maximum number of archives is reached for a particular log file, the oldest log file is deleted. Some security compliance regulations require that log files are kept for a minimum period of time. Ensure that this value is high enough to retain log files for the required duration.

Setting	Default	Recommendation	Description
Use operating system logging facilities	Unchecked	Checked	Certain log entries will be duplicated to syslog on Unix based operating system.
Enable logging for scheduled tasks	Unchecked	Checked	Log scheduled task execution.

3.15 Debugging & Logging > Remote Inspection Settings

Setting	Default	Recommendation	Description
Allow Remote Inspection	Unchecked	Unchecked	Do not enable debugging features on production.

3.16 Event Gateways > Settings

Setting	Default	Recommendation	Description
Enable ColdFusion Event Gateway Services	Unchecked	Unchecked, if not using Event Gateways	If you do not use Event Gateways, disable the Event Gateway Service.

3.17 Event Gateways > Gateway Instances

Delete the SMS Menu App and any other gateways that are not in use.

3.18 Security > Administrator

Setting	Default	Recommendation	Description
ColdFusion Administration Authentication	Separate user name and password authentication	Separate user name and password authentication	Using separate usernames and passwords allows you to specify which parts of the ColdFusion administrator each user may use.
Password Seed		Generate a Cryptographically Secure Random Value	The password seed is used to generate an encryption key to encrypt passwords for datasources, and other services.

Setting	Default	Recommendation	Description
Allow concurrent login sessions for Administrator Console	Unchecked	Checked	Check to prevent concurrent logins by the same user account in the ColdFusion Administrator.

3.19 Security > RDS

Setting	Default	Recommendation	Description
Enable RDS	Unchecked	Unchecked	RDS should not be enabled on production server. If RDS was previously enabled ensure that the /WEB-INF/web.xml does not contain a ServletMapping for the RDSServlet.

3.20 Security > Sandbox Security

Setting	Default	Recommendation	Description
Enable ColdFusion Sandbox Security	Unchecked	Checked	Sandboxes allow you to lock down which CFML source files have access the file system, tag / function execution, datasource access, and network access. It is highly recommended that you setup a sandbox or multiple sandboxes for your applications.

3.21 Security > User Manager

Add user accounts for each administrator.

3.22 Security > Allowed IP Addresses

Setting	Default	Recommendation	Description
Allowed IP Addresses for Exposed Services		None	Any IP address in this list may execute remote services that expose server functionality via web services. To invoke these web services the client must be on the allowed IP list, and have a username and password. It is recommended that you do not use this feature in environments requiring maximum security. This feature has been deprecated as of ColdFusion 11+
Allowed IP Addresses for ColdFusion Internal Components		127.0.0.1 or other internal administrative IP addresses	Specify to limit which IP addresses may connect to the ColdFusion administrator, AdminAPI.

3.23 Security > Secure Profile

Setting	Default	Recommendation	Description
Enable Secure Profile	Specified during installation.	Checked or Compare Settings	Compare the values you have specified with the secure profile recommended values. Review each setting that will be changed and test your application to ensure that the secure profile settings will not cause any issues.

3.24 Server Update > Updates > Settings

Setting	Default	Recommendation	Description
Automatically Check for Updates		Checked	Check for ColdFusion updates every time you login to ColdFusion administrator. A notification icon will show up in upper right toolbar if an update is available.
Check for Updates every N days	Unchecked	Checked	Setup email alerts to be notified when a server update is available.

Setting	Default	Recommendation	Description
Site URL	http://www.adobe.com/go/coldfusion-updates	HTTPS version of url - or specify an internal URL	Change the default URL to https to avoid a spoofed update. If your network security policy does not allow external internet connection you can maintain a internal update URL which could be updated manually.

Section 4 - Additional Lockdown Measures

The steps outlined in this section can provide additional security but may require special care or attention to configure and maintain.

4.1 Configure the Built-in Web Server

When you installed ColdFusion it setup the Tomcat web server running on a port selected at installation (8500 is the default). If you have configured a dedicated website for the ColdFusion Administrator in Apache or IIS then the built-in web server is no longer needed and should be disabled. If you plan on using the built-in web server to access ColdFusion administrator you may need to create an alias for `/cf_scripts/scripts` if you changed the *Default Script Src* setting in ColdFusion administrator.

To Disable the Built-in Web Server

Backup and edit the `{cf.instance.root}/runtime/conf/server.xml` file, and remove or comment out the `Connector` tag similar to the following:

```
<!--<Connector executor="tomcatThreadPool" maxThreads="50"
               port="8500"
protocol="org.apache.coyote.http11.Http11Protocol"
               connectionTimeout="20000"
               redirectPort="8445" />-->
```

This must be repeated for each ColdFusion instance created.

Restart ColdFusion and confirm that the server port is disabled.

Important: You must use XML comments with two dashes `<!-- xml comment -->` if you use a CFML comment (3 dashes) `<!--- cfml comment --->` ColdFusion may not start.

To Create a new Alias for /cf_scripts/scripts in the built-in web server

If you plan to use the built-in web server for accessing ColdFusion administrator then you must also add an alias by adding a Context tag inside the Host tag of `server.xml` located: `/opt/cf2016/cfusion/runtime/conf/server.xml`

```
<Context path="/"
   docBase="/opt/cf2016/cfusion/wwwroot"
   WorkDir="/opt/cf2016/cfusion/runtime/conf/Catalina/localhost/tmp"
   aliases="/cfscripts=/opt/cf2016/fusion/wwwroot/cf_scripts" />
```

Restart ColdFusion, then test by visiting `/cf_scripts/scripts/cfform.js` on your built-in server.

To Configure the Built-in Web Server to listen on a single IP Address

By default the connector will listen on all IP addresses. To configure the built-in web server to only listen on a single address (for example 127.0.0.1) locate the `<Connector />` in `{cf.instance.root}/runtime/conf/server.xml` with a port attribute matching the port your built-in web server is running on, add an address attribute. For example:

```
<Connector address="127.0.0.1" ...>
```

Restart ColdFusion and confirm that the built-in web server now only listens on the specified address. See https://tomcat.apache.org/tomcat-8.0-doc/config/http.html for more information.

4.2 Configure Sandbox Security

Login to the ColdFusion administrator and select *Enable Sandbox Security* from the *Security > Sandbox Security* page.

Configure sandboxes for each site, or high risk portions of each site. Using the principal of least privilege deny access to any tags, functions, data sources, file paths, and IP / ports that do not need to be accessed by code in the particular sandbox.

The sandbox path of the requested CFM / CFC is the active sandbox for all code executed in a particular request.

Fully test your web applications to ensure that everything is functioning properly.

4.3 Lockdown the ColdFusion Add-on Services

If you installed the *ColdFusion (2016 release) Add-on Services* for Solr (`cfsearch`, `cfcollection`, `cfindex`) or the PDF Service (`cfhtmltopdf`) they run as a separate process / service. The Add-on Services leverage Jetty as the JEE servlet container instead of Tomcat (which is used by the ColdFusion Application Server).

If you do not use `cfsearch`, `cfcollection`, `cfindex`, or `cfhtmltopdf` ensure that you have disabled the service.

Next ensure that it is not running under a privileged user account such as root, or System. You may create a dedicated user specifically for the Add-on Services. This user simply needs read / write permission on the folder `{cf.root}/cfusion/jetty`

Consider using a non-default port (8989 is the default) and enabling HTTPS.

For maximum isolation, consider installing the ColdFusion Add-on Services on a dedicated server.

Consult the Jetty Documentation for more information:
http://www.eclipse.org/jetty/documentation/

4.4 Lockdown File Extensions

ColdFusion provides a number of capabilities that are not used commonly which can be blocked. A good example of this is JSP file execution. Here is a list of file extensions that *usually* can be blocked (check with developers first):

File Extension	Purpose	Safe to Block
.cfml	Executes CFML templates (same as .cfm files)	The .cfml file is not typically used by developers, if you don't use .cfml block this file extension.
.jsp	JavaServer Pages	Yes, if your applications do not require JSP.
.jws	Java Web Services - allows you to easily write and deploy SOAP web services in Java similar to a CFC.	Yes if not used.
.cfr	CFReport Files	Yes if cfreport is not used.
.cfswf	Dynamically generated swf files from flash forms.	Yes if flash forms are not used.
.hbmxml	Hybernate XML mappings	Yes this should always be blocked.

Blocking by File Extension with Apache

To block .cfml, .jsp, .jws and .hbmxml files add the following to your Apache `httpd.conf` file:

```
RedirectMatch 404 (?i).*\.(cfml|jsp|jws|hbmxml).*
```

Restart apache and create a `test.cfml` file to confirm that the rule is working.

Blocking by File Extension on IIS

Click on the root node of IIS and then double click *Request Filtering*. Click on the *File Name Extensions* tab, and then click *Deny File Name Extension* in the *Actions* menu on the right. Add a file name extension including the dot and click ok.

File Extension Whitelisting

A more robust solution is to specify a whitelist of allowed file extensions, and block the rest. For example allow only .cfm .css .js .png and block anything else. Your application may require additional extensions.

File Extension Whitelisting on IIS

Click on the root node of IIS and then double click *Request Filtering*. Click on the *File Name Extensions* tab, and then click *Allow File Name Extension*. Allow each file extension your sites serve (for example cfm, css, js, png, html, jpg, swf, ico, etc).

You must also ensure that the `.dll` file extension is allowed in the `/jakarta` virtual directory in order for ColdFusion resources to be served.

Test your web sites after making changes in this section.

4.5 Optionally Remove ASP.NET (Windows Only)

Once you have all websites configured in IIS, you may consider removing the IIS Role Services: ASP.NET, .NET Extensibility and CGI which are required by the connector installer, however may not be needed at runtime.

If you are running the IIS WebSocket proxy then ASP.NET support is required and must not be removed.

This approach while it may provide additional security by allowing removal of unused software, does have two drawbacks. First this is not a procedure that is officially documented or supported by Adobe. Adobe does not test without these settings enabled so you may encounter something unexpected. Second when a ColdFusion update is released for the connector or if you want to add/update/delete an IIS connector you must re-enable these role services before updating the connector.

4.6 Change the Tomcat Shutdown Port

Tomcat listens on a TCP port (8007 by default, may differ if multiple instances) for a SHUTDOWN command. When the command is received on the specified port the server will shut down.

Edit the file `{cf.instance.home}/runtime/conf/server.xml` and locate the line similar to:

```
<Server port="8007" shutdown="SHUTDOWN">
```

Change `8007` to -1 to disable this feature, or to random port number. Tomcat should only listen on 127.0.0.1 for this port, however you should also ensure that your firewall does not allow external connections to this port.

Also consider changing the shutdown command that is the value of the `shutdown` attribute of the `Server` tag. This string is essentially a password used to shut down the server locally when the port is enabled.

Next look in: `{cf.instance.home}/bin/port.properties` and edit the following line to match `server.xml` port value:

```
SHUTDOWN=8007
```

Ensure that global read permission is denied for both these files.

Please note: Changing the port setting may cause the shutdown of the ColdFusion Service on Windows to fail, you may need to kill the process manually to stop ColdFusion. The Linux shutdown script should still work properly when the port is changed.

4.7 Add a connector shared secret

Specify a shared secret for the AJP connector by editing `{cf.instance.home}/runtime/conf/server.xml`

Look for a line similar to:

```
<Connector port="8012" protocol="AJP/1.3" redirectPort="8445"
tomcatAuthentication="false" />
```

Add a `requiredSecret` attribute with a random strong password:

```
<Connector port="8012" protocol="AJP/1.3" redirectPort="8445"
tomcatAuthentication="false" requiredSecret="yourSecret" />
```

Next edit the corresponding `workers.properties` file, eg `{cf.home}/config/wsconfig/1/workers.properties` and add a line:

```
worker.cfusion.secret=yourSecret
```

Please note: If you add, update or reinstall your web server connector you will need to update the `workers.properties` file with the shared secret again.

Restart IIS and ColdFusion then test your websites.

4.8 Disable Unused Servlet Mappings

All JEE web applications have a file in the `WEB-INF` directory called `web.xml` this file defines the servlets and servlet mappings for the JEE web application. A servlet mapping defines a URI pattern that a particular servlet responds to. For example the servlet that handles requests for `.cfm` files is called the `CfmServlet` the servlet mapping for that looks like this:

```
<servlet-mapping id="coldfusion_mapping_3">
   <servlet-name>CfmServlet</servlet-name>
   <url-pattern>*.cfm</url-pattern>
</servlet-mapping>
```

The servlets are also defined in the `web.xml` file. The `CfmServlet` is also defined in web.xml as follows:

```
<servlet id="coldfusion_servlet_3">
  <servlet-name>CfmServlet</servlet-name>
  <display-name>CFML Template Processor</display-name>
  <description>Compiles and executes CFML pages and tags</description>
  <servlet-class>coldfusion.bootstrap.BootstrapServlet</servlet-class>
  <init-param id="InitParam_1034013110656ert">
     <param-name>servlet.class</param-name>
     <param-value>coldfusion.CfmServlet</param-value>
  </init-param>
  <load-on-startup>4</load-on-startup>
</servlet>
```

We can remove servlet mappings in the `web.xml` to reduce the surface of attack. You don't typically want to remove the `CfmServlet` or the `*.cfm` servlet mapping, but there are other servlets and mappings that may be removed.

In addition some servlets may depend on each other, so it may be better to just remove the `servlet-mapping` instead.

Be sure to backup `web.xml` before making changes, as incorrect changes may prevent the server from starting.

Servlet Mapping	Servlet	Purpose
*.cfm *.CFM *.Cfm	CfmServlet	Handles execution of CFML in cfm files. Required
*.cfml *.CFML *.Cfml	CfmServlet	Handles execution of CFML contained in files with the .cfml file extension. These servlet mappings can be commented out if you do not have any files with a .cfml file extension in your code base.
*.cfc *.CFC *.Cfc	CFCServlet	Handles execution of remote function calls in cfc files. These servlet mappings can be commented out if you do not use any CFCs with `access=remote`
.cfml/ *.cfm/* *.cfc/*	CfmServlet CFCServlet	These servlet mappings are used for search engine safe url's such as `/index.cfm/x/y`
/CFIDE/main/ide.cfm	RDSServlet	Used for RDS, this servlet mapping should be commented out on production servers. If you do enable RDS in production (which is highly discouraged) you should ensure that it runs over HTTPS and is locked down by IP address.
/JSDebugServlet/*	JSDebugServlet	Used for debugging cfclient, should be commented out on production servers.

Servlet Mapping	Servlet	Purpose
.jws	CFCServlet	Java Web Services - allows you to easily write and deploy SOAP web services in Java similar to a CFC. Should be commented out of your applications do not have any jws files.
.cfr	CFCServlet	Used for cfreport, can be commented out if cfreport is not used.
/CFFormGateway/*	CFFormGateway	Required for flash forms <cfform format=flash>, can be commented out if not needed.
/CFFileServlet/*	CFFileServlet	
/securityanalyzer/*	CFSecurityAnalyzerServlet	Used for CFBuilder security analyzer.
/rest/*	CFRestServlet	Used for rest web services
/api/*	CFRestServlet	Used for rest web services
*.hbmxml	CFForbiddenServlet	Used to prevent serving Hibernate mapping files. This should not be removed.
/cfform-internal/*	CFInternalServlet	Required for flash forms <cfform format=flash>, can be commented out if not needed.
*.cfswf	CFSwfServlet	Dynamically generated swf files from flash forms, can be commented out if flash forms are not needed.
*.as *.sws *.swc	CFForbiddenServlet	Used to prevent serving ActionScript / Flash source code.
/WSRPProducer/*	WSRPProducer	Allows you to publish portlets over Web Services for Remote Portlet (WSRP). Can be commented out if you do not publish portlets over WSRP.
/flashservices/gateway/*	FlashGateway	Used for Flash Remoting
/flex-internal/*	FlexInternalServlet	Used for flex history manager.

Servlet Mapping	Servlet	Purpose
*.mxml	FlexMxmlServlet	Used to compile Flex mxml files into swf
/flex2gateway/*	MessageBrokerServlet	Used for Flash Remoting

To remove a servlet mapping, you can comment it out using an XML comment `<!-- xml comment -->` for example to disable the RDS servlet mapping:

```
<!--
<servlet-mapping id="coldfusion_mapping_9">
        <servlet-name>RDSServlet</servlet-name>
        <url-pattern>/CFIDE/main/ide.cfm</url-pattern>
</servlet-mapping>
-->
```

Restart ColdFusion and test your application after commenting out servlet mappings. It is a good idea to only remove one at a time and then test again.

4.8 Additional Tomcat Security Considerations

Consult the Tomcat 8 Security Considerations document (http://tomcat.apache.org/tomcat-8.0-doc/security-howto.html) for additional tomcat specific security settings.

4.9 Additional File Security Considerations

Pay careful attention to the file permissions of sensitive configuration files located in `{cf.instance.home}/lib/` such as `password.properties`, `seed.properties` and all `neo-*.xml` files. In addition the files located in `{cf.instance.home}/runtime/conf/` contain important configuration files utilized by the Tomcat container.

4.10 Adding ClickJacking Protection

ColdFusion 10 introduced two Servlet Filters `CFClickJackFilterDeny` and `CFClickJackFilterSameOrigin`. When a URL is mapped to one of these servlets the `X-Frame-Options` HTTP header will be returned with a value of `DENY` or `SAMEORGIN`. You can add a `filter-mapping` in `web.xml` to enable these filters for a given URI, this functionality could also be accomplished at the web server level.

4.11 Restricting HTTP Verbs

Most web applications only need to function on `GET`, `HEAD` and `POST`. Applications that make use of Cross Origin Resource Sharing (CORS) will also require the `OPTIONS` header. Servers that host REST web services may require additional HTTP methods.

Whitelisting HTTP Verbs in Apache

The Limit and LimitExcept directives can be used to apply configuration based on the HTTP method. For example to deny all requests except GET, HEAD and POST you can add the following to your `httpd.conf`:

```
<Location />
    <LimitExcept GET HEAD POST>
        Order Deny,Allow
        Deny from all
    </LimitExcept>
</Location>
TraceEnable off
```

Note that LimitExcept does not apply to the HTTP `TRACE` method. The `TRACE` method can be disabled using the Apache directive `TraceEnable`. Restart Apache.

Whitelisting HTTP Verbs in IIS

Click on the root node in IIS and double click *Request Filtering* and select the HTTP Verbs tab. Click *Allow verb* and each HTTP verb you want to allow.

Now to disallow any verb that has not been explicitly allowed, click *Edit Feature Settings* and Uncheck *Allow unlisted verbs*.

4.12 Security Constraints in web.xml

The servlet container (Tomcat) can enforce certain security constraints to ensure that a given URI is secured, or to limit certain URIs to HTTP POST over a secure (SSL) connection:

```
<security-constraint>
        <display-name>POST SSL</display-name>
        <web-resource-collection>
                <web-resource-name>POST ONLY SSL</web-resource-name>
                <url-pattern>/post/*</url-pattern>
                <http-method>POST</http-method>
        </web-resource-collection>
        <user-data-constraint>
                <transport-guarantee>CONFIDENTIAL</transport-guarantee>
        </user-data-constraint>
   </security-constraint>
   <security-constraint>
        <display-name>POST ONLY</display-name>
        <web-resource-collection>
                <web-resource-name>BLOCK NOT POST</web-resource-name>
                <url-pattern>/post/*</url-pattern>
                <http-method>GET</http-method>
                <http-method>HEAD</http-method>
                <http-method>PUT</http-method>
                <http-method>DELETE</http-method>
                <http-method>TRACE</http-method>
        </web-resource-collection>
        <auth-constraint />
  </security-constraint>
```

4.13 Limit Request Size

Limiting the size of various elements of the HTTP request can help mitigate denial of service attacks and other risks.

Consider specifying smaller request size limits by default, and then use larger sizes on URIs where files are uploaded or very large form submissions occur.

Limit Request Size in IIS

In IIS you can use the Edit Feature Settings dialog in Request Filtering to control the Maximum Allowed Content Length, Maximum URL Length and Maximum Query String Length.

Limit Request Size in Apache

Apache has several directives that can be used to control the allowed size of the request. Here are a few directives you should consider setting: `LimitRequestBody`, `LimitXMLRequestBody`, `LimitRequestLine`, `LimitRequestFieldSize`, `LimitRequestFields.`

4.14 Distributed Mode or Reverse Proxy

Consider running in a reverse proxy or distributed mode, such that only the web server and ColdFusion server are on different servers. This method provides isolation between your web server and the ColdFusion application server.

In distributed mode, only the web server connector is installed on the server containing the web server.

Section 5: ColdFusion on Linux

This section covers installation of ColdFusion on Linux with Apache, Windows/IIS readers may skip to Section 4. To install ColdFusion (2016 release) on Linux we will perform the following steps:

- Perform installation prerequisites
- Create a Dedicated User Account for ColdFusion to run as.
- Install ColdFusion
- Check for, and install any ColdFusion hotfixes.
- Configure Apache
- Configure file system permissions.
- Run the web server configuration tool to connect ColdFusion to Apache
- Setup ColdFusion Administrator Site
- Update the JVM

5.1 Linux Installation Prerequisites

Before you begin the ColdFusion installation process perform the following steps:

- Configure a network firewall (and / or configure a local firewall using iptables) to block all incoming public traffic during installation.
- Read the Red Hat Enterprise Linux 7 Security Guide: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/
- Install Red Hat Linux with minimal packages, you do not need to install a graphical desktop environment.
- Enable SELinux Enforcing mode during installation. See https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/SELinux_Users_and_Administrators_Guide/ for more information about SELinux.
- Remove or disable any software on the server that is not required.
  - To see what packages are installed run: `yum list installed | more`
  - For example: `yum erase php`
- Run `yum update` and ensure that all software running on the server is fully patched.
- Download ColdFusion from adobe.com
- Verify that the MD5 checksum listed on adobe.com download page matches the file you downloaded. You can run the following in a Command Prompt: `md5sum installer-file-name.exe`

5.2 Create a Dedicated User Account for ColdFusion

Create a new group which will contain both ColdFusion users and apache's user, in this guide we will name this group `webusers`. Choose a unique name,

```
# groupadd webusers
```

Create a user for ColdFusion to run as, in this guide we use `cfuser`, but consider picking a unique username:

```
# adduser -g webusers -s /sbin/nologin -M -c ColdFusion cfuser
```

Specify a strong password for the new user:

```
# passwd cfuser
```

If you are running multiple instances of ColdFusion consider creating a dedicated user account for each instance to run as.

5.3 ColdFusion Installation

- Run the installer as root or using `sudo`.
- **Installer Configuration**: Choose #1 - *Server configuration*
  - If you are deploying ColdFusion a JEE server such as WebSphere, WebLogic, JBoss, etc. select an EAR or WAR file, otherwise choose option 1 Server configuration.
- **Select ColdFusion Server Profile**: *Production Profile + Secure Profile*
  - The *Development Profile* should not be selected, it enables features that are intended for development purposes.
  - The *Production Profile* disables development features by default.
  - The *Production Profile + Secure Profile* option has all the features of the Production Profile plus provides a more secure foundation of default settings.
  - Some of the settings that the *Secure Profile* toggles may cause application compatibility issues. Just as you should with each step in this guide, ensure that you have tested your application for such issues.
  - As of ColdFusion 11+ the Secure Profile settings can also be toggled from the ColdFusion Administrator.
- **IP Addresses allowed**: 127.0.0.1,::1
  - Comma separate any other IP addresses that need to access ColdFusion Administrator.
- **Sub-components Installation**
  - *API Manager* - Uncheck this, you can install it as a standalone later (see section 6)
  - *Solr Service* - the Solr service is needed only if you are using cfsearch, cfcollection, cfindex tags. Disable the Solr service if not needed.
  - *PDFG* - enable if you are using the cfhtmltopdf tag.
  - *Admin component for Remote Start/Stop* - disable.
  - *Start ColdFusion on system init* - enable.
- **Enabling/Disabling Servlets**
  - Uncheck RDS, JS Debug
  - Uncheck WSRP if not using Web Services for Remote Portlets
  - Uncheck CF Reporting if you are not using the cfreport tag.
  - Uncheck CFSWF and Flash Forms if not using Flash Forms
- **Access Add-on Services Remotely**

    - If you selected the PDFG (`cfhtmltopdf` tag) or Solr (`cfsearch`, `cfindex`, `cfcollection` tags) sub-components the ColdFusion (2016 release) Add-on Services will be installed. When you specify n for the *Access Add-on Services Remotely* option, the Add-on Services are only accessible from the local machine (localhost). If you want to allow access to the services from multiple ColdFusion servers, enter y and then specify the IP addresses of the remote ColdFusion servers.
- **Choose Install Folder**
    - Select a non-default installation folder, in this guide we will use `/opt/cf2016/`
- **Configure Web Servers**
    - Continue with installation - do not install the web server connector yet.
- **Runtime User**
    - Enter the name of the user created in the previous section: `cfuser`
- **Configure ColdFusion with OpenOffice**
    - Skip if not required - OpenOffice integration is used by `cfdocument` to convert Word documents to PDF or PowerPoint presentations to PDF/HTML.
- **Administrator Credentials**
    - Enter username: select a unique username (not *admin*)
    - Enter password: choose a strong password
- **Server Updates**
    - Y automatically check for server updates.

When the installer completes start the ColdFusion server by running: `service coldfusion_2016 start` as `root` or with `sudo`.

Access ColdFusion Administrator via a SSH Tunnel

To access ColdFusion Administrator you can create a SSH tunnel that points to the built-in web server port (`8500` by default), by opening a local port (`33333` in our example, but you can use any local port number you want as long as it is not in use).

If your desktop computer is running Mac or Linux you can create a SSH tunnel to port `8500` on your local port `33333` by running the following command (locally on your desktop, not on your ColdFusion server):

```
ssh -L 33333:127.0.0.1:8500 your.new.server.example.com
```

If you are running a Windows desktop you can use putty.exe (download from putty.org)

```
putty -L 33333:127.0.0.1:8500 your.new.server.example.com
```

Now open your web browser and point to http://127.0.0.1:33333/CFIDE/administrator/

The nice thing about using a SSH Tunnel is that all traffic to ColdFusion Administrator is encrypted over a SSH, similar to HTTPS.

5.4 Install ColdFusion Hotfixes / Updates

Because Apache is not configured yet you will need to login to the ColdFusion administrator via the built-in web server. See previous section to create a SSH tunnel connection from a computer with a web browser to the built-in ColdFusion web server.

Click on *Server Updates* > *Updates* and then select the latest hotfix, and click *Download*.

Verify the integrity of the download by performing an `md5sum` on the `hotfix_XXX.jar` file, see that it matches the value found in Adobe ColdFusion update feed: https://www.adobe.com/go/coldfusion-updates

If your server does not have a public internet connection you can locate the `hotfix_XXX.jar` file url using the ColdFusion update feed. Download the `hotfix_XXX.jar` file on a computer with internet access, verify the checksum, and then transfer it to the server.

If your server requires a proxy server to connect to the internet you may need to add the following *JVM Arguments* (in ColdFusion Administrator under *Server Settings* > *Java and JVM*) and then restart ColdFusion to use your proxy server:

```
-Dhttp.proxyHost=proxy.example.com -Dhttp.proxyPort=12345 -
Dhttp.proxyUser=u -Dhttp.proxyPassword=p
```

If the md5 checksum matches install the hotfix as `root` or with `sudo`:

```
/opt/cf2016/jre/bin/java -jar /opt/cf2016/cfusion/hf-
updates/hotfix_XXX.jar
```

Replace `hotfix_XXX.jar` with the filename of the hotfix jar you are installing, and follow the prompts. The installer will typically attempt to restart ColdFusion when complete. After installation login to ColdFusion administrator again and verify that the hotfix was installed.

Visit: http://www.adobe.com/support/security/ and read any pertinent ColdFusion Security Bulletins. Confirm that all security patches have been applied.

Some hot fixes or updates may require you to run the ColdFusion Web Server Configuration Tool to *Upgrade* the connector. Carefully review the hotfix release notes to determine if the connector needs to be updated. If you are following this guide on a fresh install the connector will be installed in the next step.

Consult the ColdFusion hotfix installation guide for more info: http://blogs.coldfusion.com/post.cfm/coldfusion-hotfix-installation-guide

5.5 Configure ColdFusion Administrator

Refer to section 3 and configure ColdFusion Administrator settings.

5.6 Specify permissions for ColdFusion Directories

Next we will make `cfuser` the owner and root the group of the installation directory recursively.

```
chown -R cfuser:root /opt/cf2016/
chmod -R 750 /opt/cf2016/
```

You should consider a more restrictive file permission structure which removes any unnecessary write permissions. The permissions specified above will allow ColdFusion to have full control over the files in its own directories as needed by the CF administrator or hotfix installer - a more restrictive approach while more secure may cause errors in ColdFusion administrator or elsewhere. If you do not make changes in the ColdFusion administrator and only run the hotfix installer by root you can setup more restrictive file security.

5.7 Configure Apache

In this section we will setup Apache httpd web server and connect ColdFusion to it.

Install or Update Apache

If Apache (httpd) web server has not yet been installed, install it using yum:

If Apache (httpd) has not yet been installed, install it using yum:

```
# yum install httpd
```

If Apache (httpd) was already installed, ensure that the latest version is installed:

```
# yum update httpd
```

Remove unneeded modules

Ensure that the latest version of `openssl` and `mod_ssl` are installed as well using similar yum commands as above.

Remove any unneeded modules, for example:

```
# yum erase php*
```

Edit the `/etc/httpd/conf/httpd.conf` and remove or comment out (by placing a # at the beginning of the line) any `LoadModule` lines that load unnecessary modules. Most modules will be included in separate configuration files (look in `/etc/httpd/conf.modules.d/`), you can easily find a list of files that load modules by running:

```
# fgrep --recursive LoadModule /etc/httpd/
```

Some modules that you may be able to remove (or comment out by placing a # at the beginning of the line) include: `mod_imap`, `mod_info`, `mod_userdir`, `mod_status`, `mod_cgi`, `mod_autoindex`.

Add apache user to webusers group

The Apache web server runs as user `apache` by default (consider changing this username to a non-default username) on Red Hat Enterprise Linux. Add the `apache` user to the `webusers` group we created in section 3.2:

```
# usermod -a -G webusers apache
```

See the Appendix for more information on securing the Apache Web Server installation.

Setup directories for web roots

Create a directory on the server to house the web root for your websites, in this guide we will use `/www` please choose a unique directory name.

```
# mkdir /www
```

Create a directory for the default web site.

```
# mkdir /www/default
# mkdir /www/default/wwwroot
```

Create an index.html file in the default site:

```
# echo 'Hello' > /www/default/wwwroot/index.html
```

Create a directory for your other websites:

```
# mkdir /www/example.com
# mkdir /www/example.com/wwwroot
```

Specify permissions on web root directories

```
# chown -R cfuser:webusers /www
# chmod -R 550 /www
```

The permission 550 specifies that the owner (`cfuser`) has r-x permission, the group (`webusers`) has r-x permission, and all other users have no permission to this directory. With this setup ColdFusion will not be able to create, edit or delete any files under the web root by default. If your site `example.com` needs to write files to `/www/example.com/uploads/` then you must give the `cfuser` permission to write to that directory, for example:

```
# chmod -R 750 /www/example.com/uploads/
```

```
# chcon -R -t httpd_sys_content_t -u system_u /www
```

Note: When you add new files to the web root be sure that the permissions are correct.

Configure Default Site

Edit `httpd.conf` and change the `DocumentRoot` from `/var/www/html` to your new default site root `/www/default/wwwroot`

Next tell apache that it is ok to serve files to the public from `/www` by adding:

```
<Directory "/www">
```

```
  Options None
  AllowOverride None
  Require all granted
</Directory>
```

Restart apache: `systemctl restart httpd.service`

Test apache installation by visiting http://127.0.0.1/index.html

Create an alias for /cf_scripts/scripts

The `/cf_scripts/scripts` uri is used by ColdFusion to serve static assets such as javascript, css utilized by tags that provide client side functionality. See Appendix B Table B.2 for a listing of tags that require assets in `/cf_scripts`, if your ColdFusion applications do not utilize these features you can move on to *Lock Down URIs*.

Block URIs

To block a URI for all IPs (including 127.0.0.1) you can use the `RedirectMatch` directive to instruct Apache to return a 404 or 403 error page, for example to block `/CFIDE` add the following to the bottom of your `httpd.conf` file:

```
RedirectMatch 404 (?i).*/CFIDE.*
```

You may consider creating a new file `/etc/httpd/conf.d/cf2016-lockdown.conf` and add your global settings there. On RHEL7 this file would be automatically included at the bottom of the httpd.conf file via the directive: `IncludeOptional conf.d/*.conf`

It should be safe to block `/CFIDE` globally for all public websites in ColdFusion (2016 release) without breaking any features. Consult Appendix B - Table B.1 (located at the end of this guide) to review what URIs exist under `/CFIDE` and their purpose.

As of ColdFusion (2016 release), the `/CFIDE` virtual directory is no longer created by the web server connector tools. In addition the /CFIDE/scripts directory has been moved out of /CFIDE and into a new directory called /cf_scripts.

There are several additional URIs that ColdFusion serves outside of /CFIDE by default. See Table 2.3.1 to determine which URIs you may be able to block.

```
RedirectMatch 404 (?i).*/Application\.cf.*
RedirectMatch 404 (?i).*/WEB-INF.*
RedirectMatch 404 (?i).*/cfformgateway.*
RedirectMatch 404 (?i).*/flex2gateway.*
RedirectMatch 404 (?i).*/cfform-internal.*
RedirectMatch 404 (?i).*/flex-internal.*
RedirectMatch 404 (?i).*/cffileservlet.*
RedirectMatch 404 (?i).*/rest/.*
RedirectMatch 404 (?i).*/_api_listing/.*
RedirectMatch 404 (?i).*/flashservices.*
RedirectMatch 404 (?i).*/WSRPProducer.*
RedirectMatch 404 (?i).*/JSDebugServlet.*
RedirectMatch 404 (?i).*/securityanalyzer.*
RedirectMatch 404 (?i).*\.git.*
RedirectMatch 404 (?i).*\.svn.*
```

Review See Appendix B Table B.2 to determine if you can block these URIs:

```
RedirectMatch 404 (?i).*/cf_scripts.*
```

Restart apache and test URIs that should be blocked and your applications.

5.7: Install Apache Connector

As root run the connector installer utility called wsconfig with the following options:

```
/opt/cf2016/cfusion/runtime/bin/wsconfig -ws Apache \
       -dir /etc/httpd/conf/ \
       -bin /usr/sbin/httpd
```

At this point you will find that with SELinux enabled Apache will fail to start because the `mod_jk` (the Tomcat connector module for Apache) module does not have sufficient permissions, the error may look something like this:

> *Starting httpd: httpd: Syntax error on line 1033 of /etc/httpd/conf/httpd.conf: Syntax error on line 2 of /etc/httpd/conf/mod_jk.conf: Cannot load /opt/cf2016/config/wsconfig/1/mod_jk.so into server: /opt/cf2016/config/wsconfig/1/mod_jk.so: failed to map segment from shared object: Permission denied*

If you are not running SELinux you can skip any commands that begin with `chcon` or `setsebool`.

First create an empty log file:

```
touch /opt/cf2016/config/wsconfig/1/mod_jk.log
```

Now let’s grant permission to Apache for the connector directory:

```
chown -R cfuser:apache /opt/cf2016/config/wsconfig/
chmod -R 540 /opt/cf2016/config/wsconfig/
chmod 550 /opt/cf2016/config/wsconfig/1/mod_jk.so
chmod 560 /opt/cf2016/config/wsconfig/1/mod_jk.log
```

Next we need to apply SELinux context to the `mod_jk.so` module, we’ll do this by giving it the file context type `httpd_modules` and user type `system_u`:

```
chcon -t httpd_modules_t -u system_u
/opt/cf2016/config/wsconfig/1/mod_jk.so
```

Next apply the SELinux file type context httpd_log_t to the log file that mod_jk writes to:

```
chcon -t httpd_log_t -u system_u
/opt/cf2016/config/wsconfig/1/mod_jk.log
```

The connector (mod_jk) also writes to a shared memory file called jk_shm (and other files such as jk_shm.pid and jk_shm.pid.lock where pid is the process id) in the directory of the path specified in the JkShmFile directive. Instead of writing multiple files in the connector directory, you can specify a path under /var/cache/httpd/ which should already have SELinux appropriate SELinux file labels.

Look for the JkShmFile directive in /etc/httpd/conf/mod_jk.conf and change it to something like this:

```
JkShmFile "/var/cache/httpd/1_jk_shm"
```

Where 1 corresponds to your wsconfig folder number.

Finally we need to allow Apache to make network connections so mod_jk can talk to ColdFusion. We can allow Apache to connect to any port by running:

```
setsebool httpd_can_network_connect 1
```

A more restrictive and secure approach is to only add the port that the ColdFusion connector is using to facilitate communications between Apache and ColdFusion. This port is listed in the workers.properties file in the /opt/cf2016/config/wsconfig/1/ folder in the worker.cfusion.port property, by default it will be 8016.

Turn off httpd_can_network_connect if enabled:

```
setsebool httpd_can_network_connect 0
```

Next we will use the semanage utility to add port 8016 to the list of ports httpd can connect to. The semanage command is part of setools-console package so you may need to run yum install setools-console to install it.

```
semanage port -a -t http_port_t -p tcp 8016
```

Restart apache and test accessing a cfm file.

If you installed multiple connectors you will need to repeat this for each connector port.

5.9 Configure /cf_scripts alias

Consult See Appendix B Table B.2 to determine if you need to allow access to the /cf_scripts URI. If you do not use any of the tags or features listed you may skip this step.
Now to allow access Apache to serve files in the /cf_scripts folder we need to ensure that apache has execute permissions on all parent folders so that it can traverse the directory structure:

```
chgrp webusers /opt/cf2016/
chgrp webusers /opt/cf2016/cfusion/
chgrp webusers /opt/cf2016/cfusion/wwwroot/
chgrp -R webusers /opt/cf2016/cfusion/wwwroot/cf_scripts/
chmod 710 /opt/cf2016/
chmod 710 /opt/cf2016/cfusion/
chmod 510 /opt/cf2016/cfusion/wwwroot/
chmod 550 /opt/cf2016/cfusion/wwwroot/cf_scripts/
```

Use `chcon` to allow `httpd` to serve the files in the `cf_scripts` folder.

```
chcon -R t httpd_sys_content_t -u system_u
/opt/cf2016/cfusion/wwwroot/cf_scripts
```

Next we can setup a non-default URI, in this guide we will setup an alias `/cf2016scripts` (but you should select a name at random) that corresponds to `/cf_scripts/scripts/`. Add the following to your `httpd.conf` or your `/etc/httpd/conf.d/cf2016-lockdown.conf` file:

```
Alias /cf2016scripts /opt/cf2016/cfusion/wwwroot/cf_scripts/scripts/
```

Restart Apache and browse to `/cf2016scripts/cfform.js` and ensure that a javascript file loads.

If you plan to use the built-in web server for accessing ColdFusion administrator then you must also add an alias by adding a Context tag inside the Host tag of `server.xml` located: `/opt/cf2016/cfusion/runtime/conf/server.xml`

```
<Context path="/"
   docBase="/opt/cf2016/cfusion/wwwroot"
   WorkDir="/opt/cf2016/cfusion/runtime/conf/Catalina/localhost/tmp"

aliases="/cf2016scripts=/opt/cf2016/cfusion/wwwroot/cf_scripts/scripts
" />
```

Finally you must specify the URI alias you selected equivalent to `/cf2016scripts` in the ColdFusion administrator under the *Default ScriptSrc Directory* on the *Server Settings > Settings Page*.

Test your websites.

5.8 Setup ColdFusion Administrator Web Site (Optional)

In ColdFusion (2016 release) the `/CFIDE` uri is blocked by the web server connector by default. You may consider running the built-in web server to access ColdFusion Administrator over a secure SSH tunnel, rather than allowing access through Apache.

If you wish to use the built-in web server to access the ColdFusion Administrator you can skip this section.

Because /CFIDE is blocked at the connector level by default, it is recommended that you run wsconfig again to create a dedicated connector to the ColdFusion Administrator virtual host. You will then have to remove the following from the uriworkermap.properties file:

```
!/CFIDE/* = cfusion
```

In addition if you blocked the URI /CFIDE using RedirectMatch in your httpd conf you will need to wrap it with an <If> block, to exclude the Admin Website, see: https://httpd.apache.org/docs/2.4/mod/core.html#if (requires Apache 2.4+).

After unblocking /CFIDE you will want to block all /CFIDE URIs except /CFIDE/administrator see Appendix B Table B.1 in the <Else> block. Here is an example If block using the REMOTE_ADDR IP address:

```
<If "-R '127.0.0.1/32'">
    # block /CFIDE if not localhost
    RedirectMatch 404 (?i).*/CFIDE.*
</If>
<Else>
    # allow only /CFIDE/administrator block all other URIs
    RedirectMatch 404 (?i!).*/CFIDE/adminapi.*
    #etc...
</Else>
```

Now we can create an Apache virtual host which will be used exclusively for accessing the ColdFusion administrator. An alternate approach is to access the ColdFusion administrator from the built-in web server instead.

To use SSL on apache make sure you have mod_ssl installed by running:

```
yum install mod_ssl
```

Next add the following to the bottom of your httpd.conf file:

```
NameVirtualHost 127.0.0.1:443
<VirtualHost 127.0.0.1:443>
    ServerName localhost
    DocumentRoot /www/administrator/wwwroot/
    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/localhost.crt
    SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
    ErrorLog logs/cfadmin.ssl.error.log
    CustomLog logs/cfadmin.ssl.access.log common
</VirtualHost>

# See https://mozilla.github.io/server-side-tls/ssl-config-generator/
# to generate a modern configuration
SSLProtocol all -SSLv2 -SSLv3
SSLCipherSuite (seek current recommendation)
SSLHonorCipherOrder on
```

Please note that the best practices for configuring TLS/SSL is frequently changing. Do not rely on the TLS configuration supplied above please refer to current sources, such as https://mozilla.github.io/server-side-tls/ssl-config-generator/

The above creates a virtual host allowing you to access the ColdFusion administrator at https://localhost/CFIDE/administrator/

In our example we use the self signed certificate generated during openssl installation, it is recommended that you use a certificate signed by a trusted certificate authority instead.

Next let's tell apache that SSL is required for the URI `/CFIDE/administrator`:

```
<LocationMatch "(?i).*/CFIDE/administrator">
    SSLRequireSSL
</LocationMatch>
```

Next let's require authentication for the `/CFIDE/administrator` URI, this will allow you to audit which administrators have made changes to the administrator settings. In this example we use Digest authentication, which requires a modern web browser (IE 6 and below may not work correctly) and `mod_auth_digest` installed on the server side. First we need to create a password file:

```
# /usr/bin/htdigest -c /etc/httpd/cfadmin.digest.pwd cfadmins
petefreitag
```

The above command will create or overwrite password file in the specified location, and create a user named `petefreitag` in group `cfadmins.` To add more users omit the `-c` flag.

Next let's specify permissions such that only root can write to this file, and apache can only read it:

```
# chown root:apache /etc/httpd/cfadmin.digest.pwd
# chmod 640 /etc/httpd/cfadmin.digest.pwd
```

Now add the following to the `httpd.conf` file:

```
<LocationMatch "(?i).*/CFIDE/administrator">
    AuthType Digest
    AuthName "cfadmins"
    AuthDigestProvider file
    AuthUserFile /etc/httpd/cfadmin.digest.pwd
    Require valid-user
</LocationMatch>
```

Restart Apache and visit https://localhost/CFIDE/administrator/ and ensure that you are prompted with a password, and that SSL is required. Also confirm that access is limited only to the IP addresses you allow.

5.9 Update Java Virtual Machine

The Java Virtual Machine included with the ColdFusion installer may not contain the latest java security hotfixes. You must periodically check with Oracle for JVM security hotfixes.

Download the RPM for the latest supported JRE from java.oracle.com. Install the rpm:

```
rpm -ivh jre-8uXX-linux-x64.rpm
```

After you run the binary the JVM is installed in `/usr/java/` a symbolic link is created pointing to the latest installed version `/usr/java/latest/` you point ColdFusion to this path to simplify future JVM updates.

Verify that the version of Java in `/usr/java/latest/` is a version supported for ColdFusion 11. At the time of this writing Java 1.7 is the latest supported major version of Java. See this page for current information about JVM version support: http://helpx.adobe.com/coldfusion/kb/upgrading-java-coldfusion.html

```
# /usr/java/latest/bin/java -version
```

Locate the `jvm.config` file, (by default it is located in `/opt/coldfusion2016/cfusion/bin/`) and make a backup:

```
# cp jvm.config jvm.config.backup
```

To update using ColdFusion Administrator: click on *Server Settings* > *Java and JVM* and then add `/usr/java/latest/` to the *Java Virtual Machine Path* text box.

To update via shell: Edit `jvm.config` in a text editor to locate the line beginning with `java.home=` for example:

```
java.home=/opt/cf2016/jre
```

Change that line to:

```
java.home=/usr/java/latest
```

Restart ColdFusion for the new JVM to take effect. Visit the System Information page of ColdFusion administrator to confirm that the JVM has been updated. To revert to the default jvm replace `jvm.config` with `jvm.config.backup` and restart ColdFusion again.

5.10 Setup Auditing

First ensure that `auditd` is installed and configured to meet your requirements in `/etc/audit/auditd.conf`

Use `auditctl` to add auditing to file system operations, for example:

```
auditctl -w /opt/cf2016 -p wax -k cf2016
```

The above will audit all write, attribute change and execute operations on the path `/opt/cf2016/` and tag all entries with the filter key `cf2016`. Now that the filter key is setup you can query the audit log using `ausearch -k cf2016`

Keep in mind that the above might get a bit noisy if ColdFusion is writing a lot of log files, placing the log files elsewhere will reduce this noise.

5.11 Add umask to startup script

Edit the `/etc/init.d/coldfusion_2016` startup script and add the line near the top but below the `#description` comment:

```
umask 007
```

Consider setting a more restrictive umask on the group permission.

5.12 Making chcon labels permanent

Changes made with chcon do not survive a file system relabel, you can use the `semanage fcontext` command is used to make permanent record of the file context labels. For example to set labels for the `/www` directory:

```
semanage fcontext -a -t httpd_sys_content_t -u system_u "/www(/.*)?"
```

It does not actually change the files in the filesystem however. To do that run restorecon to apply the labels to the files.

```
restorecon -R -v /web
```

Repeat for each file you applied chcon to in this section.

5.12 Additional Lockdown Measures

Please read section 4 *Additional Lockdown Measures* and perform any applicable measures.

Section 6: Locking down the API Manager

The API Manager consists of 3 services. The API Manager Analytics Service provides statistics and reporting. The API Manager Service provides a front end proxy to your APIs as well as management interfaces. The API Datastore Service provides a database service that the other two services depend on.

6.1 Install API Manager

Run the API Manager Installer, you can find the exe in the root of your {cf.home} directory.

Select No, when asked to Coexist with an existing ColdFusion installation.

Consider changing ports to non-default values.

Use a dedicated partition / drive for the API manager application server files.

For maximum isolation you can install the API Manager, Data Store and Analytics Server services on separate servers. If you are installing everything on a single server check the *Data Store* and *Analytics Server* checkboxes to install these services locally.

6.2 Connecting API Manager to IIS

Follow sections 2.2 to ensure that the required IIS role services are installed on the server. Create an empty directory for a new site in IIS, for example d:\sites\api.example.com\wwwroot\

Create empty subfolders called `portal`, `amp`, `analytics` and `admin`.

Table 6.2.1- API Manager URIs

URI	Purpose	Restrict
/portal	Allows publishers to create and configure API settings. Allows subscribers to subscribe to an API.	Restrict access to API admins, publishers and subscribers using the APIs. Depending on your use case you may want to grant public access to /portal

URI	Purpose	Restrict
/analytics	Allows publishers, subscribers and admins to see stats related to the API use.	Restrict to admins, publishers and subscribers
/admin	API Manager administrator interface.	Block public access.
/amp	Internal API for API Manager. Used by `/portal` `/analytics`	Restrict equivalent to `/portal` and `/analytics`.
/amp/admin	Internal API for API Manager Admin	Block public access.

Consult table 6.2.1 to block or restrict access to the URIs using request filtering, IP restrictions, or web server authentication.

6.3 Run API Manager as Dedicated User

Create a unique user for each service (for example: `apimanager`, `apidatastore`, `apianalytics`) with minimal permission. Next create a user group containing each service user, in this guide we will call the group `apimanagers`, but you should use unique usernames and group names.

Stop all API Manager Services.

Grant readonly permission to the `apimanagers` group for the entire ApiManager installation root directory `{api.root}` (for example `x:\ApiManager\ or /opt/ApiManager/`).

Next grant read and write (Full Control) permission to the `apidatastore` user for the `{api.root}/database/datastore/` directory.

Start the API Data Store Service.

Grant read and write (Full Control) permission to the `apianalytics` user for the following directories:

```
{api.root}/database/analytics/data/
{api.root}/database/analytics/logs/
```

Start the API Analytics Service

Grant read and write (Full Control) permission to the `apimanager` user for the following directories:

```
{api.root}/conf
{api.root}/logs
```

Start the API manager services and test.

On Linux you will need to create a startup script to run each of the services as their dedicated users for example:

```
su apidatastore -C "/opt/ApiManager/database/datastore/redis-server
/opt/ApiManager/database/datastore/redis.conf.properties"
su apianalytics -C
"/opt/apimanager/database/analytics/bin/elasticsearch"
su apimanager -C "/opt/ApiManager/bin/start.sh"
```

6.4 Additional Lockdown of API Manager

Consult the security documentation for Redis, ElasticSearch and Kibana to further lockdown the API Manager services.

http://redis.io/topics/security
https://www.elastic.co/blog/found-elasticsearch-security
https://www.elastic.co/guide/en/kibana/current/production.html

Section 7: Patch Management Procedures

Staying up to date with patches is essential to maintaining security on the server. The system administrator should monitor the vendor's security pages for all software in use. Most vendors have a security mailing list that will notify you by email when vulnerabilities are discovered.

Signup for the Adobe Security Notification Service:
http://www.adobe.com/cfusion/entitlement/index.cfm?e=szalert

Check the following websites frequently:

Adobe ColdFusion Security Bulletins:
https://helpx.adobe.com/security/products/coldfusion.html

Microsoft Security Tech Center: http://technet.microsoft.com/en-us/security/default.aspx

Red Hat Security: http://www.redhat.com/security/updates/

Listing of security vulnerabilities in Apache web server:
http://httpd.apache.org/security_report.html

Listing of security vulnerabilities in Tomcat: http://tomcat.apache.org/security-8.html

To keep updated with ColdFusion (2016 release) updates you can use the server update feature in ColdFusion administrator. Consider setting up an instance to email you when new updates are released.

You should also consider following http://blogs.coldfusion.com/ which is published by the ColdFusion engineering team.

Finally third a third party commercial service http://hackmycf.com will let you know when relevant ColdFusion, Java, Tomcat, etc security patches are released. It will also scan your server on a periodic basis and send you a report.

Appendix A: Sources of Information

A.1 - Microsoft Security Compliance Management Toolkit: http://www.microsoft.com/downloads/details.aspx?FamilyID=5534bee1-3cad-4bf0-b92b-a8e545573a3e

A.2 - NSA Operating System Security Guides: http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

A.3 - NSA Guide to Secure Configuration of Red Hat Enterprise Linux 5: http://www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf

A.4 - ColdFusion and SELinux: http://www.talkingtree.com/blog/index.cfm?mode=entry&entry=28ED0616-50DA-0559-A0DD2E158FF884F3

A.5 - ColdFusion MX with SELinux Enforcing: http://www.ghidinelli.com/2007/12/06/coldfusion-mx-with-selinux-enforcing

A.6 - Tips for Securing Apache: http://www.petefreitag.com/item/505.cfm

A.7 - Apache Security by Ivan Ristic, 2005 O'Reilly ISBN: 0-596-00724-8

A.8 - Tips for Secure File Uploads with ColdFusion: http://www.petefreitag.com/item/701.cfm

A.9 - HackMyCF.com Remote ColdFusion vulnerability scanner: http://hackmycf.com/

A.10 - Fixing Apache (13) Permission Denied 403 Forbidden Errors: http://www.petefreitag.com/item/793.cfm

A.11 - Apache Tomcat 8 Security Considerations: http://tomcat.apache.org/tomcat-8.0-doc/security-howto.html

A.12 - Getting started with AppCmd.exe: http://www.iis.net/learn/get-started/getting-started-with-iis/getting-started-with-appcmdexe

A.13 - Thanks to Charlie Arehart for providing several suggestions and feedback.

A.14 - Professional Microsoft IIS 8 by Schaefer, Kenneth; Cochran, Jeff; Forsyth, Scott; Glendenning, Dennis; Perkins, Benjamin. Wiley. ISBN: 978-1-118-38804-4

Appendix B: Reference Tables

Table B.1: CFIDE URIs

URI	Purpose	Safe to Block
/CFIDE/administrator	ColdFusion Administrator	Yes, you can use the built-in web server or create a dedicated web site for ColdFusion administrator access.
/CFIDE/adminapi	Admin API	Yes, if the admin api is called from internal CFML code it will still work when the URI is blocked. If the admin api is accessed through a remote cfc function call then use another method to protect this uri (eg IP restriction). Do not leave this URI open to the public.
/CFIDE/AIR	AIR Sync API	Usually, unless AIR sync API is used. AIR Integration has been deprecated as of ColdFusion 11
/CFIDE/appdeployment		Yes
/CFIDE/componentutils	CFC Documentation viewer	Yes
/CFIDE/debug	Used when debugging is enabled on the server.	Yes
/CFIDE/multiservermonitor-access-policy.xml	Used to set a policy for allowing viewing the server monitor from multiple domains.	Yes - the server monitor now runs on its own web server on port 5500.
/CFIDE/orm	Contains interfaces used with ORM. These interfaces do not need to be accessible through the web server.	Yes

URI	Purpose	Safe to Block
/CFIDE/portlets	Contains API for building portlets with JSR-286, JSR-168 or WSRP. The API does not need to be accessible through the web server.	Yes
/CFIDE/probe.cfm	You can configure probes in the ColdFusion administrator which are used to monitor a URL for failures. This will throw an exception if not run over 127.0.0.1.	Yes, however if you want to use probes you should create a web site that only listens on 127.0.0.1 and allow this URI.
/CFIDE/scheduler	Contains an interface for scheduled task event handlers. Does not need to be accessible through the web server.	Yes
/CFIDE/ServerManager	Contains the AIR application binary for the Server Manager.	Yes
/CFIDE/services	Contains CFCs that can act as a service layer to Flex, or other client side applications. The client application must have a username / password and also an allowed IP. Enabling this feature can open up a large amount of security risk to the application server.	Yes. This feature has been deprecated as of CF11.
/CFIDE/websocket	API for web socket listener CFCs. Does not need to be open via the web server if used.	Yes
/CFIDE/wizards	Possibly used for IDE integration, not needed on production.	Yes

URI	Purpose	Safe to Block
/CFIDE/main/ide.cfm	Used for RDS. Note this exists as a mapping in web.xml no actual folder exists.	Yes

Table B.2: Tags that use /cf_scripts/ assets

Note that the URI `/cf_scripts/scripts/` can be changed to a unique URI by changing the Default Script Src setting in the ColdFusion administrator. See sections 2.23 (windows), 3.1 (administrator) and 5 (linux).

Tag	URI Pattern	Notes
cfajaxproxy	/cf_scripts/scripts/ajax/	
cfajaximport	/cf_scripts/scripts/	This tags lets you override the Default Script Src setting in ColdFusion Administrator.
cfautosuggest	/cf_scripts/scripts/ajax/	
cfcalendar	/cf_scripts/scripts/ajax/	
cfchart	/cf_scripts/scripts/ajax/ /cf_scripts/scripts/chart/	
cfclient	/cf_scripts/cfclient/	
cfdiv	/cf_scripts/scripts/ajax/	
cffileupload	/cf_scripts/scripts/ajax/	
cfform	/cf_scripts/scripts/cfform.js /cf_scripts/scripts/masks.js	
cfform (format=flash)	/cf_scripts/scripts/	Deprecated since CF11
cfform (format=xml)	/cf_scripts/scripts/	Deprecated since CF11
cfgrid (html)	/cf_scripts/scripts/ajax/	

Tag	URI Pattern	Notes
cfgrid (format=applet)	/cf_scripts/classes/	Deprecated since CF11
cfinput (autosuggest, datefield)	/cf_scripts/scripts/ajax/	
cflayout	/cf_scripts/scripts/ajax/	
cfmap	/cf_scripts/scripts/ajax/	
cfmediaplayer	/cf_scripts/scripts/ajax/	
cfmenu	/cf_scripts/scripts/ajax/	
cfmessagebox	/cf_scripts/scripts/ajax/	
cfpod	/cf_scripts/scripts/ajax/	
cfprogressbar	/cf_scripts/scripts/ajax/	
cfslider	/cf_scripts/scripts/ajax/	
cfsprydataset	/cf_scripts/scripts/ajax/	Deprecated since CF11
cftextarea (richtext=true)	/cf_scripts/scripts/ajax/ /cf_scripts/scripts/ajax/FCKeditor/	Consider blocking the FCKeditor subfolder if you do not use this tag because it has cfm files.
cftooltip	/cf_scripts/scripts/ajax/	
cftree (html)	/cf_scripts/scripts/ajax/	
cftree (format=applet)	/cf_scripts/classes/	Deprecated since CF11
cfwebsocket	/cf_scripts/scripts/ajax/	
cfwindow	/cf_scripts/scripts/ajax/	

Appendix C: Revision History

Revision 1 - 2016-02-02

- Initial Release