Adobe ColdFusion 2021 Lockdown Guide

Written by Pete Freitag, Foundeo Inc.

Adobe ColdFusion (2021 release) Lockdown Guide

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

Table of Contents

1 Introduction

The *ColdFusion 2021 Lockdown Guide* is written to help server administrators secure ColdFusion 2021 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 2019 / IIS 10, and RedHat Enterprise Linux (RHEL) 8 / 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 2021 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 2021 on a Windows 2019 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.
- Run the Microsoft Security Compliance Toolkit Policy Analyzer: https://www.microsoft.com/en-us/download/details.aspx?id=55319 and adjust settings as necessary.
- 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 over HTTPS.
- 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 4.7 (or latest version)
- Application Development: ASP.NET 4.7 (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 web site configuration by requesting a static file such as a txt or js file. At this point we have not yet connected IIS to ColdFusion so ColdFusion files (cfm, cfc, etc) cannot be served yet.

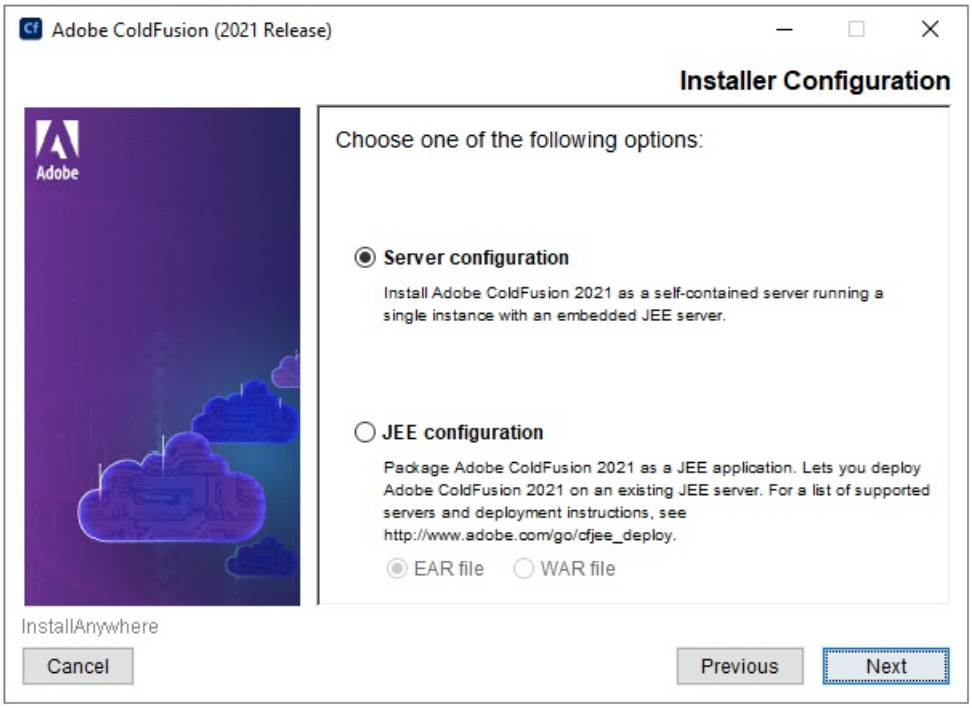
2.2.3 Remove Default Web Site

You may remove the *Default Web Site* defined by IIS, as well as any Application Pools that are not in use.

2.3 Run the Windows ColdFusion Installer

2.3.1 ColdFusion Installer: Installer Configuration

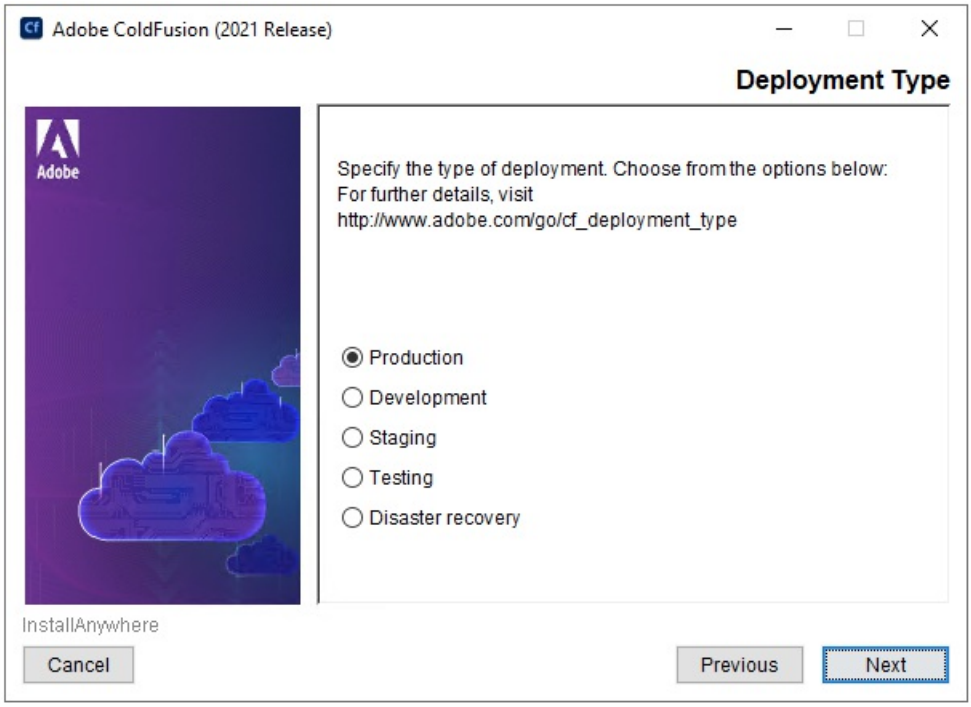
On the Installer Configuration view select **Server configuration** unless you are deploying to an external JEE server (such as JBoss, Weblogic or Websphere).



alt text

2.3.2 ColdFusion Installer: Deployment Type

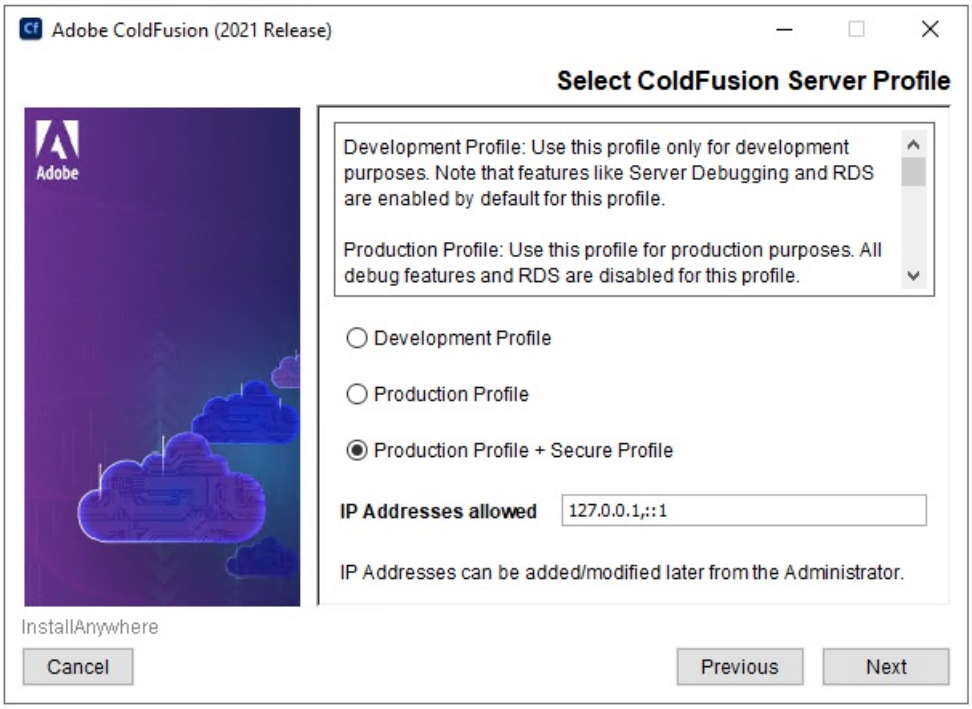
Next select the appropriate *Deployment Type* that the server is licensed for. See https://www.adobe.com/go/cf_deployment_type for details.



alt text

2.3.3 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`.

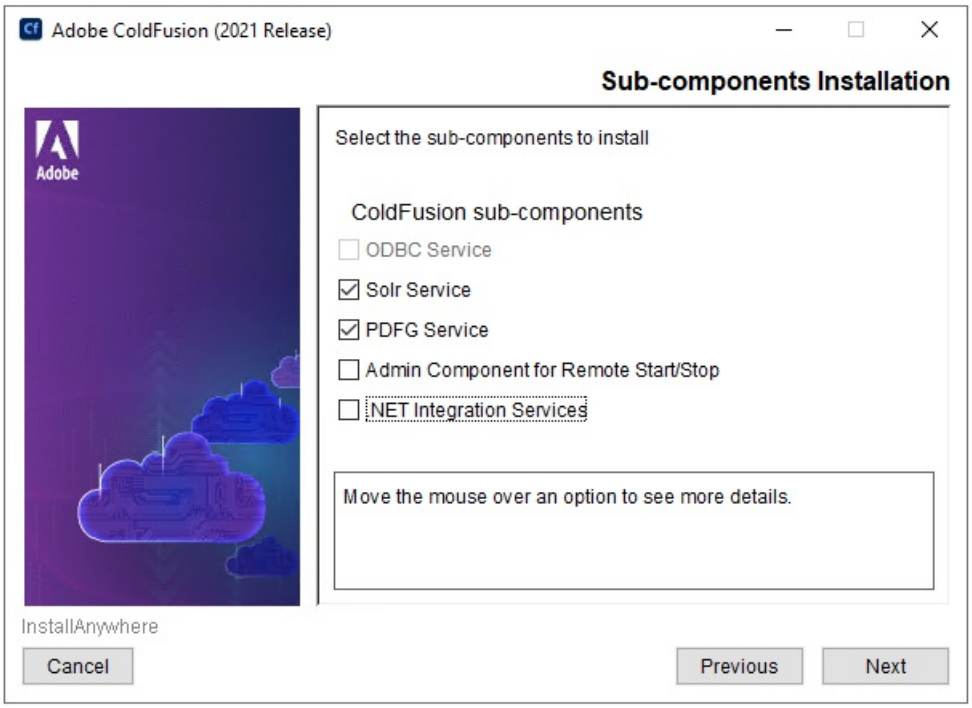
The Secure Profile option provides a more secure foundation of default settings. You can review the settings it toggles here: https://helpx.adobe.com/coldfusion/configuring-administering/administering-coldfusion-security.html

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.

2.3.4 ColdFusion Installer: Sub-components Installation

Only select Sub-components that your server applications require.

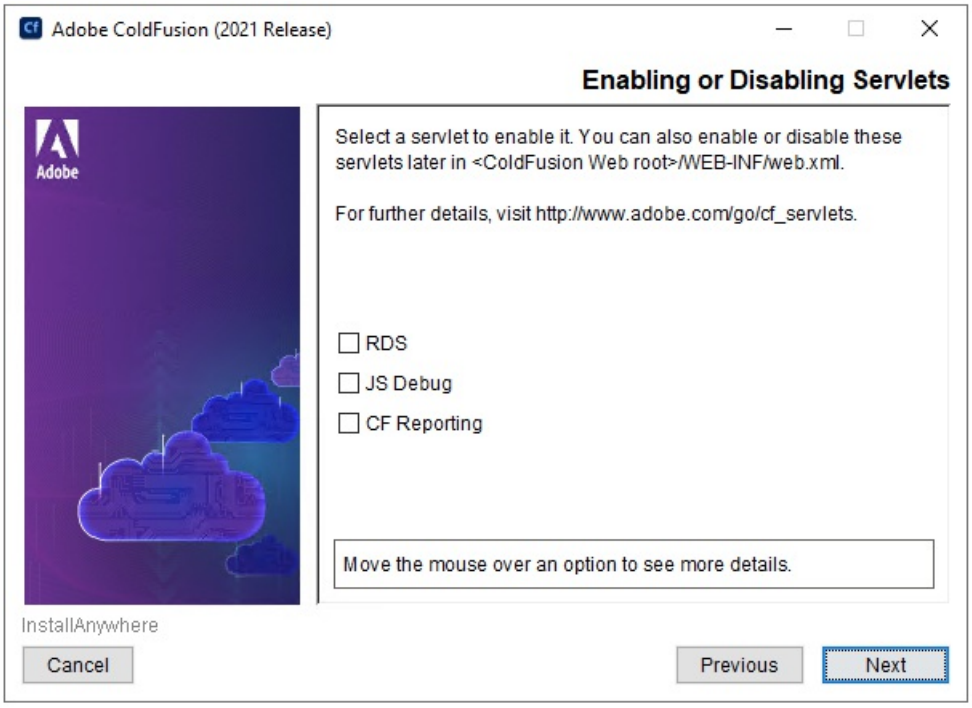


alt text

- **ODBC Service** - Required when connecting to Access Databases. ODBC is not required for SQL Server, Oracle, MySQL, PostgreSQL.
- **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. The `cfdocument` and `cfpdf` tags do not use the PDFG 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.

2.3.5 ColdFusion Installer: Enabling or Disabling Servlets

Keep all servlets unchecked (disabled) unless you use the `cfreport` tag. If you use the `cfreport` tag, then only the *CF Reporting* servlet should be checked (enabled).



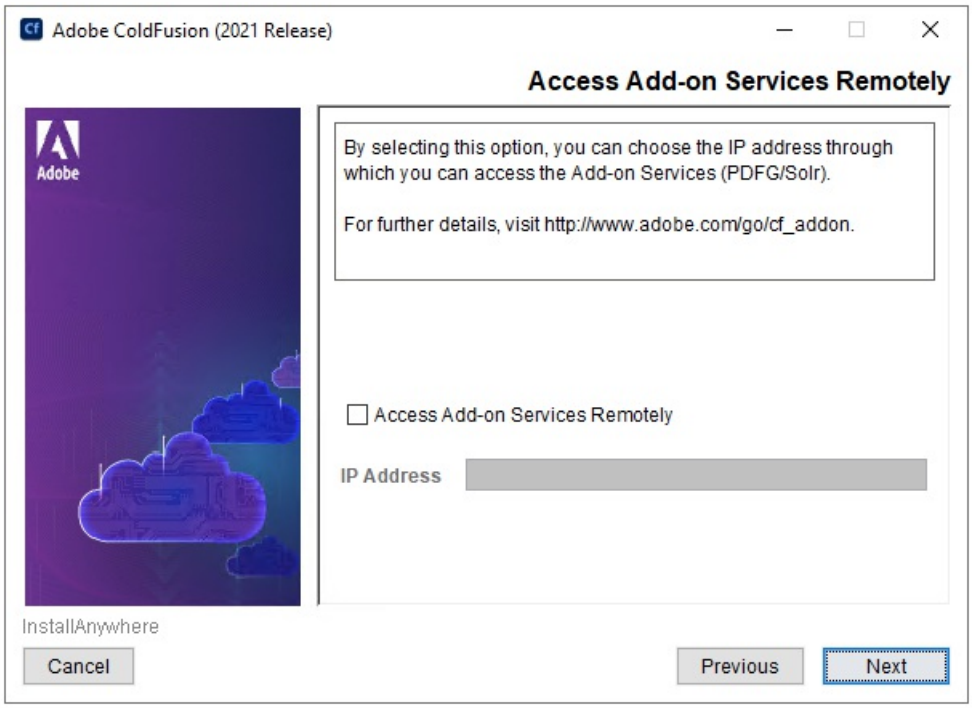
alt text

- **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.

2.3.6 ColdFusion Installer: Access Add-on Services Remotely

If you selected the PDFG (`cfhtmltopdf` tag) or Solr (`cfsearch`, `cfindex`, `cfcollection` tags) sub-components the *ColdFusion 2021 Add-on Services* windows service will be installed.

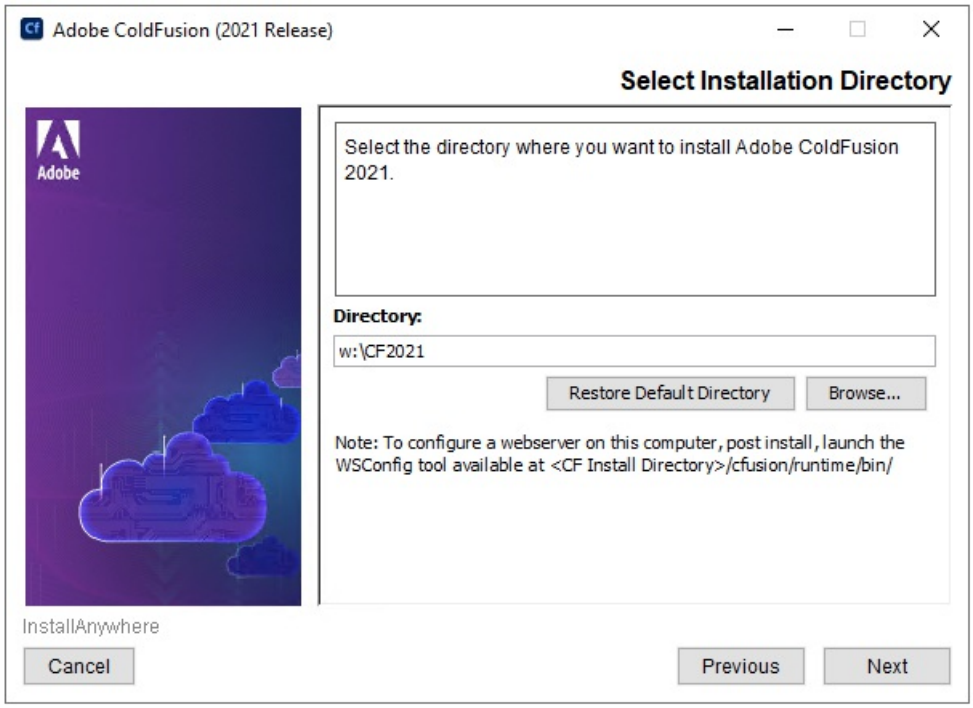
When the *Access Add-on Services Remotely* checkbox is unchecked, the Add-on Services are only accessible from the local machine, `localhost`. If you want to allow access to the services from multiple ColdFusion servers (other than localhost), check the checkbox and specify the IP addresses of the remote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



alt text

2.3.7 ColdFusion Installer: Select Installation Directory

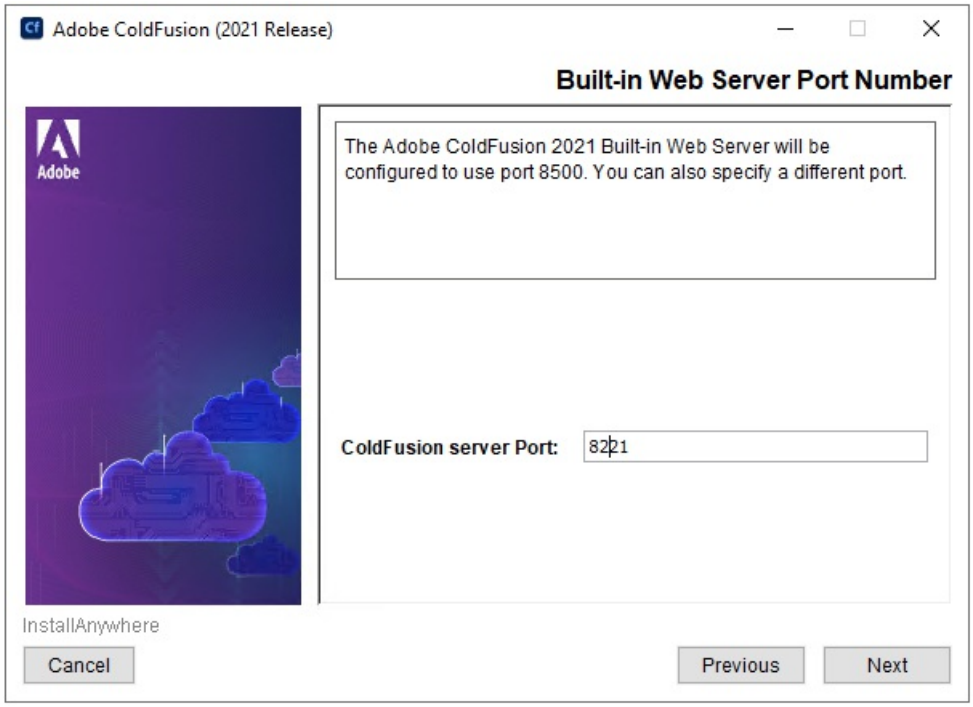
Specify a file system path for the ColdFusion Installation root `{cf.root}` - consider avoiding the default `C:\ColdFusion2021\` path.



Windows ColdFusion Installer: Select Installation Directory

2.3.8 ColdFusion Installer: Built-in Web Server Port Number

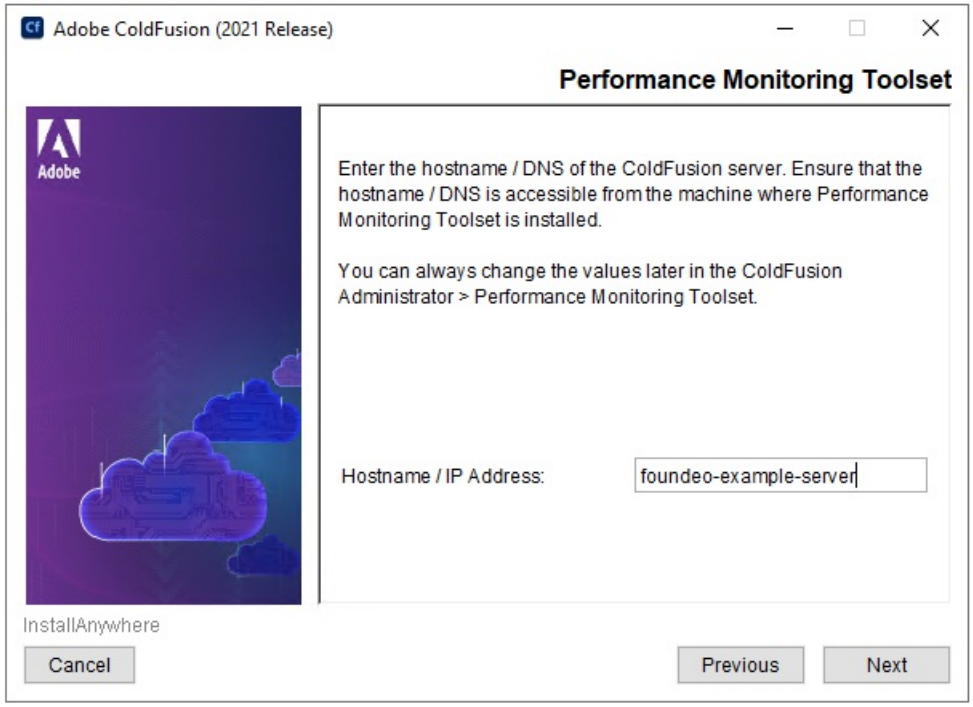
Select a non default port number. Ensure that the port number is blocked by your network/os firewall.



Windows ColdFusion Installer: Built-in Web Server Port Number

2.3.9 ColdFusion Installer: Performance Monitoring Toolset

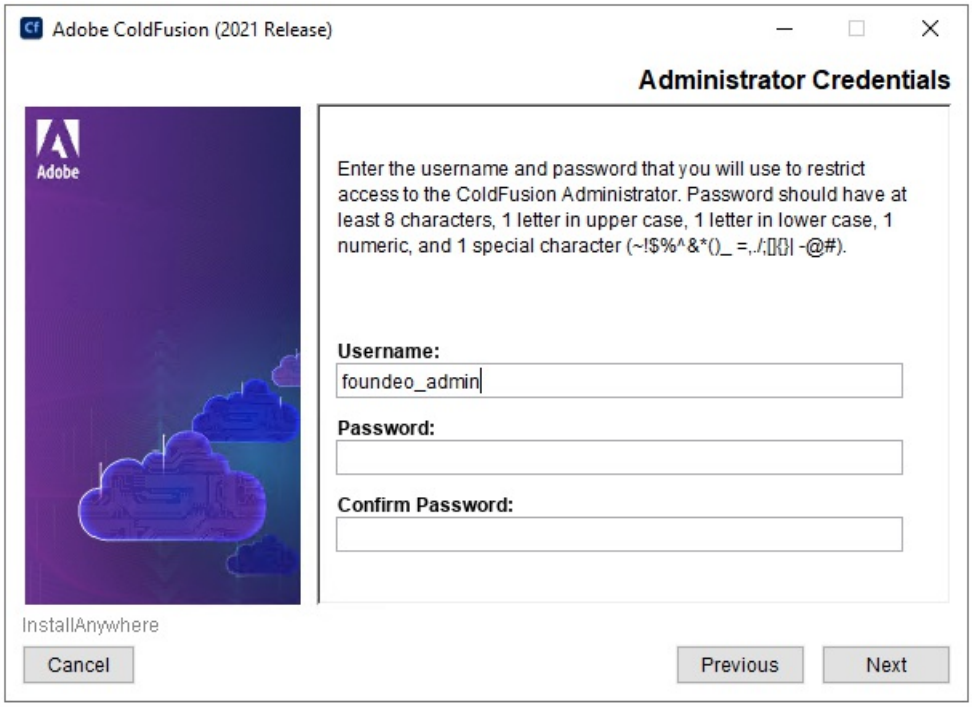
Enter the hostname or internal IP address of the server for use with the performance monitoring toolset. This value can be changed later.



Windows ColdFusion Installer: Performance Monitoring Toolset

2.3.10 ColdFusion Installer: Administrator Credentials

Enter a username other than the default (*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 **Package Manager > Core Server > Check for Updates** if any hotfixes are available select the latest hotfix, and click **Download**.

> Tip: ColdFusion Hotfixes are 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:\cf2021\jre\bin\java -jar x:\cf2021\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: https://coldfusion.adobe.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 is air-gapped, or 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 ColdFusion 2021 Lockdown Tool Pre-requisites

Before running the ColdFusion 2021 Auto-Lockdown Tool, make sure you have done the following:

- Installed ColdFusion 2021 with Secure Profile Enabled
- Login to the ColdFusion Administrator at least once.
- Setup a website in IIS for each site that will use ColdFusion on the server.

2.6 Run the ColdFusion 2021 Server Auto-Lockdown Tool

The Auto Lockdown Tool Performs the following steps for you:

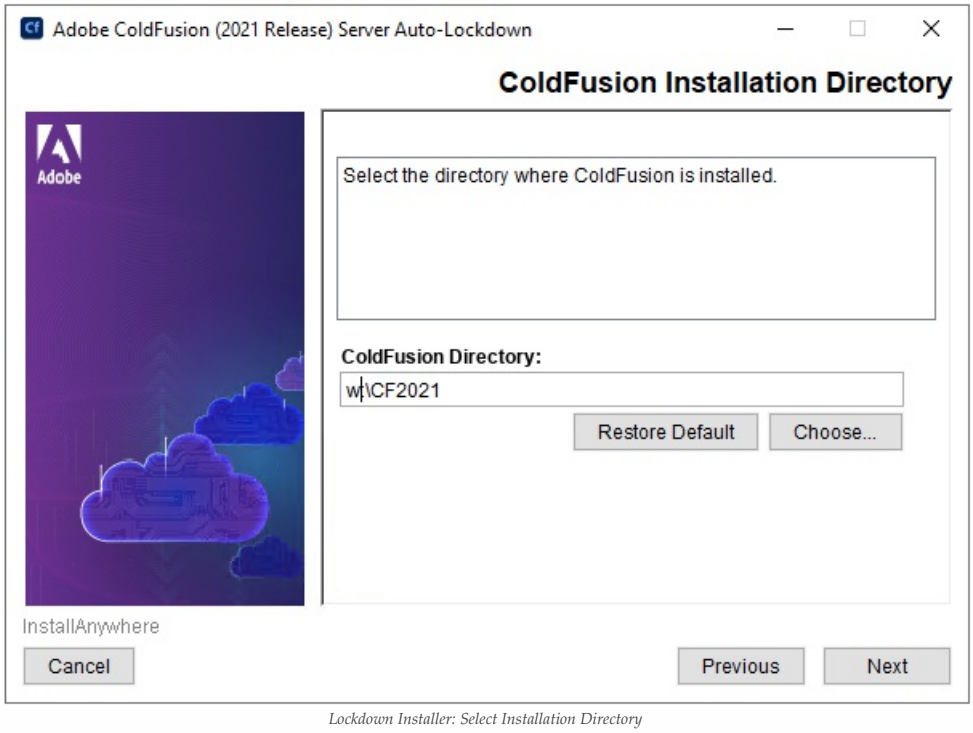
- Connects ColdFusion to the Web Server (wsconfig)
- Sets the ColdFusion Service identity to run as a dedicated account, optionally creates the account for you.
- Sets file system permissions for your web root and ColdFusion installation directory
- Adds Request Filtering Rules to block various URIs
- 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 completed the pre-requisites in the previous section.

Download and run the latest copy of the ColdFusion 2021 Server Auto-Lockdown Tool:
https://www.adobe.com/support/coldfusion/downloads.html

2.6.1 Lockdown Installer: ColdFusion Installation Directory

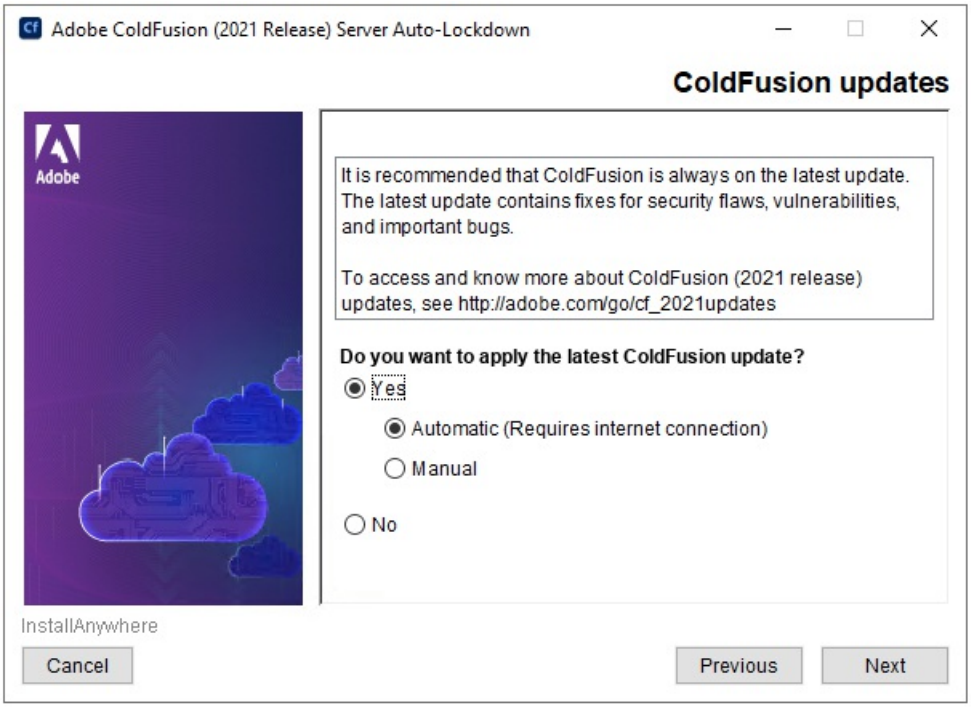
Choose the directory that ColdFusion was installed to.



Lockdown Installer: Select Installation Directory

2.6.2 Lockdown Installer: ColdFusion Updates

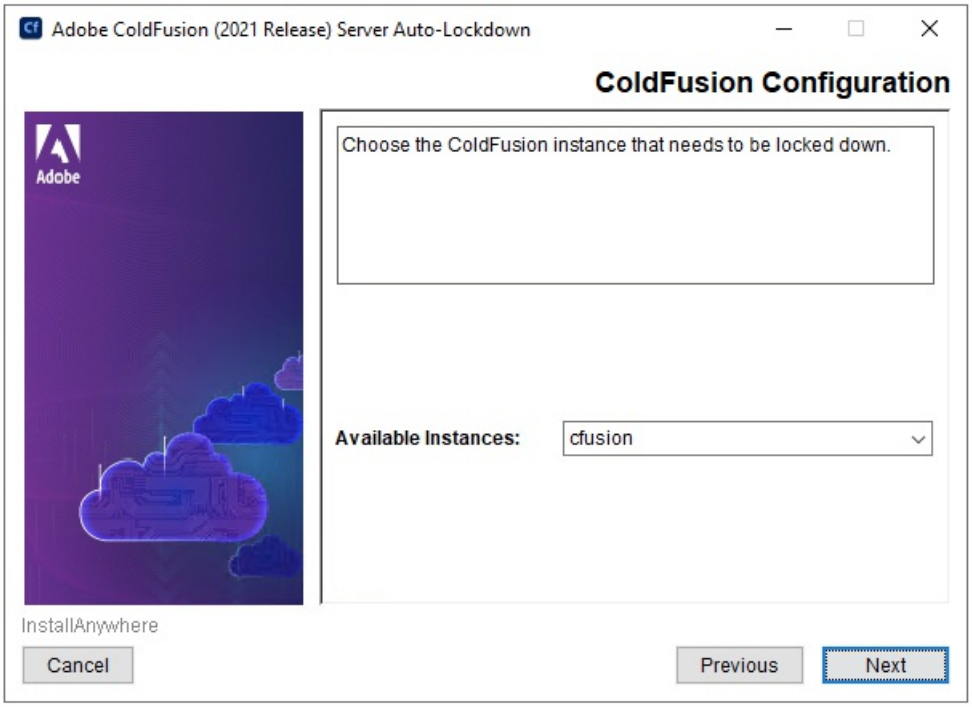
Choose *Yes* / *Automatic* to ensure that ColdFusion has been updated to the latest hotfix. Adobe recommends that you install ColdFusion updates before running the Lockdown tool.



Lockdown Installer: ColdFusion Updates

2.6.3 Lockdown Installer: ColdFusion Configuration

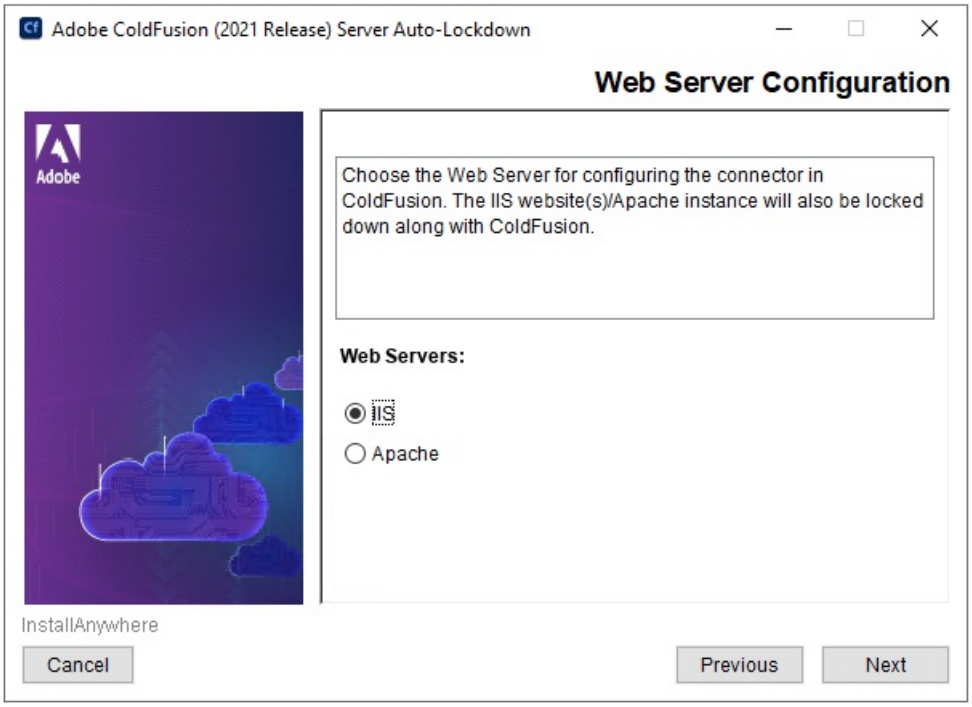
Select the instance that you want to lockdown.



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.

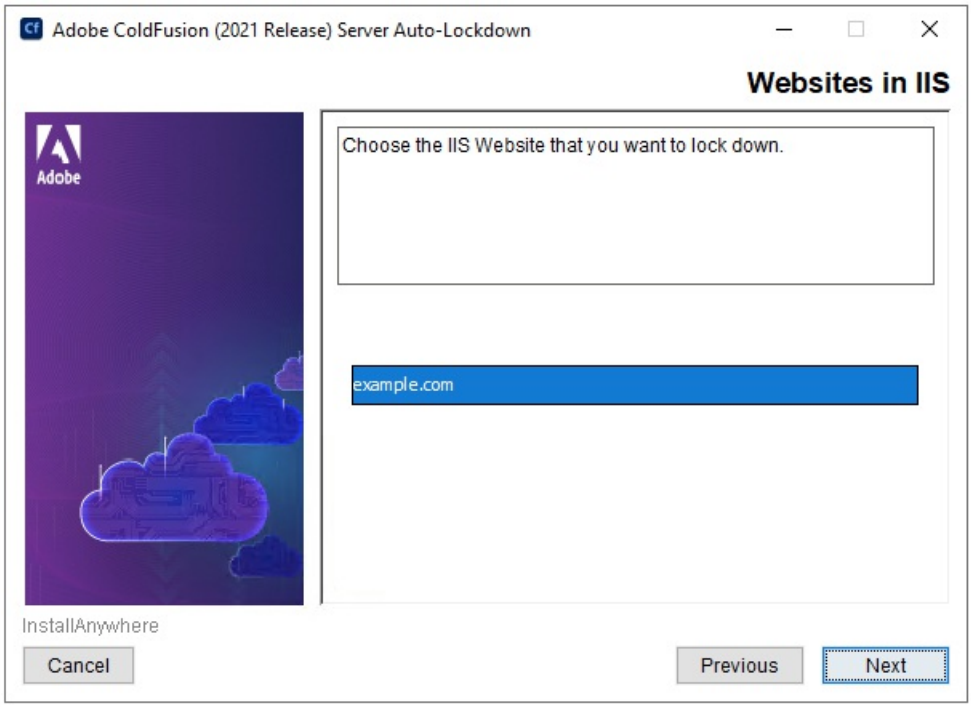


Lockdown Installer: Web Server Configuration

2.6.5 Lockdown Installer: Websites in IIS

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

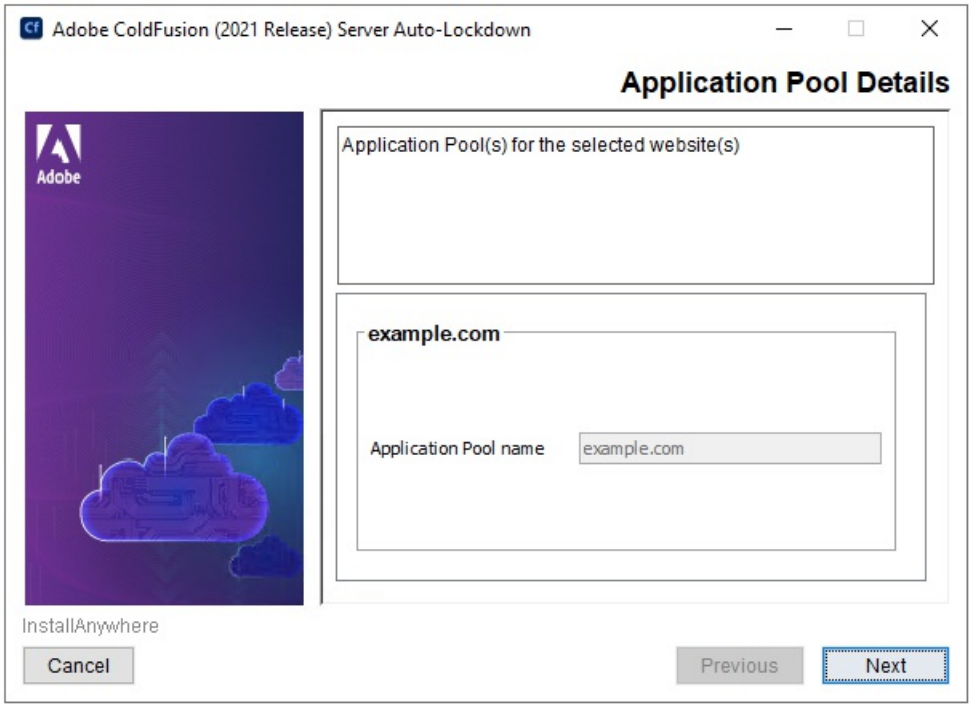
> Tip: you can hold shift or ctrl when clicking to select sites



Lockdown Installer: Websites in IIS

2.6.6 Lockdown Installer: IIS Application Pool Detail

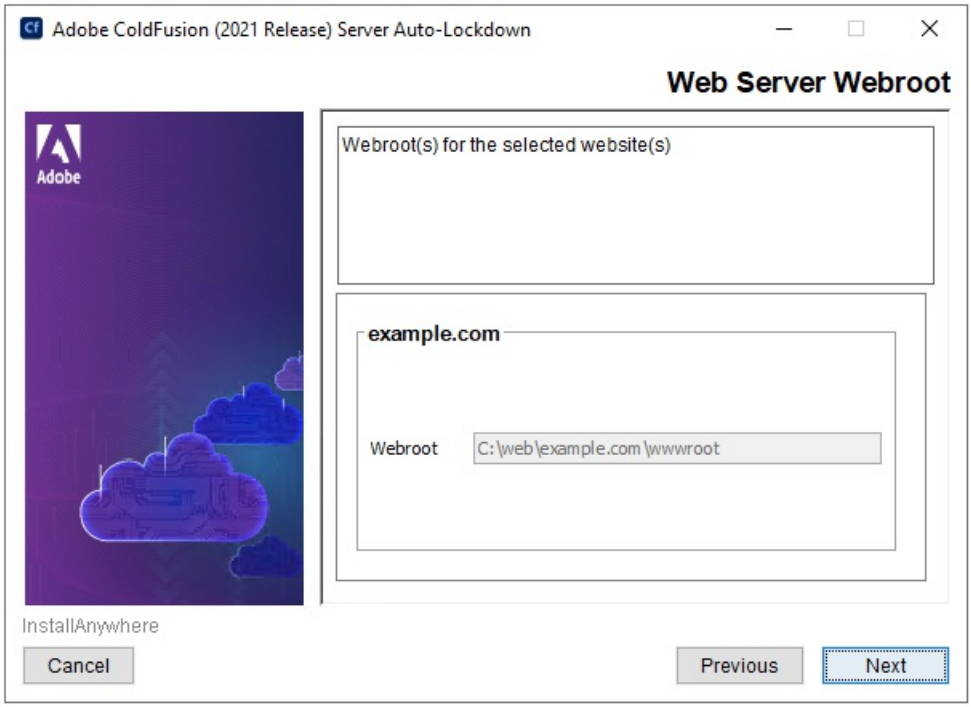
Verify that the application pool names are correct for each the website.



Lockdown Installer: IIS Application Pool Detail

2.6.7 Lockdown Installer: IIS Websites Webroot Detail

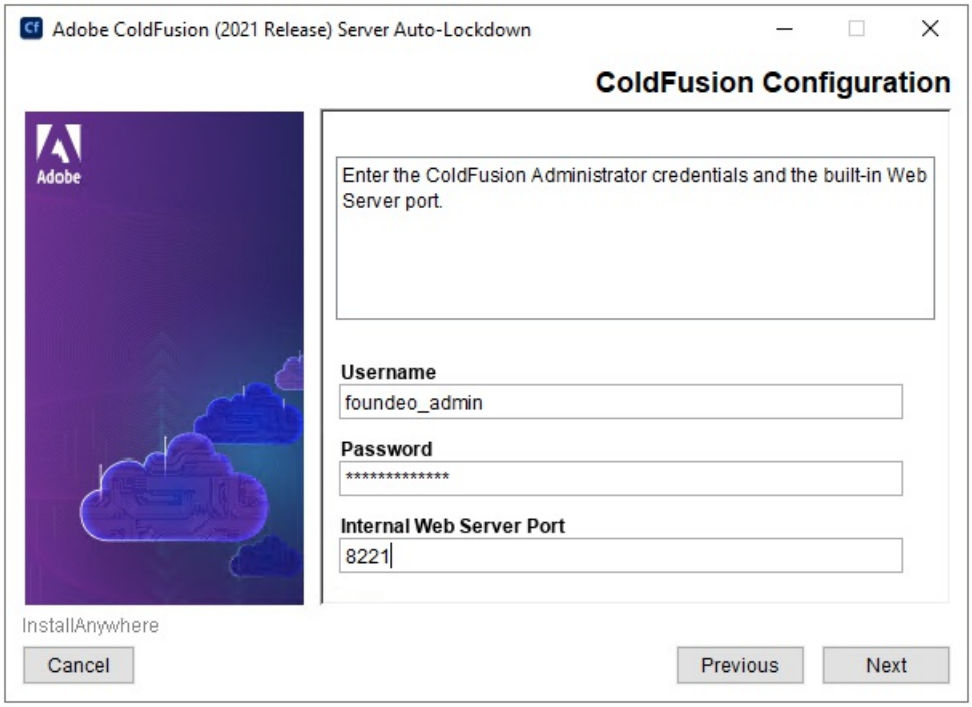
Verify that the web root paths are correct for each website.



Lockdown Installer: IIS Websites Webroot Detail

2.6.8 Lockdown Installer: ColdFusion Administrator Configuration

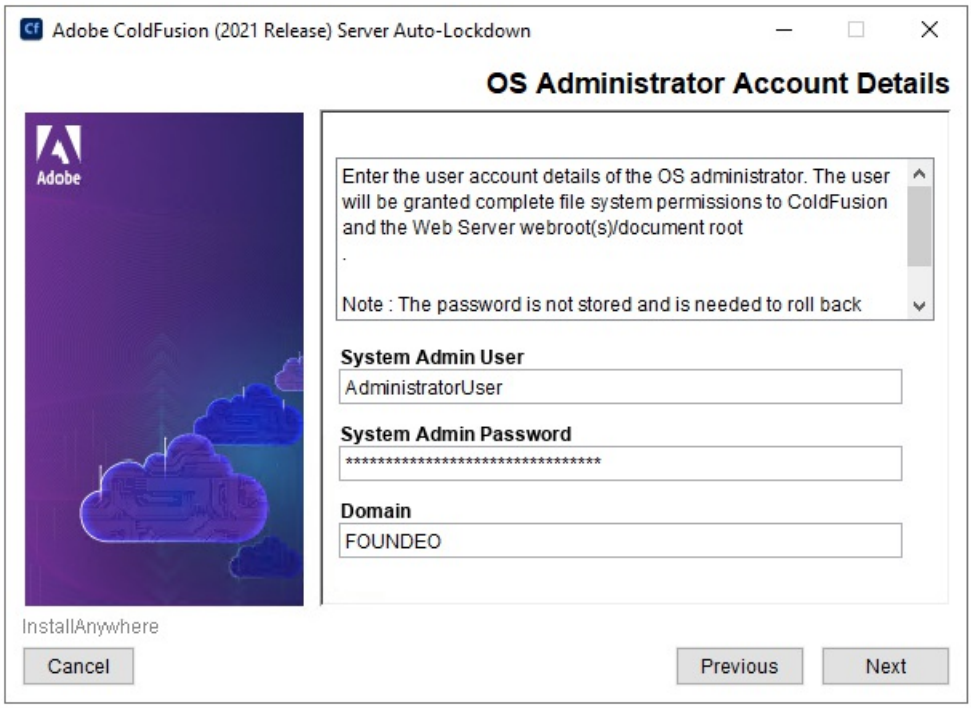
Enter the ColdFusion Administrator username and password specified during the ColdFusion Installation. Also ensure that the builtin web server port is correctly specified (default port is 8500).



Lockdown Installer: ColdFusion Administrator Configuration

2.6.9 Lockdown Installer: OS Administrator Account Details

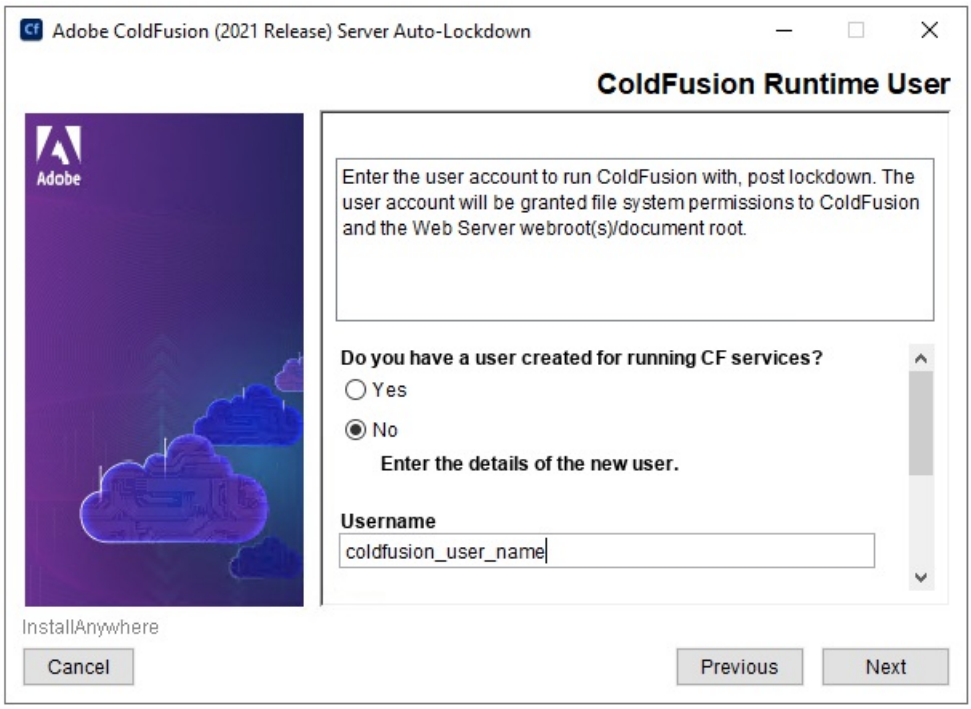
Enter the Administrator username, password and server name or domain.



Lockdown Installer: IIS Websites Webroot Detail

2.6.10 Lockdown Installer: ColdFusion Runtime User

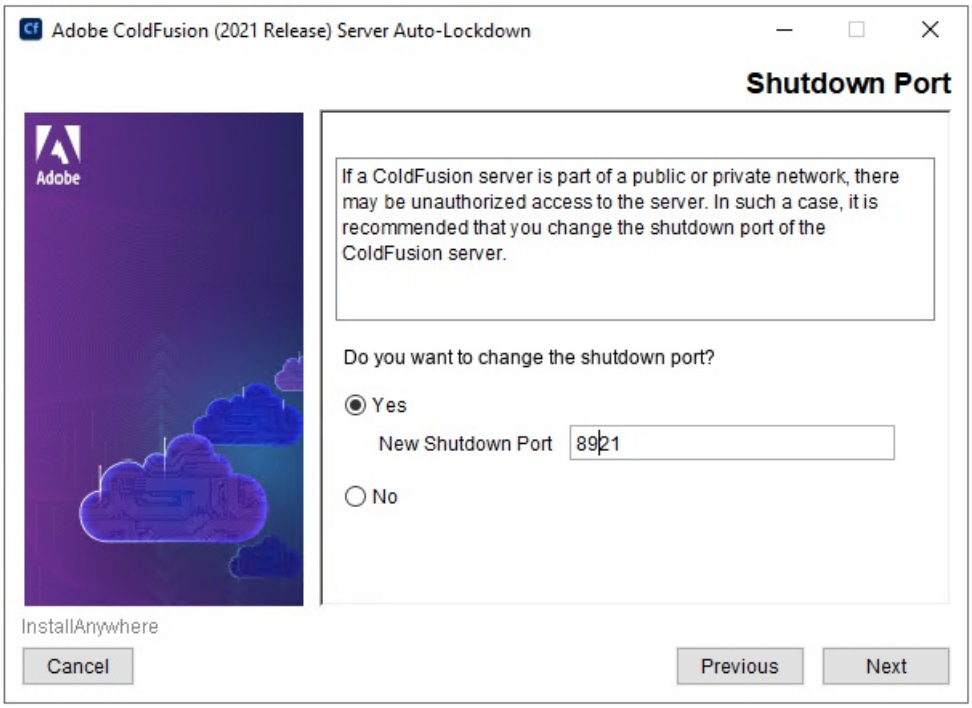
Create a unique username for the user account that ColdFusion will run as. Specify the domain, and a strong password.



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.

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.

You may also check the box *User Cannot Change Password* on the *General* tab of the User Properties window.

2.6.14 Request Filtering

The Lockdown Tool will replace the `/cf_scripts` mapping with a randomly generated URI. However the URI `/cf_scripts` should still be blocked at the web server level.

Add `/cf_scripts` as a *Deny Sequence* to the Request Filtering in the URL tab. Consider blocking additional URIs discussed in the Additional Lockdown Measures section.

2.6.15 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

> **Picking the correct version** As of this writing Java 11 is the latest supported LTS release of Java. Java 9, 10, 12, 13, 14 and 15 are all non LTS versions and are only supported for a short time (6 months). Learn more here: https://www.petefreitag.com/item/911.cfm

Download the latest LTS version of Java from https://www.adobe.com/support/coldfusion/downloads.html that ColdFusion 2021 supports (Java 11 at the time of this publication). Select the java zip distribution and download.

> Tip: Verify the checksum by running powershell: `Get-FileHash jdk-11.0.9_windows-x64_bin.zip -Algorithm sha256`

Extract the java zip file you download to a permanent location, for example `C:\Java\jdk-11.0.9\`

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-11.0.9\`

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 Disable Unused Services

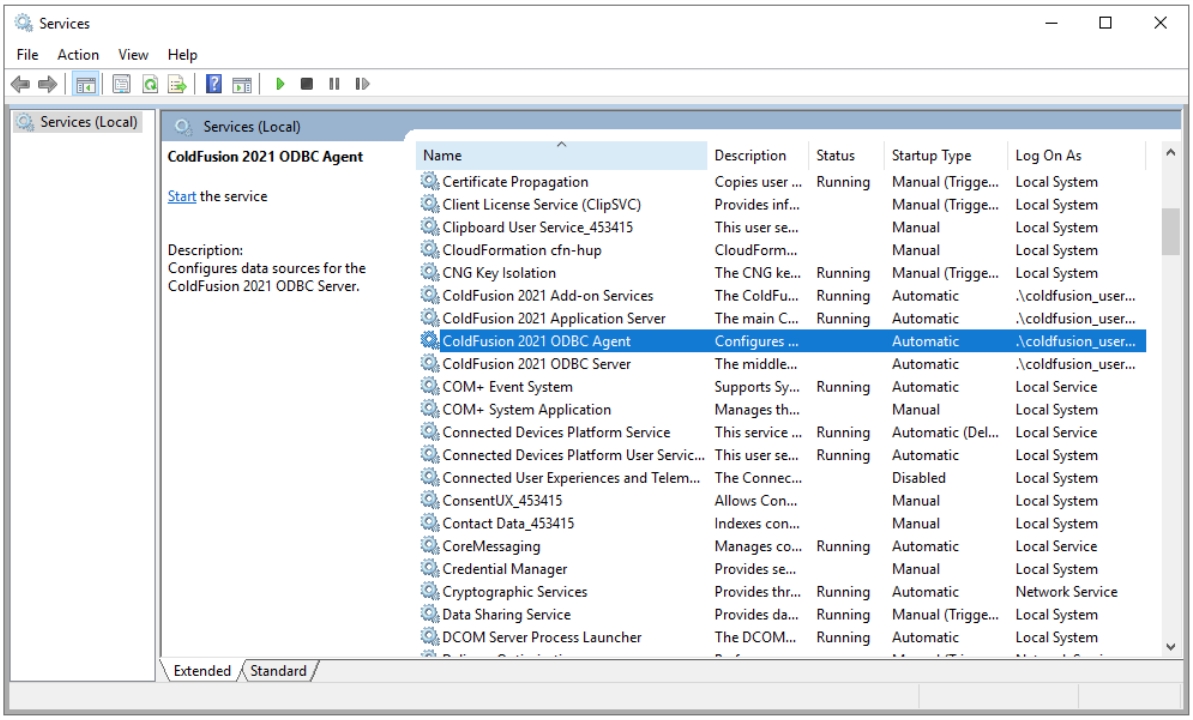
Open the Windows *Services* Application. Review each service, and disable any services that are not used.

- **ColdFusion 2021 Application Server** - this is the primary ColdFusion service, this should stay running.
- **ColdFusion 2021 Add-on Services** - this service powers the PDFg Service (`cfhtml2pdf` tag), as well as Solr Service (`cfsearch`). If you do not use these features you may disable this service.
- **ColdFusion 2021 ODBC Agent** - this can be disabled in most cases, only necessary if you have Microsoft Access ODBC datasources. Most datasources will use a JDBC driver (SQL Server, Oracle, MySQL, etc) not ODBC.
- **ColdFusion 2021 ODBC Server** - this can be disabled in most cases, only necessary if you have Microsoft Access ODBC datasources.

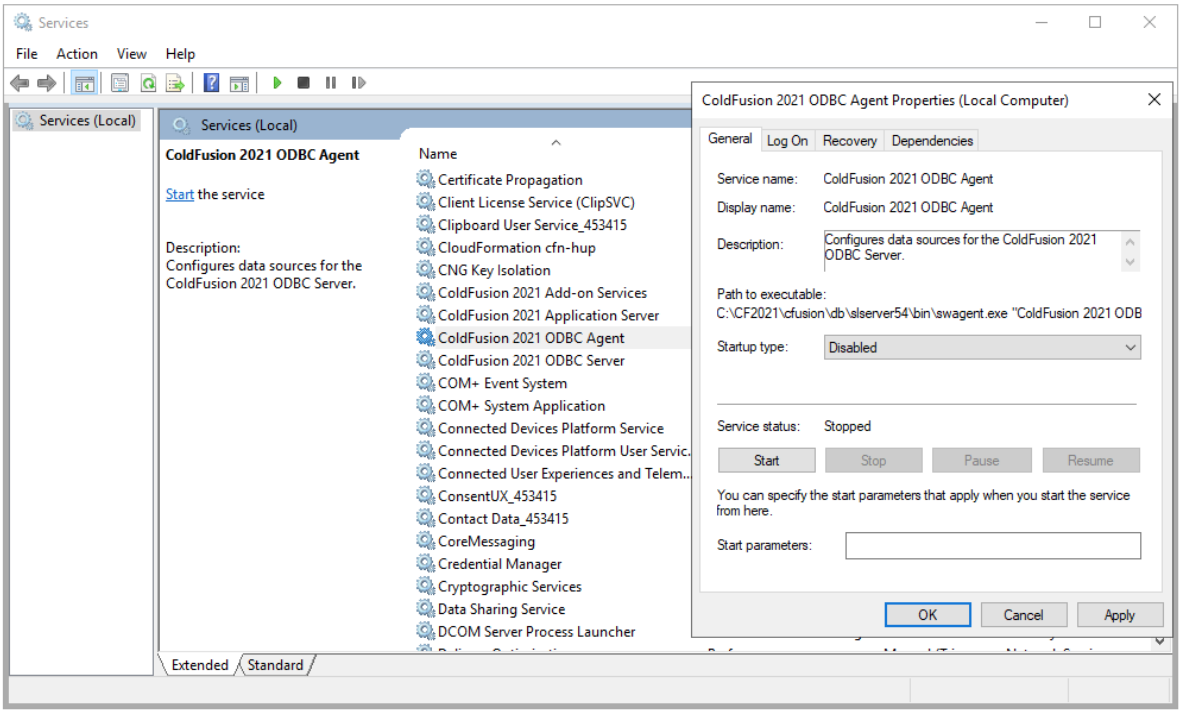
Most datasources will use a JDBC driver (SQL Server, Oracle, MySQL, etc) not ODBC.

- **ColdFusion 2021 .NET Integration Service** - this service allows integration with .NET classes via the `cfobject` tag or `createObject()` function. If you do not use this integration and the service is installed set the startup type to disabled.

To disable a service, right click on it in the Services list, select *Properties* then set the *Startup Type* to *Disabled*. If the service is running, hit the *Stop* button.



Lockdown Installer: ColdFusion Runtime User



Lockdown Installer: ColdFusion Runtime User

Verify that each ColdFusion service is set to *Log On As* the user account that was specified in the Auto-Lockdown tool.

Test your application again to ensure it is still working properly after making changes.

2.7.4 Update JVM for ColdFusion Add-on Services

If you disabled the *ColdFusion 2021 Add-on Services* service in the previous step, or you did not install it, skip to the next step.

The ColdFusion 2021 Add-on Services is used for Solr (`cfsearch`, `cfcollection`, `cfindex`) or the PDF Service (`cfhtmltopdf`) and runs in a separate process from the *ColdFusion 2021 Application Server* service. The *Add-on Services* will use the JVM that was shipped with ColdFusion `{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:\\CF2021\\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 2021 Add-on Services* service.

Test your sites again.

For additional information on updating the JVM please see:

https://www.petefreitag.com/item/860.cfm

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

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

3 ColdFusion Package Management

The ColdFusion 2021 release includes a new package management system. Packages can be installed, updated or removed from either the ColdFusion Administrator or a commandline `cfpm` utility located in the `{cf.home}/bin/` directory. Packages contain optional features of the ColdFusion server.

When you install ColdFusion using the Windows GUI installer, all packages are installed by default. When you install from a zip file using the `cfinstall` utility only required packages are installed.

3.1 Package Management From a Security Perspective

From a security perspective you should make sure that the packages you have installed are updated to the latest version.

You will also want to make sure that you remove or uninstall any packages that your application does not require. This reduces the potential attack surface of your server should a vulnerability exist in one of the packages.

3.2 Listing Installed Packages

Locate the `cfpm.bat` (Windows) or `cfpm.sh` (Linux) in the `{cf.home}/bin/` directory and execute it to start a new cfpm cli session. If it loads properly you should have a prompt:

```
cfpm>
```

At the prompt type `list` and hit enter. Type `quit` to exit.

If you prefer a GUI, you can view the list of installed packages in the ColdFusion Administrator by clicking on the *Package Manager* icon.

3.3 Update Installed Packages

Using the `cfpm` cli run the command `update packages` to update all installed packages to the latest version.

If any packages were updated, test your applications again.

3.4 Remove Unnecessary Packages

The `cfpm` tool has a code scanner which can determine which packages are required to run the given code. The scanner also takes into account certain ColdFusion Administrator settings, such as datasources to determine which database drivers are required.

3.4.1 Scan Code for Required Packages

Run the `cfpm scan` command to scan your application source code to determine what packages are required:

```
cfpm> scan /path/to/code/ http://127.0.0.1:8500
```

Where `/path/to/code/` is a file system path pointing to the source code, and `http://127.0.0.1:8500` is the path to your builtin web server. The output of the above command will be a list of package names that `cfpm` finds to be required by your code.

Compare the list of installed packages (`cfpm list`) with the list of packages required by the code. You can uninstall any packages that may be installed but are not required by your code.

3.4.2 Removing Installed Packages

Remove any unnecessary packages by running:

```
cfpm> uninstall packageName
```

Where `packageName` is the name of the package you wish to remove. If you only require a small number of packages and have many installed you can uninstall all packages by running:

```
cfpm> uninstall all
```

Then add necessary packages:

```
cfpm> install adminstrator,sqlserver
```

> You may need to restart your ColdFusion server for some package installations to be completed. The tool will indicate this in the output.

Restart ColdFusion and test your applications again.

4 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.

4.1 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: `<cfsetting requesttimeout="60">`
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.
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 to be enabled. 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.
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.

Setting	Suggestion	Additional Info
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 fully 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	*/not-default/*	Because the scripts directory also contains CFML source code, you should create a virtual directory / alias at a non-default location. The default values are `/cf_scripts/scripts` or `/cf2018_scripts` or `/cf2021_scripts` and `/CFIDE/scripts` in prior versions of CF.
Default Maximum Thread Count For Parallel Functions	Tuned	Set to 1 if not using parallel functions
Allowed file extensions for CFInclude tag	cfm	This setting restricts the file extensions which get compiled (executed) by a `cfinclude` tag. Any file file extensions not matching this list are statically included, any CFML source code would not be executed. Take care to ensure that you have specified any file extensions of files that contain CFML code and are included with `cfinclude`. This setting was added in CF2018 Update 3. It can be defined at an application level as well via `this.blockedExtForFileUpload`. If your code also uses the `.cfml` file extension to `cfinclude` files, then set to `cfm,cfml`.
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, cfc, etc) are specified as a comma separated list. You can use `:empty-extension` to block file uploads without an extension. This setting can be defined at an application level as well.
Application.cfc/Application.cfm lookup order	*Depends on Application*	Consult with developers to select the best setting that works for your Application layout. If your Applications only have `Application.cfc` or `Application.cfm` files in the web root, then set to *In webroot*.
Executor Pool: Core Pool Size	Tuned	If you do not use the async features set to 1, otherwise tune the value based on avaliable CPU threads.
Executor Pool: Maximum Pool Size	Tuned	If you do not use the async features set to 1, otherwise tune the value based on available CPU threads.
Azure Service Bus: Core Pool Size	Tuned	If you do not use the Azure Service Bus set to 1, otherwise tune the value based on available CPU threads.
Azure Service Bus: Maximum Pool Size	Tuned	If you do not use the Azure Service Bus set to 1, otherwise tune the value based on available CPU threads.
Missing Template Handler	Custom Template	The missing template handler HTML output should be equivalent to the 404 error handler specified on your web server.

Setting	Suggestion	Additional Info
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
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 `/rest/_api_listing` or `/api/_api_listing` to allow the ColdFusion API manager to get a listing of REST apis. ColdFusion Administrator authentication is required.
Enable mobile's server workflow	Unchecked	Use of this feature should be carefully considered on production servers. The mobile key is accessible to the client, making it difficult to protect.
Enable CORS	Unchecked	When this checkbox is checked it will add the following HTTP response headers: `Access-Control-Allow-Origin: *`, `Access-Control-Allow-Headers: Content-Type, Access-Control-Allow-Headers, Authorization, X-Requested-With` and `Access-Control-Allow-Methods: GET, OPTIONS, HEAD, PUT, POST` to all CFML responses. This in most cases is overly permissive (allows cross site requests on all origins), use the web server or CFML application logic to send these response headers.
Mobile server context	Non default	If you have *Enable mobile's server workflow* checked, set the mobile server context value to a non default (not `/cfmobile`) value.

4.2 Server Settings > Request Tuning

The Request Tuning settings can mitigate the impact Denial of Service (DOS) attacks against your server.

Setting	Suggestion	Additional Info

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 `access=remote` specified, when they are invoked via a HTTP request, for example: `/example.cfc?method=MethodName`. The ColdFusion AJAX proxy uses this method to invoke CFCs. If your applications do not make use of this feature set to 1. Otherwise use load testing to find the optimal value for this setting.
Maximum number of simultaneous Report threads	1	Keep at 1 unless using `cfreport` heavily.
Maximum number of threads available for CFTHREAD	1 if not using `cfthread`, tuned otherwise	
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.

4.3 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.
Redis Cache Settings Password	Specified if used	If you have a Redis Server specified, ensure that the server is configured to require a password.

4.4 Server Settings > Client Variables

Setting	Suggestion	Additional Info

Setting	Suggestion	Additional Info
Default Storage Mechanism for Client Sessions	None / Cookie	Set to `None` if possible. When 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. Client variable values stored in cookies can be tainted so they should not be used for sensitive variables. Use session variables instead.

4.5 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.
Default Timeout: Session Variables	20 minutes or less	Twenty minutes is a good default value, however applications requiring a high level of security 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.
Cookie Samesite default value	lax or strict	The strict option is the most secure, the lax option still improves security but compromises by relaxing some restrictions to improve usability. Avoid using none, as this may make your applications more susceptible to CSRF attacks.

4.6 Server Settings > Mappings

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

4.7 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*

4.8 Server Settings > WebSocket

Disable the WebSocket Service if you do not use the `cfwebsocket` tag.

4.9 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.

4.10 Data & Services > Data Sources

Remove the example data sources if they are defined: `cfartgallery`, `cfbookclub`, `cfcodeexplorer`, `cfdocexamples`.

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 *Timeout Requests after* setting.
Query Timeout (seconds)	Not `0`	Specify an upper limit to mitigate DOS attacks.
Allowed SQL	Enable only operations required by the application, eg `SELECT`, `INSERT`, `UPDATE`, `DELETE`	The CREATE, DROP, ALTER, GRANT, and REVOKE operations are not commonly required in web applications.

4.11 Data & Services > NoSQL Data Sources

Consider enabling TLS/SSL, and avoid setting the Auth Mechanism to NONE.

4.12 Data & Services > ColdFusion Collections

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

4.13 Data & Services > Solr

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

Consider running the Solr service on an external server and a non default port for additional isolation.

4.14 Data & Services > Rest Services

Consider changing the default Rest Path to something other than `/rest/` or block the default path on your web server if you do not use

ColdFusion REST services.

4.15 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.

Consider running the PDF service on an external server and a non default port for additional isolation.

4.16 Data & Services > Cloud Credentials

In the *Cloud Credentials* page of the ColdFusion Administrator you can create an alias that references an AWS or Azure Cloud credential. The credentail alias is used by the `getCloudService(cloudCred, cloudConfig)` function as the `cloudCred` argument. The `cloudCred` can also be passed as a structure.

Servers running directly on AWS or Azure should consider assigning Roles to the server instance. For example in AWS you can assign an IAM role to an EC2 instance. The instance will be granted temporary credentials at boot which will be granted to the role assigned. To use the Azure/AWS IAM instance role you will need to pass a structure to the `getCloudService()` function with credentials obtained from the Azure/AWS metadata service.

4.17 Data & Services > Cloud Configuration

The *Cloud Configuration* administrator allows you to define configuration for specific cloud services.

4.17.1 AWS Specific Cloud Configuration

The following configuration options exist for all AWS service types:

Setting	Suggestion	Additional Info
API Call Attempt Timeout	Specified	Generally this value should be less than the default request timeout.
API Call Timeout	Specified	Generally this value should be less than the default request timeout.
Connection Acquisition Timeout	Specified	Generally this value should be less than the default request timeout.
Connection Max Idle Time	Specified	Appropriate value based on the heuristics of the application. If cloud services are only used for infrequent background processing then a lower value can be used.
Connection Timeout	Specified	Depends on the latency of the network connection from your server to the cloud services. A few seconds should be appropriate in most cases.
Connection Time to Live	Specified	Appropriate value based on the heuristics of the application. If cloud services are only used for infrequent background processing then a lower value can be used.
Socket Timeout	Specified	Depends on the latency of the network connection from your server to the cloud services. A few seconds should be appropriate in most cases.
Max Connections	Specified	Tuned based on the number of available CPU threads, and feature usage.
Retry Policy	4	Avoid excessively high values.

4.17.2 AWS S3 Cloud Configuration

These configuration settings apply to AWS S3 Cloud Configurations.

Setting	Suggestion	Additional Info
Path Style Access Enabled	Unchecked	Path Style access to S3 buckets has been deprecated by AWS, so it should be avoided.
Accelerate Mode Enabled	-	Enable only if you have S3 bucket acceleration enabled for the bucket.
Dual Stack Enabled	-	Enable only if your network supports IPv6
Checksum Validation Enabled	Checked	Checksum validation will ensure that both the client (ColdFusion) and the server (AWS S3) agree that the contents of the transferred file match.
Chunked Encoding Enabled	Checked	Chunked encoding may use less disk i/o resources, test to determine which is more optimal.

4.17.3 Azure BLOB Cloud Configuration

These configuration settings apply to Azure BLOB Cloud Configurations.

Setting	Suggestion	Additional Info
Concurrent Request Count	Specified	Set an upperbound reasonable for your application heuristics and server CPU capabilities. Unless you are doing asynchronus or multithreaded programming the value should not be higher than the maximum number of simultaneous requests.
Timeout Interval (ms)	Specified	Generally this value should be less than the default request timeout.
Maximum Execution time (ms)	Specified	Generally this value should be less than the default request timeout.
Use Transactional Content	Checked	Check to enforce Content-MD5 header.
Disable content validation	Unchecked	Use the Content-MD5 header.
Store Blob Content	Checked	Use the Content-MD5 header on Uploads.
Absorb Conditional Errors on Retry	Unchecked	Unchecked to prevent suppression of errors.
Skip Etag Locking	Unchecked	Don't skip etag validation.
Enable Logging	Checked	Consider enabling logging if appropriate for your application.

4.17.4 Azure Service Bus Cloud Configuration

These configuration settings apply to Azure Service Bus Cloud Configurations.

Setting	Suggestion	Additional Info
Operation Timeout	Specified	Generally this value should be less than the default request timeout. Tune as appropriate / acceptable for your applications.

4.17.5 Cloud Configuration Retry Policies

Many of the Cloud Configurations allow you to specify retry policies in the event that a connection to the service fails. Ensure that the retry policy selected is not going to cause a cascading downtime in the event that a cloud service is experiencing downtime or high latency.

4.18 Debugging & Logging > Debug Output Settings

Setting	Suggestion	Additional Info

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.

4.19 Debugging & Logging > Developer Profile

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

4.20 Debugging & Logging > Debugger Settings

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

4.21 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.
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.

4.22 Debugging & Logging > Remote Inspection Settings

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

4.23 Event Gateways > Settings

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

4.24 Event Gateways > Gateway Instance

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

4.25 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.

4.26 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`.

4.27 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.

4.28 Security > User Manager

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

4.29 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.

4.30 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.

4.31 Security > IDP Configuration

IDP Configuration is used for configuring SAML Identity Providers allowing your ColdFusion applications to act as a SAML SP (service provider). Requests to / from the SAML IDP should be signed and encrypted.

Ensure that Sign Requests is checked.

Ensure that all URLs use HTTPS.

4.32 Security > SP Configuration

Requests to / from the SAML SP should be signed.

Ensure that *Sign Requests*, *Want Assertions Signed*, and *Logout Response Signed* are all checked.

If you have multiple ColdFusion servers, or multiple instances acting as a SAML SP make sure that the *Request Store* cache used is shared among all servers to avoid Replay Attacks.

Ensure that the *ACS URL* and the *SLO URL* use HTTPS.

4.33 Package Manager > Packages

See the section ColdFusion Package Management for guidance.

4.34 Package Manager > 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.

5 Additional Lockdown Measures

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

5.1 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.

5.2 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="TLSv1.3" />
```

Be sure to replace `{cf.root}` with the path to your ColdFusion installation root (eg `C:\ColdFusion2021`) and `{your.password}` with the value you specified when you generated your certificate. Consider changing the port `8443` to a non default value.

The `sslProtocol` in the example above is set to `TLSv1.3`, this requires a modern http client/browser to connect to the ColdFusion administrator. Additionally `TLSv1.3` requires a JVM that implements the protocol (typically found in Java 11+). You could use `"TLSv1.2"` or `"TLSv1.3,TLSv1.2"` instead if necessary.

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

5.3 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.

5.4 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`

5.5 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.

5.6 Lockdown the ColdFusion Add-on Services

If you installed the ColdFusion 2021 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/

5.7 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.

5.7.1 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.

5.7.2 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.

5.7.3 File Extension Allow Listing on IIS

A more robust solution is to specify an allow list of allowed file extensions, any file extension not in the list would be blocked. 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.

5.8 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
`/connector` `/pms` `/__cf_connector_heartbeat__`	Used by the Performance Monitoring Toolkit
`/CFFileServlet`	Serves dynamically generated assets. It supports the `cfreport`, `cfpresentation`, `cfchart`, and `cfimage` (with `action=captcha` and `action=writeToBrowser`) tags. If you are not using those tags then you can block this endpoint.
`/rest/` `/api/` `/restapps/` `/cfapiresources/`	Used for CFML Rest Web Services implemented through CFCs.

URI	Description
`/Application.cfm`	Direct requests to Application.cfm or cfc cause an error to be thrown, so you may wish to block that at the web server level.
`.env` `box.json` `server.json` `testbox` `rewrites.xml`	Additional paths which may contain configuration or non production assets. These paths should be safe to block on production servers.

The Auto-Lockdown Tool will block the following URIs:

- `/Application.cfc`
- `/WEB-INF`
- `/cfformgateway`
- `/flex2gateway`
- `/cfform-internal`
- `/flex-internal`
- `/WSRPProducer`
- `/JSDebugServlet`
- `/securityanalyzer`
- `.svn`
- `.git`
- `/CFIDE`
- `/jakarta`

5.8.1 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.

5.8.2 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.

5.9 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.

5.10 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`.

5.11 Disable Unused Servlet Mappings

All JEE web applications have a file in the `WEB-INF` directory called web.xml that 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 (most do not have any).
`*.cfr` `*.CFR` `*.Cfr`	`CFCServlet`	Used for `cfreport`, can be commented out if the `cfreport` tag is not used.

Servlet Mapping	Servlet	Purpose
`/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. Keep this mapping.
`/cfmobile/*`	`CFMobileServlet`	Used for `cfclient`
`/pms` `/connector/*`	`PMSGenericServlet`	Used by the Performance Monitoring Toolset
`/mcs/*`	`ModulesCodeScannerServlet`	Used by the `cfpm` code scanner
`/__cf_connector_heartbeat__`	`Connector`	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.

ColdFusion 2021 removed several servlets and servlet mappings related to Flash Remoting and Flash Forms:

- `/CFFormGateway/*`
- `/cfform-internal/*`
- `*.cfswf`
- `*.as` `*.sws` `*.swc`
- `/flashservices/gateway/*`
- `/flex-internal/*`
- `*.mxml`
- `/flex2gateway/*`

The above mappings should not be in the `web.xml` by default.

5.12 Additional Tomcat Security Considerations

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

5.13 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.

5.14 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 SAMEORGIN. You can add a filter-mapping in web.xml to enable these filters for a given URI, this functionality could also be accomplished at the web server level.

5.15 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.

5.15.1 Allow Listing 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.

5.15.2 Allow Listing 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*.

5.16 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>
```

5.17 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.

5.17.1 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*.

5.17.2 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`.

5.18 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: https://coldfusion.adobe.com/setting-up-coldfusion-in-distributed-envionment/

5.19 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`

5.19.1 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.

5.19.2 Adding HTTP Response Headers in Apache

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

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

6 ColdFusion Lockdown on Linux

This section covers installation of ColdFusion on Red Hat Enterprise Linux 8 with Apache. To install ColdFusion 2021 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

6.1 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 8 *Managing and Monitoring Security Updates* Guide: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/managing_and_monitoring_security_updates/index
- Read the Red Hat Enterprise Linux 8 *Security Hardening* Guide: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/index
- 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/8/html/using_selinux/index 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`
- You will need to know how to edit text files on linux, for example using `vi` or `nano`
- 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 from a shell: `md5sum installer-file-name.bin`

6.2 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.

6.3 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.
- **Access Add-on Services Remotely**: If you selected the *PDFG* or *Solr Service* sub-components the ColdFusion 2021 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/cf2021/`, however you should select a unique path.
- **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 cf2021 start
```

6.4 Access ColdFusion Administrator via a SSH Tunnel

It can be useful to create a temporary SSH tunnel when you need to connect to the ColdFusion Administrator. As of ColdFusion 2016 and up the ColdFusion Administrator is no longer accessible via the Apache web server.

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).

6.5 Install ColdFusion Hotfixes

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

Click on **Package Manager > Core Server > Check for 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):

```
java -jar /opt/cf2021/cfusion/hf-updates/hotfix_XXX.jar
```

Consult the *ColdFusion Hotfix Installation Guide* for troubleshooting hotfix installation issues:
https://coldfusion.adobe.com/2012/12/coldfusion-hotfix-installation-guide/

6.6 Install and Configure Apache Web Server

6.6.1 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
```

6.6.2 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`.

6.6.3 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` (typically located in `/etc/httpd/conf/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>
```

> Note: We are using `/www` here as a *catch all* path for all of our web root directories. If you have any files under `/www` that apache

> should not be allowed to serve, then you should add a `<Directory>` block for each web root.

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` file. If you are following along, then it should output: `Hello`.

6.6.4 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
```

6.7 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 cf2021 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: `/www/`
- **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` or `/cf2021_scripts`
- **Shutdown Port** - change the shutdown port to a non-default value.

Review the Lockdown Tool logs in `/opt/cf2021/lockdown/cfusion/Logs` (path may differ), and ensure that it states *ColdFusion Server has been locked down successfully* and that there are no errors.

6.7.1 Test the web server

The lockdown tool will connect ColdFusion to the Apache web server. Test a `.cfm` page to make sure it is working.

6.7.2 Troubleshooting the CF / Apache Connector

Test a static file (eg txt or html) to make sure that the problem is not

Take a look in the `/opt/cf2021/config/wsconfig/1/mod_jk.log` file.

If you see the following message , the problem could be one of a few scenarios:

```
(cfusion) Failed opening socket to (::1:8020) (errno=111)
(cfusion) connecting to backend failed. Tomcat is probably not started or is listening on the wrong
port (errno=111)
```

See the following sub sections for possible solutions.

6.7.2.1 Make sure CF is running

First it could be simply that ColdFusion is not running, you can check to see if it is running by issuing a `ps -aux` command or by running `service cf2021 status`. You can start CF by running: `service cf2021 start`

Though it may not be necessary, you can also restart apache `service httpd restart`. Test your cfm file again to see if the problem persists.

6.7.2.2 Use IPv4 instead of IPv6

Second you will notice from the error message above that apache is attempting to connect to `::1:8020`, the `::1` is the IPv6 version of `localhost`. You can the config to use the IPv4 version of `localhost`, which is `127.0.0.1` by editing the `workers.properties` file located in the `/etc/httpd/conf/` directory. Change the line `worker.cfusion.host=localhost` to `worker.cfusion.host=127.0.0.1`

Restart apache `service httpd restart` after making this change and test your cfm file again.

6.7.2.3 Make sure Apache and ColdFusion agree on ports and secrets

In the `workers.properties` file look for a line that starts with `worker.cfusion.port` it will be set to `8020` by default.

Next check the `{cf.home}/runtime/conf/server.xml` file for this port number, eg:

```
grep 8020
```

It should show up in a `<Connector>` tag with `protocol="AJP/1.3"`. The value of the `secret` attribute in the `Connector` tag should also match the value of the `worker.cfusion.secret` property in the `workers.properties` file.

6.7.2.4 Troubleshooting with selinux enabled

If you have selinux enabled, you may be getting a `503` error when attempting to request a cfm file.

You may need to use semanage to enable communication from the web server to tomcat.

Check and see if `semanage` is installed, if not run:

```
yum install policycoreutils-python-utils
```

Next try running:

```
semanage port -a -t http_port_t -p tcp 8020
```

You may get an error: `ValueError: Port tcp/8020 already defined`, this means that selinux already has configured a policy for this port. You can check what is configured by using:

```
semanage port --list | grep 8020
```

It may be already configured as `hadoop_namenode_port_t`, assuming you are not using hadoop, you can run the following to set the type to `http_port_t`:

```
semanage port --modify -t http_port_t -p tcp 8020
```

Restart apache `service httpd restart` after making this change and test your cfm file again.

6.8 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/

6.8.1 Using Oracle Java

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

> **Picking the correct version** As of this writing Java 11 is the latest supported LTS release of Java. Java 9, 10, 12, 13, 14 and 15 are all non LTS versions and are only supported for a short time (6 months). Learn more here: https://www.petefreitag.com/item/911.cfm

For example, to download using curl:

```
curl https://example/jdk-11.0.xx_linux-x64_bin.rpm -o ./jdk-11.0.xx_linux-x64_bin.rpm
```

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 2021.

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

> **Tip:** You will need to update Java frequently, Oracle typically releases security patches for Java on a quarterly basis. Third party tools such as https://hackmycf.com/ can help to keep you up to date.

6.8.2 Updating ColdFusion to use a new JVM Path

Locate the `jvm.config` file, (by default it is located in `/opt/coldfusion2021/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/cf2021/jre
```

Change the above line to the following:

```
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.

6.8.3 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/cf2021/jre"
```

And update it to:

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

6.9 Auditing

The Auto Lockdown Tool runs a command similar to this to enable auditing using `auditd` of file writes on the ColdFusion:

```
auditctl -w /opt/cf2021 -p wax -k ColdFusion
```

The above will audit all write, attribute change and execute operations on the path `/opt/cf2021/` and tag all entries with the filter key `ColdFusion`.

You can query the audit log using the filter key with:

```
ausearch -k ColdFusion
```

You may notice a lot of writes to log files. Placing the log files outside of your CF directory will reduce this noise, or you could configure `auditd` to ignore log folders.

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

6.10 Change umask

The Auto Lockdown Tool attempts to set the umask, however you may see in the lockdown log file: *Can't add UMask as the init file doesn't exist!* https://tracker.adobe.com/#/view/CF-4210967

To add the `umask` manually, 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.

6.11 Additional Lockdown Steps

Read and follow the instructions in the prior sections:

- ColdFusion Package Management
- ColdFusion Administrator Settings
- Additional Lockdown Measures

7 Performance Monitoring Toolset Security Considerations

7.1 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.

Each ColdFusion 2021 server that will be connected to the PMT server will need to have the `pmtagent` package installed. This can be accomplished using the ColdFusion Administrator or the `cfpm` script. See ColdFusion Package Management for details.

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

7.2 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/

7.3 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 2021 servers that are monitored require access to the PMT datastore port.
- If the PMT datastore is only connecting to a ColdFusion server on the same computer, then *Configure PMT Datastore to run on localhost* (see below).

7.4 Run PMT and PMT Datastore as Dedicated User

The *ColdFusion 2021 Performance Monitoring Toolset* service and *ColdFusion 2021 Performance Monitoring Toolset Datastore Service* 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 user 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:\ColdFusion2021PerformanceMonitoringToolset` or `/opt/ColdFusion2021PerformanceMonitoringToolset`).

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 2021 Performance Monitoring Toolset* service to point to your `pmtservice` user. Update the Service Log On Identity for the *ColdFusion 2021 Performance Monitoring Toolset Datastore* service to point to your `pmtservice` user.

Restart both services.

7.5 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:\ColdFusion2021PerformanceMonitoringToolset\jre
```

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

```
java.home=C:\Java\jdk-11.0.XX\
```

7.6 Configure PMT Datastore to run on localhost (if applicable)

If you are only monitoring one ColdFusion Server, and are running the PMT on the same server then you can configure the PMT datastore to run on localhost.

- Backup, then edit `datastore/config/elasticsearch.yml` and update `network.host` to `127.0.0.1`
- Backup, then edit `config/application.properties` and update `datastore.host` to `127.0.0.1`
- Restart both the PMT Service and PMT Datastore service
- Open the PMT Dashboard in your browser to confirm it is still running. If you have already connected your ColdFusion server to the PMT you will need to reconnect it.

7.7 Update the PMT Software

The *Performance Monitoring Toolkit* has its own update mechanism separate from the ColdFusion server hotfix installer. Therefor when ColdFusion server hotfixes are installed, they do not update the *Performance Monitoring Toolkit*.

Open the PMT dashboard in a web browser and navigate to *Settings > Updates*. Click on the *Check Updates* button.

8 API Manager Security Considerations

8.1 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.

8.2 Connect API Manager to IIS

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

8.3 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"
```

8.4 Update the API Manager JVM

Locate the `jvm.config` file in the `bin` directory, backup the file, then change the line:

```
java.home=..\\jre
```

To point to the updated JVM. Note that to use a `\` in the path it must be escaped, as `\\`

> **Note:** At the time of this writing the API Manager does not work with Java 11. The API Manager ships with Java 1.8 and you should use the latest version of Java 1.8 or check to see if Java 11 support has been added. See https://tracker.adobe.com/#/view/CF-4210978 for reference.

8.5 Update the API Manager Software

The *ColdFusion API Manager* has its own update mechanism separate from the ColdFusion server hotfix installer. Therefor when ColdFusion server hotfixes are installed, they do not update the *API Manager* software.

Open the *API Manager Administrator* (http://127.0.0.1:9000/admin/ by default) in a web browser and navigate to *Updates*. Click on the *Check Updates* button.

9 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 2021 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 https://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.

10 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: https://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: https://www.petefreitag.com/item/701.cfm
- HackMyCF.com Remote ColdFusion vulnerability scanner: https://hackmycf.com/
- Fixing Apache (13) Permission Denied 403 Forbidden Errors: https://www.petefreitag.com/item/793.cfm
- Apache Tomcat 8.5 Security Considerations: https://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

11 Reference Tables

11.1 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/`	Deprecated & Unsupported since CF2016
`cfcalendar`	`/cf_scripts/scripts/ajax/`	Deprecated & Unsupported since CF2016
`cfchart`	`/cf_scripts/scripts/ajax/` `/cf_scripts/scripts/chart/`	
`cfclient`	`/cf_scripts/cfclient/`	
`cfdiv`	`/cf_scripts/scripts/ajax/`	
`cffileupload`	`/cf_scripts/scripts/ajax/`	
`cfform`	`/cf_scripts/scripts/cfform.js` `/cf_scripts/scripts/masks.js`	
`cfform format=flash`	`/cf_scripts/scripts/ajax/`	Deprecated since CF11, Unsupported since CF2016
`cfform format=xml`	`/cf_scripts/scripts/ajax/`	Deprecated since CF11, Unsupported since CF2016
`cfgrid`	`/cf_scripts/scripts/ajax/`	
`cfgrid format=applet`	`/cf_scripts/classes/`	Deprecated since CF11, Unsupported since CF2016
`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/`	Deprecated & Unsupported since CF2016
`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, Unsupported since CF2016
`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/`	
`cftree`	`/cf_scripts/scripts/ajax/`	Deprecated & Unsupported since CF2016
`cftree format=applet`	`/cf_scripts/classes/`	Deprecated since CF11, Unsupported since CF2016
`cfwebsocket`	`/cf_scripts/scripts/ajax/`	
`cfwindow`	`/cf_scripts/scripts/ajax/`	

12 Troubleshooting

12.1 ColdFusion cannot write files under the web root

The Auto Lockdown tool grants the user that ColdFusion is running as read only permission to the web root. If you have files or folders that ColdFusion needs to write to, you need to give the ColdFusion user account (eg `cfuser`) write permission.

On Windows, in the file explorer *Right Click* on the folder or file that you want ColdFusion to be able to write to, and select *Properties*. Go to the Security tab and add the ColdFusion user, and grant the desired permissions.

To grant the user `cfuser` write permission (and ownership) of a folder on Linux:

```
chown -R cfuser /www/data-files/
chmod -R u+rw /www/data-files/
```

12.2 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 ColdFusion user account does not have permission to read the file.

12.3 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+).

12.4 Help Installing ColdFusion Hotfixes

Consult the *ColdFusion Hotfix Installation Guide* for troubleshooting hotfix installation issues:
https://coldfusion.adobe.com/2012/12/coldfusion-hotfix-installation-guide/

13 Revision History

- Version 1.0 - December 2020 - Initial Revision.
- Version 1.1 - January 2021 - Minor Updates.