Adobe® ColdFusion® 10 Server Lockdown Guide

Contents

Section 1: Introduction

The *ColdFusion 10 Server Lockdown Guide* is written to help server administrators secure their ColdFusion 10 installations. In this document you will find several tips and suggestions intended to improve the security of your ColdFusion server. 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 do not need to use the same example installation paths provided in this guide.

1.2 Operating Systems and Web Servers

This guide focuses on Windows 2008 / IIS 7, and Redhat Enterprise Linux (RHEL) 6.3 / Apache 2.2. 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 10.0 Enterprise Edition.

1.4 Scope of Document

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

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

Section 2: Installation Prerequisites

Before running the ColdFusion 10 installer follow the steps in this section to prepare your Web Server for installation.

2.1 Prerequisites for all ColdFusion installations

Create a separate partition / drive for ColdFusion Installation and website assets. This mitigates the successfulness of path traversal attacks.
Install the latest security patches for your Operating System
Install the latest security patches for your Web Server Software
Configure your Firewall to block all non-administrative traffic to the server during installation.
Download ColdFusion 10 from Adobe.com

Verify that the MD5 checksum of the downloaded file matches the MD5 specified on the Adobe.com download page.

On Mac OSX:
To obtain the MD5 checksum of a file on Mac OSX launch Terminal.app and type: `md5 filename`

On Linux:
To obtain the MD5 checksum of a file on RedHat Enterprise Linux open a shell and type: `md5sum filename`

On Windows:
Windows installations do not include a MD5 checksum verifier by default. Microsoft provides a free MD5 checksum verifier called `sigcheck.exe` as part of SysInternals toolkit. Download the utility, open the command prompt and type `sigcheck -h filename`. The `sigcheck` utility not only generates a MD5 sum, it also verifies the signature of the ColdFusion installation executable (you should see Verified: Signed in the program output).

2.2 Prerequisites for a Windows 2008 Server Installation

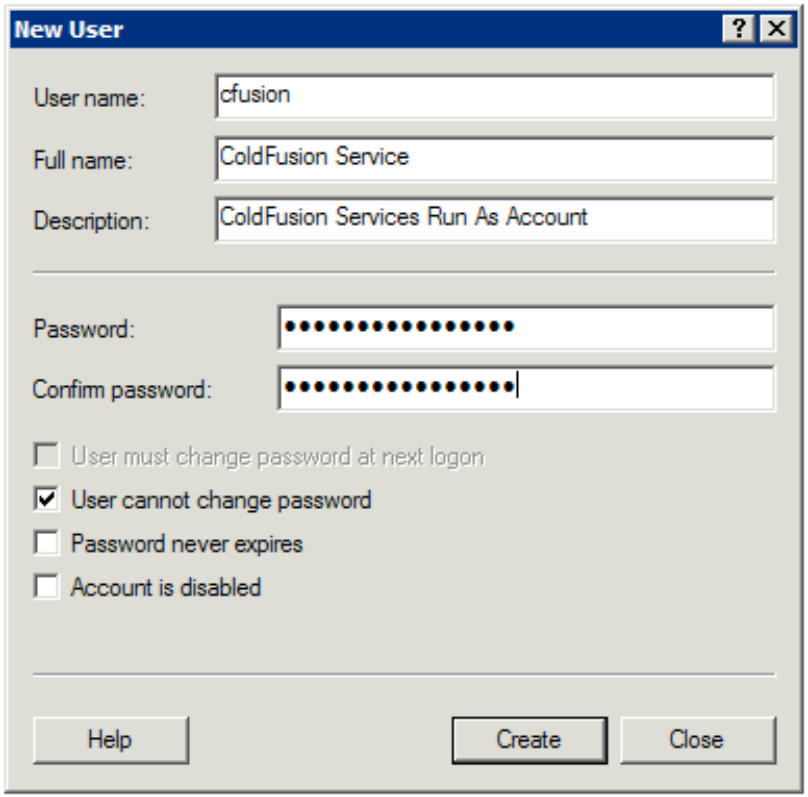
Read the Microsoft Windows Security Compliance Management Toolkit (see Appendix A.1)
Run Windows Update to ensure all software is up to date

Create Dedicated User Accounts
Ensure that all partitions use NTFS to allow for fine grained access control.
Setup a dedicated website for CF administrator

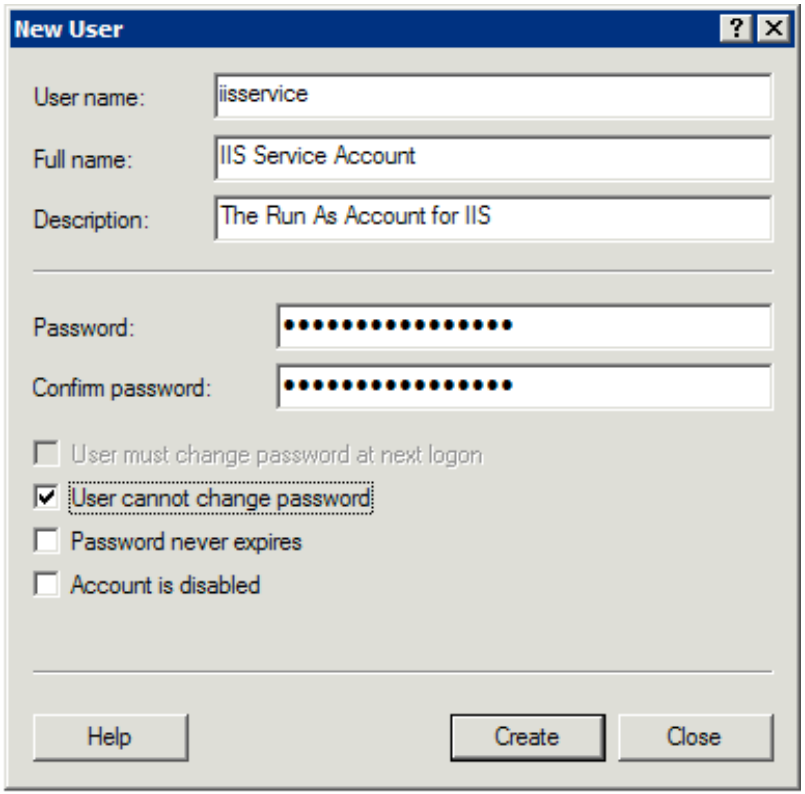
2.2.1 Create Dedicated User Accounts

Create a new User for the ColdFusion Service to Run As, in the screenshot below we call this user *cfusion*, choose a unique username that may not be easily guessed.

Create ColdFusion Service User Account



Next create a new user for the IIS Application Pool:



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

If you are setting up multiple instances of ColdFusion for different applications you will want to create dedicated user accounts for each instance to isolate them from each other. In addition each IIS application pool can have a dedicated user account, typically each website in IIS is assigned its own application pool.

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

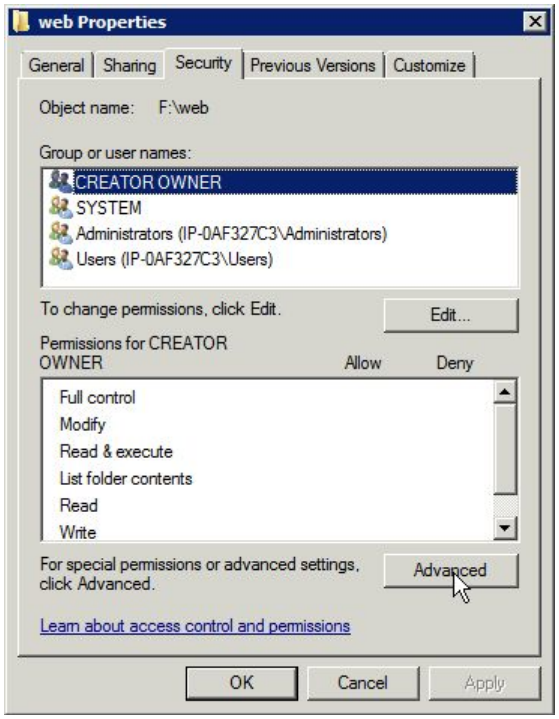
2.2.2 Create Web Root Directory

Created a separate partition for the CFML source and web site assets, for the examples in this guide it is mapped to drive `f:\`.

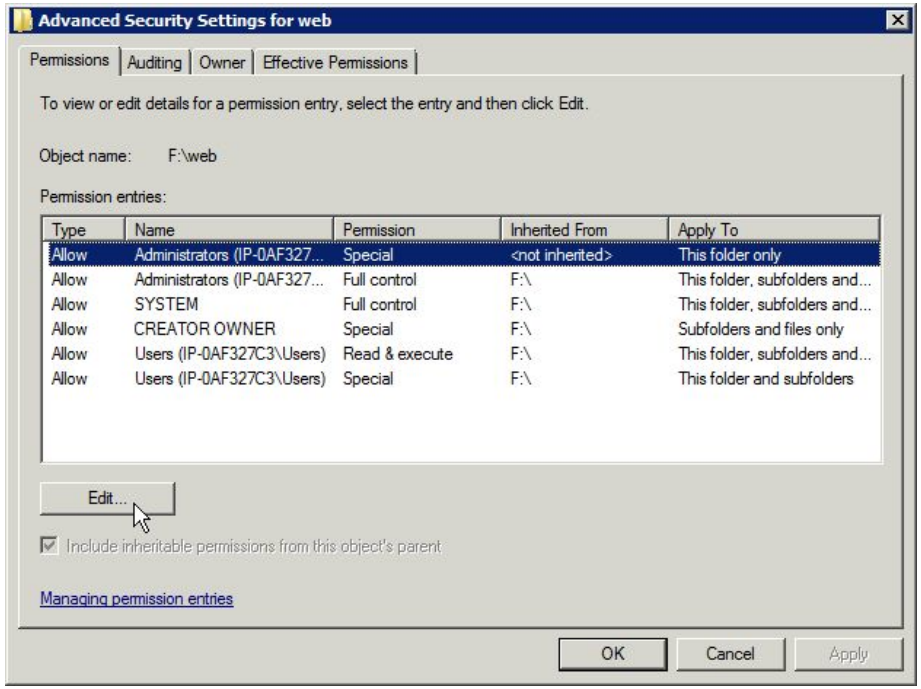
Create a directory to contain the web sites for example `f:\web\` and then create a sub directory to house each web site.

2.2.3 Grant the Permission to Web Site Root Directories

Right click on the Web site partition folder (eg `f:\web\`), and select properties. Select the *Security* tab and click the *Advanced* button:



In the Advanced Security Settings Dialog click the *Edit* Button:



Uncheck the checkbox labeled *Include inheritable permissions from this object's parent*. A confirmation box will appear, select remove:

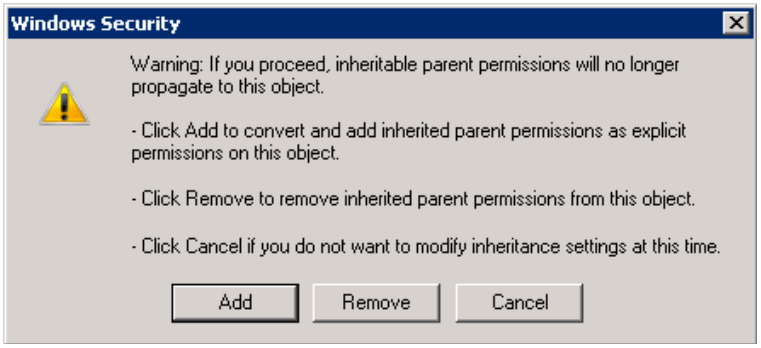


Table 2.2.3.1 Web Root Content Security Permissions

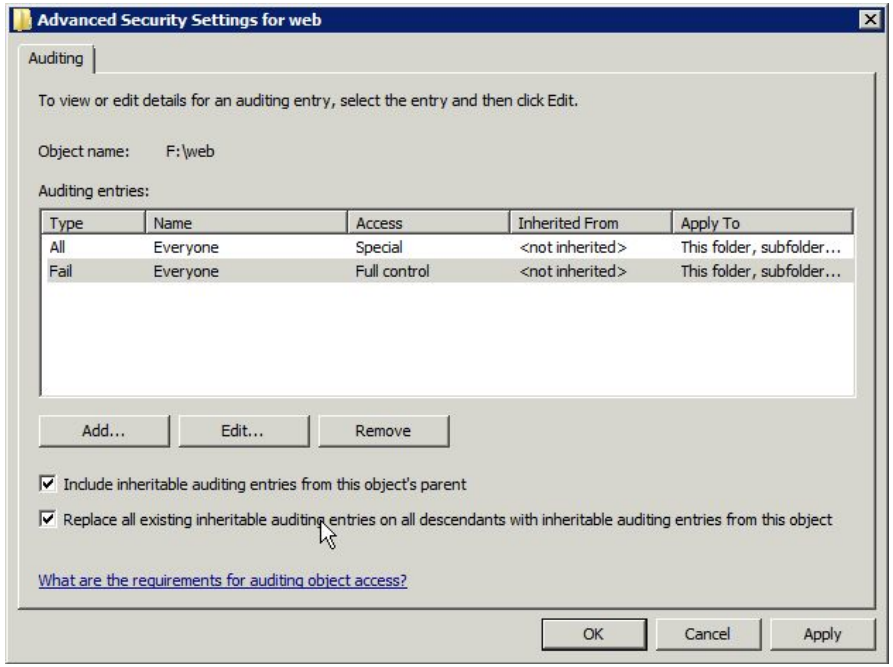
User / Group	Permissions
Administrators (or equivalent users and groups)	Full Control
iisservice (Your Application Pool Identity User)	• List folder / read data • Read attributes • Read extended attributes • Read permissions
IUSR (the anonymous authentication account)	• List folder / read data • Read attributes • Read extended attributes • Read permissions

User / Group	Permissions
cfusion (Your ColdFusion Service Identity)	• List folder / read data • Read attributes • Read extended attributes • Read permissions (Add additional write/delete permissions to folders or files that CF must write to)

Click the *Add* button and add the *iisservice* user grant Read and List Folder Contents Permission. Add the cfusion user and grant Read, List Folder Contents Permission. Grant cfusion Write and Delete permission if your applications make use of the file system via (cffile, cfdirectory, etc). Also give the *Administrators* full control over this folder, and remove any unnecessary privileges.

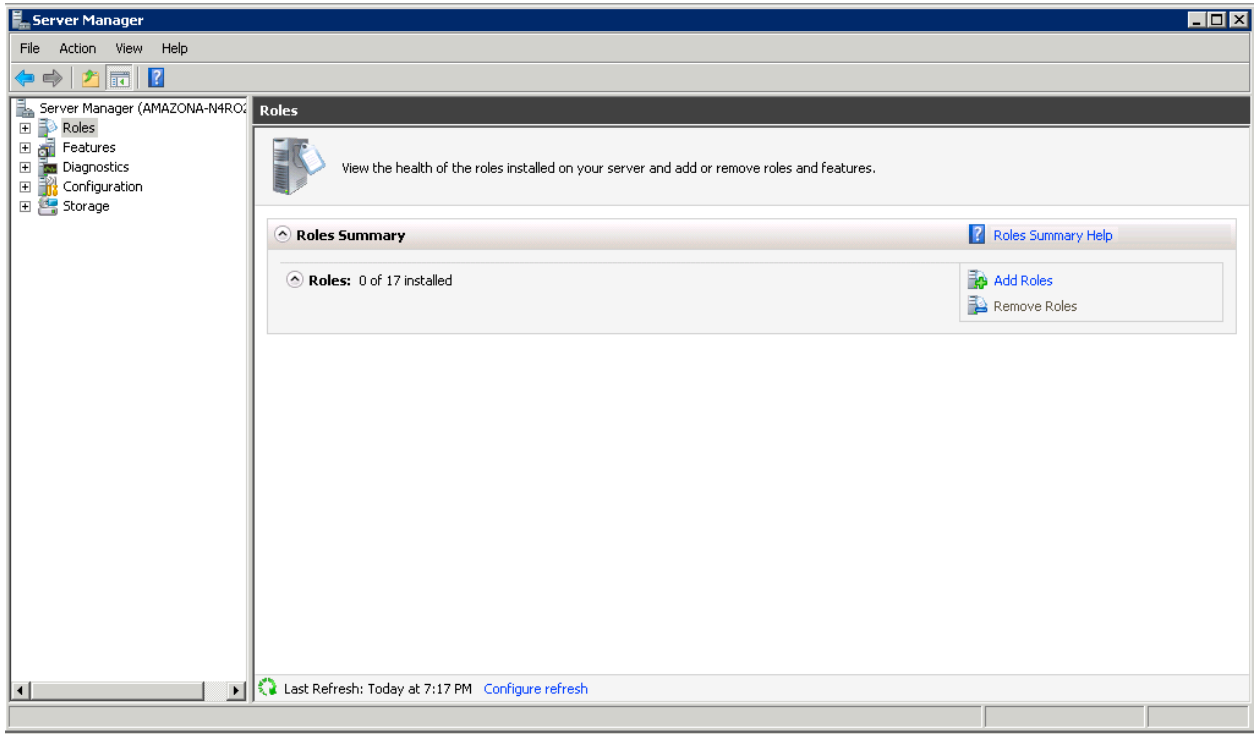
Check the *Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object* checkbox to propagate this setting to all sub folders and files existing or created below this folder.

Select the *Auditing* tab in the *Advanced Security Settings* dialog. Click the Edit button and ensure that some level of auditing exists. Auditing can generate a large amount of logs, and if too verbose can make the job of monitoring the server logs difficult. Auditing every successful file read in this directory may not be necessary. Use your judgement to determine an appropriate auditing policy based on your security requirements. A good minimal policy would be to audit all Fails, and certain Success events (Delete, Change Permissions, etc).

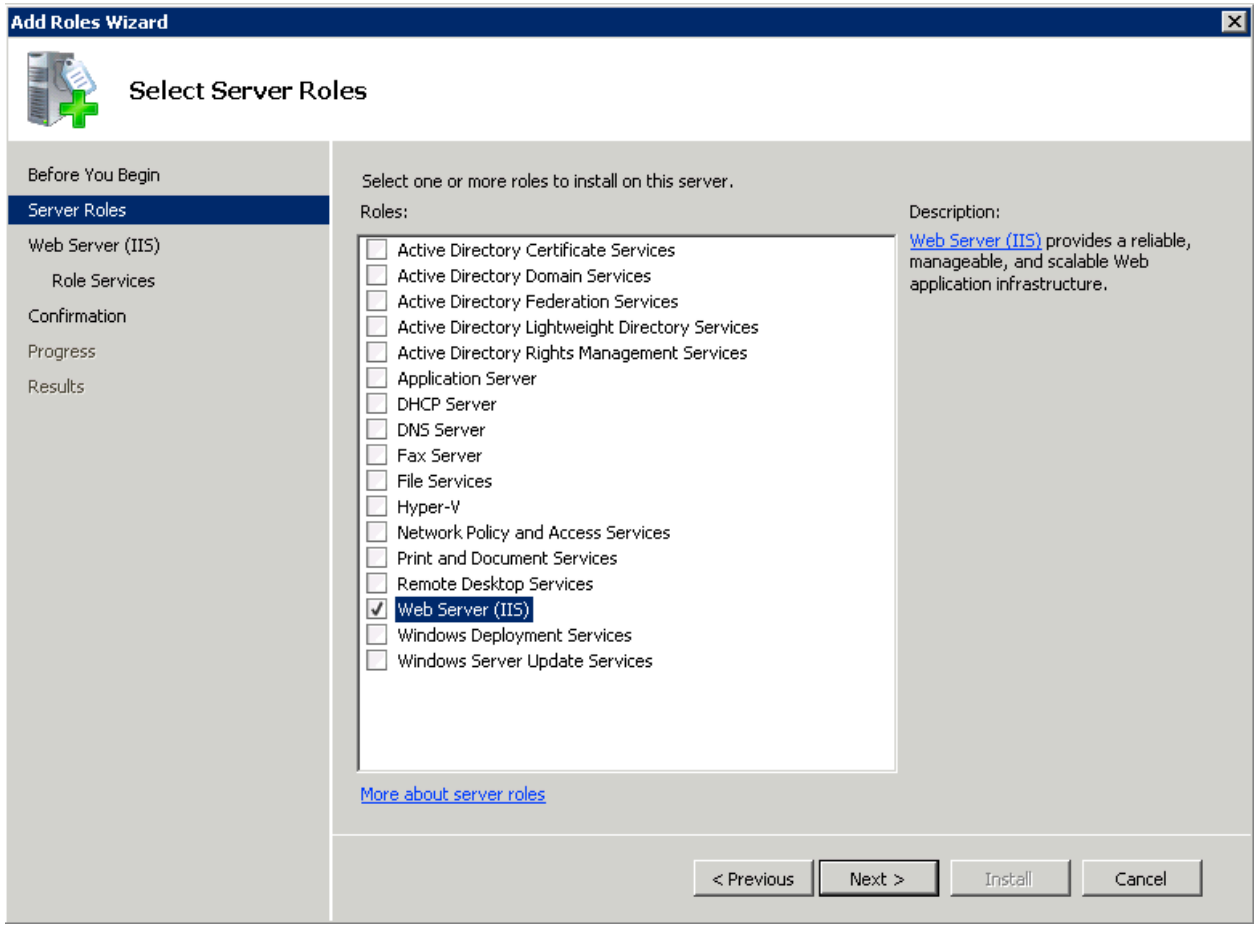


2.2.4 Add / Remove IIS Server Roles

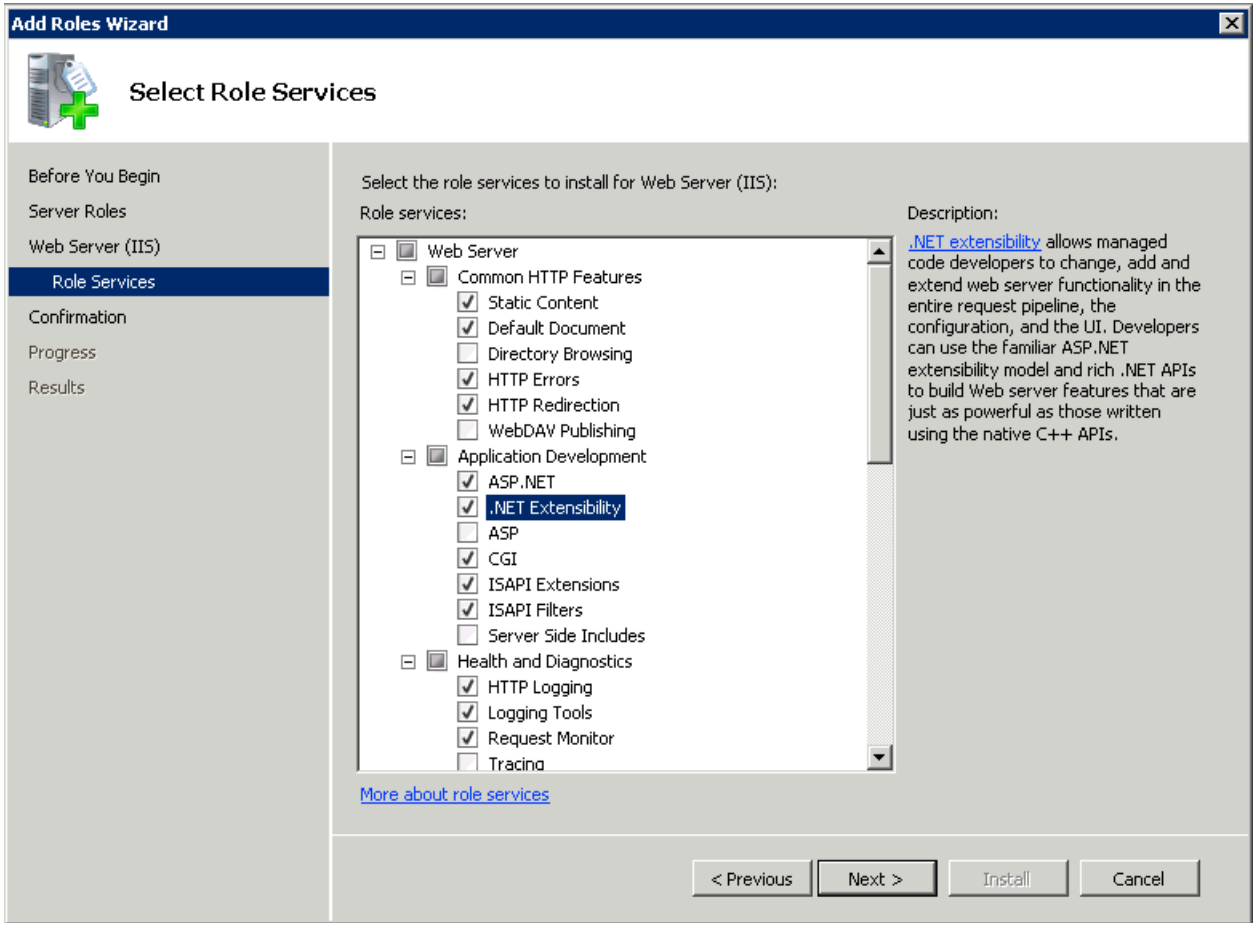
On a clean Windows 2008 install IIS may need to be installed. This is done by opening the Server Manager and selecting Roles:



Next Click Add Roles, and select the checkbox next to *Web Server (IIS)*:



The IIS role includes a number of optional sub-components called “Role Services”. ColdFusion requires that the ASP.NET, CGI, ISAPI Extensions and ISAPI Filters Role Services are selected. After we have configured the ColdFusion 10 IIS connection we can actually remove the ASP.NET and CGI Role Services.



Review the list of Role Services and remove any that may not be necessary (for example Directory Browsing). You may find other Role Services to be useful or necessary, such as Logging Tools, HTTP Redirection, Request Filtering, and IP and Domain Restrictions.

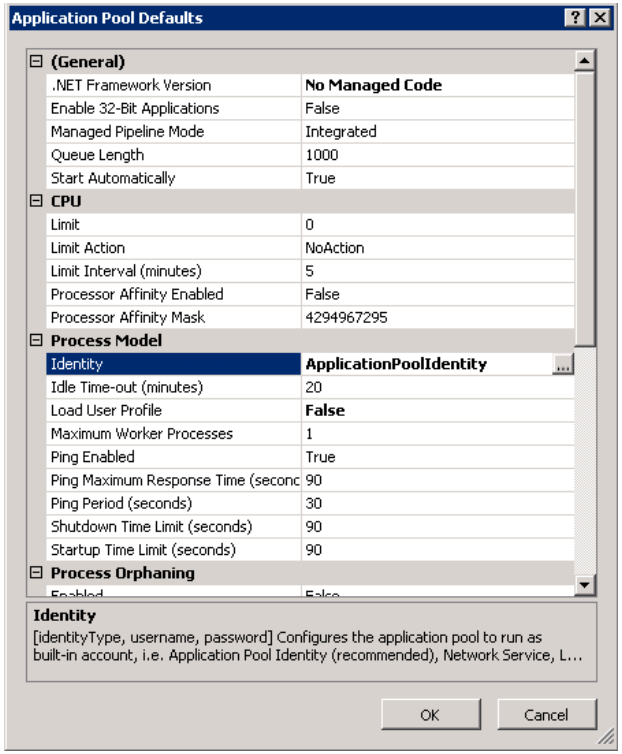
2.2.5 Delete Default IIS Web Site

A web site is installed with IIS called *Default Web Site*, right click and select Remove.

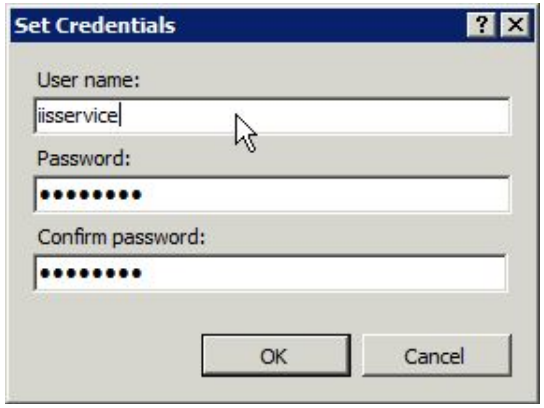
2.2.6 IIS Application Pool Settings

Click on Application Pools in IIS Manager and then click *Set Application Pool Defaults* in the Actions menu. This allows you to change the defaults used when a new Application Pool is created. By default each new web site in IIS gets it's own Application Pool. Remove any unused application pools (such as the one created by default).

Change the *.NET Framework Version* to *No Managed Code* if your web sites do not require .NET



Under Process Model change the Identity to be the IIS user you created (for example *iisservice*). You will be prompted for the password of this user:



Remove any Application Pools that are defined and not in use, such as the *DefaultAppPool*

2.2.7 Anonymous Access Identity

By default IIS7 is setup to use the built-in Windows user account called `IUSR` for anonymous request authentication. This means that when a request is made to your web site without authenticating with the web server will use IUSR for the NTFS file permissions.

The IUSR account is setup to be a low privilege account, but there may be cases where you want to change this to another account, for example if you want to isolate between multiple web sites or applications. The IUSR account is inherently a member of the Users group which may allow for additional unnecessary access to files.

2.2.8 Setup Request Filtering

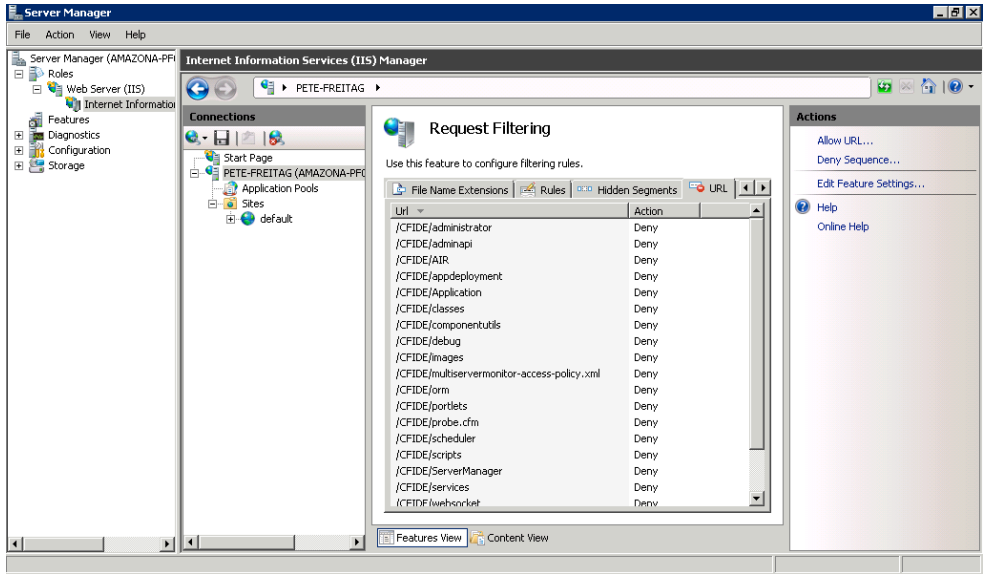
Make sure that you have the Request Filtering Role Service for IIS installed. Under the IIS root (applicable for all web sites) click on Request Filtering. Select the URL tab and click Deny Sequence.

When a string is added to the Deny Sequence if it is matched in the url IIS will return a 404 Not Found response, and the request will not reach the ColdFusion server.

URI	Purpose	Safe to Block
/CFIDE/administrator	ColdFusion Administrator	Yes, we will create a dedicated web site for ColdFusion administrator access.
/CFIDE/adminapi	Admin API	Usually, if the admin api is called from internal CFML code it will still work when the URI is blocked. If the admin api is accessed through a remote cfc function call then use another method to protect this uri (eg IP restriction)
/CFIDE/AIR	AIR Sync API	Usually, unless AIR sync API is used.
/CFIDE/appdeployment		Yes
/CFIDE/classes	Contains java applets for cfgrid, cftree, and cfslider	Usually, unless java applets are used.
/CFIDE/componentutils	CFC Documentation viewer	Yes
/CFIDE/debug	Used when debugging is enabled on the server.	Yes
/CFIDE/images	Contains two image files that do not appear to be used anymore	Yes

/CFIDE/multiservermonitor-access-policy.xml	Used to set a policy for allowing viewing the server monitor from multiple domains.	Yes - the server monitor now runs on its own web server on port 5500.
/CFIDE/orm	Contains interfaces used with ORM. These interfaces do not need to be accessible through the web server.	Yes
/CFIDE/portlets	Contains API for building portlets with JSR-286, JSR-168 or WSRP. The API does not need to be accessible through the web server.	Yes
/CFIDE/probe.cfm	You can configure probes in the ColdFusion administrator which are used to monitor a URL for failures. This will throw an exception if not run over 127.0.0.1.	Yes, however if you want to use probes you should create a web site that only listens on 127.0.0.1 and remove this block.
/CFIDE/scheduler	Contains an interface for scheduled task event handlers. Does not need to be accessible through the web server.	Yes
/CFIDE/scripts	Contains javascript and other assets for several ColdFusion features cfform, cfchart, ajax tags, etc.	Yes - we will create a new, non default URI for this folder, and specify the new URI in the ColdFusion administrator.

/CFIDE/ServerManager	Contains the AIR application binary for the Server Manager.	Yes
/CFIDE/services	Contains CFCs that can act as a service layer to Flex, or other client side applications. The client application must have a username / password and also an allowed IP. Enabling this feature can open up a large amount of security risk to the application server.	Yes
/CFIDE/websocket	API for web socket listener CFCs. Does not need to be open via the web server if used.	Yes
/CFIDE/wizards	Possibly used for IDE integration, not needed on production.	Yes
/CFIDE/GraphData	Used to render cfgraph and cfchart assets.	Only if cfchart and cfgraph is not used.
/CFIDE/main	Used for RDS	Yes



Our strategy here is to block all URI's that do not need to be accessible to the public. Some of the resources we will block here may not pose any known threat but could be used to determine the version of ColdFusion you are running. Ideally we could block all /CFIDE, however if you use cfchart the generated graphics are rendered from /CFIDE/GraphData.cfm

It is not possible using request filtering to deny the URI /CFIDE but then allow /CFIDE/GraphData.cfm for example.

If you are not using cfchart and do not need access to any of the URIs below you may simply deny /CFIDE instead of listing each sub directory.

Table 2.2.8.1 : CFIDE URIs
Additional URI Sequences to consider blocking:

URI	Purpose	Safe to Block
Application.cf	Block Application.cfc and Application.cfm requests which result in an error when accessed directly.	Yes
WEB-INF	WEB-INF contains configuration data used by the java application server. The Tomcat connector will block this already, but you can block it at the web server level as well.	Yes
/cfformgateway	Used for <cfform format=flash>	Only if Flash Forms are not used.
/flex2gateway	Flex Remoting	Only if Flex Remoting is not used.
/cfform-internal	Used for <cfform format=flash>	Only if Flash Forms are not used.
/flex-internal	Flex Remoting	Only if Flex Remoting is not used.

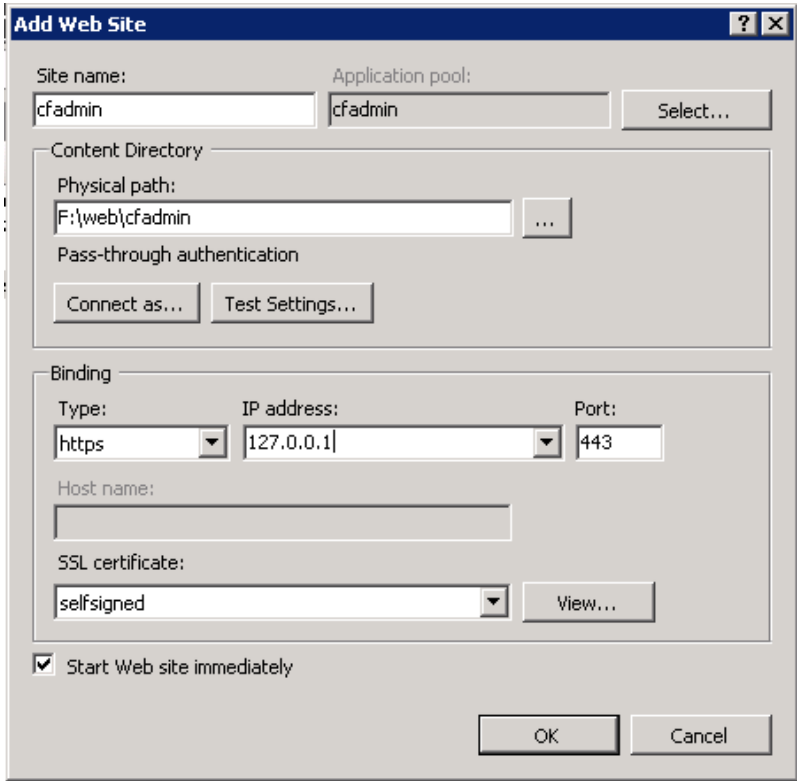
URI	Purpose	Safe to Block
/cffileservlet	Serves dynamically generated assets. It supports the cfreport, cfpresentation, and cfimage (with action=captcha and action=writeToBrowser) tags	Only if cfreport, cfpresentations and cfimage are not used.
/rest	Used for CF10 Rest web services support.	Only if CF10 REST web services are not used.
/WSRPProducer	Web Services Endpoint for WSRP.	Usually, unless WSRP is used.
.svn	If you use subversion to deploy your ColdFusion applications you can block the .svn folders, which may allow source code disclosure.	Yes

2.2.9 Create a Website For ColdFusion Administrator

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

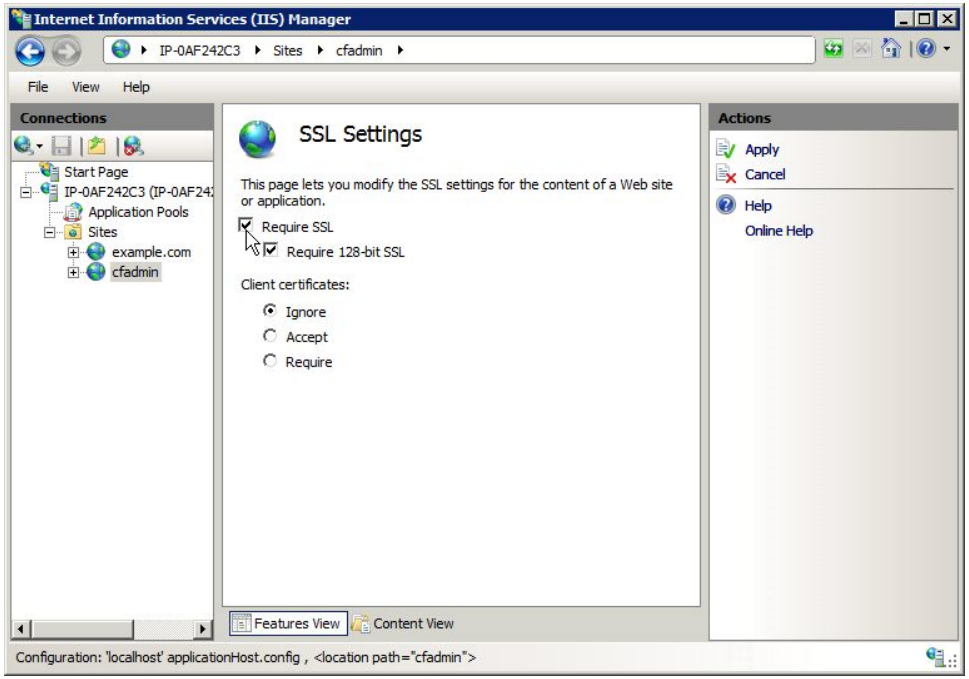
Create an empty directory for the web site root of the ColdFusion administrator web site (eg f:\web\cfadmin\)

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



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

Next Require SSL Connections for this website by double clicking on the SSL Settings icon for the *cfadmin* website:

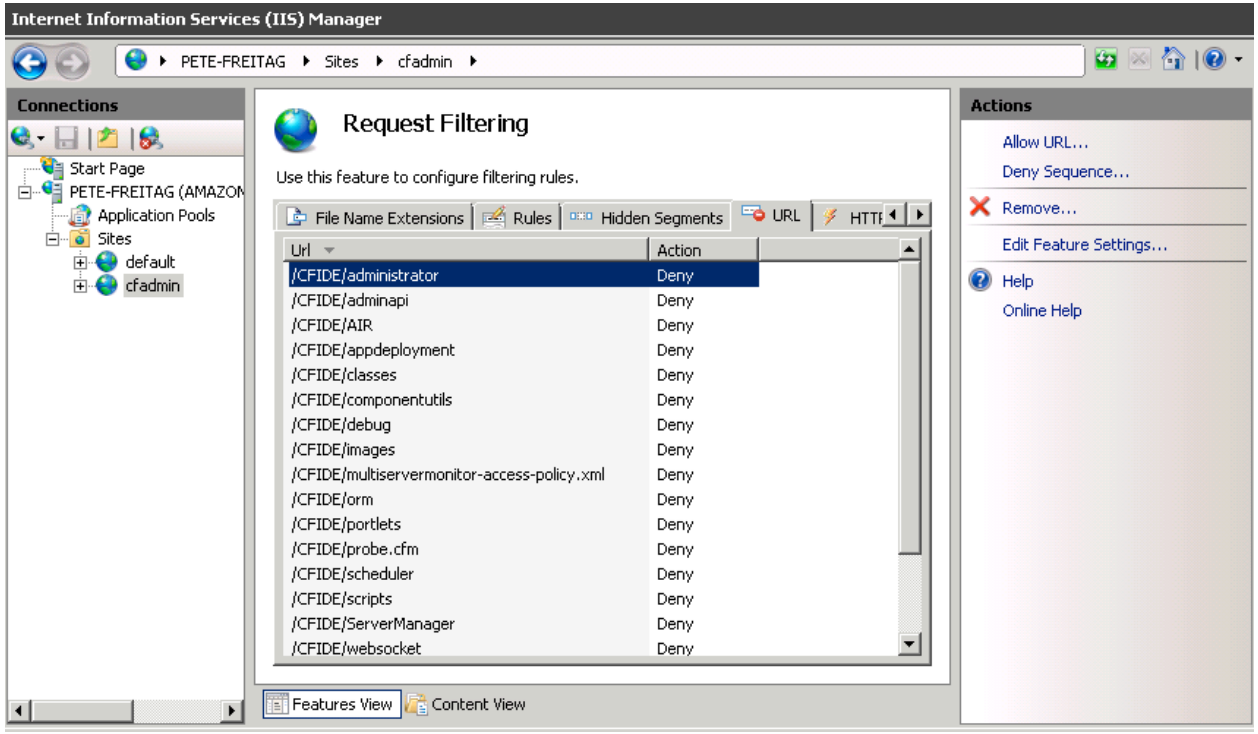


Select *Require SSL* and *Require 128-bit SSL* and click Apply.

Visit https://127.0.0.1/ and ensure that it requires SSL and authentication.

Remove Request Filtering Rule for ColdFusion Administrator Site

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


Internet Information Services (IIS) Manager
PETE-FREITAG ▸ Sites ▸ cfadmin ▸
Connections
Start Page
PETE-FREITAG (AMAZON
Application Pools
Sites
default
cfadmin
Request Filtering
Use this feature to configure filtering rules.
File Name Extensions
Rules
Hidden Segments
URL
HTTP
Url
Action
/CFIDE/administrator Deny
/CFIDE/adminapi Deny
/CFIDE/AIR Deny
/CFIDE/appdeployment Deny
/CFIDE/classes Deny
/CFIDE/componentutils Deny
/CFIDE/debug Deny
/CFIDE/images Deny
/CFIDE/multiservermonitor-access-policy.xml Deny
/CFIDE/orm Deny
/CFIDE/portlets Deny
/CFIDE/probe.cfm Deny
/CFIDE/scheduler Deny
/CFIDE/scripts Deny
/CFIDE/ServerManager Deny
/CFIDE/websocket Deny
Features View
Content View
Actions
Allow URL...
Deny Sequence...
Remove...
Edit Feature Settings...
Help
Online Help

2.3 Prerequisites for a RedHat Enterprise Linux 6.3 Installation

Take the following steps before running the ColdFusion installer on Linux

2.3.1 - Before you Install RedHat Enterprise Linux

Read through the NSA Guide to Secure Configuration of Red Hat Enterprise Linux 5 (A.3) - at the time of this writing a Guide specific to RHEL Version 6 was not yet published, check with the NSA operating system configuration guidance (A.2) list to see if an updated guide has been published.

2.3.2 - Installing RedHat Enterprise Linux

Create separate partitions for the web root(s) in this guide we will use `/web/` as the mount point for our web sites partition, please choose a unique mounting point name.

Select a minimum set of packages, it is recommended that you do not install a graphical desktop environment. Choose to enable SELinux in Enforcing mode during the installation process.

2.3.3 - Update Installed Software and Remove Unnecessary Software

To update software run:

```
# yum update
```

To see what software packages are installed run

```
# yum list installed | more
```

Remove any packages that are not required.

2.3.4 Install/Update Apache and remove Unnecessary Modules

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
```

Ensure that the latest version of `openssl` and `mod_ssl` is 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. You can easily find a list of these module by running:

```
# fgrep LoadModule /etc/httpd/conf/httpd.conf
```

Some modules that you may be able to remove include: mod_imap, mod_info, mod_userdir, mod_status, mod_cgi, mod_autoindex

See Appendix A.7 and A.8 for more information on securing the Apache Web Server.

2.3.5 Create users and groups for ColdFusion and Apache

Create a new group to contain both Apache and ColdFusion, in this guide we use the name `webservices` feel free to choose a unique name.

```
# groupadd webservices
```

The Apache web server runs as user `apache` by default on Red Hat Enterprise Linux 5. Add `apache` to the `webservices` group:

```
# usermod -a -G webservices apache
```

Create a user for ColdFusion to run as, in this guide we use `cfusion`, but again feel free to choose a unique name:

```
# adduser -g webservices -s /sbin/nologin -M -c ColdFusion cfusion
```

Specify a strong password for the new user:

```
# passwd cfusion
```

2.3.6 - Apache Configuration

Create a directory for ColdFusion Administrator web site:

```
# mkdir /web/cfadmin
# mkdir /web/cfadmin/wwwroot
```

Setup permission on web partition:

```
# chgrp -R webservices /web
# chown -R cfusion /web
# chmod -R 750 /web
```

Note the permission 750 grants rwxr-x--- permission, meaning owner (cfusion) has full control, while the group (webservices) only has read and execute permission (execute permission is needed to allow directory traversal by the user).

Most applications will require some write permission under the web root, you can change owner to `root` (by running `chgrp root /web/path`) for files and directories that do not need write permission. In addition while directories will require execute permission, files in those directories will not require execute permission.

To Lock Down `/CFIDE` add the following to your `/etc/httpd/httpd.conf` file:

```
<Location /CFIDE>
 Order Deny,Allow
```

```
 Deny from all
 Allow from 127.0.0.1
</Location>
```

The above blocks all requests starting with /CFIDE for all IP's except 127.0.0.1. You may want to change that to the IP address of an administration workstation instead, to allow yourself access to the ColdFusion Administrator.

```
<Location /CFIDE/GraphData.cfm>
 Order Deny,Allow
 Allow from all
</Location>
```

The above allows the URI `/CFIDE/GraphData.cfm` to pass through to ColdFusion. If you are not using `cfchart` you may skip this step. See Table 2.2.8.1 CFIDE URIs for a full list of URIs to determine if other URIs should be whitelisted under CFIDE.

Next lets create a virtual host for the ColdFusion administrator website. This example uses the self signed certificate generated during installation, it is recommended that you use a signed certificate instead.

```
<VirtualHost 127.0.0.1:443>
 ServerName localhost
 DocumentRoot /web/cfadmin/wwwroot/
 SSLEngine on
 SSLCertificateFile /etc/pki/tls/certs/localhost.crt
 SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
 SSLProtocol +SSLv3 +TLSv1
 SSLCipherSuite RSA:!EXP:!NULL:+HIGH:-MEDIUM:-LOW
 ErrorLog logs/cfadmin.ssl.error.log
 CustomLog logs/cfadmin.ssl.access.log common
</VirtualHost>
```

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

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

```
<Location /CFIDE/administrator>
 SSLRequireSSL
</Location>
```

The above requires that `mod_ssl` and `openssl` are installed and configured.

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

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

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

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

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

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

```
<Location /CFIDE/administrator>
 AuthType Digest
 AuthName "cfadmins"
 AuthDigestProvider file
 AuthUserFile /etc/httpd/cfadmin.digest.pwd
 Require valid-user
</Location>
```

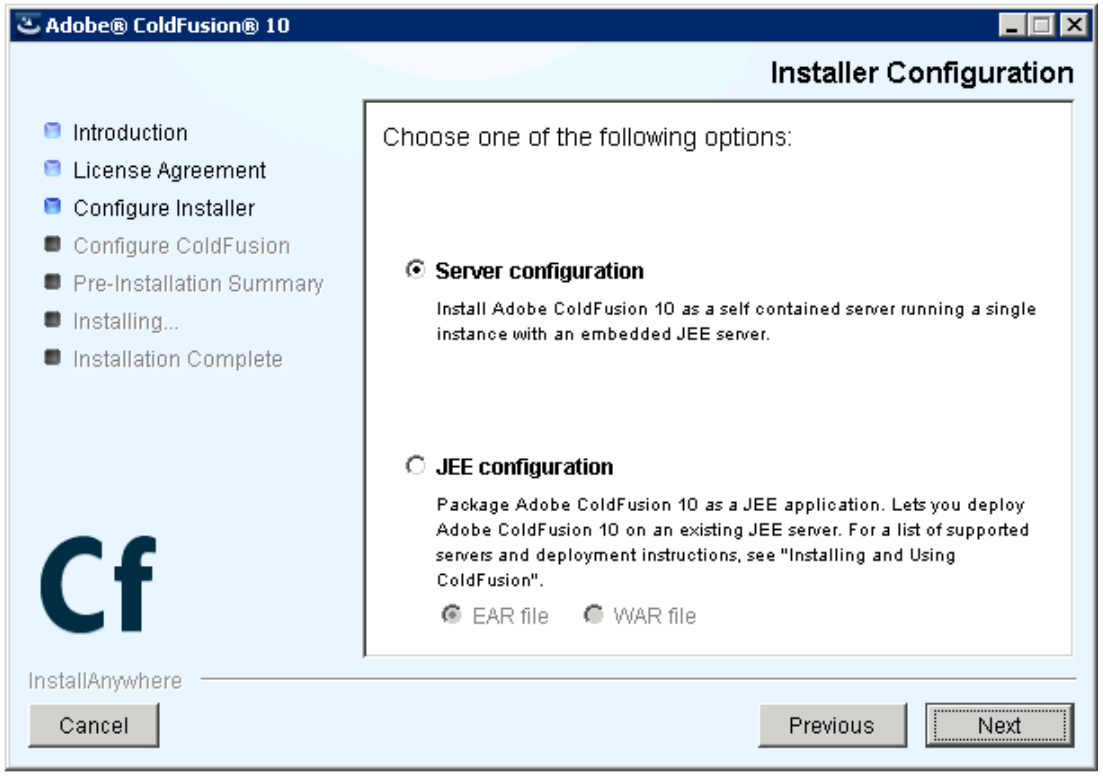
Restart Apache and visit https://localhost/CFIDE/administrator/ and ensure that you are prompted with a password, and that SSL is required. At this point since ColdFusion is not installed it should result in a 404 if authentication is successful.

If you receive a `403 Forbidden` response you may need to run `chcon` to set the SELinux context of the files, see Linux Post Installation section or Appendix A.10.

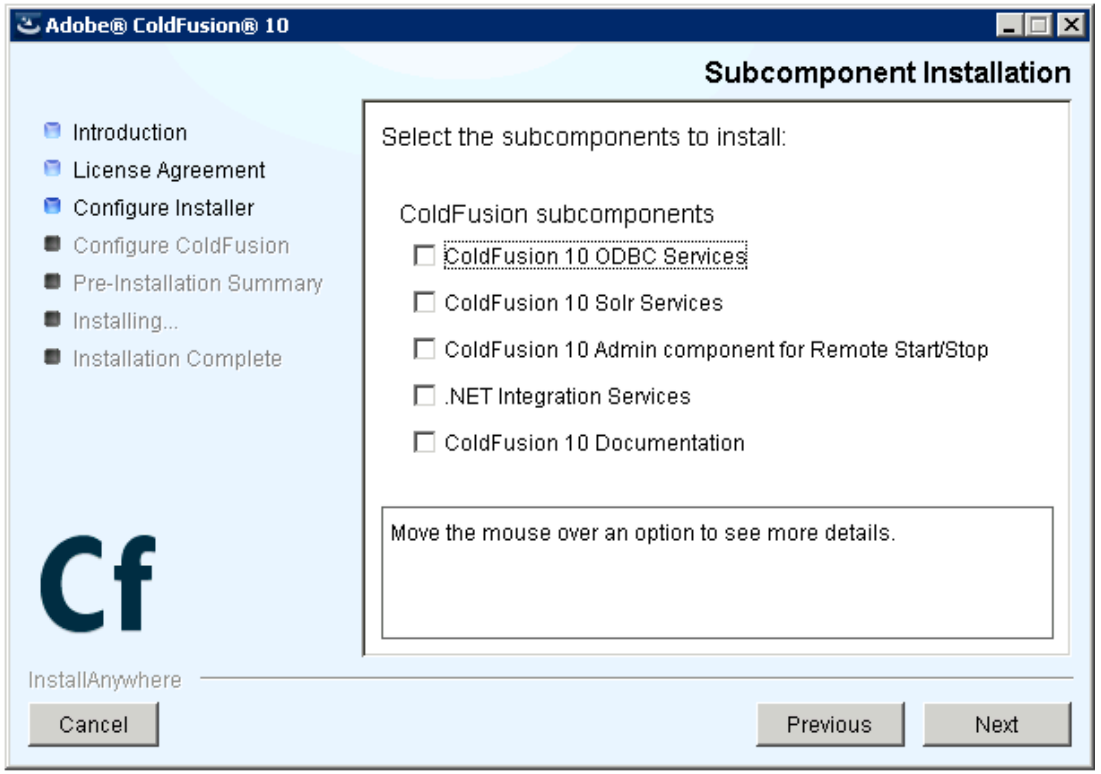
Section 3 - Installing ColdFusion

3.1 Run ColdFusion Installer

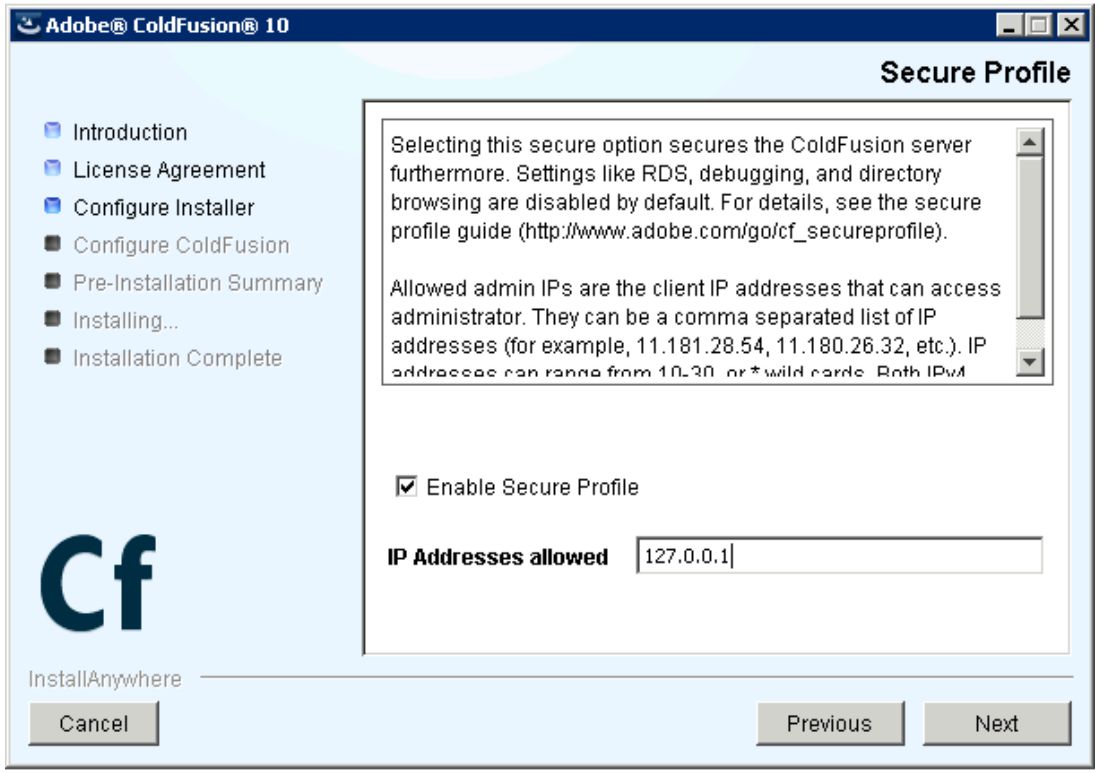
Run the ColdFusion 10 Installer. This guide covers the standard Server configuration option and does not cover installation as a WAR or EAR file, consult your JEE server vendor for installation specifics. The option to install ColdFusion in standalone or multiserver mode no longer exists as it did in previous versions, which allows ColdFusion 10 to use the same core directory structure even if multiple instances (Enterprise only) are used.


Adobe® ColdFusion® 10
Installer Configuration
Introduction
License Agreement
Configure Installer
Configure ColdFusion
Pre-Installation Summary
Installing...
Installation Complete
Choose one of the following options:
Server configuration
Install Adobe ColdFusion 10 as a self contained server running a single instance with an embedded JEE server.
JEE configuration
Package Adobe ColdFusion 10 as a JEE application. Lets you deploy Adobe ColdFusion 10 on an existing JEE server. For a list of supported servers and deployment instructions, see "Installing and Using ColdFusion".
EAR file
WAR file
Cf
InstallAnywhere
Cancel
Previous
Next

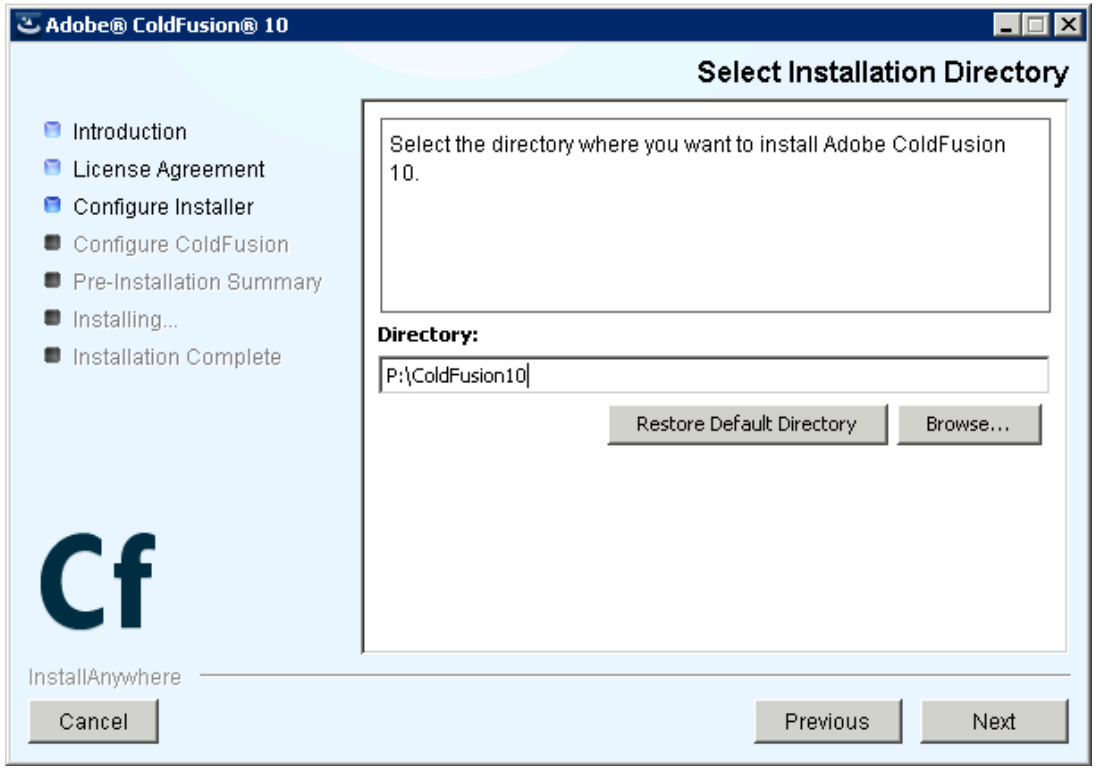
Do not install ColdFusion 10 ODBC Services, ColdFusion 10 Admin component for Remote Start/Stop or Documentation. Select only the subcomponents that are required for your application.



Enable the *Secure Profile*, and specify IP address which may access ColdFusion Administrator. The Secure Profile option is new in ColdFusion 10 and provides a more secure foundation of default settings. You can review the settings it toggles here: http://www.shilpikhariwal.com/2012/04/coldfusion-10-presents-secure-profile.html



Select an install directory, a non-standard directory location on a non-system partition is preferred.



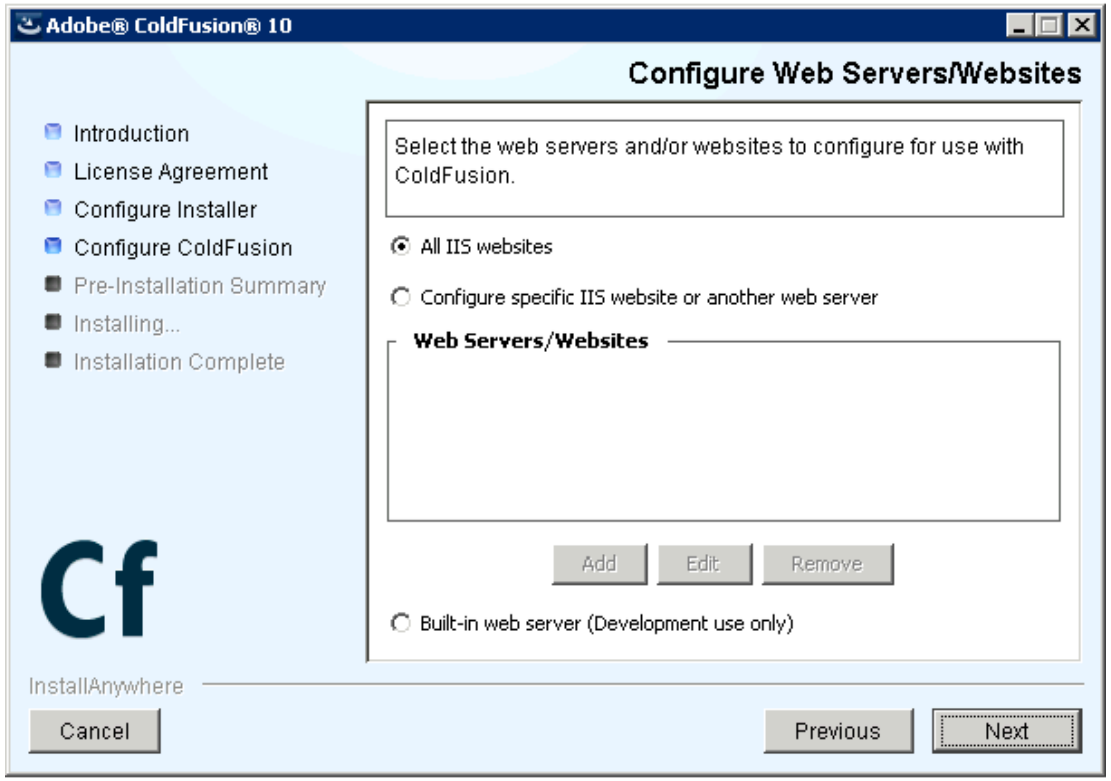
Install the connector for IIS, you can select either All IIS websites or a specific one depending on your needs. If your web server will be hosting web sites that do not require ColdFusion, do not select all IIS websites, or be sure to manually remove ColdFusion from each site that does not require it.

If any websites are added to IIS that require ColdFusion after the installation, you will need to run the web server connector tool (wsconfig.exe) again to connect ColdFusion 10 to the web site.

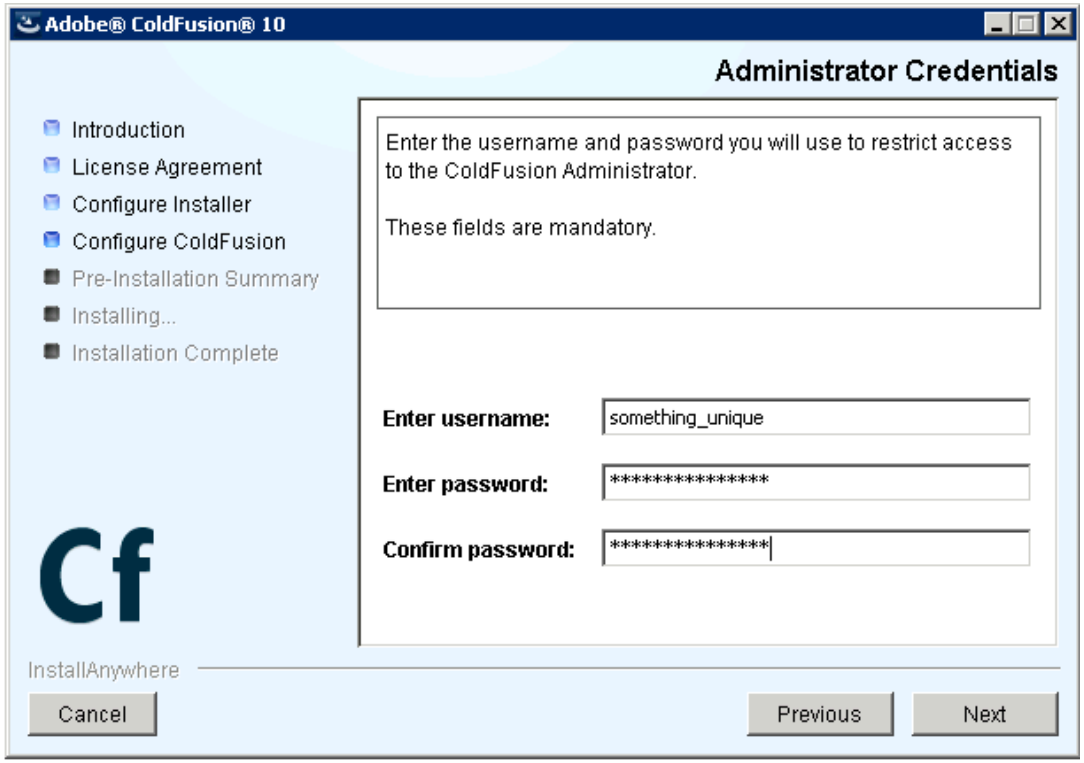
If you are installing on Linux with SELinux enabled, hold off on installing the apache connector, this is done manually later on in this guide.

For maximum security consider running the web server and ColdFusion on separate physical servers.

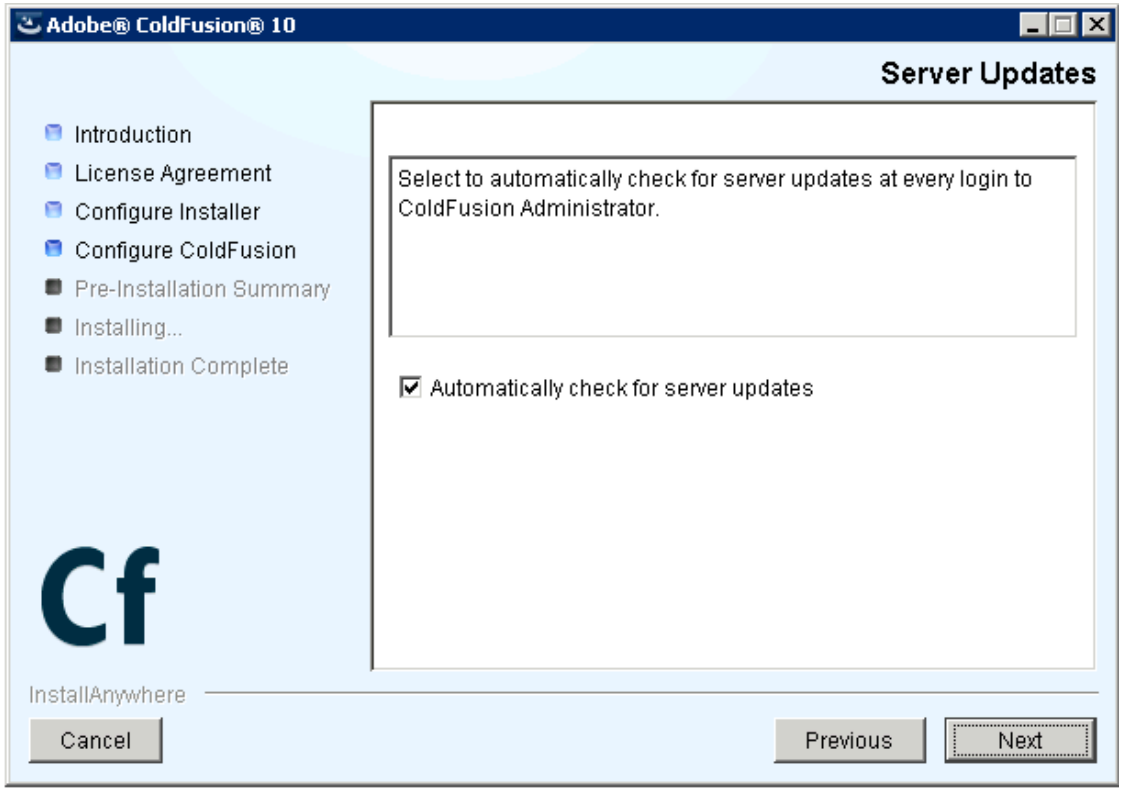
One way to separate the public facing web server and the ColdFusion server is by using a reverse proxy. In a reverse proxy setup the ColdFusion server will still have a web server installed, however all external client requests will be handled by the proxy server, and only specific requests will be sent to the ColdFusion server for processing. Consult your web servers documentation to set up a reverse proxy.


Adobe® ColdFusion® 10
Configure Web Servers/Websites
Introduction
License Agreement
Configure Installer
Configure ColdFusion
Pre-Installation Summary
Installing...
Installation Complete
Select the web servers and/or websites to configure for use with ColdFusion.
All IIS websites
Configure specific IIS website or another web server
Web Servers/Websites
Add
Edit
Remove
Built-in web server (Development use only)
InstallAnywhere
Cancel
Previous
Next

Choose a strong password and unique username for the ColdFusion administrator. Strong passwords should contain a random mix of case, numbers, special characters and at least 8 characters in length.



You may consider checking the checkbox to allow ColdFusion to check for updates when you login to ColdFusion administrator - note that it will not install the updates, only check for new updates.



Section 4 - Post ColdFusion Installation

4.1 Windows 2008 Post ColdFusion Installation

4.1.1 Install ColdFusion Hotfixes

Note: At the time of this writing you will need to install the ColdFusion 10 Mandatory Update before you can install any Hotfixes: See http://helpx.adobe.com/coldfusion/kb/coldfusion-10-mandatory-update.html

Login to ColdFusion administrator and click on *Server Updates* > *Updates* and then select the latest hotfix, and click *Download*.

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

If the md5 checksum matches install the hotfix from the command prompt:

```
java -jar {coldfusion-home}\cfusion\hf-updates\hotfix_XXX.jar
```

Replace hotfix_XXX.jar with the filename of the hotfix jar you are installing, and follow the prompts. The installer will typically attempt to restart ColdFusion when done, you can however disable that, see documentation for details.

You may need to reinstall the IIS connectors at this point, consult the hotfix release notes.

4.1.2 Setup Permissions on ColdFusion installation directory

Grant the user you created for ColdFusion to run as (cfusion in our example) and the Administrators group full control over the ColdFusion installation directory. Enable auditing on this directory as well.

In a maximum security environment you may consider a more detailed permission structure for the ColdFusion installation directory to prevent runtime changes to certain resources or configuration, this may however break features like security hotfix installation from ColdFusion administrator.

The IIS Application Pool user (iisservice in our examples) must also have permission access the Tomcat IIS connector. Grant this user permission to the `\config\wsconfig\` directory in your ColdFusion installation directory.

Folder	Permission
{coldfusion-home}	Full Control
{coldfusion-home}	Full Control
{coldfusion-home}/config/wsconfig/	• List folder / read data • Read attributes • Read extended attributes • Read permissions
{coldfusion-home}/cfusion/wwwroot/CFIDE	• List folder / read data • Read attributes • Read extended attributes • Read permissions

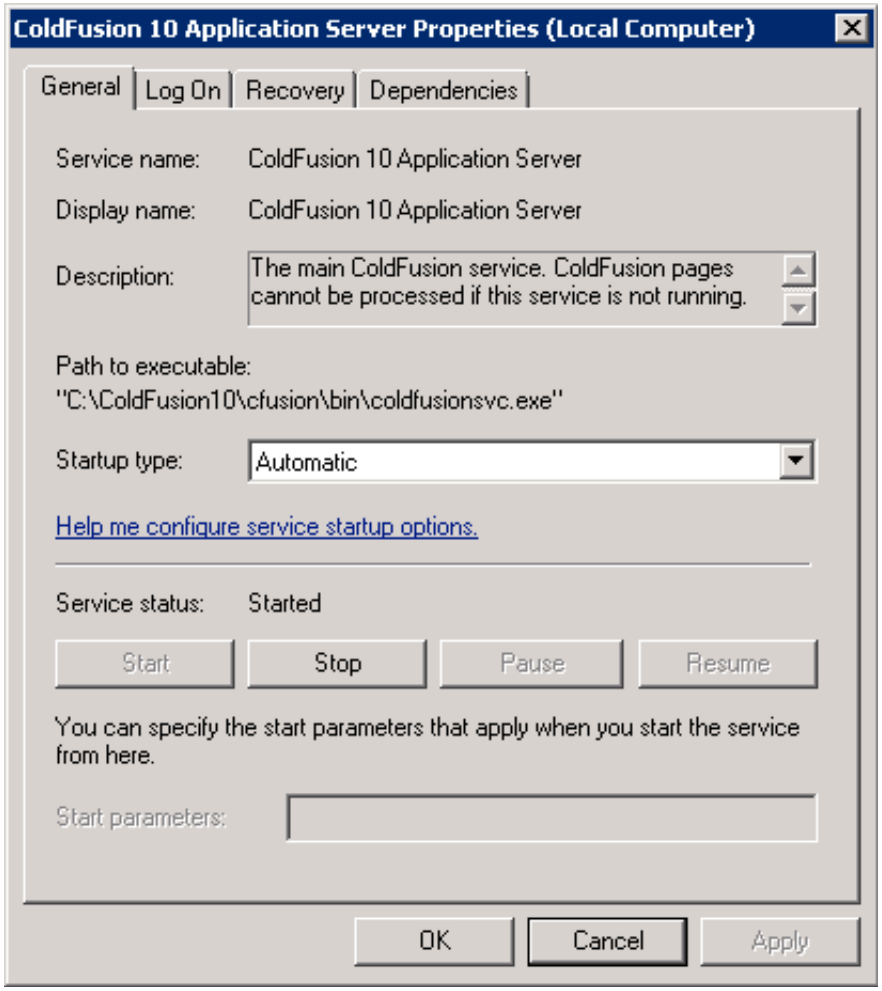
The ColdFusion IIS connector writes logs to a file called `isapi_redirect.log` - the IIS Application Pool user (iisservice in our example) needs write permission to this file. You may consider changing the location of this file, which is defined in the `isapi_redirect.properties` file to a directory elsewhere.

Note: if you choose to run Anonymous Authentication through the Application Pool user then IUSR does not need permission to these files.

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

4.1.3 Specify Log On User for ColdFusion Services

Open the Services Manager and change the user the service runs as to be the user you created (cfusion in the guide example). The installation creates a service named *ColdFusion 10 Application Server* which runs the initial ColdFusion instance. Right click the service, click Properties and select the *Log On* tab to specify the username and password for the account you created. Restart the ColdFusion 10 Service.



If you installed any optional subcomponents (such as Solr or .NET) ensure that their services run as the ColdFusion user account as well. If you installed a subcomponent but are not using it yet, you can change the service Startup type to *Disabled*.

4.1.4 Remove /CFIDE and /cfdocs virtual directories added by installer

When the ColdFusion IIS connector installs it creates two virtual directories for each site the first is called jakarta, and is necessary for ColdFusion to process requests through IIS, and the second is CFIDE which can be removed.

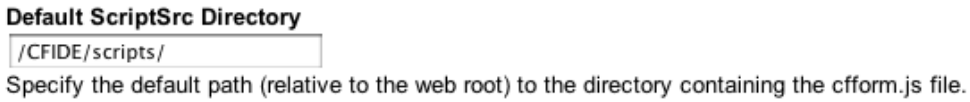
4.1.5 Setup Virtual Directory alias for /CFIDE/scripts/

Because we have blocked `/CFIDE/scripts` and it is a security best practice to change the location of this to a non-default location we must setup a virtual directory in each site that relies on the assets in there.

Here's a short list of tags or features that may require /CFIDE/scripts: cfajaxproxy, cfcalendar, cfchart (HTML5), cfdiv, cfform, cfgrid, cflayout,cfmediaplayer,cfmenu cftextarea,cfpod, cfprogressbar, cfslider, cftooltip, cfwindow

In this guide we choose a virtual directory mapping of `/cf-scripts/` but you should choose a unique mapping name for your server.

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



Replace /CFIDE/scripts/ with the new virtual directory URI, eg: `/cf-scripts/`

4.1.6 Update Java Virtual Machine

The Java Virtual Machine included with the ColdFusion installer may not be the latest JVM supported by Adobe ColdFusion 10, or it may contain security issues. Download the JVM from java.oracle.com.

4.1.7 Block Unused file types

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 ColdFusion handles by default:

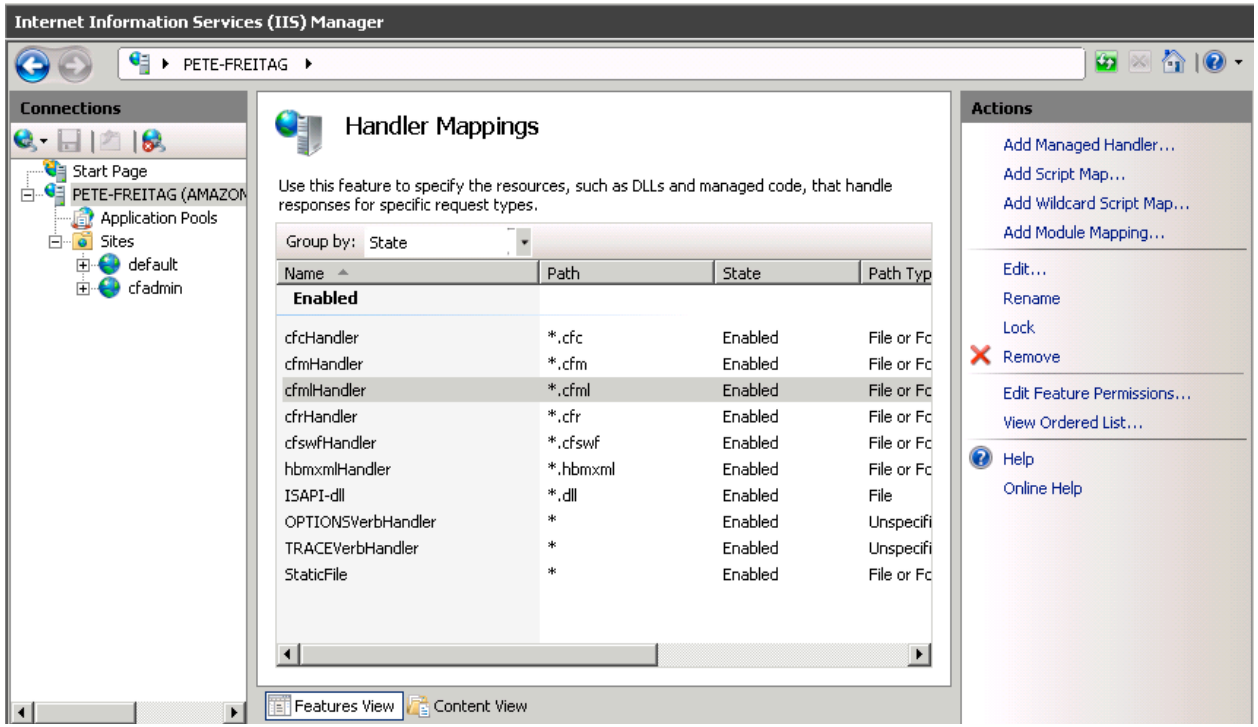
File Extensions that *usually* can be blocked (check with developers first):

Purpose	Safe to Block
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.
JavaServer Pages	Yes, if your applications do not require JSP.
Java Web Services - allows you to easily write and deploy SOAP web services in Java similar to a CFC.	Yes if not used.
Hybernate XML mappings	Yes this should be blocked.

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

4.1.8 Remove Unused Handler Mappings

The ColdFusion connector installer, adds a number of handler mappings on IIS as the following diagram shows:

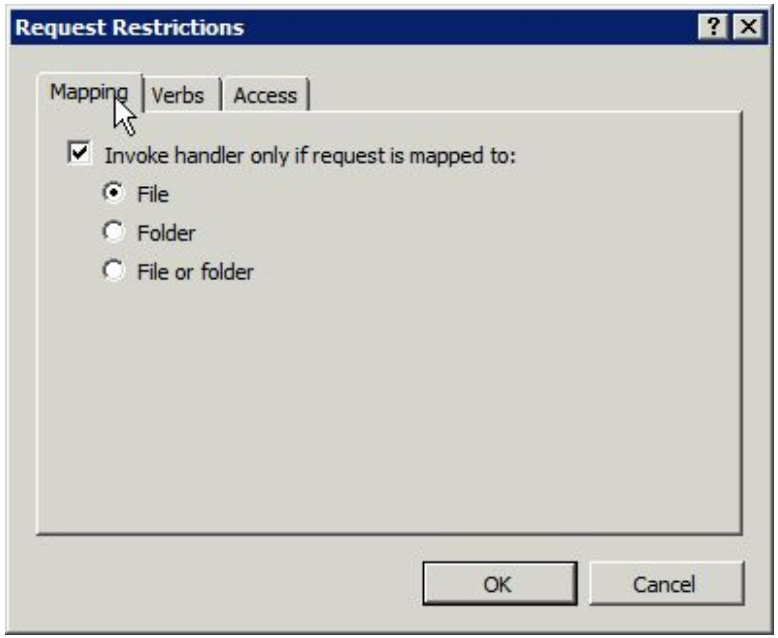


Mappings that are not used may be removed. Note that you should also block the removed extensions using Request Filtering as shown in the previous section.

Keep in mind that if you remove the mapping for a source file (such as .cfc) the source code may be downloaded when requested, if the extension has not been blocked using Request Filtering or some other method.

4.1.9 Handler Mapping Settings

Double click each ColdFusion handler mapping, and invoke handler only if request is mapped to a file.



Continue to section 4.3 for more post installation configuration.

4.1.10 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.

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, they do not test

without these settings enabled so you may encounter something unexpected. Second when a ColdFusion update is released for the connector or if you want to add/update/delete an IIS connector you must re-enable these role services before updating the connector.

4.2 Red Hat Enterprise Linux Post Installation

4.2.1 Install ColdFusion Hotfixes / Updates

Because Apache is not fully configured yet you will need to login to the ColdFusion administrator via the built-in web server, eg http://localhost:8500/

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

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

If the md5 checksum matches install the hotfix:

```
/opt/coldfusion10/jre/bin/java -jar /opt/coldfusion10/cfusion/hf-
updates/hotfix_XXX.jar
```

Replace hotfix_XXX.jar with the filename of the hotfix jar you are installing, and follow the prompts. The installer will typically attempt to restart ColdFusion when done, you can however disable that, see documentation for details.

4.2.2 Specify permissions on web sites:

```
# chown -R cfusion:webservices /web
# chmod -R 750 /web
```

SELinux requires permissions to allow apache to read the web root, we will copy the permissions from `/var/www` (the default apache web root on RHEL 6, using the `--reference` flag) and apply it to `/web` (our web site partition).

You may consider using `chmod -R 550 /web` instead of 750 if write permission is not needed by ColdFusion on all files or directories.

```
# chcon -R --reference=/var/www /web
```

4.2.3: Specify permissions for ColdFusion Directories

```
chown -R cfusion:root /opt/coldfusion10/
chmod -R 750 /opt/coldfusion10/
```

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

Now to allow access Apache to serve files in the /CFIDE we need to ensure that apache has execute permissions on all parent folders so that it can traverse the directory structure:

```
chown cfusion:webservices /opt/coldfusion10/
chown cfusion:webservices /opt/coldfusion10/cfusion/
chown cfusion:webservices /opt/coldfusion10/cfusion/wwwroot/
chmod 710 /opt/coldfusion10/
chmod 710 /opt/coldfusion10/cfusion/
chmod 710 /opt/coldfusion10/cfusion/wwwroot/
chown -R cfusion:webservices /opt/coldfusion10/cfusion/wwwroot/CFIDE/
chmod 750 /opt/coldfusion10/cfusion/wwwroot/CFIDE/
chcon -R --reference=/var/www /opt/coldfusion10/cfusion/wwwroot/CFIDE
```

4.2.4: Install Apache Connector

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

```
/opt/coldfusion10/cfusion/runtime/bin/wsconfig -ws Apache \
      -dir /etc/httpd/conf/ \
      -cfide /opt/coldfusion10/cfusion/wwwroot/CFIDE/ \
```

```
-bin /usr/sbin/httpd \
-script /etc/init.d/httpd
```

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

> *Starting httpd: httpd: Syntax error on line 1033 of /etc/httpd/conf/httpd.conf: Syntax error on line 2 of /etc/httpd/conf/mod_jk.conf: Cannot load /opt/coldfusion10/config/wsconfig/1/mod_jk.so into server: /opt/coldfusion10/config/wsconfig/1/mod_jk.so: failed to map segment from shared object: Permission denied*

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

First create an empty log file:

```
touch /opt/coldfusion10/config/wsconfig/1/mod_jk.log
```

And an empty shared memory file:

```
touch /opt/coldfusion10/config/wsconfig/1/jk_shm
```

Now lets apply proper file permissions to the connector directory:

```
chown -R cfusion:webservices /opt/coldfusion10/config/wsconfig/1/
chmod -R 640 /opt/coldfusion10/config/wsconfig/1/
chmod 750 /opt/coldfusion10/config/wsconfig/1/mod_jk.so
chmod 660 /opt/coldfusion10/config/wsconfig/1/mod_jk.log
chmod 660 /opt/coldfusion10/config/wsconfig/1/jk_shm
```

Next we need to apply SELinux context to the `mod_jk.so` module, we'll do this by referencing another apache module, we'll pick mod_rewrite.so - just make sure whatever you pick is installed:

```
chcon --reference=/etc/httpd/modules/mod_rewrite.so
/opt/coldfusion10/config/wsconfig/1/mod_jk.so
```

We must also apply the proper SELinux context to the files that `mod_jk` writes to:

```
chcon --reference=/var/log/httpd/access_log
/opt/coldfusion10/config/wsconfig/1/mod_jk.log

chcon --reference=/var/log/httpd/access_log
/opt/coldfusion10/config/wsconfig/1/jk_shm
```

Finally we need to allow Apache to make network connections so `mod_jk` can talk to ColdFusion:

```
setsebool httpd_can_network_connect 1
```

4.2.5 Create a virtual mapping for /CFIDE/scripts

If you are using `cfform` or Ajax Tags you will need to allow access to the files in `/CFIDE/scripts/`. Because files in that directory have contained vulnerabilities in the past it is recommended to only allow access if you require it, and if so, specify an alternate location. In this example we choose /cf-scripts/ you are encouraged to pick a unique value for this alias. Add the following to your `httpd.conf` file:

```
Alias /cf-scripts /opt/coldfusion10/cfusion/wwwroot/CFIDE/scripts/
```

In the above line we have created a virtual mapping `/cf-scripts/` and pointed it to the file path corresponding to the `/CFIDE/scripts/` directory. You will need to specify the mapping you used in the ColdFusion administrator in the *Default ScriptSrc Directory* on the *Server Settings* > *Settings Page*.

4.2.6 Update Java Virtual Machine

The Java Virtual Machine included with the ColdFusion installer may not be the latest JVM supported by Adobe. Download the RPM for the JVM from java.oracle.com. 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.

Locate the `jvm.config` file, (by default it is located in `/opt/coldfusion10/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/coldfusion10/jre
```

Change that line to:

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

The new jvm will be used after ColdFusion is restarted. 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.

4.2.7 Setup Auditing

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

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

```
auditctl -w /opt/coldfusion10 -p wax -k cf10
```

The above will audit all write, attribute change and execute operations on the path `/opt/coldfusion10/` and tag all entries with the filter key `cf10`. Now that the filter key is setup you can query the audit log using `ausearch -k cf10`

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

4.2.8 Add umask to startup script

Edit the `/etc/init.d/coldfusion10` startup script and add the line near the top but below the `#description` comment:

```
umask 007
```

Consider setting a more restrictive umask on for the group permission.

4.3 Post Configuration Settings for Windows and Linux

The following changes should be made to both Windows and Linux installs.

4.3.1 Enable Sandbox Security

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

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

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

If you are running Standard Edition you can still setup a sandbox but you cannot create multiple sandboxes.

4.3.2 Remove Tomcat Web Server on cfusion instance

When you install ColdFusion it will setup the Tomcat web server running on port 8500. This is not needed and should be disabled. Backup and edit the `{cf.instance.root}/runtime/conf/server.xml` file, and remove or comment out the following:

```
<Connector executor="tomcatThreadPool" maxThreads="50"
               port="8500" protocol="org.apache.coyote.http11.Http11Protocol"
```

```
connectionTimeout="20000"
redirectPort="8445" />
```

This must be repeated for each ColdFusion instance created.

4.3.3 Apply any ColdFusion additional Security Patches

Visit: http://www.adobe.com/support/security/ and read all pertinent ColdFusion Security Bulletins. Download and install any relevant security hotfixes not already installed.

4.3.4 Tomcat Shutdown Port

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

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

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

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

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

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

```
SHUTDOWN=8007
```

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

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

4.3.5 Add a connector shared secret

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

Look for a line similar to:

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

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

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

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

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

4.3.6 Additional Tomcat Security Considerations

Consult the Tomcat 7 Security Considerations document (http://tomcat.apache.org/tomcat-7.0-doc/security-howto.html) for additional tomcat specific security settings.

4.3.7 Additional File Security Considerations

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

Section 5: 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.

5.1 Server Settings > Settings

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

Setting	Default	Recommendation	Description
Disable access to internal ColdFusion Java components	Unchecked	Checked	The internal ColdFusion Java components may allow administrative duties to be performed. Some developers may write code that relies on these components. This practice should be avoided as these components are not documented.
Prefix serialized JSON with	Unchecked: //	Checked: //	This setting helps prevent JSON hijacking, and should be turned on. ColdFusion AJAX tags and functions automatically remove the prefix. If developers have written CFC functions with returnformat="json" or use the SerializeJSON function, the prefix will be applied, and should be removed in the client code before processing. Developers can override this setting at the application level.
Maximum Output Buffer size	1024KB	Lower	A lower output buffer size may reduce the memory footprint in some applications.

Setting	Default	Recommendation	Description
Enable In-Memory File System	Checked	Unchecked if not used	If your applications do not require in memory file system uncheck this checkbox. Ensure that you have sufficient heap space to accommodate the memory limit.
Watch configuration files for changes (check every N seconds)	Unchecked	Unchecked	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. 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.

Setting	Default	Recommendation	Description
Enable Global Script Protection	Unchecked	**Understand limitations**, Checked	This setting provides **very limited protection** against certain Cross Site Scripting attack vectors. It is important to understand that enabling **this setting does not protect your site from all possible Cross Site Scripting attacks**. When this setting is turned on it uses a regular expression defined in the file `neo-security.xml` to replace input variables containing following tags: `object`, `embed`, `script`, `applet`, `meta` with `InvalidTag`. This setting does not restrict any javascript strings that may be injected and executed, iframe tags, or any XSS obfuscation techniques. See Appendix A.13 for more information on XSS attack vectors.
Default ScriptSrc Directory	/CFIDE/scripts/	/*somewhere-else*/	Because the scripts directory also contains CFML source code (such as FCKeditor), you should move this directory to a non-default location.

Setting	Default	Recommendation	Description
Missing Template Handler	Blank or /CFIDE/administrator/templates/missing_template_error.cfm	Specified	The missing template handler HTML should be equivalent to the 404 error handler specified on your web server. The default missing template handler allows a potential attacker to get a rough idea of the ColdFusion version in use.
Site-wide Error Handler	Blank or /CFIDE/administrator/templates/secure_profile_error.cfm	Specified	The default site-wide error handler may expose information about the cause of exceptions. Specify a custom siite-wide error handler that discloses the same generic message to the user for all exceptions. Be sure to log the actual exception.
Maximum number of POST request parameters	100	100 or lower	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.

Setting	Default	Recommendation	Description
Maximum size of post data	100MB	As low as possible	If your application does not deal with large HTTP POST operations (such as file uploads, or large web service requests), reduce this size to 1MB. If the application does allow uploads of files set this to the maximum size you want to allow. You should also be able to specify a HTTP Request size limit on your web server.
Request Throttle Threshold	4MB	1MB	ColdFusion will throttle any request larger than this value. If your application requires a large number of concurrent file uploads to take place, you may need to increase this setting.
Request Throttle Memory	200MB	100MB on 32 bit installations.	On a 32 bit installation the default value would be close to 20% of the heap. 64 bit servers allow for much larger heap sizes. Aim for 10% of the maximum heap size as an upper limit for this setting.

5.2 Server Settings > Request Tuning

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

Setting	Default	Recommendation	Description
Maximum number of simultaneous Template requests	25	Tuned based on hardware capabilities, and application characteristics.	When this setting is too high or too low the ability to perform a denial of service attack increases. When too low requests will be queued when the server is placed under load. When too high requests may not be queued under load causing the CPU time of all requests to increase significantly (known as context switching). Find a good medium by performing load tests against your production environment, use the value that has the ability to serve the most requests per second.
Maximum number of simultaneous Flash Remoting requests	5	1 if not using Flash Remoting, otherwise tuned.	If your applications do not use flash remoting set this value to 1. If you do use flash remoting use a load testing approach to find the optimal value for this setting.
Maximum number of simultaneous Web Service requests	5	1 if not using SOAP web services, otherwise tuned	If your applications do not use SOAP web services set this value to 1. Otherwise tune this setting using load tests.

Setting	Default	Recommendation	Description
Maximum number of simultaneous CFC function requests	15	1 if not using Remote CFC function requests, otherwise tuned.	This setting applies only to CFC functions that have access=remote specified, as they are invoked using /example.cfc?method=MethodName. This applies to methods invoked via the ColdFusion AJAX proxy as well. If your applications do not make use of this feature set to 1. Otherwise use load testing to find the optimal value for this setting.
Maximum number of simultaneous Report threads	1	1	Keep this value at 1 unless you are using cfreport heavily.
Maximum number of threads available for CFTHREAD	10	1 if not using cfthread, tuned otherwise.	Set this value to 1 if you are not using cfthread. If you do use cfthread setting a value too high can lead to context switching.
Timeout requests waiting in queue after	60 seconds	5 seconds (Match Request Timeout)	This setting can generally be set equivalent to the *Timeout Requests After* value specified in the Settings section. A lower setting here can mitigate the effectiveness of DOS attacks.
Request Queue Timeout Page	Blank or /CFIDE/administrator/templates/request_timeout_error.cfm	Specified	Specify a HTML file giving the user a message to wait and retry their request again. The message should not disclose the fact that the queue timed out.

5.3 Server Settings > Client Variables

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

5.4 Server Settings > Memory Variables

Setting	Default	Recommendation	Description
Use J2EE session variables	Unchecked	Checked if J2EE interoperability required.	When checked ColdFusion will use the session management of the underlying JEE container (eg Tomcat) instead of it's own CFID/CFTOKEN.
Enable Session Variables	Checked	Unchecked only if not using sessions	Most applications require session variables but if none of the applications on the server require them uncheck this box.

Setting	Default	Recommendation	Description
Maximum Timeout: Session Variables	2 Days	Lower	Two days is generally too long for sessions to persist. Lower session timeouts reduce the window of risk of session hijacking.
Default Timeout: Session Variables	20 Minutes	Lower	Twenty minutes is a good default value, but high security applications will require a lower timeout value.
Cookie Timeout	1440 Minutes	-1	By setting to -1 ColdFusion will set the session cookie as a browser session cookie, which is valid as long as the users browser window is open. As of this writing you cannot specify a value of -1 using ColdFusion administrator, however you can set this value by editing the `sessionCookieTimeout` value in the `neo-runtime.xml` file.
HTTPOnly	Checked	Checked	Session cookies should always be marked as HTTPOnly to prevent JavaScript or other client side technologies from accessing their values (on supported clients).
Secure	Unchecked	Checked if all sites require SSL.	A client will only transmit a *secure* cookie over a secured connection (eg SSL).

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

5.5 Server Settings > Mail

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

5.6 Data & Services > Data Sources

Setting	Default	Recommendation	Description
Login Timeout (sec)	30 Seconds	5 Seconds	Decrease this value to be less than the *Timeout Requests after* setting.

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

5.7 Data & Services > Flex Integration

Setting	Default	Recommendation	Description
Enable Flash Remoting support	Checked	Unchecked if not used.	Disable Flash Remoting if it is not being used.
Enable RMI over SSL for Data Management	Unchecked	Checked if using LiveCycle Data Services ES	Enable and specify a keystore and password if using LiveCycle Data Services ES with Flex.

5.8 Debugging & Logging > Debug Output Settings

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

5.9 Debugging & Logging > Debugger Settings

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

5.10 Debugging & Logging > Logging Settings

Setting	Default	Recommendation	Description
Log directory	{cf-root}/logs		Ensure that the location of this directory has sufficient storage space to hold Maximum File Size multiplied by the Maximum number of archives multiplied by the number of log files (6 or more).
Maximum number of archives	10	Larger	When a log file reaches the Maximum File Size (5000KB by default), it is archived. When the maximum number of archives is reached for a particular log file, the oldest log file is deleted. Some security compliance regulations require that log files are kept for a minimum period of time. Ensure that this value is high enough to retain log files for the required duration.
Use operating system logging facilities	Unchecked	Checked	Certain log entries will be duplicated to syslog on Unix based operating system.

5.11 Event Gateways > Settings

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

5.12 Security > Administrator

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

5.13 Security > RDS

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

5.14 Security > Sandbox Security

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

5.15 Security > Allowed IP Addresses

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

5.16 Server Update > Updates > Settings

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

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

ColdFusion provides a large number of services for developers to take advantage of. Most applications do not make use of all these services, and can therefore be disabled to improve security.

6.1 Servlets and Servlet Mappings in web.xml

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

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

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

```
<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 its 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.

6.2 Disabling RDS if Already Installed

If RDS was installed on the server it may be disabled by placing XML comments around the RDS Servlet Mapping and the RDS Servlet.

Remove 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>
```

Remove the RDS Servlet definition:

```
<servlet id="coldfusion_servlet_8789">
  <servlet-name>RDSServlet</servlet-name>
  <display-name>RDS Servlet</display-name>
  <servlet-class>coldfusion.bootstrap.BootstrapServlet</servlet-class>
  <init-param id="InitParam_103401311065856789">
      <param-name>servlet.class</param-name>
      <param-value>coldfusion.rds.RdsFrontEndServlet</param-value>
  </init-param>
</servlet>
```

6.3 Disabling support for JWS files

JWS Files are Java Web Services files most ColdFusion applications do not use them. To remove support, simply remove the servlet mapping:

```
<servlet-mapping id="coldfusion_mapping_10">
        <servlet-name>CFCServlet</servlet-name>
        <url-pattern>*.jws</url-pattern>
</servlet-mapping>
```

Note that the jws mapping should also be removed on your webserver.

6.4 Disabling the GraphServlet

The `GraphServlet` is used to serve SWF's or images generated by `cfchart` and the deprecated `cfgraph` tags.

Remove Servlet Mappings that point to the GraphServlet:

```
<servlet-mapping id="coldfusion_mapping_2">
        <servlet-name>GraphServlet</servlet-name>
        <url-pattern>/CFIDE/GraphData</url-pattern>
</servlet-mapping>

<servlet-mapping id="coldfusion_mapping_11">
        <servlet-name>GraphServlet</servlet-name>
        <url-pattern>/CFIDE/GraphData.cfm</url-pattern>
</servlet-mapping>
```

6.5 Disabling Flash Remoting Servlet Mappings

If you are not using Flash or Flex Remoting, and don't plan on using the ColdFusion Server Monitor you can remove the the servlet mappings.

Remove Servlet Mappings:

```
<servlet-mapping id="coldfusion_mapping_0">
```

```
        <servlet-name>MessageBrokerServlet</servlet-name>
        <url-pattern>/flex2gateway/*</url-pattern>
</servlet-mapping>

<servlet-mapping id="coldfusion_mapping_1">
        <servlet-name>FlashGateway</servlet-name>
        <url-pattern>/flashservices/gateway/*</url-pattern>
</servlet-mapping>
```

6.6 Disabling Flash Form Servlet Mappings

If you are not using Flash forms (`<cfform format="flash" ...>`)you can disable the servlet mappings used to serve flash forms.

Remove flash form servlet mappings:

```
<servlet-mapping id="coldfusion_mapping_13">
        <servlet-name>CFFormGateway</servlet-name>
        <url-pattern>/CFFormGateway/*</url-pattern>
</servlet-mapping>

<servlet-mapping>
        <servlet-name>CFInternalServlet</servlet-name>
        <url-pattern>/cfform-internal/*</url-pattern>
</servlet-mapping>

<servlet-mapping>
        <servlet-name>CFSwfServlet</servlet-name>
        <url-pattern>*.cfswf</url-pattern>
</servlet-mapping>
```

6.7 Disabling the CFReport Servlet Mapping

If you are not using the cfreport you can change the servlet mapping for *.cfr to point to the CFForbiddenServlet, this servlet will return 403 forbidden response if a cfr file is requested:

```
<servlet-mapping id="coldfusion_mapping_12">
        <servlet-name>CFCServlet</servlet-name>
        <url-pattern>*.cfr</url-pattern>
</servlet-mapping>
```

Change to:

```
<servlet-mapping id="coldfusion_mapping_12">
        <servlet-name>CFForbiddenServlet</servlet-name>
        <url-pattern>*.cfr</url-pattern>
</servlet-mapping>
```

Be sure to remove the .cfr mapping on the web server.

6.8 Remove WSRP Servlet Mapping

The WSRP Servlets and Filters are used to support Web Services for Remote Portlets, a SOAP based API for serving portlets. If this feature is not used the web services
Remove the WSRPFilter Servlet Mapping:

```
<servlet-mapping>
  <servlet-name>WSRPProducer</servlet-name>
  <url-pattern>/WSRPProducer/*</url-pattern>
</servlet-mapping>
```

6.9 Disabling the CFFileServlet Mapping

The CFFileServlet is used to serve dynamically generated assets. It is used to support the following tags cfreport, cfpresentation, and cfimage (with action=captcha and action=writeToBrowser). If you are not using these features you may remove the servlet mapping:

```
<servlet-mapping id="coldfusion_mapping_14">
  <servlet-name>CFFileServlet</servlet-name>
  <url-pattern>/CFFileServlet/*</url-pattern>
</servlet-mapping>
```

6.10 Disabling Remote CFC Invocation

The `CFCServlet` is used to serve SOAP web service requests, remote CFC method invocation (eg file.cfc?method=doSomething), AIR synchronization, and flash remoting. If you do not require these features you can change the servlet mappings that point to the `CFCServlet` to the `CFForbiddenServlet`. Change the servlet mappings:

```
<servlet-mapping id="coldfusion_mapping_8">
    <servlet-name>CFCServlet</servlet-name>
    <url-pattern>*.cfc/*</url-pattern>
</servlet-mapping>

<servlet-mapping id="coldfusion_mapping_4">
        <servlet-name>CFCServlet</servlet-name>
        <url-pattern>*.cfc</url-pattern>
</servlet-mapping>
```

Change to the following:

```
<servlet-mapping id="coldfusion_mapping_8">
    <servlet-name>CFForbiddenServlet</servlet-name>
    <url-pattern>*.cfc/*</url-pattern>
</servlet-mapping>

<servlet-mapping id="coldfusion_mapping_4">
        <servlet-name>CFForbiddenServlet</servlet-name>
        <url-pattern>*.cfc</url-pattern>
</servlet-mapping>
```

Note: it is important that you do not delete these mappings, as this will allow your CFC source code to be downloaded.

6.11 Adding ClickJacking Protection

ColdFusion 10 includes two new 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.

6.12 Security Constraints in web.xml

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

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

Section 7: Patch Management Procedures

Staying up to date with patches is essential to maintaining security on the server. The system administrator should monitor the 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.

Check the following websites frequently:

Adobe Security Bulletins: http://www.adobe.com/support/security/

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

RedHat Security: http://www.redhat.com/security/updates/

Changelog for Apache 2.2 web server: http://www.apache.org/dist/httpd/CHANGES_2.2

To keep updated with ColdFusion 10 updates you can use the server update feature in ColdFusion administrator. Consider setting up an instance to email you when new updates are released. You should also consider following http://blogs.coldfusion.com/ which is published by the ColdFusion engineering team, Shilpi Khariwal's blog (the Security Czar on the ColdFusion engineering team) http://www.shilpikhariwal.com and finally third a third party commercial service http://hackmycf.com/

Appendix A: Sources of Information

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

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

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

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

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

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

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

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

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

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

A.11 - Apache Tomcat 7 Security Considerations: http://tomcat.apache.org/tomcat-7.0-doc/security-howto.html

Appendix B: List of Acronyms

Acronym	Meaning
RHEL	Red Hat Enterprise Linux
IIS	(Microsoft) Internet Information Server
DOS	Denial of Service
SSL	Secure Socket Layer - Protocol often used for https
HTTPS	Hypertext Transfer Protocol Secure - Encryption layer for HTTP
HTTP	Hypertext Transfer Protocol
SSH	Secure Shell - Protocol used to connecting to a remote server, typically on unix.
NTFS	New Technology File System - File System for Windows which allows for fine grained ACL
ACL	Access Control List
XML	Extensible Markup Language
JSP	Java Server Page
JWS	Java Web Service
CFML	ColdFusion Markup Language

RDS	Remote Development Services
XSS	Cross Site Scripting
CSRF	Cross Site Request Forgery. Also referred to as XSRF.
CFC	ColdFusion Component
IP	Internet Protocol

Written by Pete Freitag

For more information

Solution details: *www.adobe.com/go/coldfusion*

Adobe Systems Incorporated
345 Park Avenue
San Jose, CA 95110-2704
USA
www.adobe.com

11/12