



Adobe® ColdFusion® 9 Server Lockdown Guide

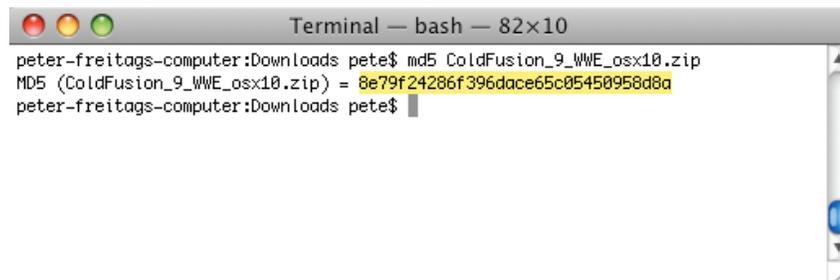
Table of contents

- 1 Prerequisites for all ColdFusion installations
- 2 Prerequisites for a Windows 2008 server installation
- 11 Prerequisites for a RedHat Enterprise Linux 5.3 installation
- 13 Installing ColdFusion
- 16 Windows post installation
- 21 Red Hat post installation
- 22 Post-configuration settings for Windows and Linux
- 23 ColdFusion administrator settings
- 29 ColdFusion server services
- 33 ColdFusion programming security issues
- 34 Patch Management Procedures
- 35 Appendix A: Sources of information

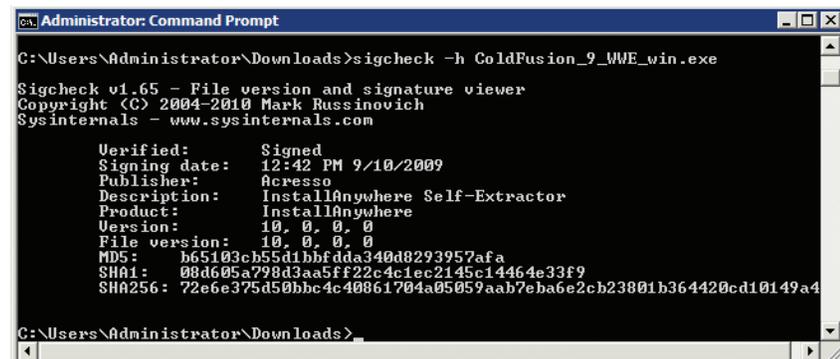
This guide describes how server administrators can improve the security of their ColdFusion server. Although the examples provided are for Microsoft® Windows® 2008 using Internet Information Services (IIS) 7 and Redhat® Enterprise Linux® (RHEL) 5.3 using Apache 2.2, many of the suggestions presented can be extrapolated to apply to similar operating systems and web servers. You should test and validate all suggestions in this document on a nonproduction environment before deploying to production.

Prerequisites for all ColdFusion installations

- Create a separate partition or drive for ColdFusion installation and website assets. This helps reduce path traversal attacks.
- Install the latest security patches for your operating system.
- Install the latest security patches for your web server software.
- Download ColdFusion 9 from Adobe.com
- Verify that the MD5 checksum of the downloaded file matches the MD5 specified on the Adobe.com download page.
- Mac OS X: To obtain the MD5 checksum, start the Terminal application and type `md5 filename`.



- Linux: To obtain the MD5 checksum, open a shell and type `md5sum filename`.
- Windows: Windows installations do not include a MD5 checksum verifier by default. Microsoft provides a free MD5 checksum verifier called Sigcheck as part of the SysInternals toolkit. Download the utility, open the command prompt, and type `sigcheck -h filename`. Sigcheck also verifies the signature of the ColdFusion installation executable (you should see Verified: Signed in the program output).

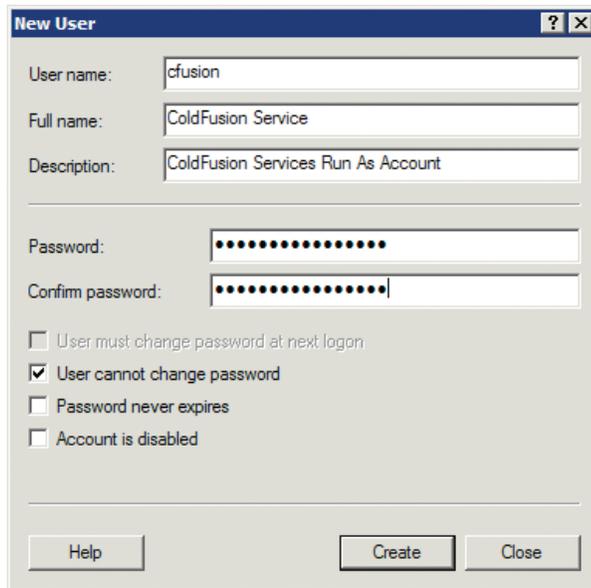


Prerequisites for a Windows 2008 server installation

- Read the Microsoft Windows Security Compliance Management Toolkit (available at www.microsoft.com/downloads/details.aspx?FamilyID=5534bee1-3cad-4bf0-b92b-a8e545573a3e).
- Run Windows Update to ensure that all software is up to date.
- Create a directory for the ColdFusion Administrator website.
- Ensure that all partitions use NTFS to allow for fine-grained access control.

Create users and groups

Create a new user for the ColdFusion service as a Run As account. The example uses cfusion. Choose a username that might not easily be guessed.

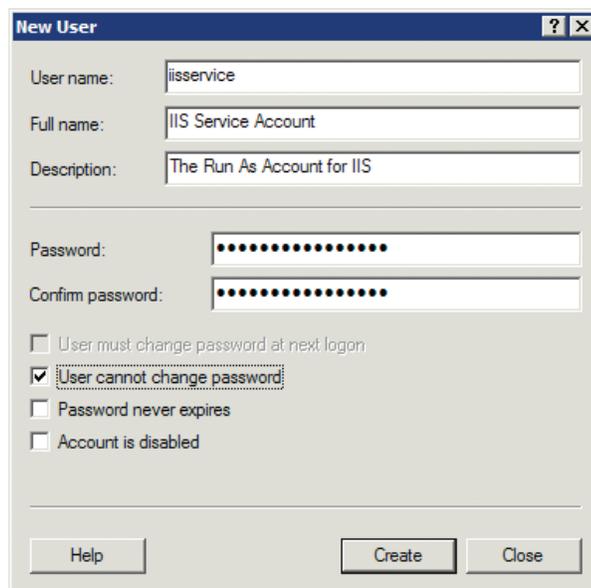


The screenshot shows the 'New User' dialog box with the following fields and options:

- User name: cfusion
- Full name: ColdFusion Service
- Description: ColdFusion Services Run As Account
- Password: [masked]
- Confirm password: [masked]
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

Buttons: Help, Create, Close

Create a new user for the IIS application pool identity.



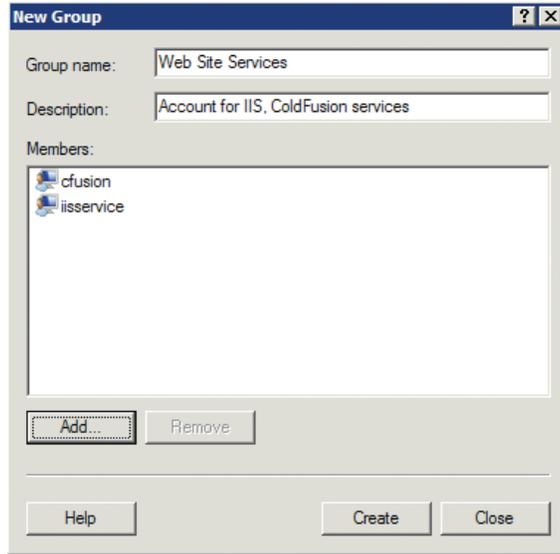
The screenshot shows the 'New User' dialog box with the following fields and options:

- User name: iisservice
- Full name: IIS Service Account
- Description: The Run As Account for IIS
- Password: [masked]
- Confirm password: [masked]
- User must change password at next logon
- User cannot change password
- Password never expires
- Account is disabled

Buttons: Help, Create, Close

For each new user, right-click and select Properties. On the Terminal Services Profile tab, check Deny This User Permission to Log on to Terminal Server.

Create a group and add the ColdFusion and IIS users to it.



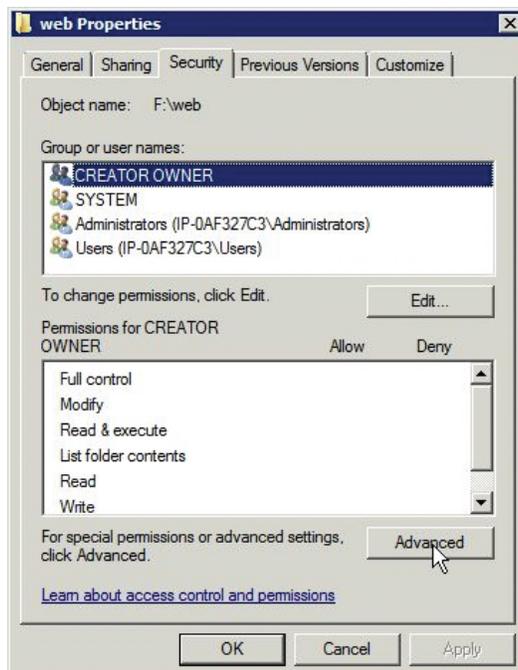
Create a web root for the ColdFusion administrator

Create a separate partition for the CFML source and website assets. For the examples in this guide, it is mapped to drive f:\.

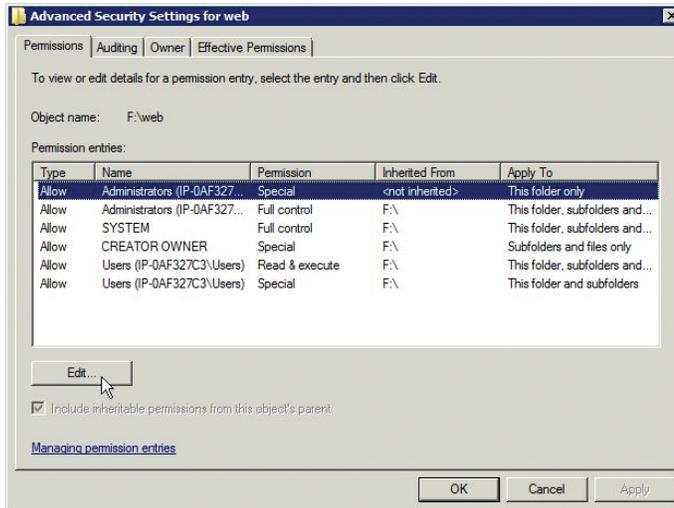
Create a directory to contain the websites, for example, f:\web. Then create a subdirectory to house the ColdFusion Administrator website. This guide uses f:\web\cfadmin\wwwroot, but you can create a different location.

Grant permissions to website root directories

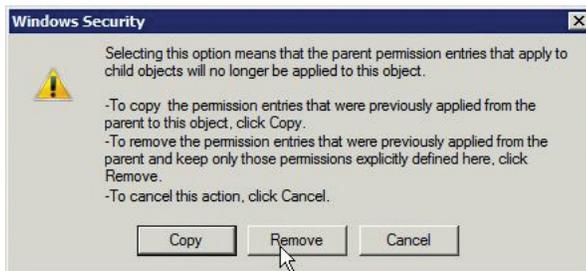
Right-click the website partition folder (for example, f:\web\) and select properties. Select the Security tab and click the Advanced button.



In the Advanced Security Settings dialog box, click the Edit button.



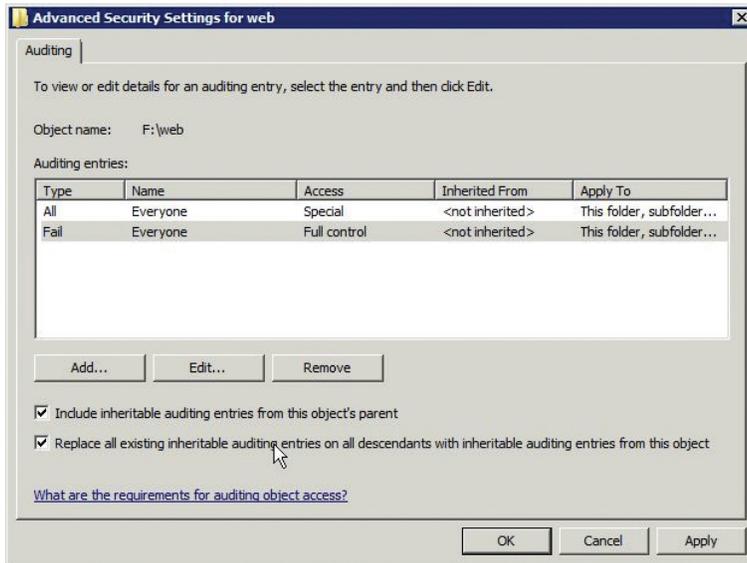
Deselect Include Inheritable Permissions From This Object's Parent. In the confirmation box that appears, select Remove.



Click the Add button, and add the iisservice and cfusion users. Grant them Read and List Folder Contents permissions. Also grant cfusion Write and Delete permissions if your applications make use of the file system via cffile, cfdirectory, and so on. Grant Administrators full control over this folder, and remove any unnecessary privileges.

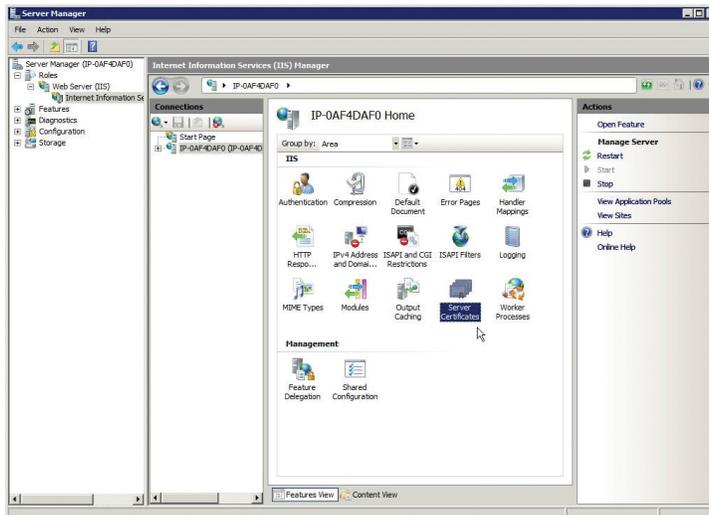
Check the Replace all existing inheritable auditing entries on all descendants with inheritable auditing entries from this object check box to propagate this setting to all subfolders and files existing or created below this folder.

Select the Auditing tab in the Advanced Security Settings dialog box. Click the Edit button and ensure that some level of auditing exists. Auditing can generate a large amount of logs, and it can make the job of monitoring the server logs difficult. Auditing every successful file read in this directory might not be necessary. Use your judgement to determine an appropriate auditing policy based on your security requirements. A good baseline policy is to audit all fails and certain success events (delete, change permissions, and so on).



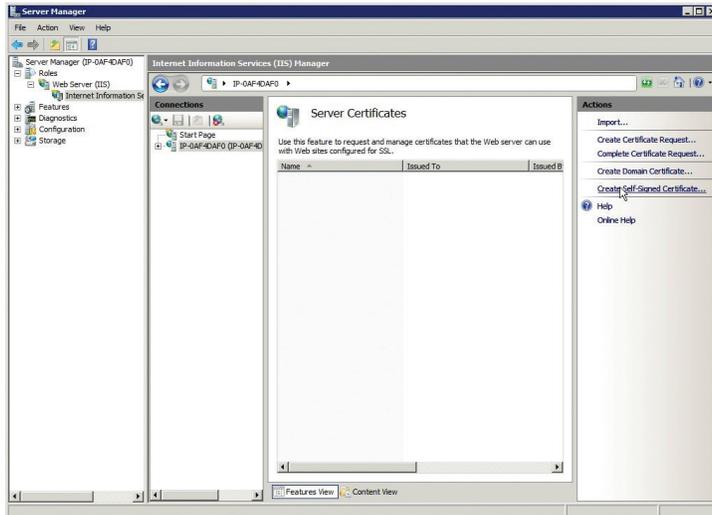
Create or install an SSL Certificate for the ColdFusion administrator website

Open Internet Information Services (IIS) Manager and double-click Server Certificates.

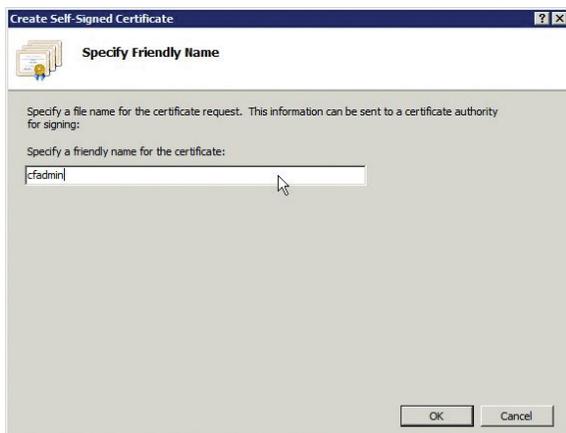


On the right under Actions, click Create Certificate Request to have a certificate signed by a trusted authority. This is the preferred method. If you choose Create Self-Signed Certificate, keep in mind that anyone can create a self-signed certificate.

A certificate signed by a trusted authority is always better than a self-signed certificate because anyone can create a self-signed certificate. To have a certificate signed by a trusted authority, click Create Certificate Request instead.



Follow the steps of the wizard to create an SSL certificate.



Now you should have a certificate called cfadmin that you can use for the ColdFusion administrator website.

Delete the default IIS website

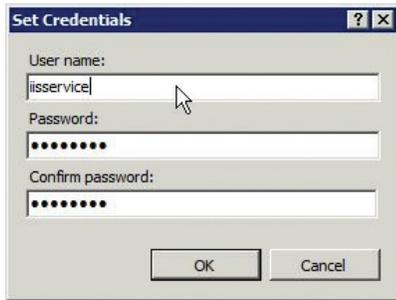
A website is installed with IIS called Default Web Site. Right-click and select Remove.

Change the IIS application pool settings

By default, when a new website is added in IIS, it gets its own application pool. To be able to change the defaults used when a new application pool is created, click Application Pools in IIS Manager. In the Actions menu, click Set Application Pool Defaults.

Change the .NET Framework Version to No Managed Code if your websites do not require .NET.

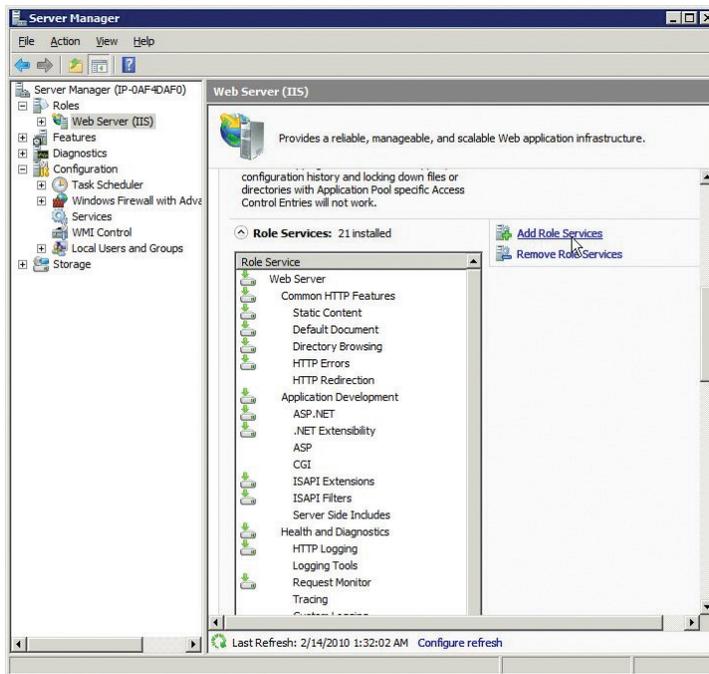
Under Process Model, change the identity to the IIS user that you created (for example, iisservice). You are prompted for the password of this user.



Remove any application pools that are defined and not in use, such as DefaultAppPool.

Add and remove IIS server roles

By default, IIS 7 installs with minimal server roles. To add roles, open Server Manager and select Web Server (IIS) under the Roles.



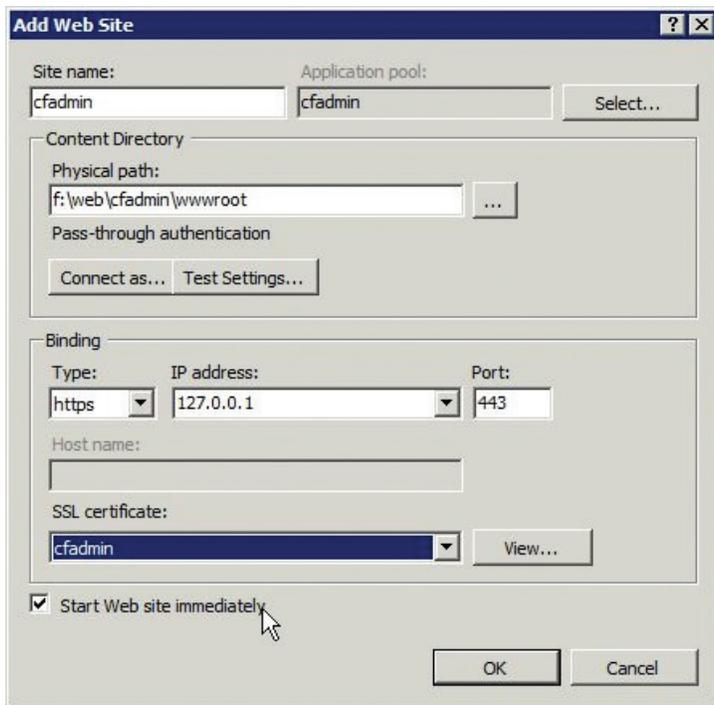
Click Add Role Services to start the Add Role Services wizard. Under Security, select IIS 6 Metabase Compatibility service, which is required for the ColdFusion 9 IIS connection, Request Filtering and Windows Authentication. You might also find it useful to install IP and Domain Restrictions and URL Authorization.



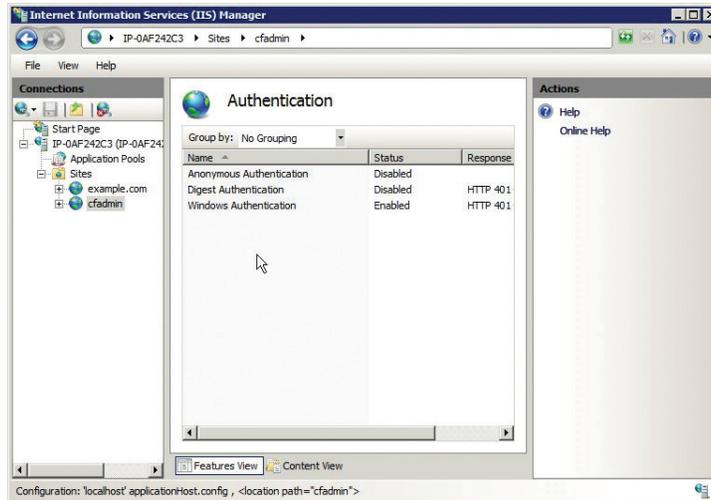
Next remove any roles that are not needed by clicking the Remove Role Services link (for example, if ASP.NET was installed but is not needed).

Create the ColdFusion administrator website

In IIS Manager, right-click Sites and select Add Web Site. For the binding type, use HTTPS and listen on IP address 127.0.0.1 on port 443. Select the cfadmin SSL certificate that you created.

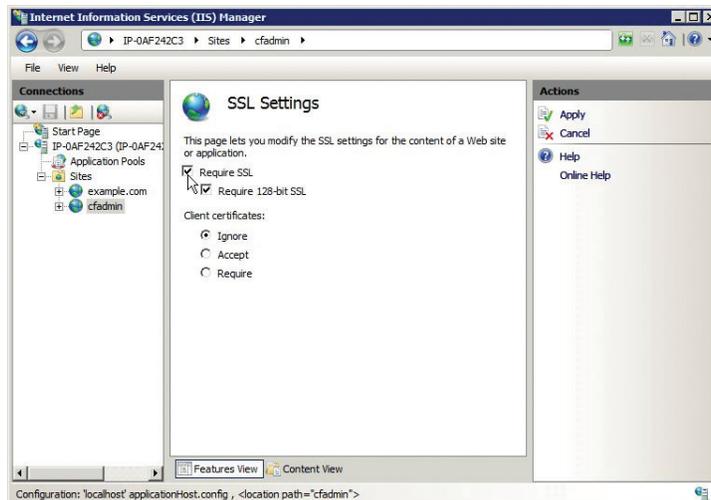


Next, you must ensure user authentication is enabled for the CF Administrator web site. In IIS manager select the newly created CF Administrator site under the Sites node and double-click Authentication. Once in the Authentication screen disable Anonymous Authentication, and enable Windows Authentication.



Note: In order to audit which users are accessing the ColdFusion Administrator, be sure to create dedicated user accounts for each administrator rather than using a single user account.

Next, require SSL connections for this website by double-clicking 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.

Block /CFIDE requests

Even if you do not have a virtual directory specified for /CFIDE on your IIS sites, the ColdFusion IIS connector will still pass through requests for /CFIDE/administrator/index.cfm. Therefore, you must explicitly block /CFIDE requests.

IIS 7 has powerful request filtering capabilities that can enhance the security of your web server. Make sure that the Request Filtering feature is installed. Create a global Request Filtering rule for all sites on the server by editing the applicationHost.config file, which is located in the c:\windows\system32\inetsrv\config directory by default. Before editing the file, make a backup of this file.

This file is an XML configuration file, so all changes must result in a valid XML document. Locate the <requestFiltering> tag, which is located in the <configuration> <system.webServer> <security> <requestFiltering> hierarchy.

Add a child tag to <requestFiltering> named <denyUrlSequences> with the following information:

```
<denyUrlSequences>
  <add sequence="/CFIDE/administrator" />
  <add sequence="/CFIDE/adminapi"/>
  <add sequence="/CFIDE/AIR"/>
  <add sequence="/CFIDE/appdeployment"/>
  <add sequence="/CFIDE/componentutils"/>
  <add sequence="/CFIDE/debug"/>
  <add sequence="/CFIDE/orm"/>
  <add sequence="/CFIDE/portlets"/>
  <add sequence="/CFIDE/probe.cfm"/>
  <add sequence="/CFIDE/scripts"/>
  <add sequence="/CFIDE/services"/>
  <add sequence="/CFIDE/wizards"/>
</denyUrlSequences>
```

If there is already a <denyUrlSequences> tag, append the <add sequence> tags to the existing tag.

Next, you must allow access to the /CFIDE/administrator URI in the cfadmin website. Create a file called web.conf in the web root with the following content:

```
<configuration>
  <system.webServer>
    <security>
      <requestFiltering>
        <denyUrlSequences>
          <remove sequence="/CFIDE/administrator"/>
        </denyUrlSequences>
      </requestFiltering>
    </security>
  </system.webServer>
</configuration>
```

The above configuration overrides the global request filtering and removes the deny rule for the URI /CFIDE/administrator.

If you are using Adobe AIR® synchronization or ColdFusion as a service, you must explicitly allow the URI /CFIDE/AIR and /CFIDE/services, respectively, on a site-per-site basis as done with the ColdFusion administrator website.

If you are not using cfchart or cfgraph, you can simply deny the URI /CFIDE instead of specifying each folder in the CFIDE directory, as done in the above example. The cfchart and cfgraph tags make requests to /CFIDE/GraphData.cfm to serve generated chart files. You cannot allow only that URI if /CFIDE has been globally denied using request filtering in IIS 7.

Now is a good point to take a look at the powerful request filtering capabilities in IIS 7. Request Filtering can be used to greatly enhance the security of your web server.

Prerequisites for a RedHat Enterprise Linux 5.3 installation

Take the following steps before running the ColdFusion installer on Linux. It is recommended that before you install RedHat Enterprise Linux to review the NSA Guide to Secure Configuration of Red Hat Enterprise Linux 5 ([/www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf](http://www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf)).

Install RedHat Enterprise Linux

Create separate partitions for the web roots. This guide uses `/web/` as the mount point for the website partition, but you can use any mounting point.

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

Update installed software and remove unnecessary software

To update software, run:

```
# yum update
```

To see which software packages are installed, run:

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

Remove any packages that are not needed.

Update Apache and remove unnecessary modules

To update Apache, run:

```
# yum update httpd
```

Remove any unnecessary modules. For example:

```
# yum erase php*
```

Edit the `/etc/httpd/conf/httpd.conf` file, and remove any `LoadModule` lines that load unnecessary modules. To get a list of the modules, run:

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

Some of the modules that you might be able to remove include `mod_imap`, `mod_include`, `mod_info`, `mod_userdir`, `mod_status`, `mod_cgi`, and `mod_autoindex`.

For more information on securing the Apache web server, go to www.petefreitag.com/item/505.cfm or see *Apache Security* by Ivan Ristic.

Create users and groups for ColdFusion and Apache

Create a new group to contain both Apache and ColdFusion. This guide uses the name `webservices`, but you can use any name.

```
# groupadd webservices
```

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

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

Create a user for ColdFusion as a Run As account. This guide uses the name `cfusion`, but you can use any name.

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

Specify a password for the new user:

```
# passwd cfusion
```

Add the user to the `/etc/nologin` list of users. This list is used by PAM and is checked by services such as `sshd`.

```
# echo cfusion >> /etc/nologin
```

Configure Apache

Create a directory for the ColdFusion administrator website:

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

Set up the permissions on the web partition:

```
# chgrp -R webservices /web
# chown -R cfusion /web
# chmod -R g+rw /web
# chmod -R o-rwx /web
```

To lock down `/CFIDE`, add the following lines to your `/etc/httpd/httpd.conf` file. This blocks all requests that for all IP addresses that start with `/CFIDE`, except `127.0.0.1`. You might want to change this configuration to the IP address of an administration workstation instead to allow yourself access to the ColdFusion administrator.

```
<Location /CFIDE>
    Order Deny,Allow
    Deny from all
    Allow from 127.0.0.1
</Location>
```

The following configuration allows the URI `/CFIDE/GraphData.cfm` to pass through to ColdFusion. If you are not using `cfchart`, you can skip this step. Alternatively, you can set up a different servlet mapping URI for the `GraphServlet`.

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

Next, 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. It creates a virtual host that allows you to access the ColdFusion administrator at `https://localhost/CFIDE/administrator`.

```
<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>
```

Configure Apache to require SSL for the URI `/CFIDE/administrator`:

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

Require authentication for the /CFIDE/administrator URI. This allows you to audit which administrators have made changes to the administrator settings. The following example uses digest authentication, which requires an up-to-date web browser (IE 6 and earlier might not work correctly).

You must first create a password file. The following command creates or overwrites the password file in the specified location. To add more users, omit the -c flag.

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

Specify permissions so that only root can write to this file and only apache can 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 go to <https://localhost/CFIDE/administrator>. Make sure that you are prompted with a password and that SSL is required. Because ColdFusion is not installed, you should see a 404 error if authentication is successful.

Installing ColdFusion

Run ColdFusion installer

Run the ColdFusion Installer and choose the installation type that best meets your needs.

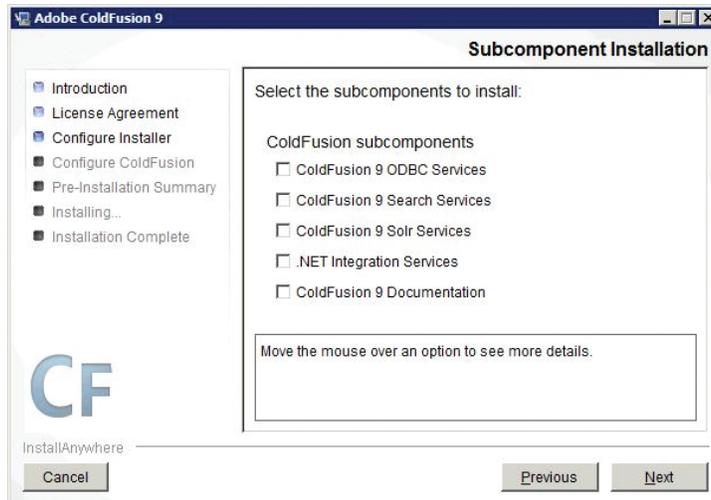
If you only need one instance of ColdFusion, select Server Configuration. This installs an embedded version of Adobe JRun™, and does not install the JRun admin server console, which reduces the attack surface.

Choose Enterprise Multiserver Configuration if you plan on running multiple instances of ColdFusion on this server. This option installs an expanded JRun server and deploys ColdFusion as an enterprise application. Because multiserver is the most common choice, we will be using this configuration throughout the guide. This option installs the JRun admin server, which should be disabled when not in use.

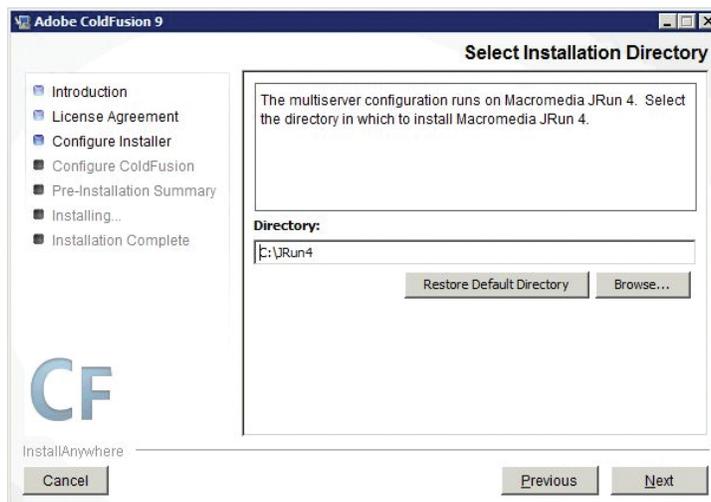
If you plan on installing ColdFusion on a JEE server other than JRun, select J2EE Configuration.



Do not install ColdFusion 9 ODBC servers or ColdFusion 9 documentation. Select only subcomponents that are required for your application.



Select an install directory. On Windows, the default install directory for Multiserver is c:\JRun4 . Select standard directory on a non-system partition.



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 websites 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.

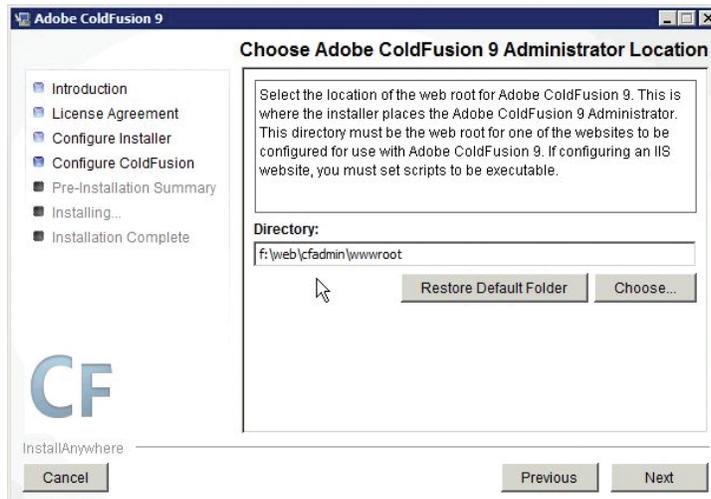
If you are installing on RedHat Enterprise Linux 5, do not install the Apache connector yet. This is done manually later.

You might also consider installing ColdFusion in distributed mode. This allows the web server to reside on a physically separate server from the ColdFusion server. You can also connect multiple web servers to a single ColdFusion server (this is called multihoming in the ColdFusion 9 documentation). This separation can provide additional security and should be considered in environments requiring maximum security. To install distributed mode, select the built-in web server option. For information about configuring distributed mode, see www.adobe.com/support/coldfusion/administration/cfmx_in_distributed_mode/cfmx_in_distributed_mode02.html. For details about multihoming, see http://help.adobe.com/en_US/ColdFusion/9.0/Admin/WSc3ff6d0ea77859461172e0811cbf364104-7fc3.html.

Another 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 still has a web server installed, but all external client requests are handled by the proxy server, and certain requests are sent to the ColdFusion server for processing.



Specify the location of the web root for the ColdFusion Administrator website you have created.



Choose a strong password for the ColdFusion administrator.



Do not enable RDS.



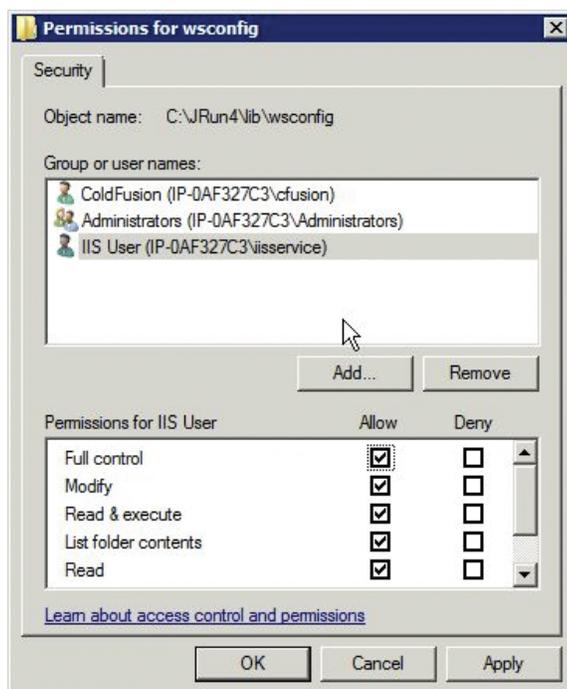
Windows post installation

Follow these steps after you run the ColdFusion installer.

Set up permissions on the ColdFusion installation directory

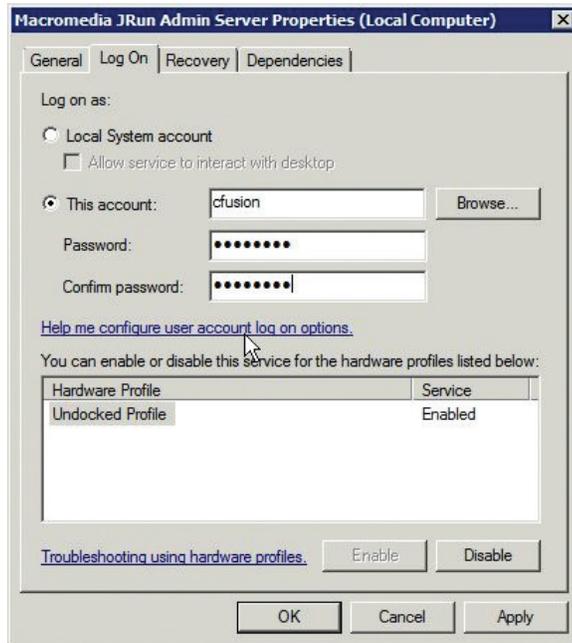
Grant the user that you created for ColdFusion (cfusion in our example) as a Run As account. Grant the Administrators group full control over the ColdFusion installation directory. Enable auditing on this directory as well.

The IIS application pool user (iisservice in our example) must also have permission to access the JRun IIS connector. Grant this user permission to the \lib\wsconfig directory in your ColdFusion installation directory (if you selected the standard configuration, it might be located in \runtime\lib\wsconfig).

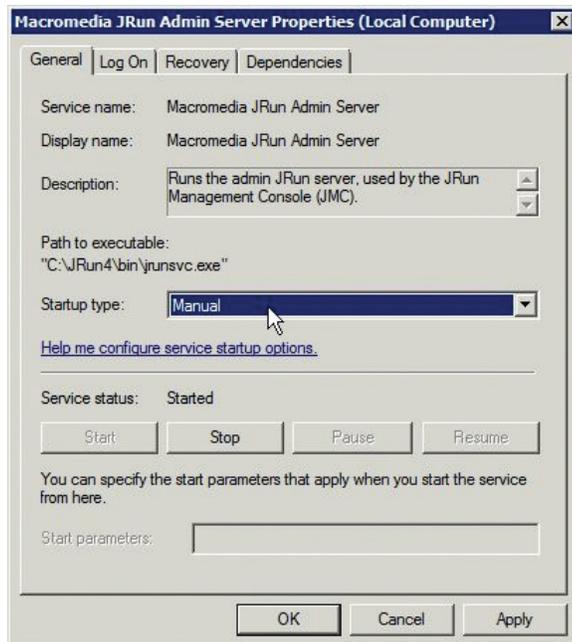


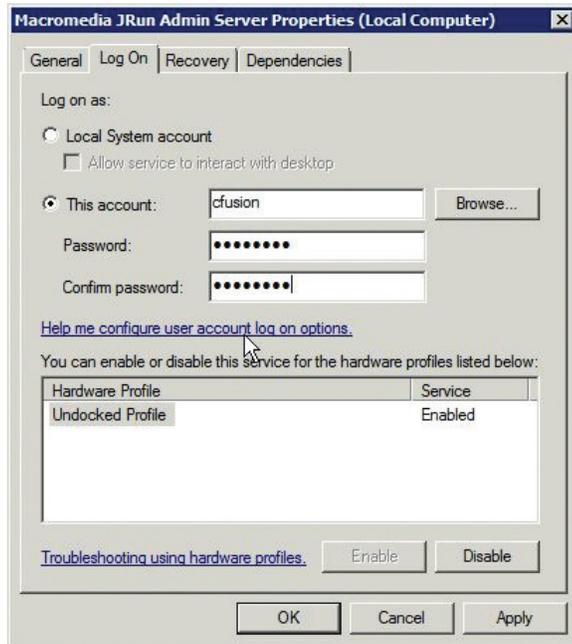
Specify the user for ColdFusion services

Open the Services Manager and change the user that the service runs as to the ColdFusion user that you created. The multiserver installation creates a service named "Macromedia JRun CFusion Server," which runs the initial ColdFusion instance. Right-click the service and click Properties. On the Log On tab of the Properties dialog box, specify the username and password for the account you created.



The ColdFusion Multiserver installation also creates a service called "Macromedia JRun Admin Server." You must also change the log on user for this service and set it to manual startup, instead of automatic. Click Stop to stop the service.





If you installed any optional subcomponents (such as search services), ensure that their services run as the ColdFusion user account as well.

Remove /CFIDE and /cfdocs virtual directories added by installer

If you had any websites set up in IIS when the ColdFusion IIS connector was executed, ColdFusion would have added virtual directory mappings. Open the applicationHost.config file, which is located in the c:\windows\system32\inetsrv\config directory by default. Remove any lines that look like the following:

```
<virtualDirectory path="/CFIDE" physicalPath="F:\web\cfadmin\wwwroot\CFIDE" />
<virtualDirectory path="/cfdocs" physicalPath="F:\web\cfadmin\wwwroot\cfdocs" />
```

Set up a 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, you must set up a virtual directory in each site that uses the cform tag or Ajax tags.

This guide uses /cf-scripts for the virtual directory mapping, but you can use any mapping name for your server.

In the applicationHost.config file, locate the <sites> node. Add a <virtualDirectory> tag with the mapping inside of the <application> tag for each <site> tag. For example:

```
<sites>
  <site name="example.com" id="1">
    <application path="/" applicationPool="coldfusion">
      <virtualDirectory path="/"
        physicalPath="f:\web\example.com\wwwroot" />
      <virtualDirectory path="/cf-scripts"
        physicalPath="f:\web\cfadmin\wwwroot\CFIDE\scripts" />
    </application>
    <bindings>
      <binding protocol="http" bindingInformation="*:80:" />
    </bindings>
  </site>
  <site name="cfadmin" id="2" serverAutoStart="true">
<!-- etc... -->
  </site>
</sites>
```

Set the Default ScriptSrc path on the ColdFusion administrator Server settings page to match the virtual directory path you defined.

Update the Java™ virtual machine

The Java virtual machine (JVM) included with the ColdFusion installer might not be the latest supported by ColdFusion 9. Download the JVM from www.java.sun.com.

Make a backup of the jvm.config file (located in c:\jrun4\bin by default). Using a text editor, locate the line beginning with java.home. For example:

```
java.home=c:\jrun4\jre
```

Change this line to the path of the newly installed JVM. For example:

```
java.home=C:/Program Files/Java/jdk1.6.X_XX/jre
```

The path must use forward slashes. The server does not start if backslashes are used.

Block unused file types

ColdFusion provides a number of capabilities that are not always taken advantage of, such as JSP file execution.

Back up the applicationHost.config file and then edit it to block additional files in IIS 7. Look for the <fileExtensions> tag located inside the <requestFiltering> tag and append the <add> tags to it.

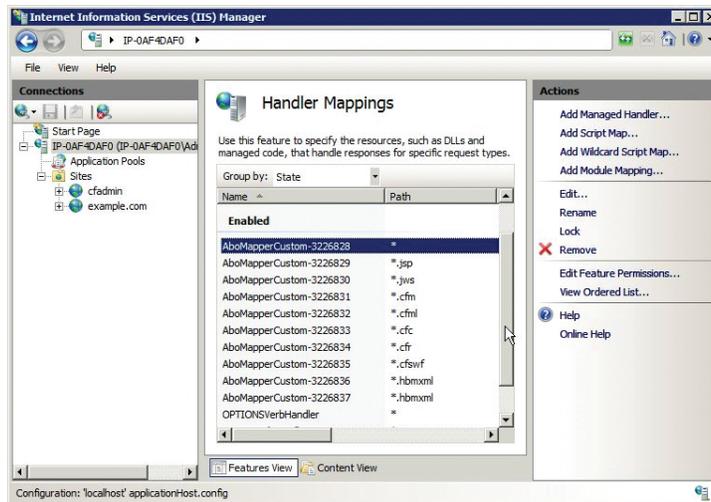
```
<requestFiltering>
  <fileExtensions allowUnlisted="true" applyToWebDAV="true">
    <add fileExtension=".cfml" allowed="false" />
    <add fileExtension=".jsp" allowed="false" />
    <add fileExtension=".jws" allowed="false" />
    <add fileExtension=".hbxml" allowed="false" />
  </fileExtensions>
</requestFiltering>
```

A more robust solution is to specify a white list of allowed file extensions and block the rest. This is done by changing the allowUnlisted attribute to false and specifying only the file extensions that are allowed. Here is a minimal example. You might need to add more extensions to support your application requirements.

```
<requestFiltering>
  <fileExtensions allowUnlisted="false" applyToWebDAV="true">
    <add fileExtension=".cfm" allowed="true" />
    <add fileExtension=".js" allowed="true" />
    <add fileExtension=".css" allowed="true" />
    <add fileExtension=".html" allowed="true" />
    <add fileExtension=".swf" allowed="true" />
  </fileExtensions>
</requestFiltering>
```

Remove unused handler mappings

The ColdFusion installer adds a number of handler mappings on IIS, as shown in the following screen shot:



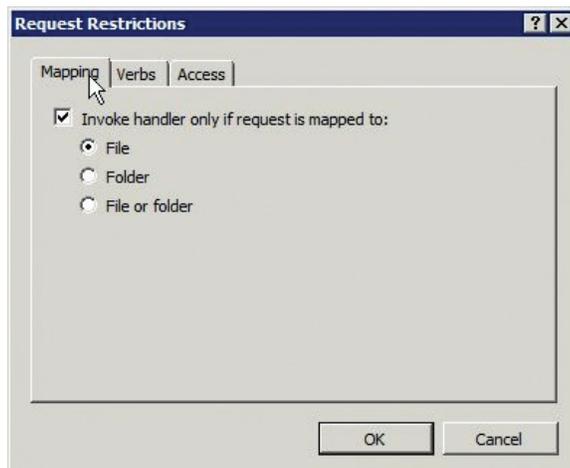
Mappings that are not used can be removed. You should also block the removed extensions using request filtering, as described in the installation section.

Keep in mind that if you remove the mapping for a source file (such as .cfc), the source code might be downloaded when requested if the extension has not been blocked.

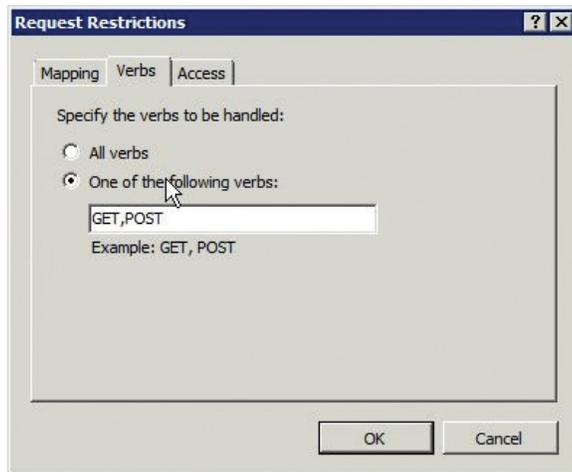
Take note of the path = * mapping. This is a wildcard passthrough that causes all requests to be sent through the ColdFusion connector to determine if the request should be handled by ColdFusion using the mappings defined in web.xml, see Section 6 for more info. Features such as Adobe Flash® forms, flash remoting, and WSRP rely on this wildcard mapping. If these features are not in use, you can remove this mapping.

Configure handler mapping settings

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



On the Verbs tab, specify only the HTTP verbs that the application requires, typically, GET and POST.



Repeat these steps for each ColdFusion handler mapping. The cfswf handler mapping should not check to see if the file exists and only requires the GET verb.

Remove unnecessary binaries

Remove sniffer.exe and migrate.exe from the bin directory of the ColdFusion installation root.

Continue to the section "Post-configuration settings for Windows and Linux" for more post-installation instructions.

Red Hat post installation

Follow these steps after you run the ColdFusion installer.

Specify permissions on websites:

```
# chgrp -R webservices /web
# chown -R cfusion /web
# chmod -R g+rx /web
# chmod -R o-rwx /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 5) using the --reference flag and apply them to /web (the website partition).

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

Specify a shell in the ColdFusion startup script

If you selected Start ColdFusion on System Init during the installation process, you should have a ColdFusion startup script located in /etc/init.d. If you installed the multiserver edition, the script is called coldfusion9multi. Otherwise, it is called coldfusion_9.

Because we created the ColdFusion user shell /sbin/nologin, the ColdFusion startup script will not be able to run. In the startup script, add -s /bin/sh to each line that starts with the su command. For example, if the line looks like this:

```
su $RUNTIME_USER -c "$CF_DIR/bin/jrun -stop cfusion"
```

Change it to:

```
su -s /bin/sh $RUNTIME_USER -c "$CF_DIR/bin/jrun -stop cfusion"
```

There should be at least two lines in the file that require this change.

Remove the cfide symbolic link

The ColdFusion server installation creates the symbolic link `cfide` that points to CFID. This link exists only for convenience and should be removed.

```
# rm /web/cfdamin/wwwroot/cfid
rm: remove symbolic link `cfide'? y
```

Create a virtual mapping for /CFIDE/scripts

If you are using `cform` or `Ajax` tags, you must 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. This example uses `/cf-scripts`, but you should specify the mapping you used for Default ScriptSrc Directory on the ColdFusion administrator Server Settings > Settings page.

```
Alias /cf-scripts /web/cfadmin/wwwroot/CFIDE/scripts
```

Update the Java virtual machine

The JVM included with the ColdFusion installer might not be the latest supported by Adobe. Download the RPM for the JVM from developers.sun.com/downloads. After you run the binary, the JVM is installed in `/usr/java`. A symbolic link is created pointing to the latest installed version in `/usr/java/latest`. Point ColdFusion to this path to simplify further JVM updates.

Back up the `jvm.config` file (located in `/opt/jrun4/bin` by default).

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

Using a text editor, locate the line beginning with `java.home=`. For example:

```
java.home=/opt/jrun4/jre
```

Change the line to:

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

The new JVM will be used after ColdFusion is restarted. Go to the System Information page of the ColdFusion administrator to confirm that the JVM has been updated.

Remove unnecessary binaries

Remove `sniffer` and `migrate` from the `bin` directory of the ColdFusion installation root.

Post-configuration settings for Windows and Linux

Make the following changes to your Windows or Linux installation.

Enable sandbox security

Log in to the ColdFusion administrator and select `Enable Sandbox Security` on the `Security > Sandbox Security` page.

If you are running a multiserver installation, you must add the following configuration at the end of the `java.args` line of your `jvm.config` file. It must be on one line and not have any breaks.

```
-Djava.security.manager -Djava.security.policy={application.home}/servers/cfusion/
cfusion-ear/cfusion-war/WEB-INF/cfusion/lib/coldfusion.policy -Djava.security.
auth.policy={application.home}/servers/cfusion/cfusion-ear/cfusion-war/WEB-INF/
cfusion/lib/neo_jaas.policy
```

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, IP addresses, and 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.

Remove the JRun web server on the cfusion instance

When you install ColdFusion, it sets up the JRun web server running on port 8300. This is not needed and should be disabled. Back up the {cf.install.root}/servers/cfusion/SERVER-INF/jrun.xml file, and then remove the following:

```
<service class="jrun.servlet.http.WebService" name="WebService">
  <attribute name="activeHandlerThreads">25</attribute>
  <attribute name="backlog">500</attribute>
  <attribute name="interface">*</attribute>
  <attribute name="keepAlive">>false</attribute>
  <attribute name="maxHandlerThreads">1000</attribute>
  <attribute name="minHandlerThreads">1</attribute>
  <attribute name="port">8300</attribute>
  <attribute name="threadWaitTimeout">300</attribute>
  <attribute name="timeout">300</attribute>
</service>
```

You must remove this information for each ColdFusion instance created.

Apply ColdFusion and JRun patches

Visit: www.adobe.com/support/coldfusion/downloads_updates.html to obtain any ColdFusion updates.

Important: ColdFusion security hotfixes might not be included in the cumulative hotfix bundles found on this page. Visit: www.adobe.com/support/security to read the pertinent ColdFusion and JRun security bulletins to see if a security hotfix must be applied that is not included in a cumulative hotfix. Download and install any relevant security hotfixes.

ColdFusion administrator settings

Although the server settings described in this section are recommended, changes to some of these settings might affect how your website functions and performs. Be sure to understand the implications of all settings before making any changes.

Server Settings > Settings

To access these settings, select Server Settings > Settings.

Setting	Default	Recommendation	Description
Timeout Requests after	Selected (60 seconds)	Select (5 seconds)	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	Deselected	Select	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 required if J2EE sessions are enabled, however, it doesn't hurt to turn it on.
Disable CFC Type check	Deselected	Deselect	Enabling this setting might allow attackers to cause new exceptions in the application. You can enable this setting if the developer relies on the argument types and has built the application to account for attackers.

Setting	Default	Recommendation	Description
Disable access to internal ColdFusion Java components	Deselected	Select	<p>The internal ColdFusion Java components might allow administrative duties to be performed.</p> <p>Some developers might write code that relies on these components. This practice should be avoided because these components are not documented.</p>
Prefix serialized JSON with	Deselected: //	Select: //	<p>Selecting this setting helps prevent JSON hijacking.</p> <p>If developers have written CFC functions with <code>returnformat="json"</code> or use the <code>SerializeJSON</code> function, the prefix is applied to the result of the function and the client code will need to remove the prefix from the message before processing. Does not apply when using AJAX tags as ColdFusion removes the prefix upon execution of AJAX tags.</p> <p>Developers can override this setting at the application level.</p>
Watch configuration files for changes (check every N seconds)	Deselected	Deselect	<p>If an attacker is able to modify the configuration of your ColdFusion server, the changes can become active within a short period of time if this setting is enabled.</p> <p>If your configuration requires this setting to be enabled (if using WebSphere ND vertical cluster, for example), increase the time as much as possible.</p>
Enable Global Script Protection	Deselected	Select, but understand limitations	<p>This setting provides limited protection against certain cross-site scripting (XSS) attack vectors. Enabling this setting does not protect your site from all possible (XSS) attacks.</p> <p>It uses a regular expression defined in the file <code>neo-security.xml</code> to replace input variables containing the following tags: <code>object</code>, <code>embed</code>, <code>script</code>, <code>applet</code>, <code>meta</code> with <code>InvalidTag</code>. This setting does not restrict JavaScript strings that might be injected and executed, <code>iframe</code> tags, or any XSS obfuscation techniques. See http://hackers.org/xss.html for more information on XSS attack vectors.</p>
Default ScriptSrc Directory	<code>/CFIDE/scripts/</code>	<code>/somewhere-else/</code>	<p>Because the <code>scripts</code> directory also contains CFML source code (such as <code>FCKeditor</code>), move this directory to a non-default location.</p>
Missing Template Handler	Blank	Specify handler	<p>The missing template handler HTML should be equivalent to the 404 error handler specified on your web server.</p> <p>The default missing template handler allows a potential attacker to get a rough idea of the ColdFusion version in use.</p>

Setting	Default	Recommendation	Description
Site-wide Error Handler	Blank	Specify handler	The default site-wide error handler might 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 the actual exception.
Maximum size of post data	100MB	As low as possible	<p>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.</p> <p>If the application does allow uploads of files, set this to the maximum size you want to allow.</p> <p>You should also be able to specify an HTTP request size limit on your web server.</p>
Request Throttle Threshold	4MB	1MB	ColdFusion throttles any request larger than this value. If your application requires a large number of concurrent file uploads to take place, you might 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.

Request Tuning Settings

The Request Tuning settings can help mitigate the ability to perform a successful denial of service (DOS) attack on your server. To access these settings, select **Server Settings > Request Tuning**.

Setting	Default	Recommendation	Description
Maximum number of simultaneous Template requests	10	Tune based on hardware capabilities and application characteristics	When this setting is too high or too low, the ability to perform a DoS attack increases. When too low, requests are queued when the server is placed under load. When too high, requests might 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, tune	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, tune	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	10	1 if not using remote CFC function requests; otherwise, tune	This setting applies only to CFC functions that have access=remote specified, because they are invoked using / example.cfc?method=MethodName. This also applies to methods invoked via the ColdFusion Ajax proxy. If your applications do not make use of this feature, set to 1. Otherwise, use load testing to find the optimal value.
Maximum number of running JRun threads	50	Tuned	This value should be slightly larger than the sum of the simultaneous request maximum settings specified above.
Maximum number of queued JRun Threads	1000	Tune	To mitigate the effectiveness of a DoS attack, ensure that your server has enough resources to handle this amount of queued requests after the maximum number of running threads has been reached. Use the cfstat tool located in the bin directory of your ColdFusion installation to make sure that you fill the queue during testing.
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		If you are not using cfthread, set this value to 1. If you do use cfthread, setting a value too high can lead to context switching.
Timeout requests waiting in queue after	60 seconds		This setting can generally be set equivalent to the Timeout Requests After value specified in the Settings section. A lower setting can mitigate the effectiveness of DoS attacks.
Request Queue Timeout Page	Blank	html file reference	Specify an 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.

Client Variables Settings

To access these settings, select [Server Settings > Client Variables](#).

Setting	Default	Recommendation	Description
Default Storage Mechanism for Client Sessions	Registry	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.

Memory Variable Settings

To access these settings, select Server Settings > Memory Variables.

Setting	Default	Recommendation	Description
Use J2EE session variables	Deselected	Select	When this setting is selected, the session management is handled by the underlying J2EE container. This allows you to specify cookie settings, such as Secure, HttpOnly, domain, path, and expires, in the J2EE configurations. In JRun, this is configured in jrun-web.xml (see www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml for more information). Consult your J2EE server documentation for more information. If you do not enable this setting, ensure that you have selected the Use UUID for cftoken server setting.
Enable Session Variables	Select	Deselect only if not using sessions	Most applications require session variables, but if none of the applications on the server require them, deselect this option.
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 for high-security applications	High-security applications require a lower timeout value. Otherwise, the default is fine.

Mail Settings

To access these settings, select Server Settings > Mail.

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

Data Sources Settings

To access these settings, select 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 server setting.
Query Timeout (seconds)	0 (no timeout)	Specify	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 user that ColdFusion connects as has permissions to only what is necessary.

Flex Integration Settings

To access these settings, select Data & Services > Flex Integration.

Setting	Default	Recommendation	Description
Enable Flash Remoting support	Selected	Deselect if not used	Disable flash remoting if it is not being used.
Enable RMI over SSL for Data Management	Deselected	Select if using Adobe LiveCycle® Data Services ES2	Enable and specify a keystore and password if using LiveCycle Data Services ES.

Debug Output Settings

To access these settings, select Debugging & Logging > Debug Output Settings.

Setting	Default	Recommendation	Description
Enable Robust Exception Information	Deselected	Deselect	When robust exception information is enabled, sensitive information can be disclosed when exceptions occur.
Enable AJAX Debug Log Window	Deselected	Deselect	Do not enable debugging on a production server.
Enable Request Debugging Output	Deselected	Deselect	Do not enable debugging on a production server.

Debugger Settings

To access these settings, select Debugging & Logging > Debugger Settings.

Setting	Default	Recommendation	Description
Allow Line Debugging	Deselected	Deselect	Do not enable debugging on a production server.

Logging Settings

To access these settings, select 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 the 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	Deselected	Select	Certain log entries are duplicated to syslog on UNIX® based operating systems.

Event Gateways Settings

To access these settings, select Event Gateways > Settings.

Setting	Default	Recommendation	Description
Enable ColdFusion Event Gateway Services	Selected	Deselect if not using event gateways	If you do not use event gateways, disable the Event Gateway Service.

Administrator Settings

To access these settings, select Security > Administrator.

Setting	Default	Recommendation	Description
ColdFusion Administration Authentication	Use a single password only	Separate username and password authentication	Using separate usernames and passwords allows you to specify which parts of the ColdFusion administrator each user can use.

Security > Sandbox Security Settings

To access these settings, select Security > Sandbox Security.

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

Allowed IP Addresses

Any IP address in the Security > Allowed IP Addresses list can execute remote services that expose server functionality via web services. To invoke these web services the client must be on the allowed IP address list, and have a username and password. It is recommended that you do not use this feature in environments requiring maximum security.

ColdFusion server services

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 be disabled to improve security.

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>
```

You can remove servlet mappings in the web.xml file to reduce the surface of attack. Typically, you don't want to remove the CfmServlet or its servlet mapping, but other servlets and mappings can be removed.

Be sure to back up web.xml before making changes, because incorrect changes can prevent the server from starting.

Disabling RDS if already installed

If RDS was installed on the server, it can 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>
```

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>
```

You should also remove the JWS mapping on your web server.

Disabling the GraphServlet

The GraphServlet is used to serve SWF files 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>
```

Disabling Adobe 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 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>
```

Disabling Adobe Flash form servlet mappings

If you are not using Flash forms (<cfform format="flash" ...>), you can disable the 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>
```

Disabling the CFReport servlet mapping

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

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

Change the mapping 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.

Removing 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, you can remove the mapping:

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

Disabling the CFFileServlet mapping

The CFFileServlet serves dynamically generated assets. It supports the cfreport, cfpresentation, and cfimage (with action=captcha and action=writeToBrowser) tags. If you are not using these features, you can remove the servlet mapping:

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

Disabling remote CFC invocation

The CFCServlet serves SOAP web service requests, remote CFC method invocation (for example, 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 point 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: Do not delete these mappings because this allows your CFC source code to be downloaded.

ColdFusion programming security issues

While this guide is focused on providing security guidelines for ColdFusion server administrators, a large part of the security burden is placed on the application developer. ColdFusion administrators should become familiar with the following web application vulnerabilities, which are outlined in no particular order.

File upload vulnerabilities

File uploads are potentially dangerous. Uploaded files should not be placed in a directory that might allow remote execution. Ideally, files are stored outside of the web root and served via a static content server, or via cfcontent. For tips on secure file uploads with ColdFusion, see www.petefreitag.com/item/701.cfm.

SQL injection

All ColdFusion variables inside of cfquery tags should be parameterized using the cfqueryparam tag. A simple example of vulnerable code looks like this:

```
<cfquery>
    SELECT * FROM Table
    WHERE id = #url.id#
</cfquery>
```

On many databases, a user can specify an IP address such as script.cfm?id=1;DROP+TABLE to run multiple commands. Even when multiple SQL statements are not supported, there are other ways in which SQL can be manipulated to cause a security risk. The above code should be rewritten as:

```
<cfquery>
    SELECT * FROM Table
    WHERE id = <cfqueryparam value="#url.id" cfsqltype="cf_sql_integer">
</cfquery>
```

Cross-site scripting

Cross-site scripting vulnerabilities allow an attacker to trick users into giving up information about themselves, including usernames, passwords, and session identifiers.

A simple example of code vulnerable to XSS is the following:

```
<cfoutput>Your search for #url.search# did not match any documents</cfoutput>
```

An attacker could pass in JavaScript into the url.search variable, which will be executed on the client's browser.

To prevent XSS, developers must validate and sanitize all variables before they are returned to the client.

Cross-site request forgery

A cross-site request forgery (CSRF) exists when an attacker is able to perform an action on behalf of an authenticated user. For example, suppose you are logged into an application as an administrator, and a malicious user posts a comment with the following HTML code:

```

```

When you visit the page with this img tag, your browser makes a request to the URL /admin/delete-user.cfm?id=1, possibly deleting a user.

Authorization flaws

Authorization flaws might exist in your application if there is reliance on variables that can be manipulated. A common example is relying on a cookie.userid variable to determine if a user is authenticated. An attacker can simply change the value of the cookie.

Session hijacking

The session identifiers equate to a temporary password for any given user. If attackers obtain the session identifier values, they can make requests as the authenticated user.

Ensure that session tokens, such as CFID, CFTOKEN, and JSESSIONID, are not passed in the URL. Users might share the URL with third parties without understanding that their authentication is embedded within the URL. When using cflocation, specify addtoken=false; otherwise, the session IDs are appended to the URL automatically.

Remote file access

Avoid the use of variables in tags or functions that access the file system. For example, the following code allows any file to which ColdFusion has access to be read or executed:

```
<cfinclude template="#url.file#">
```

Denial of service

Developers should be aware of how user input might impact resource utilization. In the following example, an attacker can create a long running page by passing a very large number into the url.limit variable:

```
<cfloop from="1" to="#url.limit#" index="i">
    <!--- doing something --->
</cfloop>
```

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 notifies you by email when vulnerabilities are discovered.

Check the following websites frequently:

Adobe security bulletins: www.adobe.com/support/security

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

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

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

Appendix A: Sources of information

- Microsoft Security Compliance Management Toolkit: www.microsoft.com/downloads/details.aspx?FamilyID=5534bee1-3cad-4bf0-b92b-a8e545573a3e
- NSA Operating System Security Guides: www.nsa.gov/ia/guidance/security_configuration_guides/operating_systems.shtml
- NSA Guide to Secure Configuration of Red Hat Enterprise Linux 5: www.nsa.gov/ia/_files/os/redhat/rhel5-guide-i731.pdf
- JRun Session Config Documentation: http://livedocs.adobe.com/jrun/4/Programmers_Guide/techniques_servlet13.htm
- ColdFusion and SELinux: www.talkingtree.com/blog/index.cfm?mode=entry&entry=28ED0616-50DA-0559-A0DD2E158FF884F3
- ColdFusion MX with SELinux Enforcing: www.ghidinelli.com/2007/12/06/coldfusion-mx-with-selinux-enforcing
- Tips for Securing Apache: 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: www.petefreitag.com/item/701.cfm
- HackMyCF.com Remote ColdFusion vulnerability scanner: <http://hackmycf.com>
- Configuring Distributed Mode: www.adobe.com/support/coldfusion/administration/cfmx_in_distributed_mode/cfmx_in_distributed_mode02.html
- Multihoming: http://help.adobe.com/en_US/ColdFusion/9.0/Admin/WSc3ff6d0ea77859461172e0811cbf364104-7fc3.html
- Cross-Site Scripting Cheat Sheet: <http://hackers.org/xss.html>

Written by Pete Freitag

For more information

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



Adobe

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

Adobe, the Adobe logo, Adobe AIR, AIR, ColdFusion, Flash, JRun, and LiveCycle are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Mac OS is a trademark of Apple Inc., registered in the U.S. and other countries. Linux is the registered trademark of Linus Torvalds in the U.S. and other countries. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat is a trademark or registered trademark of Red Hat, Inc. in the United States and other countries. Java is a trademark or registered trademark of Sun Microsystems, Inc. in the United States and other countries. UNIX is a registered trademark of The Open Group in the US and other countries. All other trademarks are the property of their respective owners.

© 2010 Adobe Systems Incorporated. All rights reserved. Printed in the USA.

91025512 5/10