Hardening ColdFusion

Pete Freitag, Foundeo Inc.

foundeo

Who is Pete Freitag?

- Owner of Foundeo, Inc.
- Blog: petefreitag.com
- 10+ Years working with ColdFusion

Agenda

- Installation Tips
- ColdFusion Administrator Settings
- Sandbox Security
- Hiding Version Information
- Overview of Web App Firewalls

Out of Scope

- Network, Operating System, or Web Server Security
- Writing Secure CFML

However...

- Before Installing ColdFusion...
  - Make sure your OS and Web Server have been patched and updated with the latest security fixes.
  - Make sure your server is behind a network firewall.

Installation Tips

- Choose a non-default installation path.
- Create a dedicated user account for ColdFusion to use.
- Don’t Install Components You Aren’t Using
- Choose a Strong Administrator Password

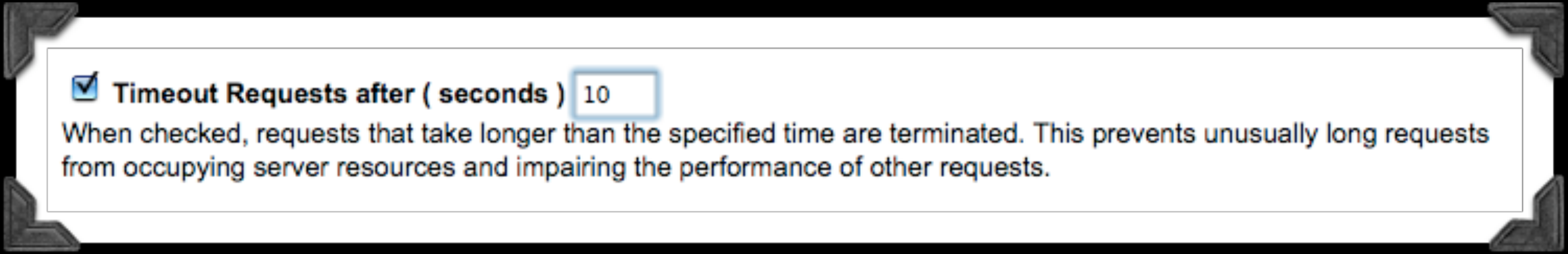
foundeo

Installation Tips

- Make sure ColdFusion Administrator is only accessible via a restricted IP, such as 127.0.0.1
- Require SSL to connect to Administrator.
- Add Web Server Password (useful for auditing who changed what)

ColdFusion Administrator Settings

Server Settings



☑ **Timeout Requests after (seconds)** 10

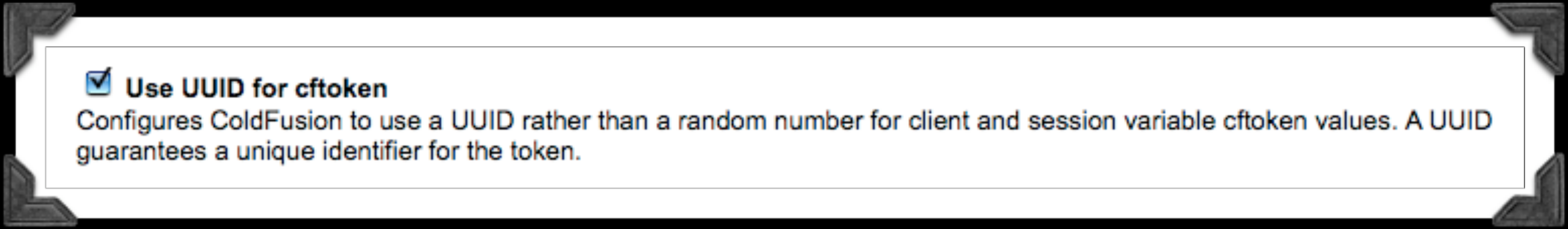
When checked, requests that take longer than the specified time are terminated. This prevents unusually long requests from occupying server resources and impairing the performance of other requests.

Default: 60 seconds
Recommendation: 5-10 seconds

Why: DOS Mitigation

foundeo

Server Settings



☑ **Use UUID for cftoken**

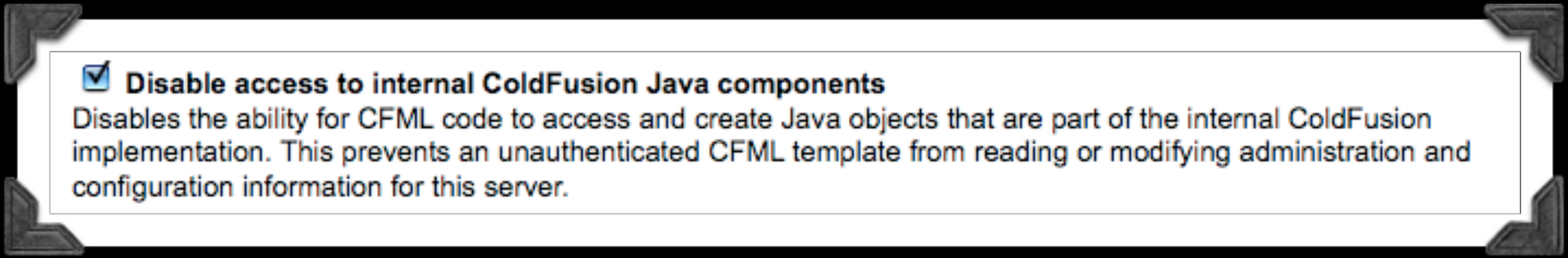
Configures ColdFusion to use a UUID rather than a random number for client and session variable cftoken values. A UUID guarantees a unique identifier for the token.

Default: Unchecked
Recommendation: Checked

Why: Session Hijacking, increases entropy of session id

foundeo

Server Settings



☑ **Disable access to internal ColdFusion Java components**

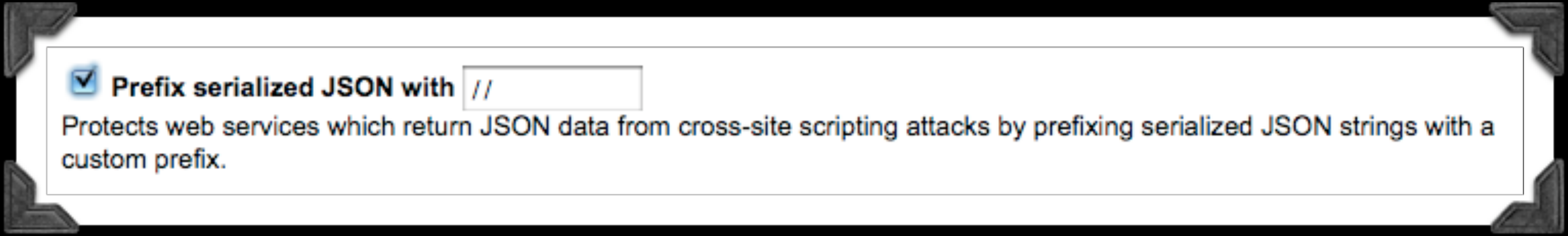
Disables the ability for CFML code to access and create Java objects that are part of the internal ColdFusion implementation. This prevents an unauthenticated CFML template from reading or modifying administration and configuration information for this server.

Default: Unchecked
Recommendation: Checked

Why: Developers can monkey with server. May be used by frameworks or apis.

foundeo

Server Settings



☑ **Prefix serialized JSON with** //

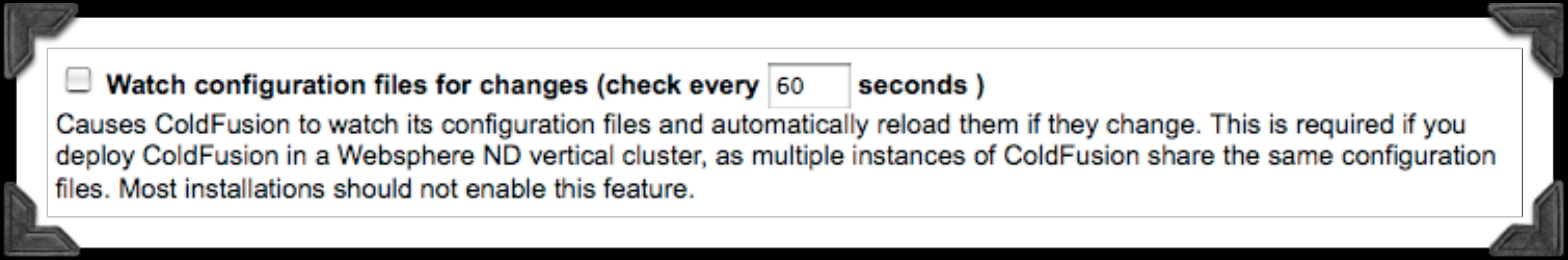
Protects web services which return JSON data from cross-site scripting attacks by prefixing serialized JSON strings with a custom prefix.

Default: Unchecked with “//”
Recommendation: Checked with “//”

Why: JSON Hijacking

foundeo

Server Settings



□ **Watch configuration files for changes (check every** 60 **seconds)**

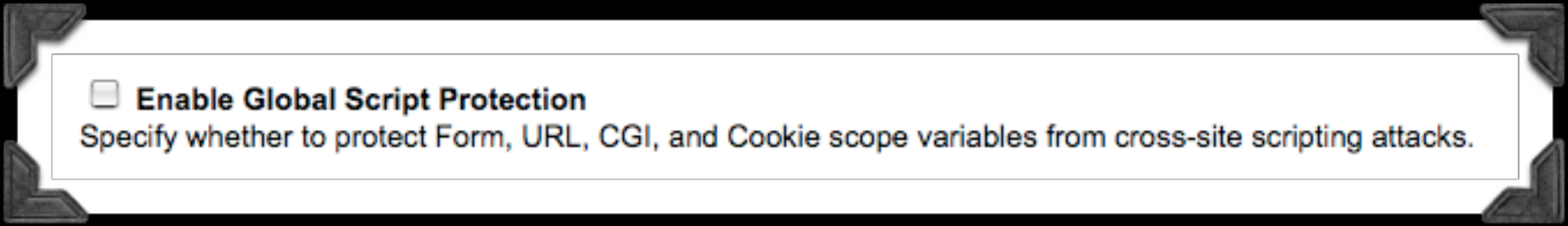
Causes ColdFusion to watch its configuration files and automatically reload them if they change. This is required if you deploy ColdFusion in a Websphere ND vertical cluster, as multiple instances of ColdFusion share the same configuration files. Most installations should not enable this feature.

Default: Checked every 60 seconds
Recommendation: Unchecked

Why: If attacker modifies config it won't take effect until restart, otherwise you need to respond to attacks in less than 60 seconds.

foundeo

Server Settings



□ **Enable Global Script Protection**

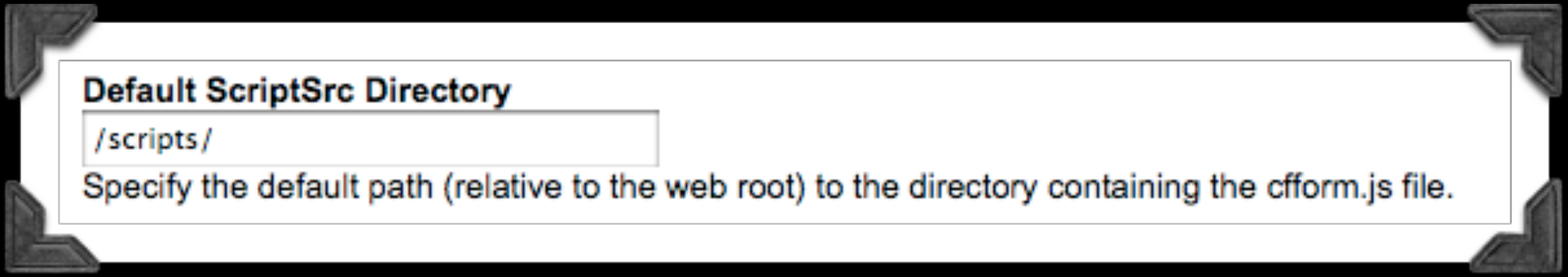
Specify whether to protect Form, URL, CGI, and Cookie scope variables from cross-site scripting attacks.

Default: Unchecked
Recommendation: Understand it

Why: This feature has a VERY LIMITED ability to protect you from Cross Site Scripting. Don’t let this setting give you a false sense of security. See my blog for explanation.

foundeo

Server Settings



Default ScriptSrc Directory

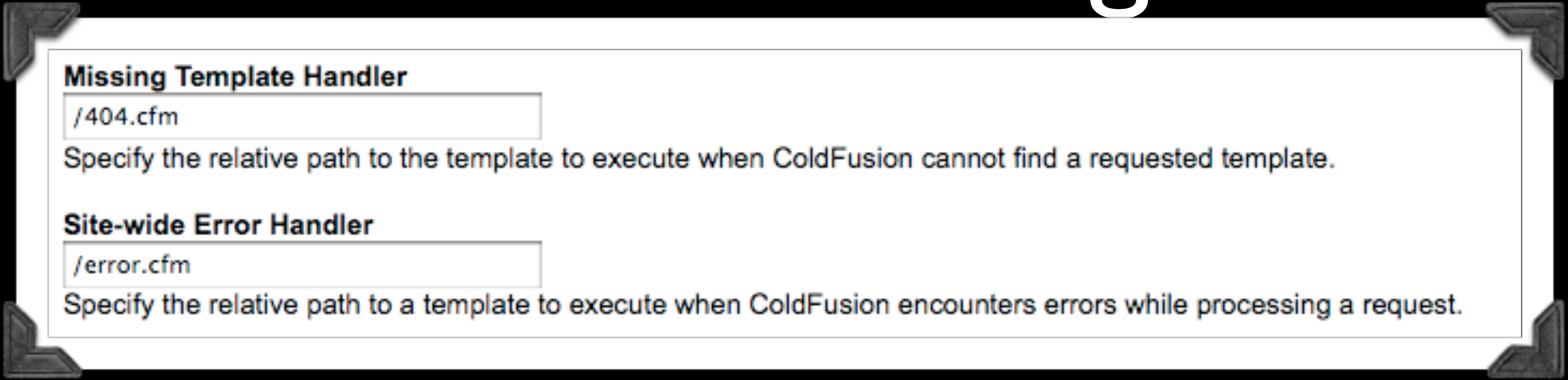
/scripts/

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

Default: /CFIDE/scripts/
Recommendation: Something else

Why: Allows for CF Server Version Detection.

Server Settings



Missing Template Handler

/404.cfm

Specify the relative path to the template to execute when ColdFusion cannot find a requested template.

Site-wide Error Handler

/error.cfm

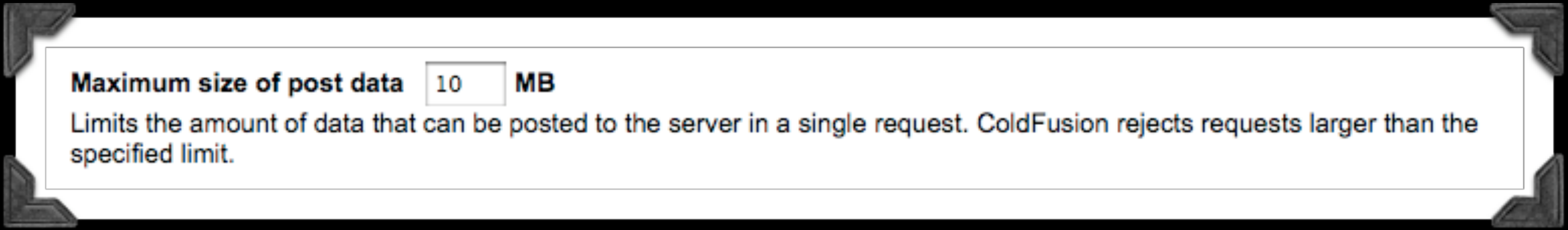
Specify the relative path to a template to execute when ColdFusion encounters errors while processing a request.

Default: Empty
Recommendation: Create custom handlers

Why: Information Disclosure. The default handlers disclose CF, and possibly other information. The missing template handler should match your server 404 handler.

foundeo

Request Size Limits



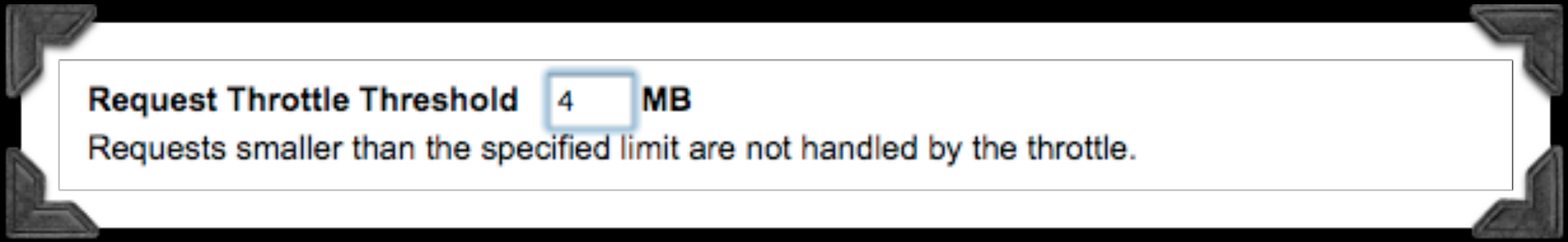
Maximum size of post data 10 **MB**

Limits the amount of data that can be posted to the server in a single request. ColdFusion rejects requests larger than the specified limit.

Default: 100mb
Recommendation: 1-10mb

Why: DOS Mitigation. Most applications only need to upload small files, 100mb is generally too big. This limit can and should be setup on your web server as well.

Request Size Limits



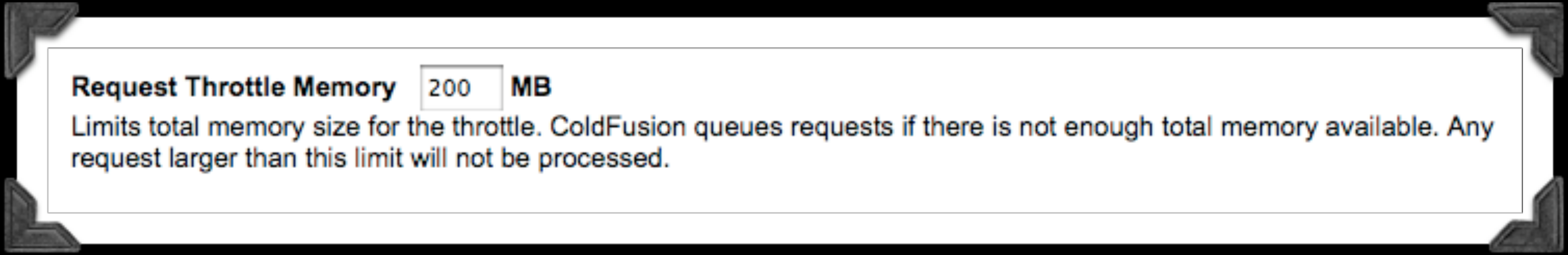
Request Throttle Threshold 4 **MB**

Requests smaller than the specified limit are not handled by the throttle.

Default: 4mb
Recommendation: 1mb

Why: DOS Mitigation. For most applications a majority of requests will be under 1mb.

Request Size Limits



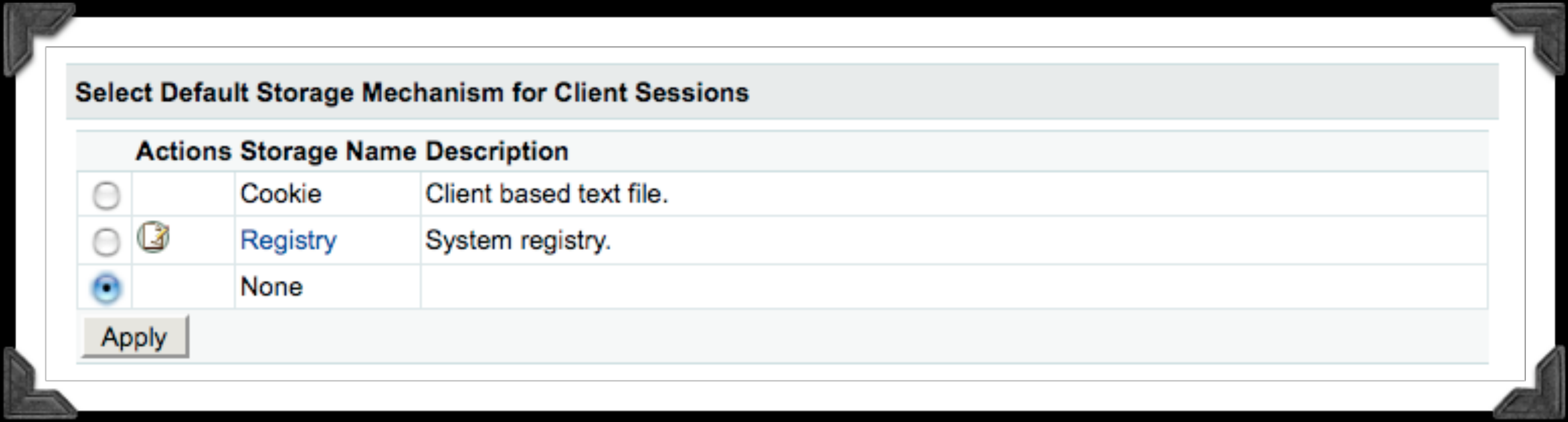
Request Throttle Memory 200 **MB**

Limits total memory size for the throttle. ColdFusion queues requests if there is not enough total memory available. Any request larger than this limit will not be processed.

Default: 200mb
Recommendation: 1-50mb

Why: DOS Mitigation. Limits the total number of queued requests. 200mb of Heap is almost half the default max heap size.

Client Variables



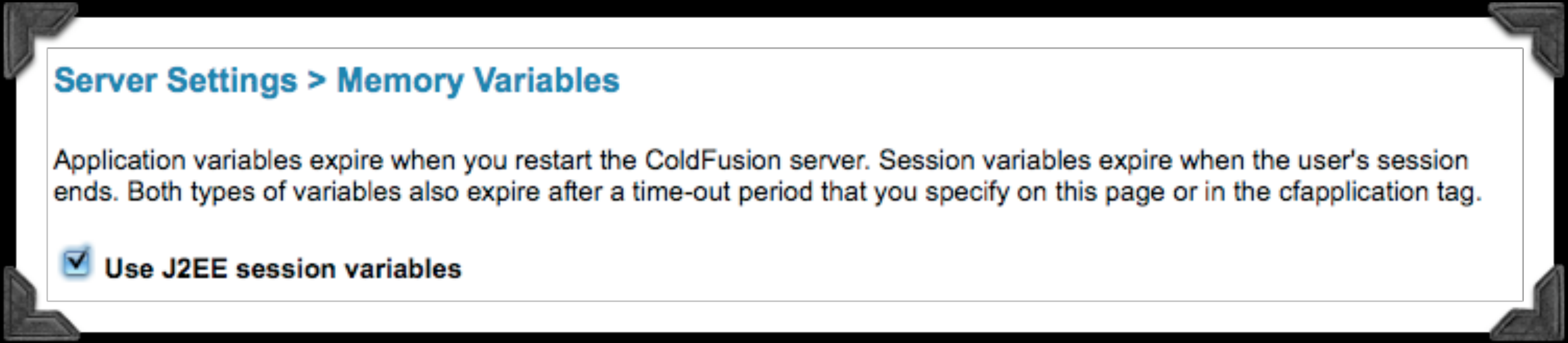
Select Default Storage Mechanism for Client Sessions

	Actions	Storage Name	Description
○		Cookie	Client based text file.
○	✎	Registry	System registry.
●		None	

Default: Registry
Recommended: None

Why: DOS Mitigation.

Memory Variables



Server Settings > Memory Variables

Application variables expire when you restart the ColdFusion server. Session variables expire when the user's session ends. Both types of variables also expire after a time-out period that you specify on this page or in the cfapplication tag.

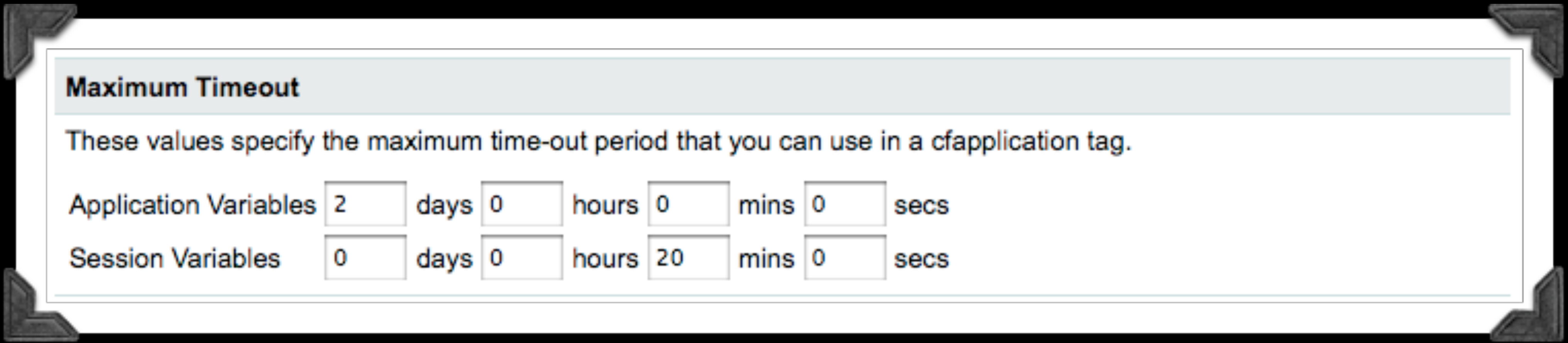
☑ Use J2EE session variables

Default: Unchecked
Recommended: Checked

Why: Session Hijacking. J2EE Sessions use a cookie that expires when the browser closes by default. The generated session id is also typically generated using a highly random algorithm.

foundeo

Memory Variables



Maximum Timeout

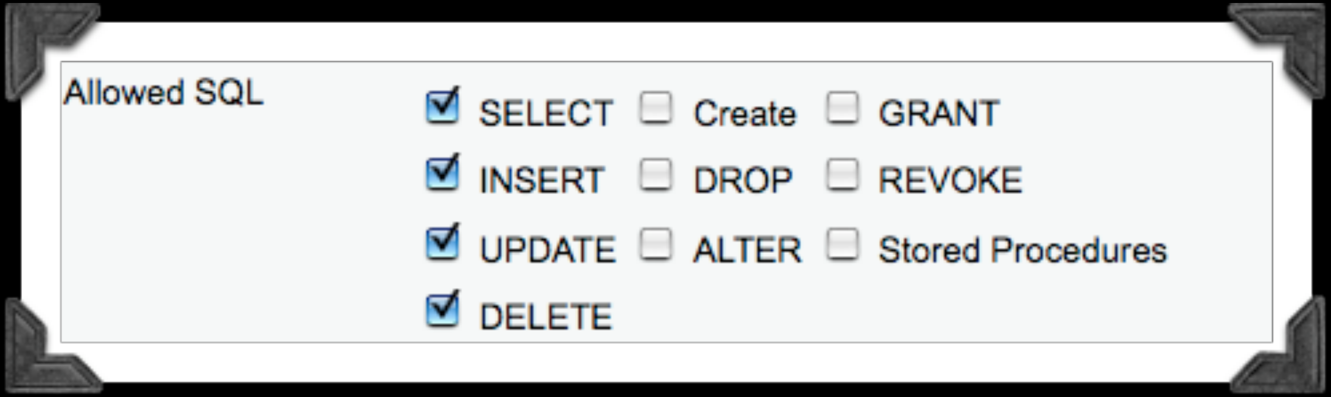
These values specify the maximum time-out period that you can use in a cfapplication tag.

Application Variables	2	days	0	hours	0	mins	0	secs
Session Variables	0	days	0	hours	20	mins	0	secs

Default: 2 days
Recommended: As low as possible

Why: Session Hijacking. The lower the session timeout, the smaller the window of opportunity for session hijacking is.

Datasources



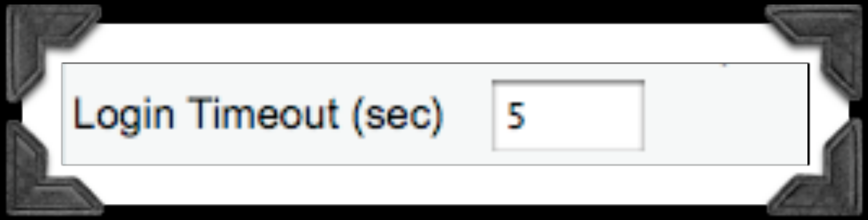
Allowed SQL

☑ SELECT □ Create □ GRANT
☑ INSERT □ DROP □ REVOKE
☑ UPDATE □ ALTER □ Stored Procedures
☑ DELETE

Default: SELECT, INSERT, UPDATE, DELETE, Create, DROP,ALTER, GRANT, REVOKE, Stored Procedures

Recommendation: SELECT, INSERT, UPDATE, DELETE
Or less

Datasources

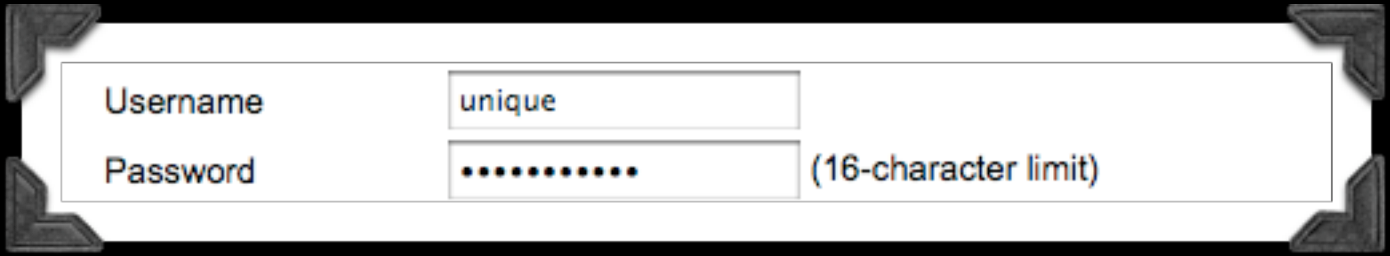


Login Timeout (sec) 5

Default: 30 seconds
Recommendation: 5 seconds

Why: Ties up threads if database is down.

Datasources



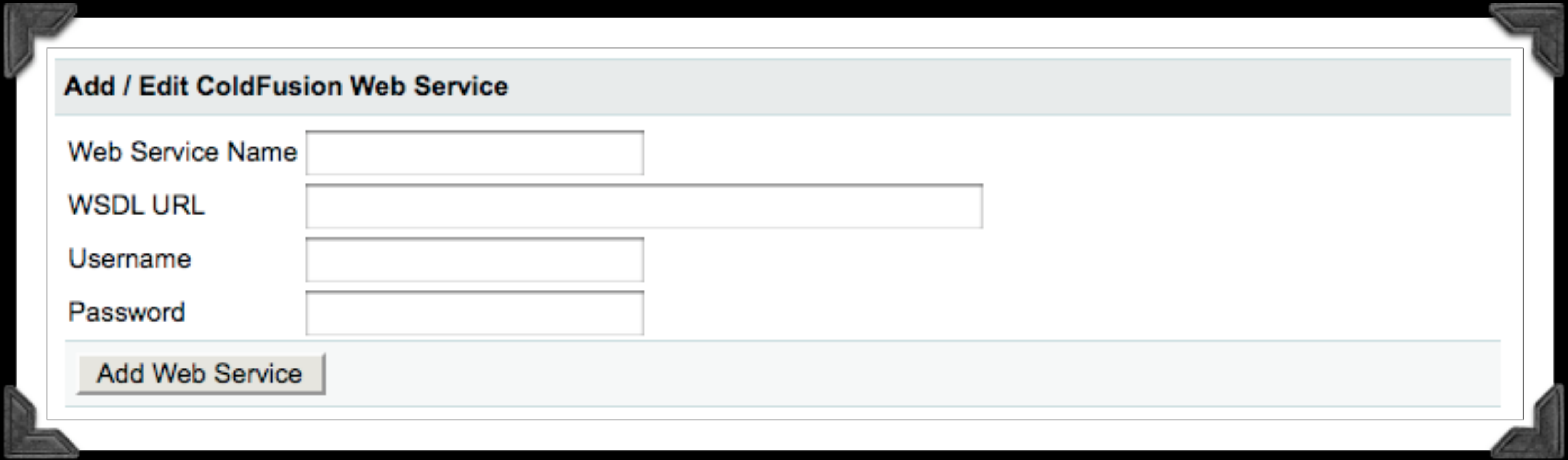
Username	unique	
Password	••••••••••••	(16-character limit)

- Each datasource should have its own username
- DB User should have limited permissions.

Datasources

- Remove Example Datasources

Web Services



Add / Edit ColdFusion Web Service

Web Service Name

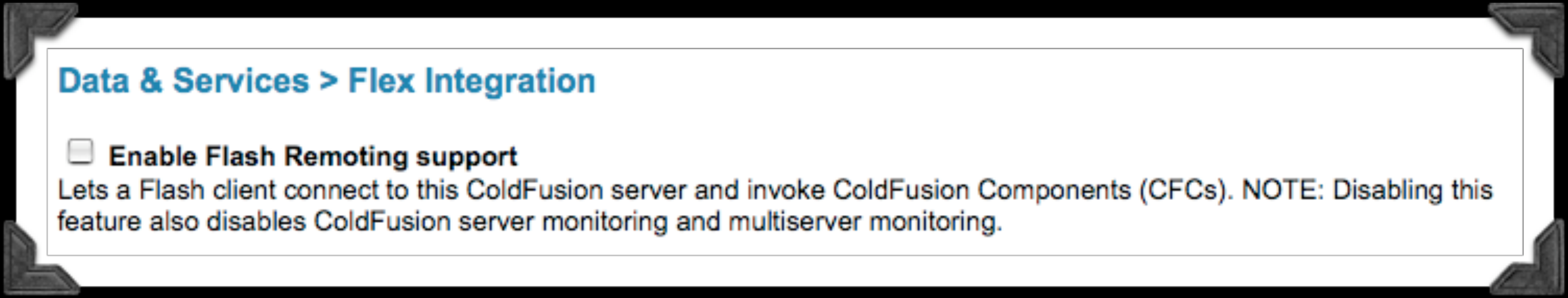
WSDL URL

Username

Password

If you are using Web Services you can hide the end point, username, and password from the code.

Flex Integration



Data & Services > Flex Integration

□ **Enable Flash Remoting support**

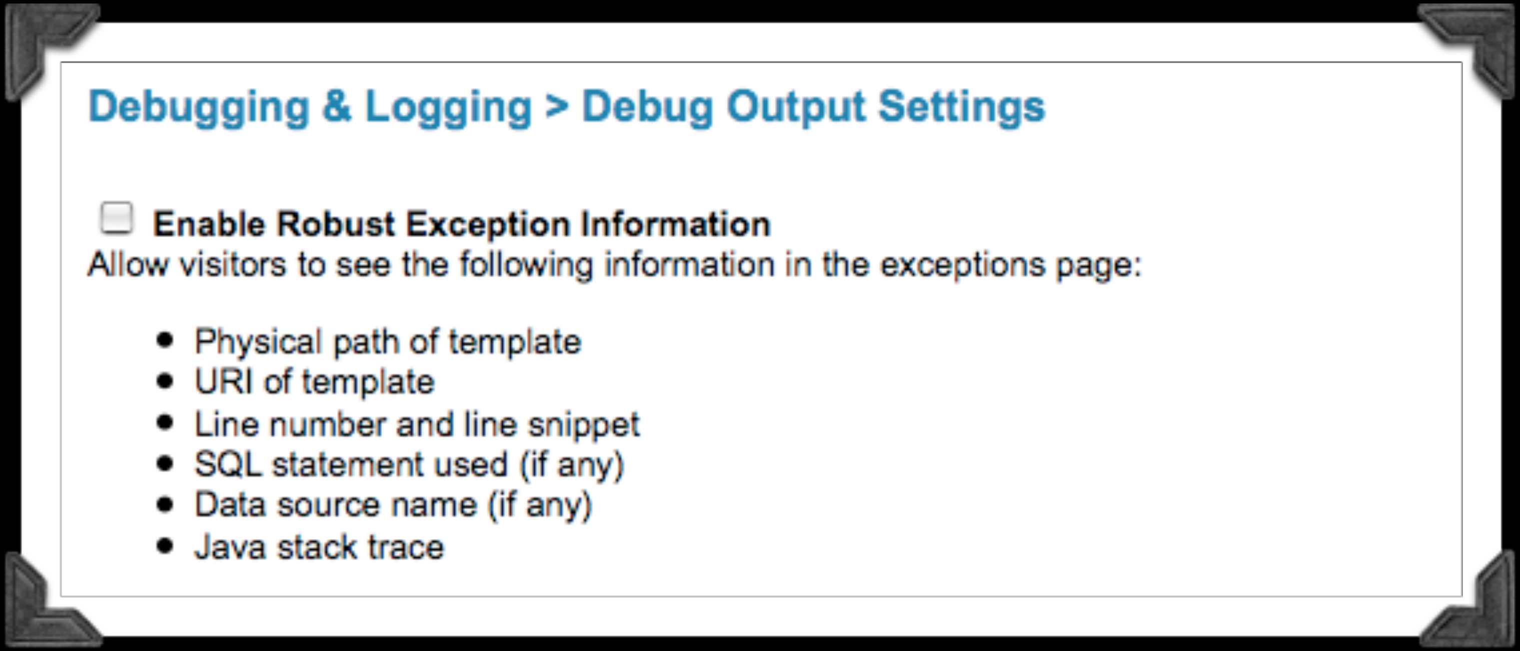
Lets a Flash client connect to this ColdFusion server and invoke ColdFusion Components (CFCs). NOTE: Disabling this feature also disables ColdFusion server monitoring and multiserver monitoring.

Default: Checked
Recommendation: Unchecked if not needed

Why: Anything you can turn off that is not in use should be turned off.

foundeo

Debug Output Settings



Debugging & Logging > Debug Output Settings

□ **Enable Robust Exception Information**
Allow visitors to see the following information in the exceptions page:

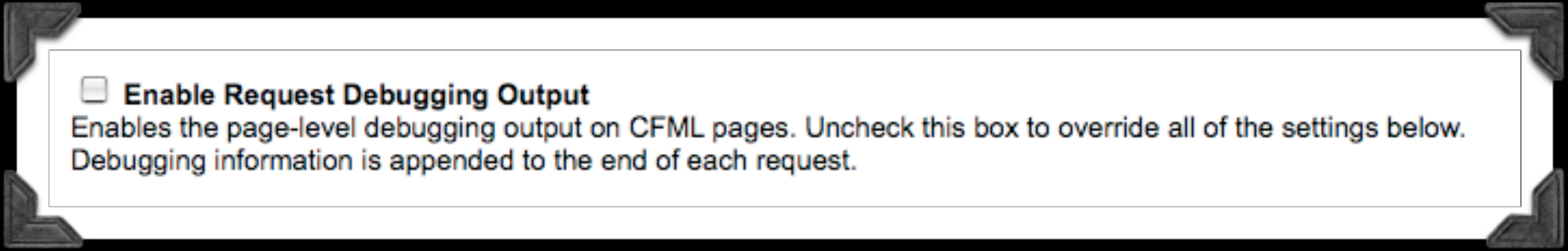
- Physical path of template
- URI of template
- Line number and line snippet
- SQL statement used (if any)
- Data source name (if any)
- Java stack trace

Default: Checked
Recommendation: Unchecked

Why: Information Disclosure. You should NOT disclose paths, SQL, source code, etc.

foundeo

Debug Output Settings



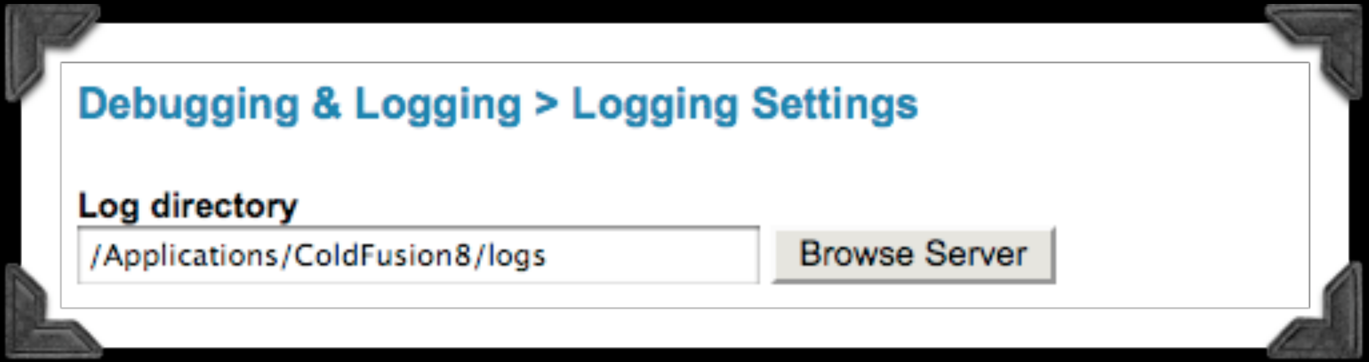
☐ **Enable Request Debugging Output**

Enables the page-level debugging output on CFML pages. Uncheck this box to override all of the settings below. Debugging information is appended to the end of each request.

Default: Unchecked
Recommendation: Unchecked

Why: Information Disclosure

Logging Settings


Debugging & Logging > Logging Settings

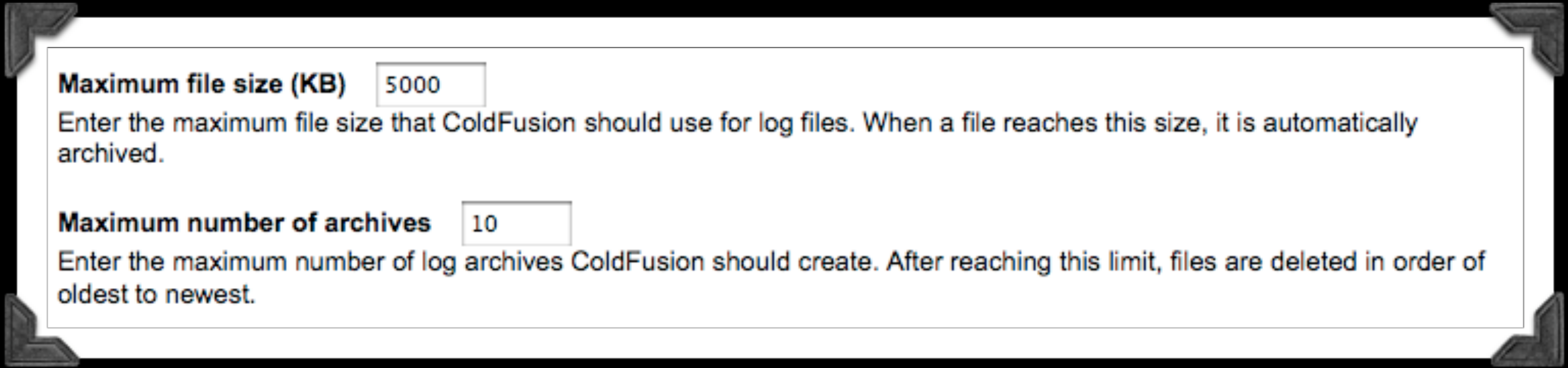
Log directory

/Applications/ColdFusion8/logs

Default: {cfroot}/logs
Recommendation: Somewhere else

Why: Harder for an attacker to cover their tracks

Logging Settings



Maximum file size (KB) 5000

Enter the maximum file size that ColdFusion should use for log files. When a file reaches this size, it is automatically archived.

Maximum number of archives 10

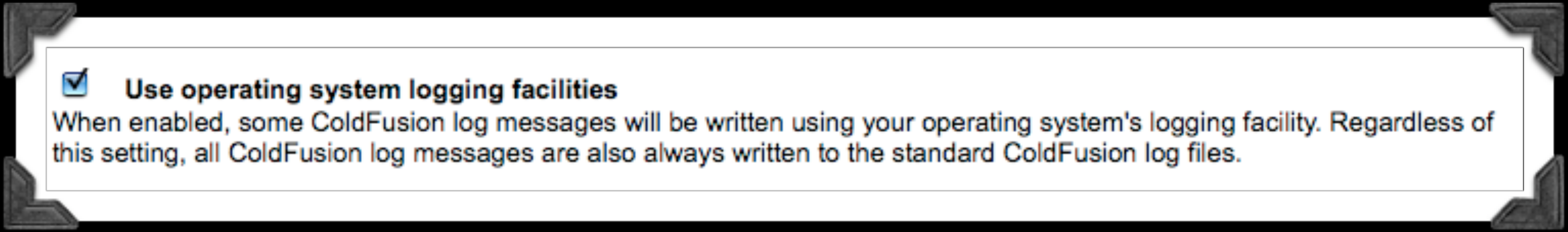
Enter the maximum number of log archives ColdFusion should create. After reaching this limit, files are deleted in order of oldest to newest.

Default: 5000KB, 10
Recommendation: Higher Values

Why: Should be high enough to make sure an attacker can't cover their tracks. PCI or other standards may require you to keep logs for at least a year.

foundeo

Logging Settings



☑ **Use operating system logging facilities**

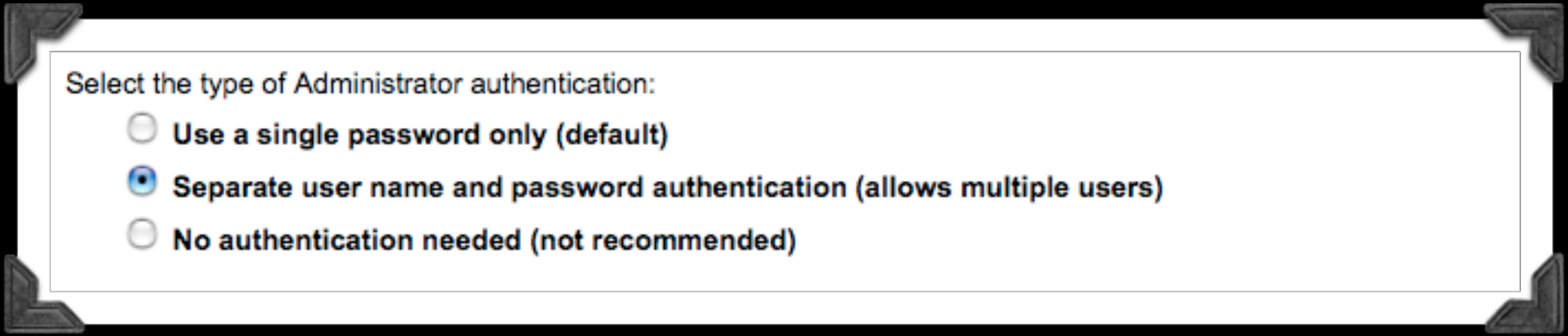
When enabled, some ColdFusion log messages will be written using your operating system's logging facility. Regardless of this setting, all ColdFusion log messages are also always written to the standard ColdFusion log files.

Default: Unchecked
Recommendation: Checked

Why: Lots of tools available to work with syslog

foundeo

Security: Administrator



Select the type of Administrator authentication:

○ Use a single password only (default)

● Separate user name and password authentication (allows multiple users)

○ No authentication needed (not recommended)

Default: Single Username & Password
Recommendation: Separate user name and password

Why: Principal of least privilege.

foundeo

User Manager

- Restrict Access to Parts Of Administrator
- Restrict Access to Admin API
- Restrict Access to sandbox settings
- Unfortunately the super user is always has the username “admin”, can’t change this.

Sandbox Security

- Restrict Access to:
  - Tags
  - Functions
  - Datasources
  - Network IP's and Ports
  - Filesystem Access

Sandbox Security

- Requested Template's Security Policy Overrides any Included Templates
- Remove Execute Permission on directories that shouldn't contain cfm's (such as images, js, or css folders)
  - /images/- (Recursive)
  - /images/* (Folder Only)

Sandbox Security

- May need to edit jvm.config on enterprise / multiserver to enable it.
- You can also setup a sandbox on Standard Edition, however you can only have one sandbox for the entire server.

foundeo

Hiding ColdFusion

- Why Hide It?
    - To mitigate effectiveness of attacks that might target ColdFusion, or a specific version of ColdFusion.

Hiding ColdFusion

- Disable "Server" HTTP Header
    - Discloses Version Numbers
    - A Web Server Setting

Content Generating Tags

- Content Generating Tags May Disclose the ColdFusion Version
  - Examples: cfform, cfchart, ajax tags, etc.

Disable Direct CFC Access

- Can be 404'd with a URL rewriting filter on the web server such as mod_rewrite, or ISAPI Rewrite.
- Or by removing CFCServlet from web.xml
    - Also disables SOAP Web Services

Hiding ColdFusion

- CFM File Extensions
  - Choose a file extension other than .cfm (configured in web.xml)
  - Use mod_rewrite (Apache), or ISAPI Rewrite (IIS).

CFIDE

- Make Sure /CFIDE/* does not resolve.
- /CFIDE/administrator/ better not resolve publicly.

Web Application Firewalls

- Application Layer Firewall for HTTP
- Log, block, filter malicious requests
- Software or Hardware Based
- PCI DSS 6.6
- Commonly called a "WAF"

Foundeo Web App Firewall for ColdFusion

- Commercial Product
- Software Based - written in CFML
- Works on most Shared Hosts
- Works on CF6+, Railo 3+, OpenBD 1+
- CFC API for custom filters and loggers
- http://foundeo.com/security/

Summary

- Eliminate Defaults
- Remove / Disable things that are not used.
- Use the minimum amount of privilege possible.
- Tradeoffs
  - Security vs. Performance
  - Security vs. Usability

Thank You

Questions?

foundeo.com | pete@foundeo.com | petefreitag.com

foundeo