



Adobe ColdFusion 2018 Lockdown Guide

Written by Pete Freitag, Foundeo Inc.

© 2018 Adobe Systems Incorporated and its Licensors. All Rights Reserved.

Adobe ColdFusion (2018 release) Lockdown Guide

If this guide is distributed with software that includes an end user agreement, this guide, as well as the software described in it, is furnished under license and may be used or copied only in accordance with the terms of such license. Except as permitted by any such license, no part of this guide may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, recording, or otherwise, without the prior written permission of Adobe Systems Incorporated. Please note that the content in this guide is protected under copyright law even if it is not distributed with software that includes an end user license agreement.

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, the Adobe logo, Adobe Content Server, Adobe Digital Editions, and Adobe PDF are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft, Windows and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Macintosh and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries. All other trademarks are the property of their respective owners.

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

- 1 Introduction
 - 1.1 Default File Paths and Usernames
 - 1.2 Operating Systems and Web Servers
 - 1.3 ColdFusion Version
 - 1.4 Scope of Document
 - 1.5 Applying to Existing Installations
 - 1.6 Naming Conventions
- 2 ColdFusion On Windows
 - 2.1 Installation Prerequisites
 - 2.2 Install & Configure IIS
 - 2.3 Run the Windows ColdFusion Installer
 - 2.4 Install ColdFusion Hotfixes
 - 2.5 Setup Websites in IIS
 - 2.6 Run the ColdFusion 2018 Server Auto Lockdown Tool
 - 2.7 Update JVM
- 3 ColdFusion Administrator Settings
 - 3.1 Server Settings > Settings
 - 3.2 Server Settings > Request Tuning
 - 3.3 Server Settings > Caching
 - 3.4 Server Settings > Client Variables
 - 3.5 Server Settings > Memory Variables
 - 3.6 Server Settings > Mappings
 - 3.7 Server Settings > Mail
 - 3.8 Server Settings > WebSocket
 - 3.9 Server Settings > Charting
 - 3.10 Data & Services > Data Sources
 - 3.11 Data & Services > ColdFusion Collections
 - 3.12 Data & Services > Solr
 - 3.13 Data & Services > Flex Integration
 - 3.14 Data & Services > PDF Service
 - 3.15 Debugging & Logging > Debug Output Settings
 - 3.16 Debugging & Logging > Developer Profile
 - 3.17 Debugging & Logging > Debugger Settings
 - 3.18 Debugging & Logging > Logging Settings
 - 3.19 Debugging & Logging > Remote Inspection Settings
 - 3.20 Event Gateways > Settings
 - 3.21 Event Gateways > Gateway Instance
 - 3.22 Security > Administrator
 - 3.23 Security > RDS
 - 3.24 Security > Sandbox Security
 - 3.25 Security > User Manager
 - 3.26 Security > Allowed IP Addresses
 - 3.27 Security > Secure Profile
 - 3.28 Server Update > Updates : Settings
- 4 Additional Lockdown Measures
 - 4.1 To Configure the Builtin Web Server to bind to 127.0.0.1 only
 - 4.2 To Run the Builtin Web Server over TLS
 - 4.3 To Disable the Builtin Web Server
 - 4.4 Deny ColdFusion Write Permission to Builtin Web Server wwwroot
 - 4.5 Restrict ColdFusion File System Permissions
 - 4.6 Lockdown the ColdFusion Add-on Services
 - 4.7 Lockdown File Extensions
 - 4.8 Additional URIs to Consider Blocking
 - 4.9 Optionally Remove ASP.NET
 - 4.10 Remove ASP.NET ISAPI Filters and Handler Mappings
 - 4.11 Disable Unused Servlet Mappings
 - 4.12 Additional Tomcat Security Considerations
 - 4.13 Additional File Security Considerations
 - 4.14 Adding ClickJacking Protection
 - 4.15 Restricting HTTP Verbs
 - 4.16 Security Constraints in web.xml
 - 4.17 Limit Request Size

- 4.18 Distributed Mode or Reverse Proxy
- 4.19 HTTP Response Headers to improve Security
- 5 ColdFusion Lockdown on Linux
 - 5.1 Linux Installation Prerequisites
 - 5.2 Create a Dedicated User Account for ColdFusion
 - 5.3 ColdFusion Installation
 - 5.4 Access ColdFusion Administrator via a SSH Tunnel
 - 5.5 Install ColdFusion Hotfixes
 - 5.6 Install and Configure Apache Web Server
 - 5.7 Run the Linux ColdFusion Auto Lockdown Tool
 - 5.8 Update JVM
 - 5.9 Setup Auditing
 - 5.10 Change umask
 - 5.11 Additional Lockdown Steps
- 6 Performance Monitoring Toolset Security Considerations
 - 6.1 Installing the PMT
 - 6.2 ColdFusion Server Auto Discovery
 - 6.3 PMT Datastore
 - 6.4 Run PMT and PMT Datastore as Dedicated User
 - 6.5 Update PMT JVM
- 7 API Manager Security Considerations
 - 7.1 Install API Manager
 - 7.2 Connect API Manager to IIS
 - 7.3 Run API Manager as a Dedicated User
- 8 Patch Management Procedures
- 9 Sources of Information
- 10 Reference Tables
 - 10.1 Tags that use /cf_scripts/ assets
- 11 Troubleshooting
 - 11.1 ColdFusion cannot write files under the web root
 - 11.2 Requesting a cfm results in a 404 after Lockdown tool
 - 11.3 IIS does not have permission to read web.config file
 - 11.4 WebSockets are not working after running lockdown tool
 - 11.5 Help Installing ColdFusion Hotfixes
- 12 Revision History

1 Introduction

The *ColdFusion 2018 Lockdown Guide* is written to help server administrators secure their ColdFusion 2018 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 2016 / IIS 9, and RedHat 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 2018 Enterprise Edition.

1.4 Scope of Document

This document does not detail security settings for the Operating System, the Web Server, Databases, 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/`

2 ColdFusion On Windows

This section covers the installation and configuration of ColdFusion 2018 on a Windows 2016 server. If you are running Linux please start at the section 5 [ColdFusion Lockdown on Linux](#).

In this section we will perform the following:

- Installation Prerequisites
- Install & Configure IIS
- Install ColdFusion
- Run the ColdFusion Auto Lockdown Tool
- Update the JVM

2.1 Installation Prerequisites

Before you begin the installation process please review the following:

- 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 could 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 or SHA checksum listed on adobe.com download page matches the file you downloaded. In PowerShell you can run `Get-FileHash installer-file-name.exe -Algorithm md5` to obtain the checksum.

2.2 Install & Configure IIS

IMPORTANT: Before configuring IIS ensure that public traffic is blocked by your network or OS firewall. You should only enable public traffic after completing all the steps in the lockdown guide.

2.2.1 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)**.

A minimal set of IIS Role Services may include the following:

- 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 4.6 (or latest version)
- Application Development: ASP.NET 4.6 (or latest version)
- Application Development: CGI
- Application Development: ISAPI Extensions
- Application Development: ISAPI Filters
- Management Tools: IIS Management Console

If the server application uses WebSockets also install:

- Application Development: WebSocket Protocol

If you wish to add web server level authentication to any sites you should also install one of the Authentication modules such as:

- 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.

2.2.2 Add WebSites to IIS

At a minimum **create a web root directory for each website** on the server file system. To increase isolation between websites you may consider placing each site on a unique drive letter.

Next **copy the website source code into each web root directory**.

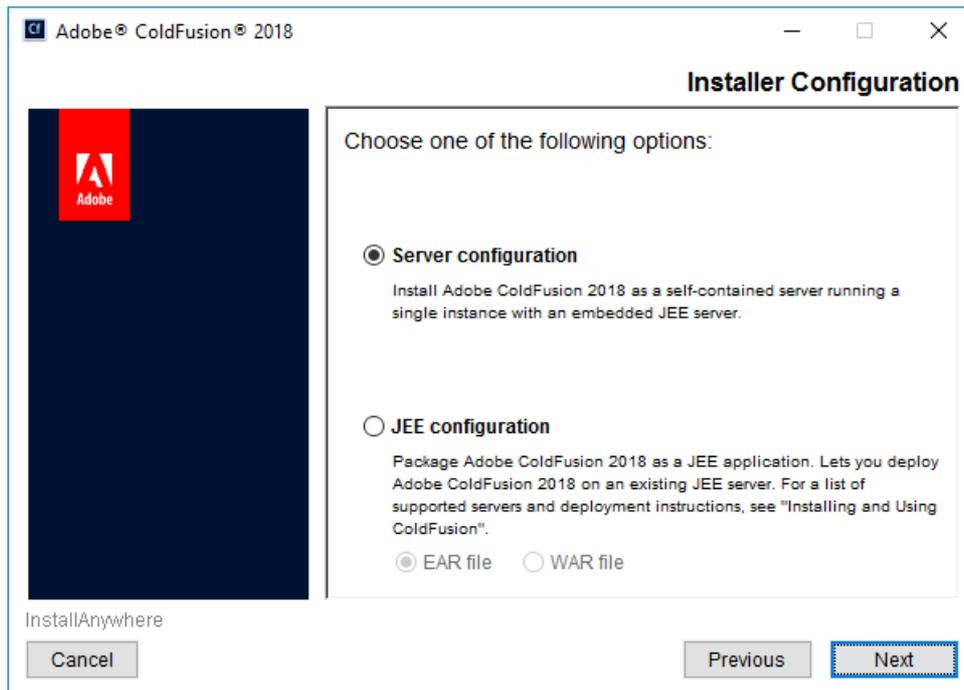
In IIS add your web site.

Test your IIS configuration by requesting a static file such as a txt or js file.

2.3 Run the Windows ColdFusion Installer

2.3.1 ColdFusion Installer: Installer Configuration

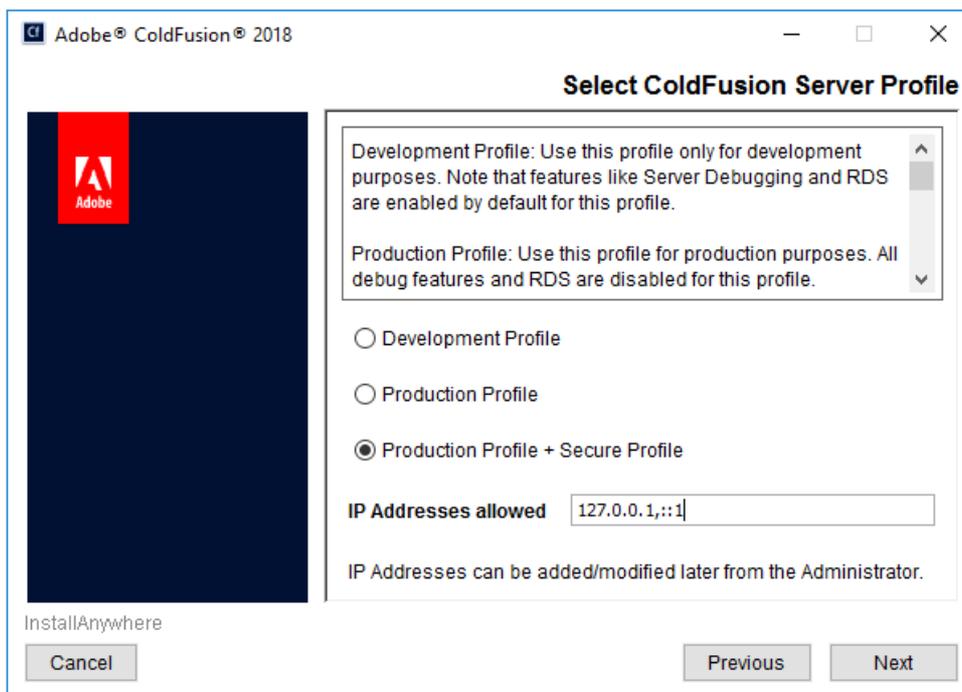
On the Installer Configuration view select **Server configuration** unless you are deploying to an external JEE server (such as JBoss, Weblogic or Websphere).



alt text

2.3.2 ColdFusion Installer: Server Profile

Next select **Production Profile + Secure Profile** and enter a comma separated list of IP addresses that are allowed to access the ColdFusion Administrator.



alt text

Tip: if you want to allow **localhost** access to the ColdFusion Administrator, enter both the IPv4 **127.0.0.1** and IPv6 **::1** version of **localhost**. Some browsers may use IPv6 by default for **localhost**.

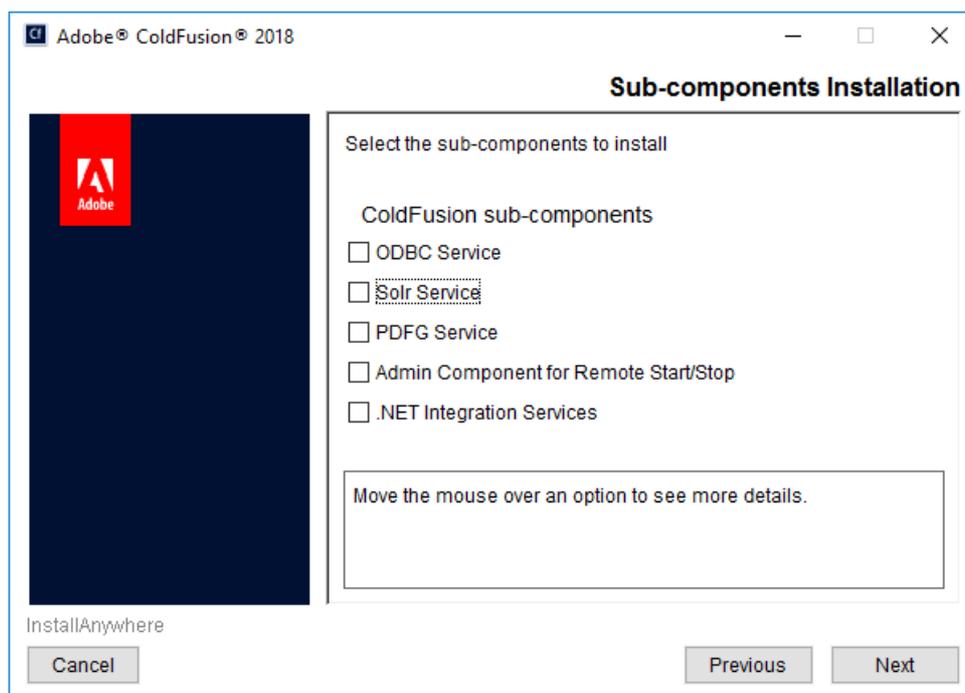
The Secure Profile option provides a more secure foundation of default settings. You can review the settings it toggles here: <https://helpx.adobe.com/coldfusion/configuring-administering/administering-coldfusion-security.html>

Some of the settings that the Secure Profile toggles could 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.

2.3.3 ColdFusion Installer: Sub-components Installation

Only select Sub-components that your server applications require.



alt text

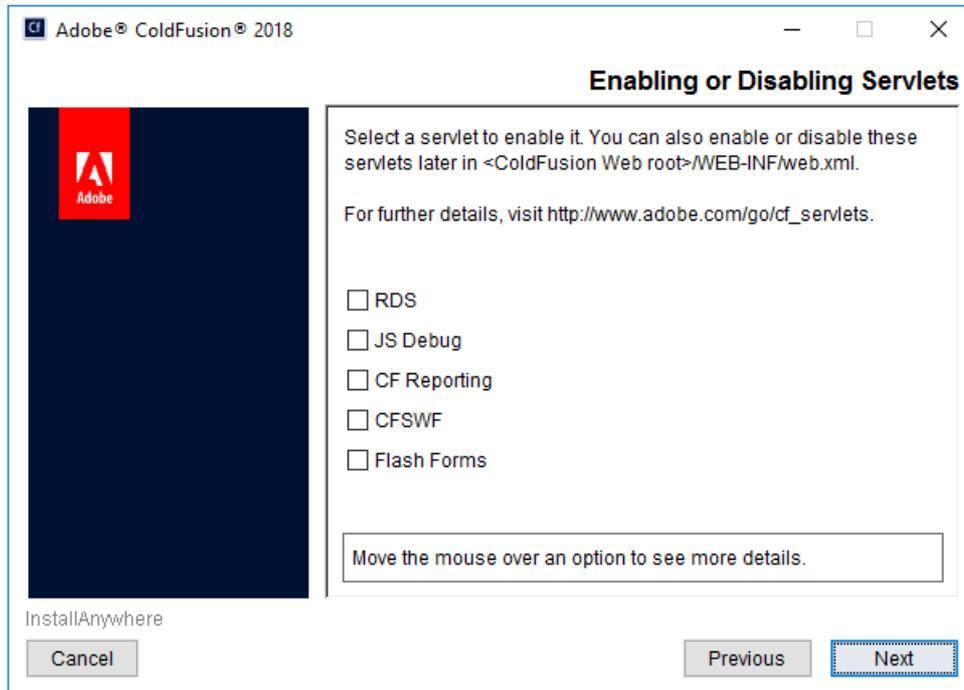
- **ODBC Service** - Required when connecting to Access Databases, not required for SQL Server.
- **Solr Service** - Full text search engine used by `cfindex`, `cfsearch` and `cfcollection` tags.
- **PDFG Service** - Webkit based PDF Rendering engine used by the `cfhtmltopdf` tag. You can still use `cfdocument` and `cfpdf` without installing this service.
- **Admin Component for Remote Start/Stop** - Allows ColdFusion Builder or Server Manager AIR app to start or stop ColdFusion.

Not recommended for production servers.

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

2.3.4 ColdFusion Installer: Enabling or Disabling Servlets

Check any servlets that are required by your application. Most ColdFusion applications do not require any of these servlets to be enabled.



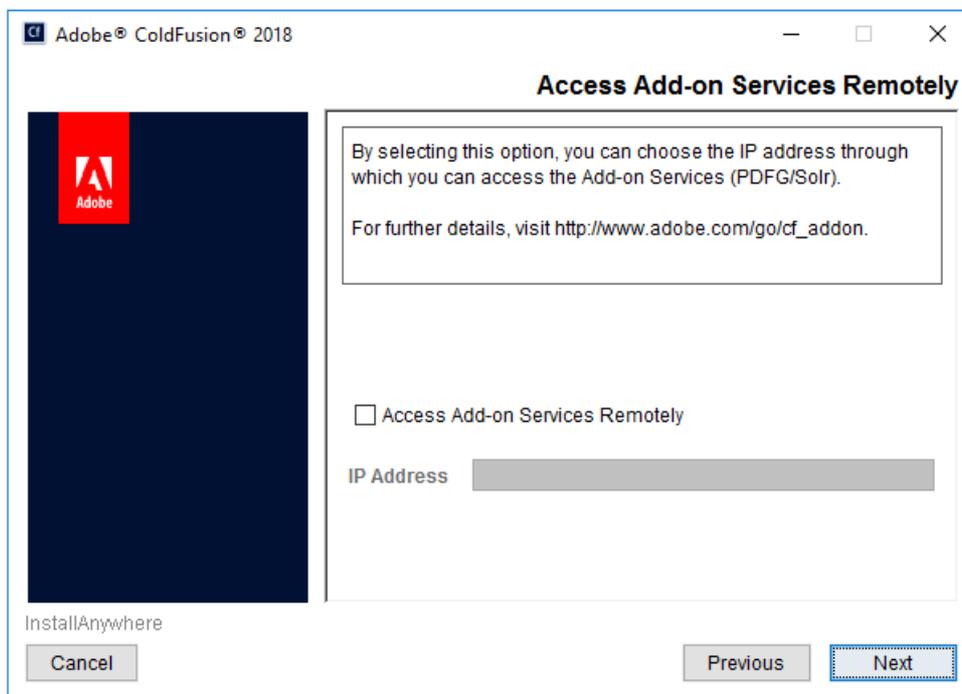
alt text

- **RDS** - Used for development, allows remote access to the file system and databases. This should not be enabled on a production server.
- **JS Debug** - Used for debugging, should not be enabled on a production server.
- **CF Reporting** - Only required if the `cfreport` tag is used.
- **CFSWF** - Used by flash forms `<cfform format="flash">` to generate Flash swf files dynamically.
- **Flash Forms** - Used by flash forms `<cfform format="flash">`

2.3.5 ColdFusion Installer: Access Add-on Services Remotely

If you selected the PDFG (`cfhtmltopdf` tag) or Solr (`cfsearch`, `cfindex`, `cfcollection` tags) sub-components the *ColdFusion 2018 Add-on Services* windows service will be installed.

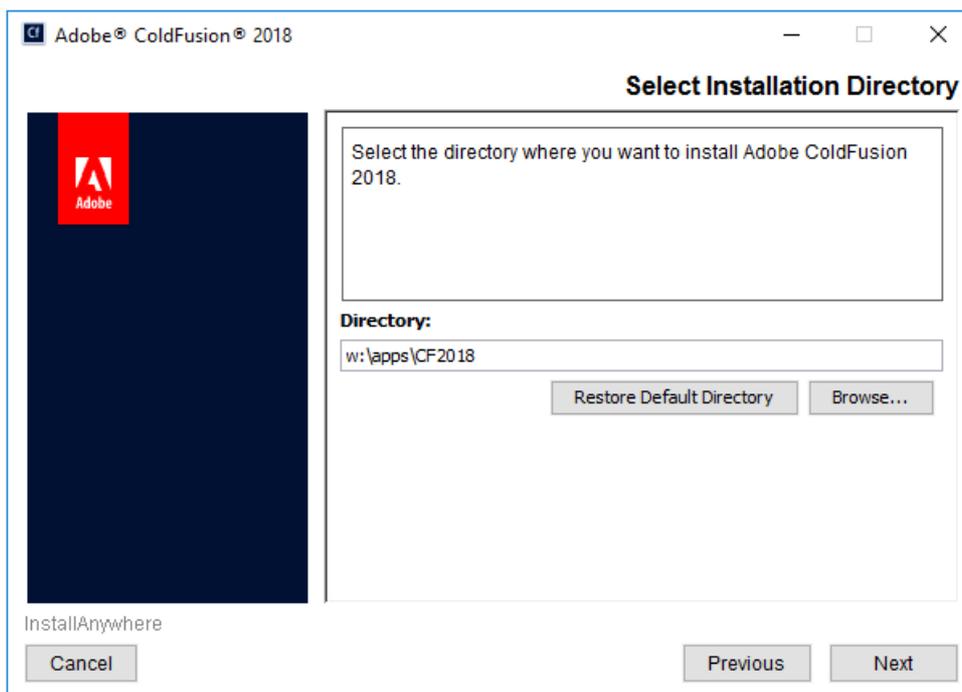
When the *Access Add-on Services Remotely* checkbox is unchecked, the Add-on Services are only accessible from the local machine, `localhost`. If you want to allow access to the services from multiple ColdFusion servers (other than `localhost`), check the checkbox and specify the IP addresses of the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



alt text

2.3.6 ColdFusion Installer: Select Installation Directory

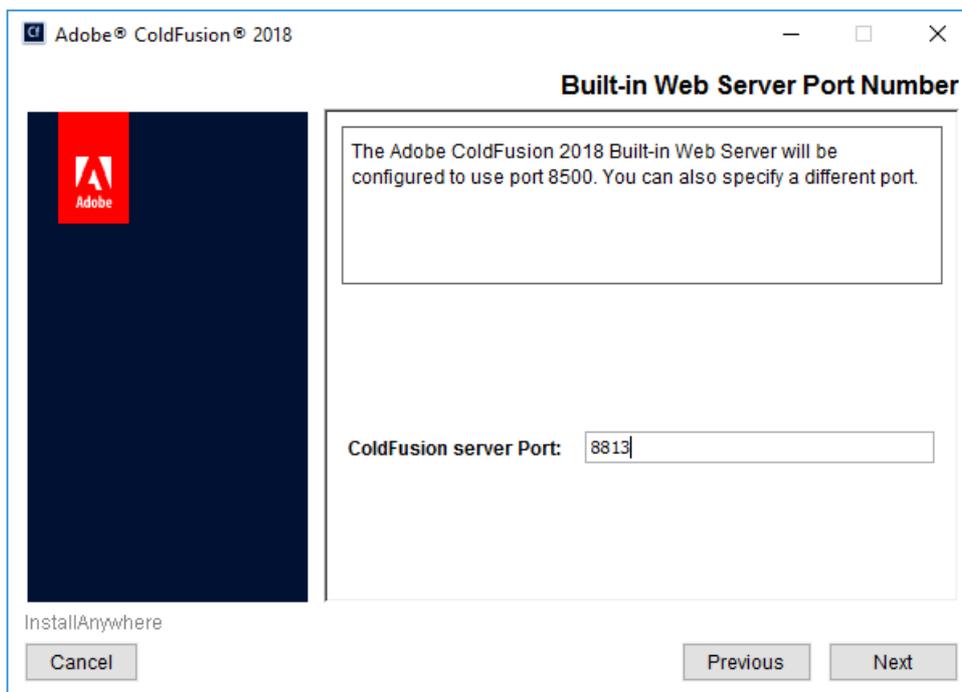
Specify a file system path for the ColdFusion Installation root `{cf.root}` - consider avoiding the default `C:\ColdFusion2018\` path.



Windows ColdFusion Installer: Select Installation Directory

2.3.7 ColdFusion Installer: Built-in Web Server Port Number

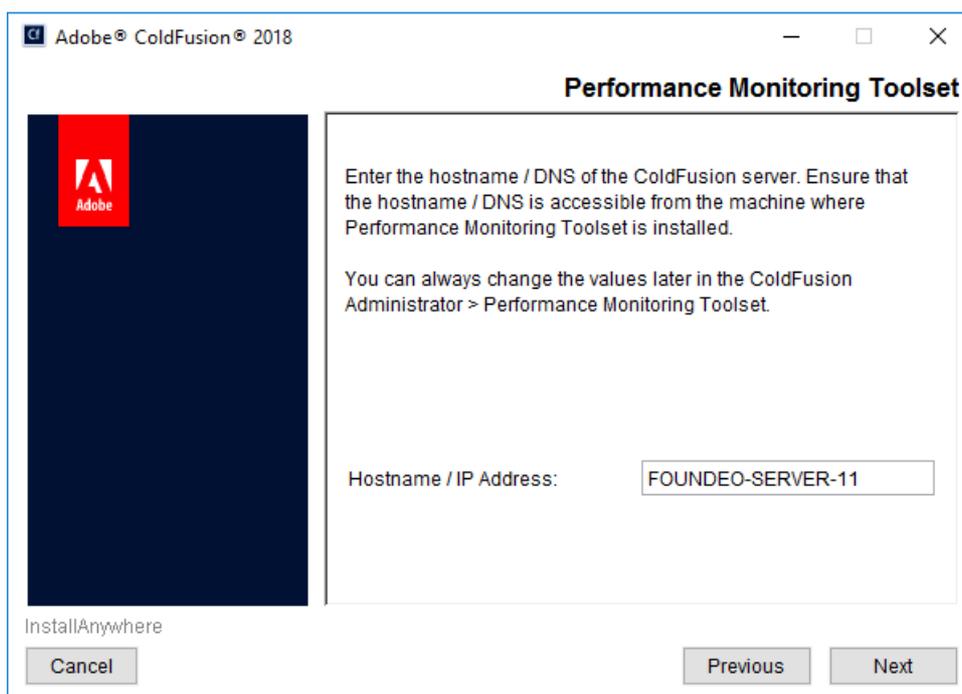
Select a non default port number. Ensure that the port number is blocked by your network/os firewall.



Windows ColdFusion Installer: Built-in Web Server Port Number

2.3.8 ColdFusion Installer: Performance Monitoring Toolset

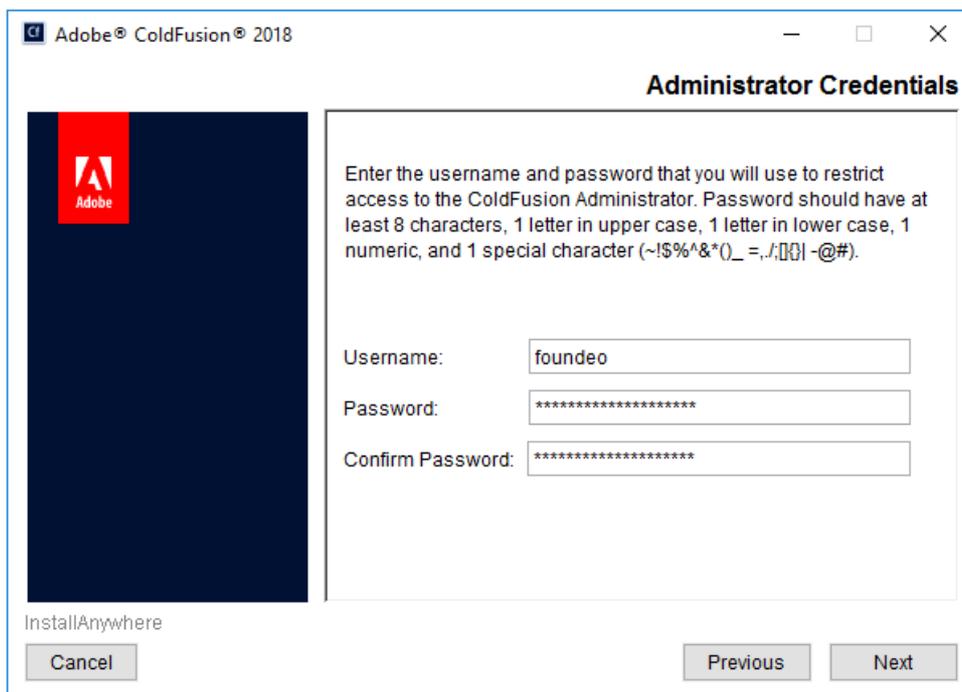
Enter the hostname or internal IP address of the server for use with the performance monitoring toolset. This value can be changed later.



Windows ColdFusion Installer: Performance Monitoring Toolset

2.3.9 ColdFusion Installer: Administrator Credentials

Enter a username other than *admin* and select a strong password.



Windows ColdFusion Installer: Administrator Credentials

2.4 Install ColdFusion Hotfixes

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**.

Tip: Hotfixes are typically cumulative, so if there are multiple hotfixes, you typically only need to install the latest one. Security hotfixes may have additional steps such as updating the JVM or updating connectors - be sure to read each Security Bulletin for details.

Run the hotfix installer from an elevated (Run as Administrator) Command Prompt or PowerShell terminal (replace `hotfix_XXX.jar` with the actual hotfix file name):

Tip: You can verify the integrity of the downloaded hotfix by running `Get-FileHash hotfix_XXX.jar -Algorithm md5` (in PowerShell), see that the checksum matches the value found in Adobe ColdFusion update feed: <https://www.adobe.com/go/coldfusion-updates>

```
x:\cf2018\jre\bin\java -jar x:\cf2018\cfusion\hf-updates\hotfix_XXX.jar
```

Visit: <https://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 there are any additional steps that should be performed.

Consult the *ColdFusion Hotfix Installation Guide* for troubleshooting hotfix installation issues: <http://blogs.coldfusion.com/post.cfm/coldfusion-hotfix-installation-guide>

2.4.1 Downloading Hotfixes Via Proxy

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
```

2.4.2 Servers Without a Public Internet Connection

If your server does not have a public internet connection you can locate the `hotfix_XXX.jar` file url using the ColdFusion Update Feed: <https://www.adobe.com/go/coldfusion-updates>. Download the `hotfix_XXX.jar` file on a computer with internet access, verify the checksum, and then transfer it to the server.

2.5 Setup Websites in IIS

First ensure that the firewall is configured to block live traffic.

Next create the file system for each website that will use ColdFusion and copy all the web files into the file system.

Create and configure each website that will use ColdFusion in IIS.

2.6 Run the ColdFusion 2018 Server Auto Lockdown Tool

The Auto Lockdown Tool Performs the following steps for you:

- Connects ColdFusion to the Web Server (wsconfig)
- Sets the ColdFusion Service identity to run as a dedicated account, optionally creates the account for you.
- Sets file system permissions for your web root and ColdFusion installation directory
- Adds Request Filtering Rules to block various URIs
- Adds a Connector Shared Secret
- Optionally Change the Tomcat Shutdown Port
- Configures a new cf_scripts alias
- Changes Registry Permissions

Before you run the tool, make sure have done the following:

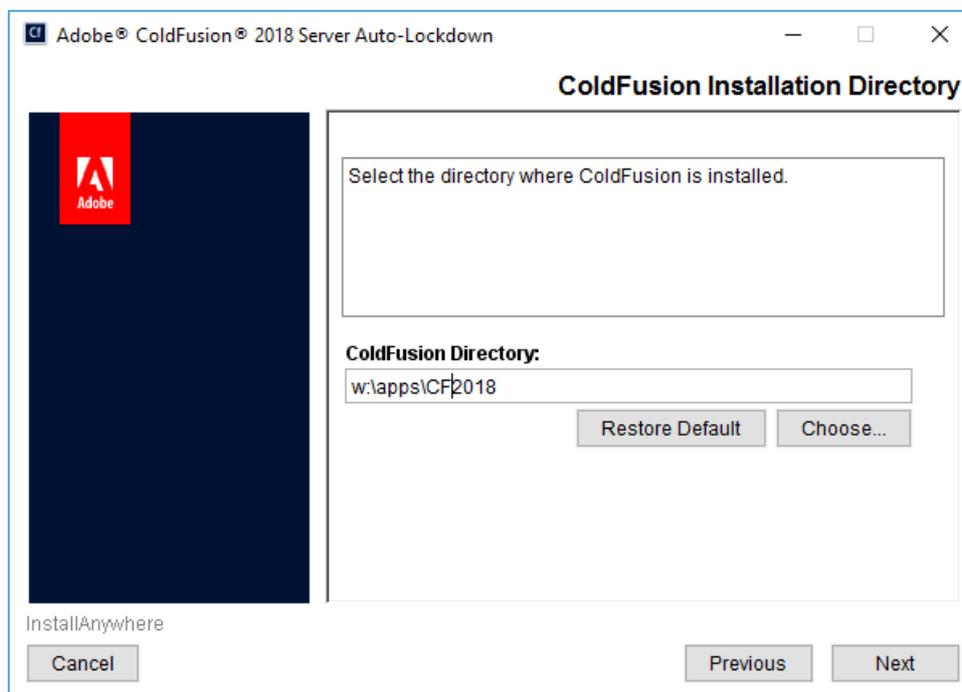
- Installed ColdFusion 2018 with Secure Profile Enabled
- Logged in to the ColdFusion Administrator at least once
- Created your websites in IIS, and copied website files

Download and run the latest copy of the ColdFusion 2018 Server Auto Lockdown Tool:

<https://www.adobe.com/support/coldfusion/downloads.html>

2.6.1 Lockdown Installer: ColdFusion Installation Directory

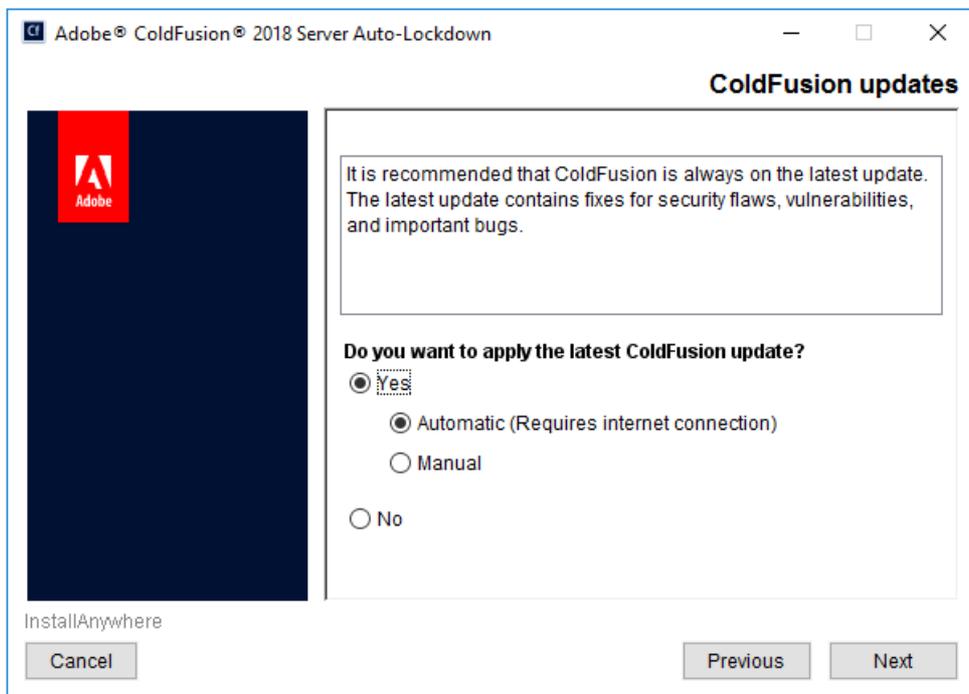
Choose the directory that ColdFusion was installed to.



Lockdown Installer: Select Installation Directory

2.6.2 Lockdown Installer: ColdFusion Updates

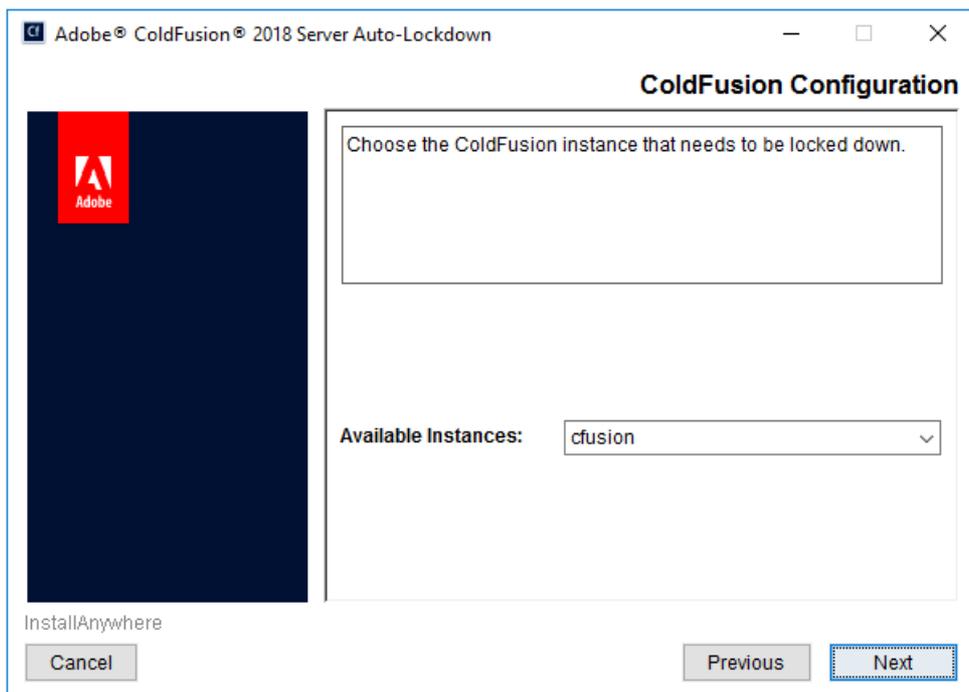
Choose *Yes / Automatic* to ensure that ColdFusion has been updated to the latest hotfix. Adobe recommends that you install ColdFusion updates before running the Lockdown tool.



Lockdown Installer: ColdFusion Updates

2.6.3 Lockdown Installer: ColdFusion Configuration

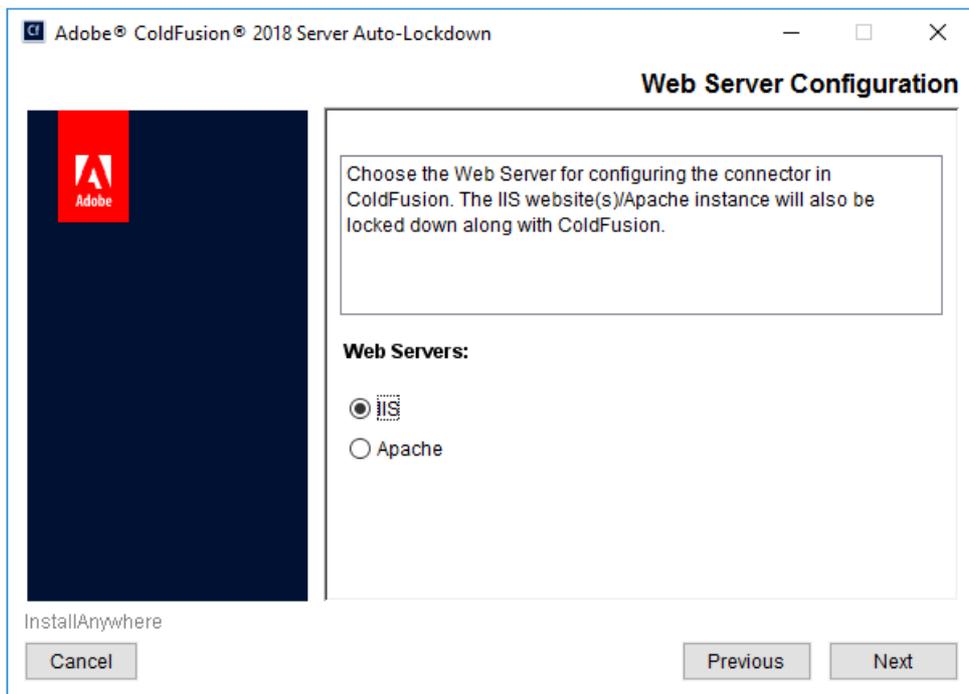
Select the instance that you want to lockdown.



Lockdown Installer: ColdFusion Configuration

2.6.4 Lockdown Installer: Web Server Configuration

Select the type of web server you are using, IIS in this case.

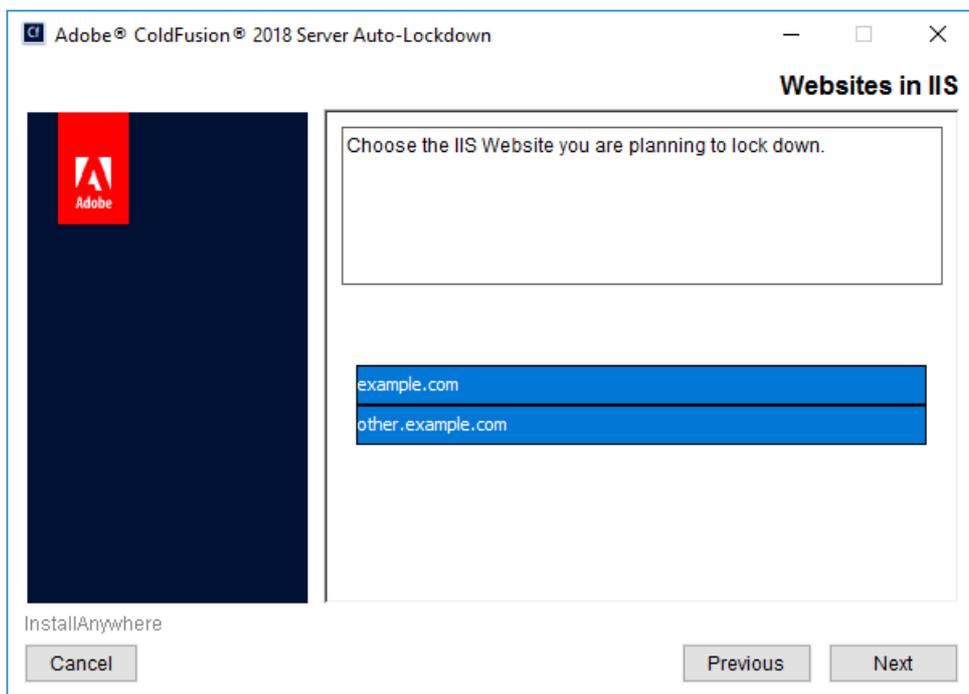


Lockdown Installer: Web Server Configuration

2.6.5 Lockdown Installer: Websites in IIS

Select the websites that you wish to connect ColdFusion to and to lockdown.

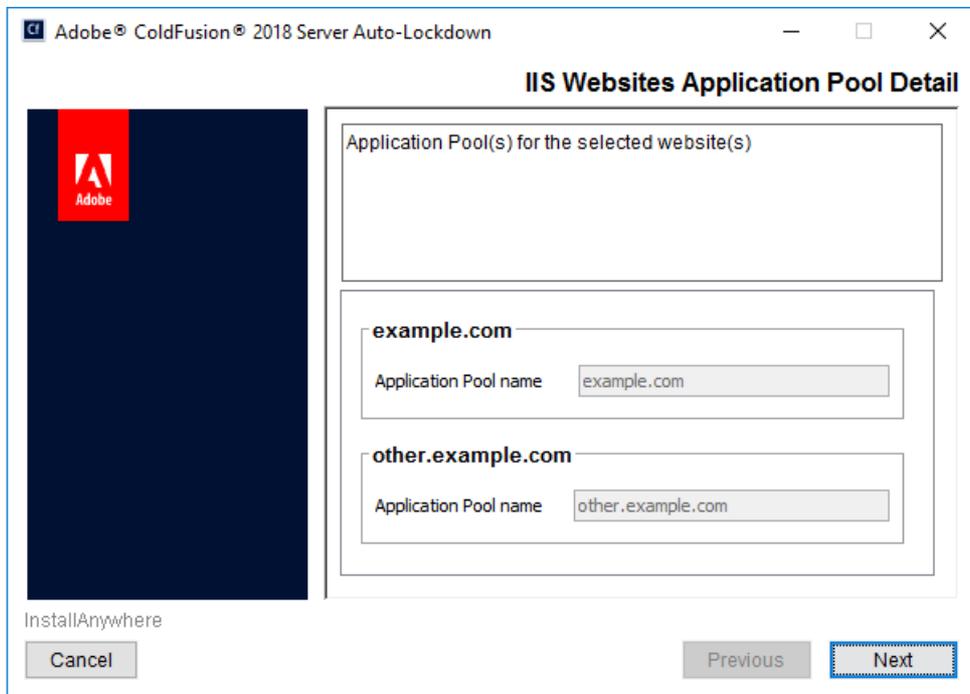
Tip: you can hold shift or ctrl when clicking to select sites



Lockdown Installer: Websites in IIS

2.6.6 Lockdown Installer: IIS Application Pool Detail

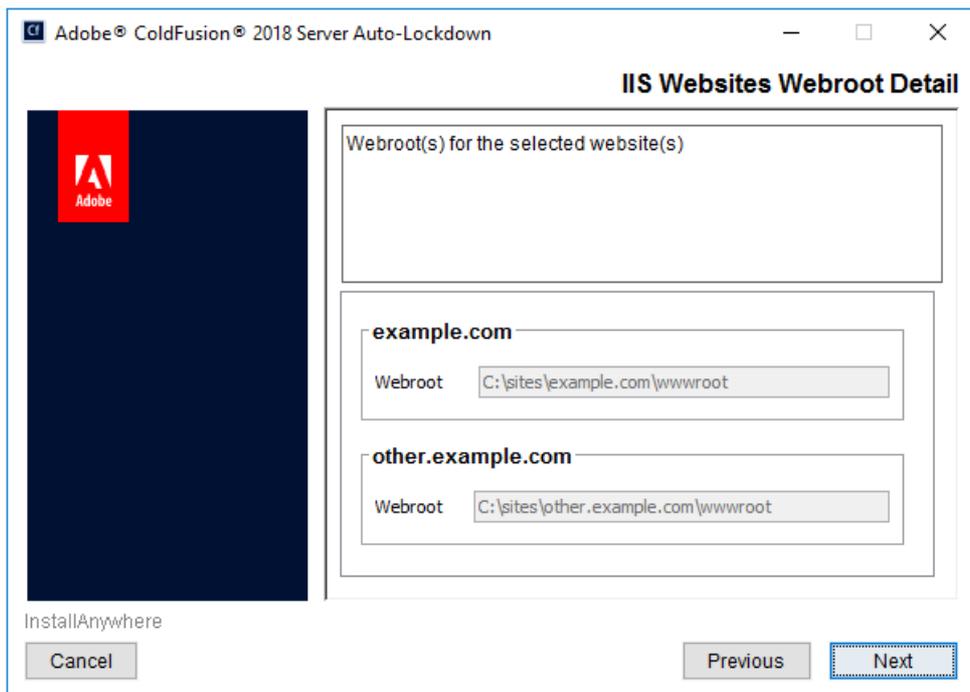
Verify that the application pool names are correct for each the website.



Lockdown Installer: IIS Application Pool Detail

2.6.7 Lockdown Installer: IIS Websites Webroot Detail

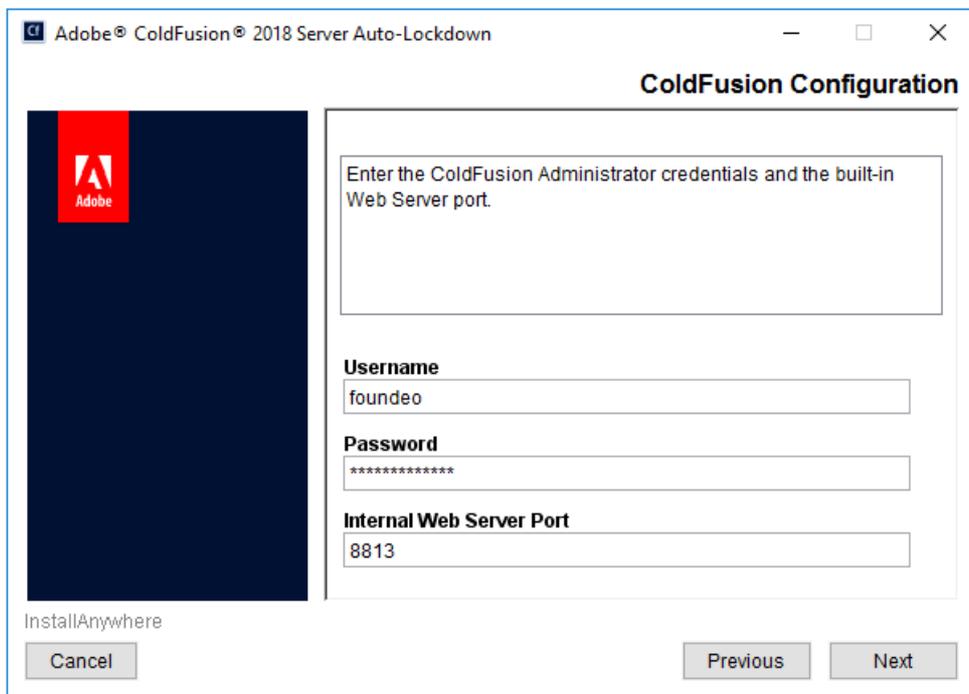
Verify that the web root paths are correct for each website.



Lockdown Installer: IIS Websites Webroot Detail

2.6.8 Lockdown Installer: ColdFusion Administrator Configuration

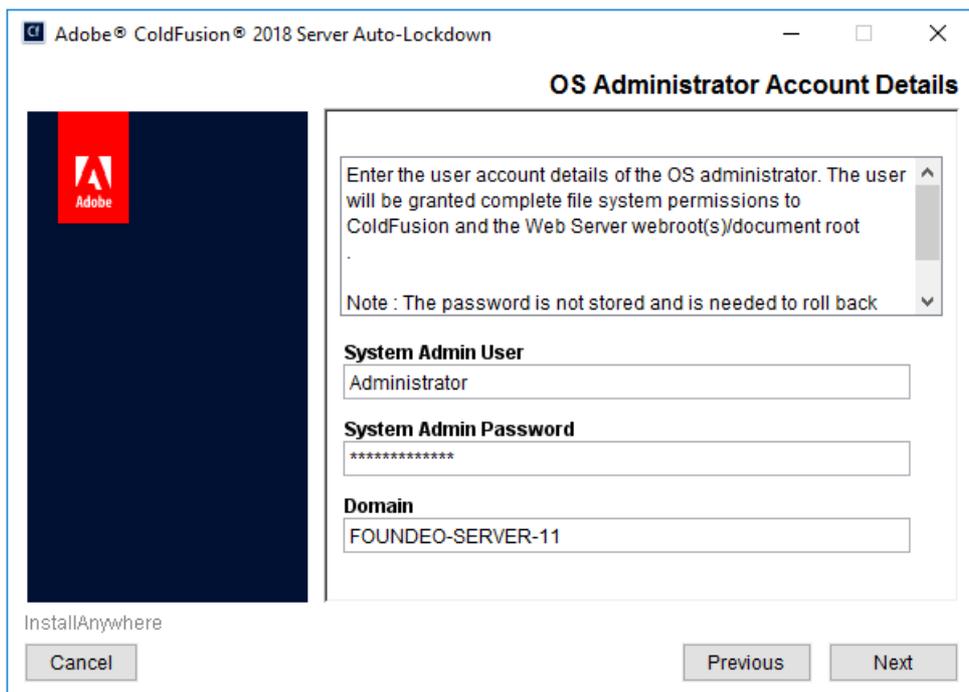
Enter the ColdFusion Administrator username and password specified during the ColdFusion Installation. Also ensure that the builtin web server port is correctly specified (default port is 8500).



Lockdown Installer: ColdFusion Administrator Configuration

2.6.9 Lockdown Installer: OS Administrator Account Details

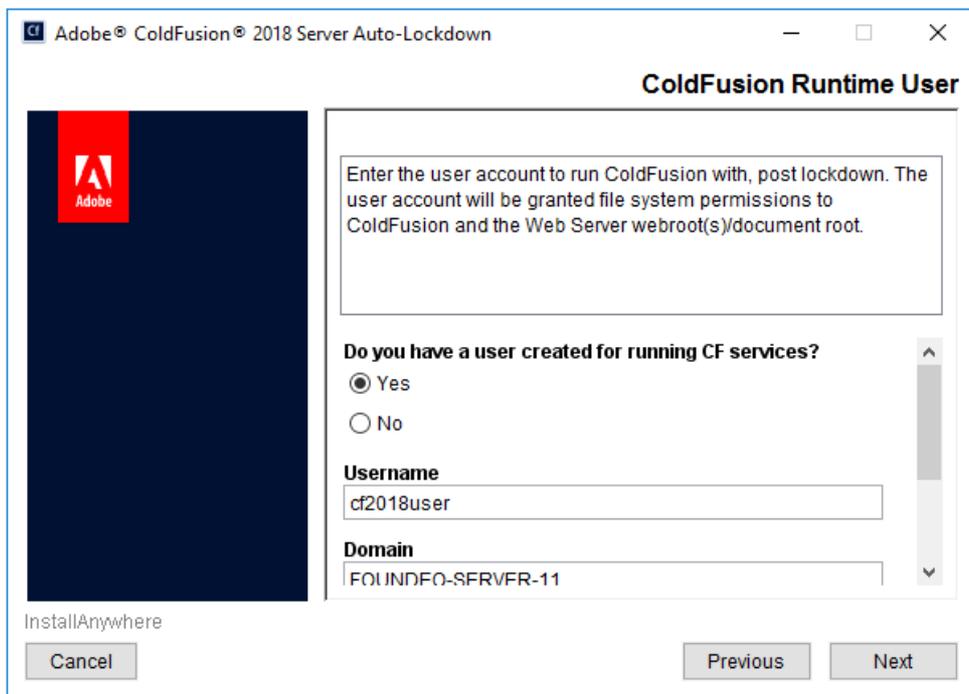
Enter the Administrator username, password and server name or domain.



Lockdown Installer: IIS Websites Webroot Detail

2.6.10 Lockdown Installer: ColdFusion Runtime User

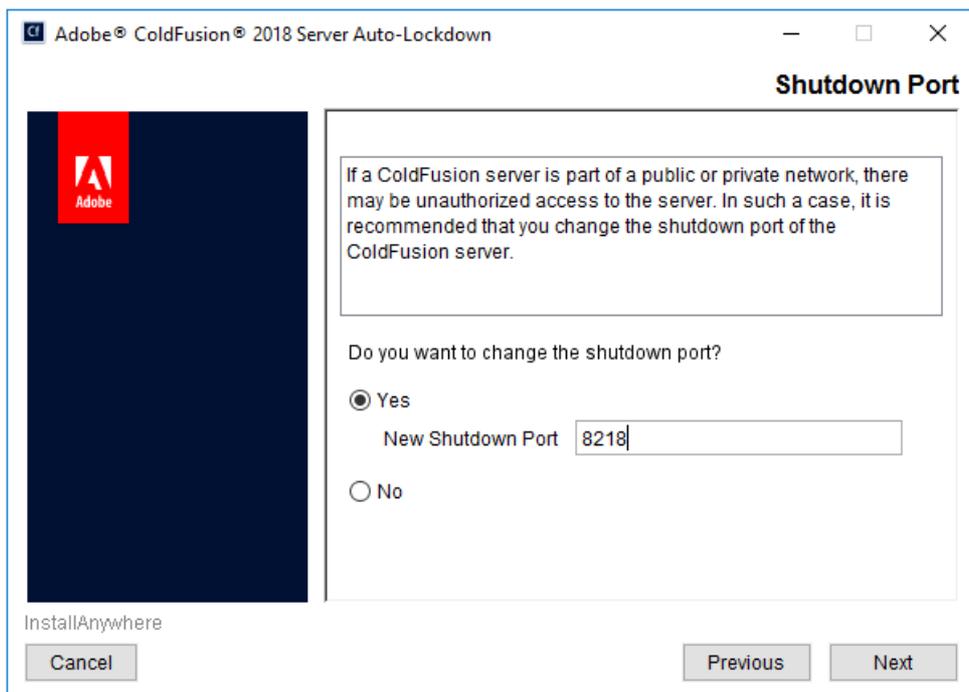
Create a unique username for the user account that ColdFusion will run as. Specify the domain, and a strong password.



Lockdown Installer: ColdFusion Runtime User

2.6.11 Lockdown Installer: Shutdown Port

Choose *Yes* and Enter a random port number that is not in use.



Lockdown Installer: ColdFusion Runtime User

2.6.12 Confirm that the Auto Lockdown Tool Ran Successfully

Open the `{cf.root}/lockdown/{cf.instance}/Logs/` folder and review the log files to confirm that the installer completed without fatal errors. Specifically look in the log file(s) that begin with `ServerLockdown_` and look for a line containing: *Successfully locked down ColdFusion!*

2.6.13 Check User Account Permissions

When the lockdown installer creates a Windows user account for ColdFusion to run as, it does not check the box *Deny this user permissions to log on to Remote Desktop Session Host server* in the User Account Properties.

To fix this open the *Computer Management* app, under *Local Users and Groups* find the user account and click *Properties*. Select the *Remote Desktop Services Profile* tab and then check the box.

2.6.14 Additional Resources for the Auto Lockdown Tool:

- <https://helpx.adobe.com/coldfusion/using/server-lockdown.html>
- <https://coldfusion.adobe.com/2018/07/server-auto-lockdown/>

2.7 Update JVM

Oracle releases Java security updates on a quarterly basis, most of these updates include security vulnerabilities that could be exploited in a server environment.

Important Note: As of 2019 Oracle no longer allows commercial use of Java without a license. However ColdFusion “Customers shall be supported on Oracle Java SE without having to contract for support directly with Oracle in order to run ColdFusion”. Details here: <https://coldfusion.adobe.com/2019/01/oracle-java-support-adobe-coldfusion/>

2.7.1 Download and Install Java

First download the latest version of Java from <https://www.adobe.com/support/coldfusion/downloads.html> that ColdFusion 2018 supports (Java 11 at the time of this publication). Select the java zip distribution and download.

Tip: Verify the checksum by running

Extract the java zip file you download to a permanent location, for example `C:\Java\jdk-11.0.2\`

2.7.2 Update ColdFusion Server JVM

Tip: Make a backup of the `{cf.instance.root}/bin/jvm.config` file and the `{cf.root}/cfusion/jetty/jetty.lax` file before making changes. If you type the path incorrectly ColdFusion will fail to start.

Login to the ColdFusion Administrator, then click on **Server Settings** then **Java and JVM**. Update the *Java Virtual Machine Path* setting to point to the new JVM, for example: `C:\Java\jdk-11.0.2\`

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.

2.7.3 Update JVM for ColdFusion Add-on Services

If you installed the ColdFusion 2018 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:\\ColdFusion2018\\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\\jdk-11.0.xx\\jre\\bin\\javaw.exe
```

Restart the ColdFusion 2018 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>

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	Suggestion	Additional Info
Timeout Requests After	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: <code><cfsetting requesttimeout="60"></code>
Use UUID for CFToken	Checked	When unchecked the 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	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. Performance may degrade when this setting is Unchecked.
Disable access to internal ColdFusion Java components	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.
Prefix serialized JSON with	Checked ://	This setting helps prevent JSON hijacking, a vulnerability which was exploitable in very old browsers (IE9 and below). 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 or 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	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	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	Tuned based on JVM heap size and feature usage	Ensure that you have sufficient JVM heap space to accommodate the memory limit.

Setting	Suggestion	Additional Info
Watch configuration files for changes (check every N seconds)	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.
Enable Global Script Protection	Understand Limits , 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 .
Disable creation of unnamed applications	Checked	Applications should have a name so they can be isolated from each other.
Allow adding application variables to Servlet Context	Unchecked	Keep unchecked to improve application isolation.
Default ScriptSrc Directory	<i>/not-default/</i>	Because the scripts directory also contains CFML source code, you should create a virtual directory / alias at a non-default location. Default values are <code>/cf_scripts/scripts</code> or <code>/cf2018_scripts</code>
Allowed file extensions for CFInclude tag	cfm	This setting restricts the file extensions which get compiled (executed) by a <code>cfinclude</code> 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 <code>cfinclude</code> . This setting was added in CF2018 Update 3. It can be defined at an application level as well via <code>this.blockedExtForFileUpload</code> .
Blocked file extensions for CFFile uploads	* or list	This setting restricts what file extensions are allowed to be uploaded by ColdFusion. If you do not allow file uploads you should set this to * to block all extensions. If you do allow uploads, ensure that all executable file extensions (such as cfm) are specified as a comma separated list. This setting can be defined at an application level as well.
Missing Template Handler	Custom Template	The missing template handler HTML output should be equivalent to the 404 error handler specified on your web server.
Site-wide Error Handler	Custom Template	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	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 https://www.petefreitag.com/item/808.cfm

Setting	Suggestion	Additional Info
Maximum size of post data	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	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	Tuned	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.
Allow REST Discovery	Unchecked if not used.	This setting enables the end point <code>/rest/_api_listing</code> or <code>/api/_api_listing</code> 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 mitigate the impact Denial of Service (DOS) attacks against your server.

Setting	Suggestion	Additional Info
Maximum number of simultaneous Template requests	Tuned based on hardware	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	1 if not using Flash Remoting otherwise tuned.	If your applications do not use flash remoting set this value to 1 and disable flash remoting. 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	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	1 if not using Remote CFC function requests, otherwise tuned	This setting applies only to CFC functions that have <code>access=remote</code> specified, when they are invoked via a HTTP request, for example: <code>/example.cfc?method=MethodName</code> . 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	Keep at 1 unless using <code>cfreport</code> heavily.
Maximum number of threads available for CFTHREAD	1 if not using <code>cfthread</code> , tuned otherwise	

Setting	Suggestion	Additional Info
Timeout requests waiting in queue after	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 may decrease the effectiveness of DOS attacks.
Request Queue Timeout Page	Custom Template	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	Suggestion	Additional Info
Trusted Cache	Checked	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	Suggestion	Additional Info
Default Storage Mechanism for Client Sessions	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	Suggestion	Additional Info
Use J2EE session variables	Checked if JEE interoperability required	When checked ColdFusion will use the session management of the underlying JEE container (eg Tomcat). Instead of using CFID and CFTOKEN the JSESSIONID cookie is used. 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 not operate on J2EE sessions.
Enable Session Variables	Unchecked only if not using sessions	Most applications require session variables, however if none of the applications on the server require session variables then you may uncheck this box.
Session Storage	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	Less than 2 days	The default of two days is generally too long for sessions to persist. Lower session timeouts reduce the window of risk of session hijacking.

Setting	Suggestion	Additional Info
Default Timeout: Session Variables	20 minutes or less	Twenty minutes is a good default value, but maximum security applications may require a lower timeout value.
Cookie Timeout	-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	Session cookies should always be marked as HTTPOnly to prevent JavaScript or other client side technologies from accessing their values (on supported clients).
Secure	Checked if all sites use HTTPS	A client will only transmit a secure cookie over a secured connection (HTTPS)
Disable updating ColdFusion internal cookies using ColdFusion tags/functions.	Checked if all sites use HTTPS	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

Consider using SSL or TLS to connect to the mail server to encrypt the email in transit.

Consider enabling *Log all mail messages sent by ColdFusion*

3.8 Server Settings > WebSocket

Disable the WebSocket Service if it is not used by any applications on the server.

3.9 Server Settings > Charting

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`, `cfdoexamples`.

Ensure that the database user that ColdFusion connects as, also has limited permissions to only what is necessary. You should not use `sa` or `root` accounts.

Setting	Suggestion	Additional Info
Login Timeout (sec)	5 Seconds	Decrease this value to be less than the <i>Timeout Requests after</i> setting.
Query Timeout (seconds)	Not 0	Specify an upper limit to mitigate DOS attacks.
Allowed SQL	Enable only operations required by the application, eg <code>SELECT</code> , <code>INSERT</code> , <code>UPDATE</code> , <code>DELETE</code>	The <code>CREATE</code> , <code>DROP</code> , <code>ALTER</code> , <code>GRANT</code> , and <code>REVOKE</code> operations are not commonly required in web applications.

3.11 Data & Services > ColdFusion Collections

Remove the example collection: `bookc1ub` if it exists.

3.12 Data & Services > Solr

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

3.13 Data & Services > Flex Integration

Uncheck **Enable Flash Remoting** and **Enable Remote Adobe LiveCycle Data Management access** if they are not used by your application.

If using LiveCycle Data Services ES consider checking the **Enable RMI over SSL for Data Management** checkbox and specify a keystore and password.

3.14 Data & Services > PDF Service

If the PDF Service is used to generate PDFs containing sensitive data, or if the PDF service running on a remote server, ensure that HTTPS is enabled.

3.15 Debugging & Logging > Debug Output Settings

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

3.16 Debugging & Logging > Developer Profile

The *Developer Profile* should not be enabled on Production servers.

3.17 Debugging & Logging > Debugger Settings

Setting	Suggestion	Additional Info
Allow Line Debugging	Unchecked	Debugging should not be enabled on a production server.

3.18 Debugging & Logging > Logging Settings

Setting	Suggestion	Additional Info
Log directory	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). Consider a separate drive / partition for storing logs.

Setting	Suggestion	Additional Info
Maximum number of archives	10 or more	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.
Use operating system logging facilities	Checked	Certain log entries will be duplicated to syslog on Unix based operating system.
Enable logging for scheduled tasks	Checked	Log scheduled task execution.

3.19 Debugging & Logging > Remote Inspection Settings

Setting	Suggestion	Additional Info
Allow Remote Inspection	Unchecked	Debugging features should not be enabled on a production server.

3.20 Event Gateways > Settings

Uncheck **Enable ColdFusion Event Gateway Services** if your applications do not require the use of event gateways.

3.21 Event Gateways > Gateway Instance

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

3.22 Security > Administrator

Setting	Suggestion	Additional Info
ColdFusion Administration 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 generate an encryption key to encrypt and decrypt passwords for datasources and other services.
Allow concurrent login sessions for Administrator Console	Unchecked	Uncheck to prevent concurrent logins by the same user account in the ColdFusion Administrator.

3.23 Security > RDS

RDS should not be enabled on production server.

If RDS was previously enabled ensure that the `{cf.instance.root}/wwwroot/WEB-INF/web.xml` does not contain a `ServletMapping` for the `RDSServlet`.

3.24 Security > Sandbox Security

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.

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

Your application should be thoroughly tested before enabling sandbox security to ensure that your sandbox has been configured correctly.

3.25 Security > User Manager

Add user accounts for each person that will login to the ColdFusion Administrator.

3.26 Security > Allowed IP Addresses

Setting	Suggestion	Additional Info
Allowed IP Addresses for Exposed Services	Empty	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	List of internal / administrative IP addresses	Specify to limit which IP addresses may connect to the ColdFusion administrator and AdminAPI.

3.27 Security > Secure Profile

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.

3.28 Server Update > Updates : Settings

Setting	Suggestion	Additional Info
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	Checked	Setup email alerts to be notified when a server update is available.
Site URL	https://www.adobe.com/go/coldfusion-updates	Ensure that the URL is correct and uses HTTPS.

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 To Configure the Builtin Web Server to bind to 127.0.0.1 only

By default the connector will listen on all IP addresses. To configure the builtin 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 builtin web server is running on, add an `address` attribute. For example:

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

Restart ColdFusion and confirm that the builtin web server now only listens on the specified address. See <https://tomcat.apache.org/tomcat-9.0-doc/config/http.html> for more information.

4.2 To Run the Builtin Web Server over TLS

The builtin web server can be configured to run over TLS / HTTPS. This is highly recommended, especially if the builtin server is configured to listen on addresses other than localhost.

First, a certificate must be generated. You may obtain a certificate from a trusted certificate authority (recommended) or generate a self signed certificate.

To generate a self signed certificate, run the following command:

```
{cf.root}/jre/bin/keytool -genkey -alias tomcat -keyalg RSA -keystore {cf.root}/tomcat.keystore
```

Specify a unique password for the keystore when prompted.

Next make a backup of, then edit `{cf.instance.root}/runtime/conf/server.xml` and locate the `<Connector>` tag that has a port value matching your builtin web server. Comment out the default builtin web server Connector tag and replace with something like this:

```
<Connector port="8443" protocol="HTTP/1.1"
  SSLEnabled="true" scheme="https"
  secure="true"
  keystoreFile="{cf.root}\tomcat.keystore"
  keystorePass="{your.password}"
  keyAlias="tomcat"
  clientAuth="false"
  sslProtocol="TLSv1.2" />
```

Be sure to replace `{cf.root}` with the path to your ColdFusion installation root (eg `C:\ColdFusion2018`) and `{your.password}` with the value you specified when you generated your certificate. Consider changing the port `8443` to a non default value.

Restart the ColdFusion instance, and visit <https://127.0.0.1:8443/CFIDE/administrator/> (change port to match value you used). If you used a self signed certificate you will receive a certificate warning.

Consider specifying the `ciphers` attribute and `useServerCipherSuitesOrder="true"` to ensure a strong TLS cipher is favored. Because the recommendations for preferred TLS protocols and ciphers change frequently please seek the current advice of cryptography experts for optimal TLS configuration.

For more information about configuring Tomcat with TLS, see: <https://tomcat.apache.org/tomcat-9.0-doc/ssl-howto.html> and https://tomcat.apache.org/tomcat-9.0-doc/config/http.html#SSL_Support

4.3 To Disable the Builtin Web Server

The builtin web server may be used on production servers to serve the ColdFusion Administrator. It may also be used by the Performance Monitoring Toolkit. You may disable the builtin web server when its use is not required.

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 port="8500" protocol="HTTP/1.1"
    connectionTimeout="20000"
    redirectPort="8451" />
```

-->

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 has two dashes -->` if you use a CFML comment (3 dashes) `<!--- cfml comment has three --->` ColdFusion may not start.

4.4 Deny ColdFusion Write Permission to Builtin Web Server wwwroot

ColdFusion will have *Full Control* of the `wwwroot` folder in your `{cf.instance.root}` you may consider restricting that directory to read only, because the `cf_scripts` folder may be served over the IIS or Apache web server. If you do restrict write permission on `wwwroot` you will need to allow write permission to the following sub directories:

- `WEB-INF/cfclasses`
- `WEB-INF/rest-skeletons`
- `WEB-INF/cfc-skeletons`

4.5 Restrict ColdFusion File System Permissions

ColdFusion will have *Full Control* of its installation directory by default. You may consider restricting full control to only files and folders that ColdFusion needs to write to. You can use file system auditing to determine which files ColdFusion writes to during normal operation of your application.

Some directories that are commonly written to include:

- `{cf.instance.root}/logs`
- `{cf.instance.root}/tmpCache`
- `{cf.instance.root}/stubs`
- `{cf.instance.root}/Mail`
- `{cf.instance.root}/runtime/work`
- `{cf.instance.root}/jetty/logs`
- `{cf.instance.root}/jetty/work`
- `{cf.instance.root}/jetty/multicore/collections/`

Note that use of ColdFusion Administrator may write configuration to several locations, you should ensure that your Administrator settings have been specified and will not change before restricting the file system permissions.

4.6 Lockdown the ColdFusion Add-on Services

If you installed the ColdFusion 2018 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 are not currently using the `cfsearch`, `cfcollection`, `cfindex`, or `cfhtmltopdf` tags 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 Solr Home folder. By default Solr Home will point to `{cf.root}/cfusion/jetty` you can find the exact path by going to the ColdFusion Administrator and looking at the Solr Home setting under *Data & Services > Solr Server*.

Consider using a non-default port (8989 is the default) and enabling HTTPS. Go to the ColdFusion Administrator and click the Show Advanced Settings button on the Data & Services > Solr Server to change these settings.

For maximum isolation, consider installing the ColdFusion Add-on Services on a dedicated server. Using HTTPS is highly recommended when Solr is running on a different server.

Consult the Jetty Documentation for more information: <https://www.eclipse.org/jetty/documentation/>

4.7 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 use jsp
.jws	Java Web Services	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	Hibernate XML Mappings	Yes, these files should always be blocked.

4.7.1 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.

4.7.2 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.

4.7.3 File Extension Whitelisting on IIS

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.

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.

4.8 Additional URIs to Consider Blocking

Here are some additional URIs that ColdFusion may serve requests on that you can consider blocking if you do not use the features it supports.

URI	Description
<code>/connector</code>	Used by the Performance Monitoring Toolkit
<code>/CFFileServlet</code>	Serves dynamically generated assets. It supports the cfreport , cfpresentation , cfchart , and cfimage (with action=captcha and action=writeToBrowser) tags
<code>/rest/ /api/ /restapps/ /cfapiresources/</code>	Used for CFML Rest Web Services

4.8.1 Blocking URIs in IIS

Click on the root node of IIS and then double click *Request Filtering*. Click on the *URL* tab. Click the *Deny Sequence* button and enter the URI to block.

Note the Auto Lockdown Tool blocks URIs using Request Filtering as well, however it applies the settings to the web site level, not the global IIS level. You may consider adding the URIs it blocks to the global level to ensure they will be blocked by sites on the server.

4.8.2 Blocking URIs in Apache

To block a URI, add the following to the `httpd.conf` file:

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

The above would block and return a 404 HTTP status when the case insensitive `(?i)` pattern `/CFIDE` is found anywhere `.*` in the URI.

4.9 Optionally Remove ASP.NET

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.

4.10 Remove ASP.NET ISAPI Filters and Handler Mappings

If you do not require ASP.NET functionality, and you do not want to fully remove ASP.NET from the server due to issues outlined in the previous section you can remove the ISAPI Filters and Handler Mappings that ASP.NET uses to process requests.

First make a backup of the `applicationHost.config` file, typically located in `C:\Windows\System32\inetsrv\config\`, and any `web.config` files.

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. A minimal configuration includes only `StaticFile`, `ISAPI-DLL`, and `cfmHandler`.

4.11 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.
/JSDebugServlet/*	JSDebugServlet	Used for debugging cfclient, should be commented out on production servers.
*.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 used.
/CFFileServlet/*	CFFileServlet	Used for serving files generated dynamically from various tags such as cfchart , cfimage , etc.
/securityanalyzer/*	CFSecurityAnalyzerServlet	Used for CFBuilder security analyzer. Not needed on production servers.
/rest/* /api/* /restapps/* /cfapiresources/*	CFRestServlet	Used to serve CFML 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.
/flashservices/gateway/*	FlashGateway	Used for Flash Remoting
/flex-internal/*	FlexInternalServlet	Used for Flex History Manager
*.mxml	FlexMxmlServlet	Used to compile Flex mxml files into swf
/flex2gateway/*	MessageBrokerServlet	Used for Flash Remoting
/cfmobile/*	CFMobileServlet	Used for cfclient
/pms /connector/*	PMSGenericServlet	Used by the Performance Monitoring Toolset

To remove a servlet mapping, you can comment it out using an 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.

4.12 Additional Tomcat Security Considerations

Consult the Tomcat 9 Security Considerations document <http://tomcat.apache.org/tomcat-9.0-doc/security-howto.html> for additional tomcat specific security settings.

4.13 Additional File Security Considerations

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

4.14 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 SAMEORIGIN. 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.

4.15 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.

4.15.1 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.

4.15.2 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*.

4.16 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>

```

4.17 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.

4.17.1 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*.

4.17.2 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`.

4.18 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.

For more information on configuring ColdFusion to run in distributed mode consult this blog entry: <http://blogs.coldfusion.com/setting-up-coldfusion-in-distributed-environment/>

4.19 HTTP Response Headers to improve Security

There are several HTTP response headers that you may consider adding to the web server to improve security. Some headers you may consider adding include:

- `Strict-Transport-Security`
- `X-Frame-Options`
- `Content-Security-Policy`
- `X-Content-Type-Options`
- `X-XSS-Protection`

- Referrer-Policy

4.19.1 Adding HTTP Response Headers in IIS

Open IIS and double click the **HTTP Response Headers** icon. Then click **Add** and specify a header name and value.

4.19.2 Adding HTTP Response Headers in Apache

Add a **Header** directive to your `httpd.conf`:

```
Header set Strict-Transport-Security "maxage=31536000"
```

5 ColdFusion Lockdown on Linux

This section covers installation of ColdFusion on Linux with Apache. To install ColdFusion 2018 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 RedHat 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` to remove a package: `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.bin`

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` please choose a unique name:

```
groupadd webusers
```

Create a `system` user for ColdFusion to run as, in this guide we use the username `cfuser`, but again, pick a unique username:

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

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

5.3 ColdFusion Installation

Run the installer as the `root` user or by 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:** Choose `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:** Select only services that are required by your application.
 - 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 CF Reporting if you are not using the `cfreport` tag.
 - Uncheck CFSWF and Flash Forms if not using Flash Forms (`cfform format=flash`)
- **Access Add-on Services Remotely:** If you selected the PDFG (`cfhtmltopdf` tag) or Solr (`cfsearch`, `cfindex`, `cfcollection` tags) sub-components the ColdFusion 2018 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. Select `n` unless remote access is required.
- **Choose Install Folder:** Select a non default installation folder, in this guide we will use `/opt/cf2018/`
- **Built-in Web Server Port Number:** Select a non-default port number.
- **Performance Monitory Toolset Hostname / IP Address:** Enter the internal IP address of the server if you wish to use the PMT. This value can be changed later in the Administrator.
- **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:** select a unique username (not `admin`), and choose a strong password.
- **Server Updates:** `Y` automatically check for server updates.

Now start ColdFusion:

```
service cf2018 start
```

5.4 Access ColdFusion Administrator via a SSH Tunnel

Because most linux servers do not have a desktop installed, and because the ColdFusion administrator is no longer accessible via the Apache web server as of CF2016+ it can be useful to create a temporary SSH tunnel when you need to connect to the ColdFusion Administrator.

To access ColdFusion Administrator you can create a SSH tunnel that points to the builtin 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) on your desktop.

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 user@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 traffic between your server and desktop will be encrypted over the SSH protocol. You can also configure the builtin web server to use HTTPS on top of that as well (see section 4.2).

5.5 Install ColdFusion Hotfixes

Login to the ColdFusion Administrator via the built-in web server.

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

Tip: You can verify the integrity of the downloaded hotfix by running `md5sum` 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>

Run the hotfix installer as `root` or with `sudo` (replace `hotfix_XXX.jar` with the actual hotfix file name):

```
/opt/cf2018/jre/bin/java -jar /opt/cf2018/cfusion/hf-updates/hotfix_XXX.jar
```

Consult the *ColdFusion Hotfix Installation Guide* for troubleshooting hotfix installation issues:

<http://blogs.coldfusion.com/post.cfm/coldfusion-hotfix-installation-guide>

5.6 Install and Configure Apache Web Server

5.6.1 Install or Update Apache

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
```

5.6.2 Remove Unnecessary 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`.

5.6.3 Setup Directory for Web Roots

Optional: If you wish to setup a non default web root follow the instructions in this section. If you plan to use the default web root `/var/www/html` then copy your CFML files into that directory.

If you have multiple web sites you may wish to create a folder for all your sites. In this guide we will use `/www/` as the root folder, but you should choose a unique path name.

```
mkdir -p /www/default/wwwroot/  
mkdir -p /www/example.com/wwwroot/  
mkdir -p /www/other.example.com/wwwroot/
```

Copy your CFML source code into the directory, the `/www/default/wwwroot/` could be setup as a default site for Apache.

Next lets add the `apache` user to the `webusers` group we created previously.

```
usermod -aG webusers apache
```

Setup some file system permissions:

```
chown -R root:webusers /www  
chmod -R 750 /www  
chcon -R -t httpd_sys_content_t -u system_u /www/default/wwwroot/  
chcon -R -t httpd_sys_content_t -u system_u /www/example.com/wwwroot/  
chcon -R -t httpd_sys_content_t -u system_u /www/other.example.com/wwwroot/
```

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

Next tell apache that it is allowed to serve files to the public under the folder `/www` by adding:

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

Create an `index.html` file in the default site:

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

Restart Apache

```
service httpd restart
```

Test to make sure Apache is working:

```
curl http://localhost/
```

The above `curl` command should output the contents of the `/www/default/wwwroot/index.html` which should be `Hello`.

5.6.4 Start Apache on Boot

By default Apache will not start up on system boot, you need to tell `systemctl` to enable the service. As `root` or using `sudo` run the following:

```
systemctl enable httpd.service
```

5.6.5 Connect Apache to ColdFusion

Note that there is a bug in the Auto Lockdown Tool when it configures the connector when SELinux is enabled. You may be able to skip this step (and allow the Auto Lockdown Tool to connect Apache to ColdFusion) if you do not have SELinux enabled or if the bug has been resolved: <https://tracker.adobe.com/#/view/CF-4203248>

Run `wsconfig` as `root` or with `sudo` to connect ColdFusion to Apache:

```
/opt/coldfusion2018/cfusion/runtime/bin/wsconfig -ws Apache -dir /etc/httpd/conf -bin /usr/sbin/httpd
```

You may see an error that Apache was unable to start, this is due to the bug mentioned above. To correct this, run the following commands:

```
WSCONFIG_DIR=/opt/coldfusion2018/config/wsconfig
NUM=1
```

```
#Create a `mod_jk.log` file:
```

```
touch $WSCONFIG_DIR/$NUM/mod_jk.log
```

```
#Set file system permissions:
```

```
chown -R cfuser:apache $WSCONFIG_DIR
chmod -R 540 $WSCONFIG_DIR
chmod 550 $WSCONFIG_DIR/$NUM/mod_jk.so
chmod 560 $WSCONFIG_DIR/$NUM/mod_jk.log
```

```
chcon -t httpd_modules_t -u system_u $WSCONFIG_DIR/$NUM/mod_jk.so
chcon -t httpd_log_t -u system_u $WSCONFIG_DIR/$NUM/mod_jk.log
chcon -t httpd_config_t -u system_u $WSCONFIG_DIR/$NUM/uriworkermap.properties
chcon -t httpd_config_t -u system_u $WSCONFIG_DIR/$NUM/mod_jk_vhost.conf
```

```
#allow apache to connect to CF AJP connector port (defined in server.xml)
semanage port -a -t http_port_t -p tcp 8018
```

```
#update JkShmFile path mod_jk.conf
sed '/JkShmFile/s/.*JkShmFile "\/var\/cache\/httpd\/1_jk_shm\/" /etc/httpd/conf/mod_jk.conf >
/etc/httpd/conf/mod_jk.conf
```

Tip: you can put the above commands into a file that begins with `#!/bin/bash` and then run them all at once as a script.

At this point you can restart apache, and try accessing a test.cfm file to see if it works.

5.7 Run the Linux ColdFusion Auto Lockdown Tool

Before running the ColdFusion Auto Lockdown Tool please ensure the following:

- ColdFusion is running, and you have logged in to the ColdFusion Administrator at least once. `service cf2018 start`
- Apache is running `service httpd start` test by accessing port 80 or 443.

Run the auto lockdown tool as the `root` user or by using `sudo`.

- **ColdFusion Installation Directory** - enter the directory where ColdFusion is installed.
- **Apply latest ColdFusion update** - select **Yes** to have the lockdown tool check for updates and install them.
- **Automatic Update or Manual** - select Automatic if the server is connected to the internet.
- **ColdFusion Instance** - enter the name of the instance to lockdown, select the default `cfusion`.

- **Web Server** - select Apache
- **Admin Username** - enter your ColdFusion Administrator user name.
- **Admin Password** - enter your ColdFusion Administrator password.
- **Internal Web Server Port** - enter port number you choose for the internal web server during installation (default is 8500).
- **System Admin User** - enter the username for your root user account.
- **System Admin Password** - if root has a password you may enter it, if it does not have a password configured just hit enter.
- **Do you have a user created for running CF services?** - select Yes.
- **ColdFusion Runtime Username** - enter the username for the ColdFusion user you created, eg `cfuser`.
- **ColdFusion Runtime User Password** - hit enter because the user was created as a system account so it does not have a password.
- **ColdFusion Runtime User Group** - enter the name of the group you created, for example `webusers`
- **Do you have a user created for running Web Server services?** - select Yes.
- **Web Server Group** - the name of the group that the web server user belongs to (default is `apache` on RedHat Linux).
- **Web Server Username** - the username for the web server user (default is `apache` on RedHat Linux).
- **Web Server Password** - hit enter, the web server user is created as a system account so it does not have a password by default on RedHat Linux.
- **Web Server Conf Directory Path** - enter the path to the folder that contains `httpd.conf` on RedHat Linux it will be `/etc/httpd/conf`
- **Web Server Binary Path** - enter the path to the `httpd` binary, on RedHat Linux it will be `/usr/sbin/httpd`
- **Web Server Web Root Path** - enter the path to the web root directory you created, for example: `/web/`
- **File Upload Path** - the lockdown installer will grant write permissions to the folder specified. If you have more than one folder, you can do this manually with `chmod`, for example `chmod u+w /web/example.com/path-to-write-to/`
- **Alias for cf_scripts** - select a path other than the defaults, not `/cf_scripts` and not `/cf2018_scripts`
- **Shutdown Port** - change the shutdown port to a non-default value.

Review the Lockdown Tool logs in `/opt/coldfusion2018/lockdown/cfusion/Logs` (path may differ), and ensure that it states *ColdFusion Server has been locked down successfully* and that there are no errors.

5.8 Update JVM

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

Important Note: As of 2019 Oracle no longer allows commercial use of Java without a license. However ColdFusion “Customers shall be supported on Oracle Java SE without having to contract for support directly with Oracle in order to run ColdFusion”. Details here: <https://coldfusion.adobe.com/2019/01/oracle-java-support-adobe-coldfusion/>

Download the RPM for the latest supported JRE from Adobe <https://www.adobe.com/support/coldfusion/downloads.html>. Install the rpm:

```
rpm -ivh jre-11.0.xx_linux-x64_bin.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 2018. At the time of this writing Java 10 is the latest supported major version of Java.

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

Locate the `jvm.config` file, (by default it is located in `/opt/coldfusion2018/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/coldfusion2018/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.

5.8.1 Update JVM Add-On Services

If you installed the add-on services ensure that the startup script points to the updated JVM, look for the line:

```
SOLR_JVM="/opt/coldfusion2018/jre"
```

And update it to:

```
SOLR_JVM="/usr/java/latest"
```

5.9 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/coldfusion2018 -p wax -k cf2018
```

The above will audit all write, attribute change and execute operations on the path `/opt/coldfusion2018/` and tag all entries with the filter key `cf2018`. Now that the filter key is setup you can query the audit log using:

```
ausearch -k cf2018
```

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.

You may also consider setting up auditing on other important paths such as `/etc/` or your web root file system.

5.10 Change umask

Edit the `{cf.root}/bin/sysinit` 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.

5.11 Additional Lockdown Steps

Go back Section 3 [ColdFusion Administrator Settings](#) and then to Section 4 [Additional Lockdown Measures](#) to perform additional steps.

6 Performance Monitoring Toolset Security Considerations

6.1 Installing the PMT

Select a non-default path to install to. Select a non-default port numbers. Enter a username other than `admin` and use a strong password.

For additional isolation consider installing the PMT on a dedicated server. The PMT Service and PMT Datastore could also be isolated to dedicated servers.

6.2 ColdFusion Server Auto Discovery

The PMT auto discovery feature can detect ColdFusion servers over multicast (default port 46864). Ensure that your network firewall or operating system firewall is configured to limit access accordingly.

More information about auto discovery: <https://coldfusion.adobe.com/2018/07/auto-discovery/>

6.3 PMT Datastore

The PMT datastore is an Elasticsearch server. Any computer with access to the port that the PMT datastore is running on can access all the data it contains.

- Ensure that the PMT datastore is not running on the default port `9200` to `9300`
- Ensure that a network or OS firewall has been configured to deny external access to this port.
- ColdFusion 2018 servers that are monitored require access to the PMT datastore port.

6.4 Run PMT and PMT Datastore as Dedicated User

The *ColdFusion 2018 Performance Monitoring Toolset* service and *ColdFusion 2018 Performance Monitoring Toolset Datastore* service run as Local System by default.

Create two Local User Accounts in this guide we will use the usernames: `pmtdatastore` and `pmtservice` however you should create unique names. Next create a group that contains both users for example `pmtgroup`.

Grant read only permission to the group (eg `pmtgroup`) on the Performance Monitoring Toolset installation directory (the default is `C:\ColdFusion2018PerformanceMonitoringToolset` or `/opt/ColdFusion2018PerformanceMonitoringToolset`).

Grant Full Control (read and write) permission to the `logs` and `config` directory under the PMT installation directory to the `pmtservice` user account.

Grant Full Control (read and write) permission to the `datastore/data` and `datastore/logs` directory under the PMT installation directory to the `pmtdatastore` user account.

Note that the `pmtservice` user does not need access to the `datastore` subfolder, you may consider denying the `pmtservice` user access to the `datastore` folder.

Update the Service Log On Identity for the *ColdFusion 2018 Performance Monitoring Toolset* service to point to your `pmtservice` user.

Update the Service Log On Identity for the *ColdFusion 2018 Performance Monitoring Toolset Datastore* service to point to your `pmtservice` user.

Restart both services.

6.5 Update PMT JVM

Edit the `jvm.config` file located in the `config` subfolder of the PMT installation directory. Replace the following line:

```
java.home=C:\ColdFusion2018PerformanceMonitoringToolset\jre
```

With a path pointing to your current JVM, for example:

java.home=C:\Java\jdk-11.0.xx\

7 API Manager Security Considerations

7.1 Install API Manager

Download and Run the API Manager Installer.

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.

7.2 Connect 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`.

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

Block or restrict access to the URIs using request filtering, IP restrictions, or web server authentication.

7.3 Run API Manager as a 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 Datastore 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"
```

8 Patch Management Procedures

Staying up to date with patches is essential to maintaining security on the server. The system administrator should monitor the vendors 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: <https://www.adobe.com/subscription/adbeSecurityNotifications.html>

Check the following websites frequently:

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

Microsoft Security Tech Center: <https://www.microsoft.com/en-us/msrc>

RedHat Security: <https://www.redhat.com/security/updates/>

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

Listing of security vulnerabilities in Tomcat: <https://tomcat.apache.org/security-9.html>

To keep updated with ColdFusion 2018 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 subscribing to the ColdFusion Community Portal <https://coldfusion.adobe.com/>.

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.

9 Sources of Information

Sources of Information

- Microsoft Security Compliance Management Toolkit: <http://www.microsoft.com/downloads/details.aspx?FamilyID=5534bee1-3cad-4bf0-b92b-a8e545573a3e>
- NSA Operating System Security Guides:
http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml
- NSA Guide to Secure Configuration of Red Hat Enterprise Linux 5: http://www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf
- Tips for Securing Apache: <http://www.petefreitag.com/item/505.cfm>
- Apache Security by Ivan Ristic, 2005 O'Reilly ISBN: 0-596-00724-8
- Tips for Secure File Uploads with ColdFusion: <http://www.petefreitag.com/item/701.cfm>
- HackMyCF.com Remote ColdFusion vulnerability scanner: <http://hackmycf.com/>
- Fixing Apache (13) Permission Denied 403 Forbidden Errors: <http://www.petefreitag.com/item/793.cfm>
- Apache Tomcat 8.5 Security Considerations: <http://tomcat.apache.org/tomcat-8.5-doc/security-howto.html> * Getting started with AppCmd.exe: <http://www.iis.net/learn/get-started/getting-started-with-iis/getting-started-with-appcmdexe>
- Thanks to Charlie Arehart for providing several suggestions and feedback on prior versions of the guide.
- Professional Microsoft IIS 8 by Schaefer, Kenneth; Cochran, Jeff; Forsyth, Scott; Glendenning, Dennis; Perkins, Benjamin. Wiley. ISBN: 978-1-118-38804-4
- ColdFusion and SELinux: <http://www.talkingtree.com/blog/index.cfm?mode=entry&entry=28ED0616-50DA-0559-A0DD2E158FF884F3>
- ColdFusion MX with SELinux Enforcing: <http://www.ghidinelli.com/2007/12/06/coldfusion-mx-with-selinux-enforcing>

10 Reference Tables

10.1 Tags that use /cf_scripts/ assets

Tag	URI Pattern	Notes
cfajaxproxy	/cf_scripts/scripts/ajax/	
cfajaximport	/cf_scripts/scripts/	This tag lets you override the default script src setting
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/cform.js /cf_scripts/scripts/masks.js	
cfform format=flash	/cf_scripts/scripts/ajax/	Deprecated since CF11
cfform format=xml	/cf_scripts/scripts/ajax/	Deprecated since CF11
cfgrid	/cf_scripts/scripts/ajax/	
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	/cf_scripts/scripts/ajax/ /cf_scripts/scripts/ckeditor/	Consider blocking the ckeditor subfolder if you do not use this tag because it has cfm files in it.
cftooltip	/cf_scripts/scripts/ajax/	
cfree	/cf_scripts/scripts/ajax/	
cfree format=applet	/cf_scripts/classes/	Deprecated since CF11
cfwebsocket	/cf_scripts/scripts/ajax/	
cfwindow	/cf_scripts/scripts/ajax/	

11 Troubleshooting

11.1 ColdFusion cannot write files under the web root

The Auto Lockdown tool gives ColdFusion read only permission to the web root, if there are files or folders that ColdFusion must write to you need to give the ColdFusion user account (eg cfuser) write permission.

11.2 Requesting a cfm results in a 404 after Lockdown tool

Here are two possible causes.

The IIS Application Pool .NET Framework Version may not have been set to *No Managed Code*.

The auto lockdown tool does not create inheritable file system permission, so ColdFusion's user account may not have permission to read the file if it was created after the lockdown tool ran. See the section titled [Adjust Windows File System Permissions](#).

11.3 IIS does not have permission to read web.config file

If you made a change in IIS after running the lockdown tool that caused a new `web.config` file to be created, the new file may not have the appropriate permissions. See the section titled [Adjust Windows File System Permissions](#).

11.4 WebSockets are not working after running lockdown tool

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

11.5 Help Installing ColdFusion Hotfixes

Consult the *ColdFusion Hotfix Installation Guide* for troubleshooting hotfix installation issues:
<http://blogs.coldfusion.com/post.cfm/coldfusion-hotfix-installation-guide>

12 Revision History

Version 1.0 - 2018-08-13 - Initial Release.

Version 1.1 - 2018-10-05

- Typo in section 4.11 Disable Unused Servlet Mappings on Page 34 `/flex/internal/` should be `/flex-internal/`

Version 1.2 - 2019-03-19

- Removed section (previously 2.7) *Adjust Windows File System Permissions* because it is no longer necessary due to bug fixes: <https://tracker.adobe.com/#/view/CF-4202957>
- Revised the Update JVM sections pertaining to Oracle licensing changes.
- Changed *Allow concurrent login sessions for Administrator Console* from checked to unchecked.

Version 1.3 - 2020-03-31

- Added note in section 4.4 about write permission to WEB-INF cfclasses, rest-skeletons, and cfc-skeletons