

# Locking Down CF Servers

Pete Freitag, Foundeo Inc.

---

[foundeo.com](http://foundeo.com) | [hackmycf.com](http://hackmycf.com) | [fuseguard.com](http://fuseguard.com)

# About Pete Freitag

---

- ❖ Owner of Foundeo Inc. (Gold Sponsor)
  - ❖ HackMyCF - Remote ColdFusion Security Scanner
  - ❖ FuseGuard - Web App Firewall for CFML
  - ❖ Consulting - Install, Configure, Review, CFML Dev
- ❖ 18+ Years working with CF
- ❖ Author of CF9-2016 Lockdown Guides, CFMX Cookbook (SAMs)
- ❖ blog: [petefreitag.com](http://petefreitag.com) twitter: @pfreitag slack: @foundeo



# Our Focus Today

---

- ❖ Securing your ColdFusion Server Install
- ❖ Not covering:
  - ❖ Hardening Your Operating System
  - ❖ Database Security
  - ❖ Securing your Application Source Code

# Agenda

---

- ❖ Guiding Principals
- ❖ Installation
- ❖ Post Installation Lockdown
- ❖ ColdFusion Administrator Configuration
- ❖ Tomcat Configuration



# Heavily Based on:

---

- ❖ ColdFusion 2016 Lockdown Guide: <http://bit.ly/cf2016lockdown>
- ❖ ColdFusion 11 Lockdown Guide: <http://bit.ly/cf11lockdown>
- ❖ ColdFusion 10 Lockdown Guide: <http://bit.ly/cf10lockdown>
- ❖ ColdFusion 9 Lockdown Guide: <http://bit.ly/cf9lockdown>
- ❖ This talk assumes CF2016, but is most applies for CF10-11 as well
- ❖ CF9 and below are no longer supported (*no more security patches*)



# Why Do I need to Lockdown my install?

---

Can't the installer do everything for me?

What is secure?

What tradeoffs are acceptable?

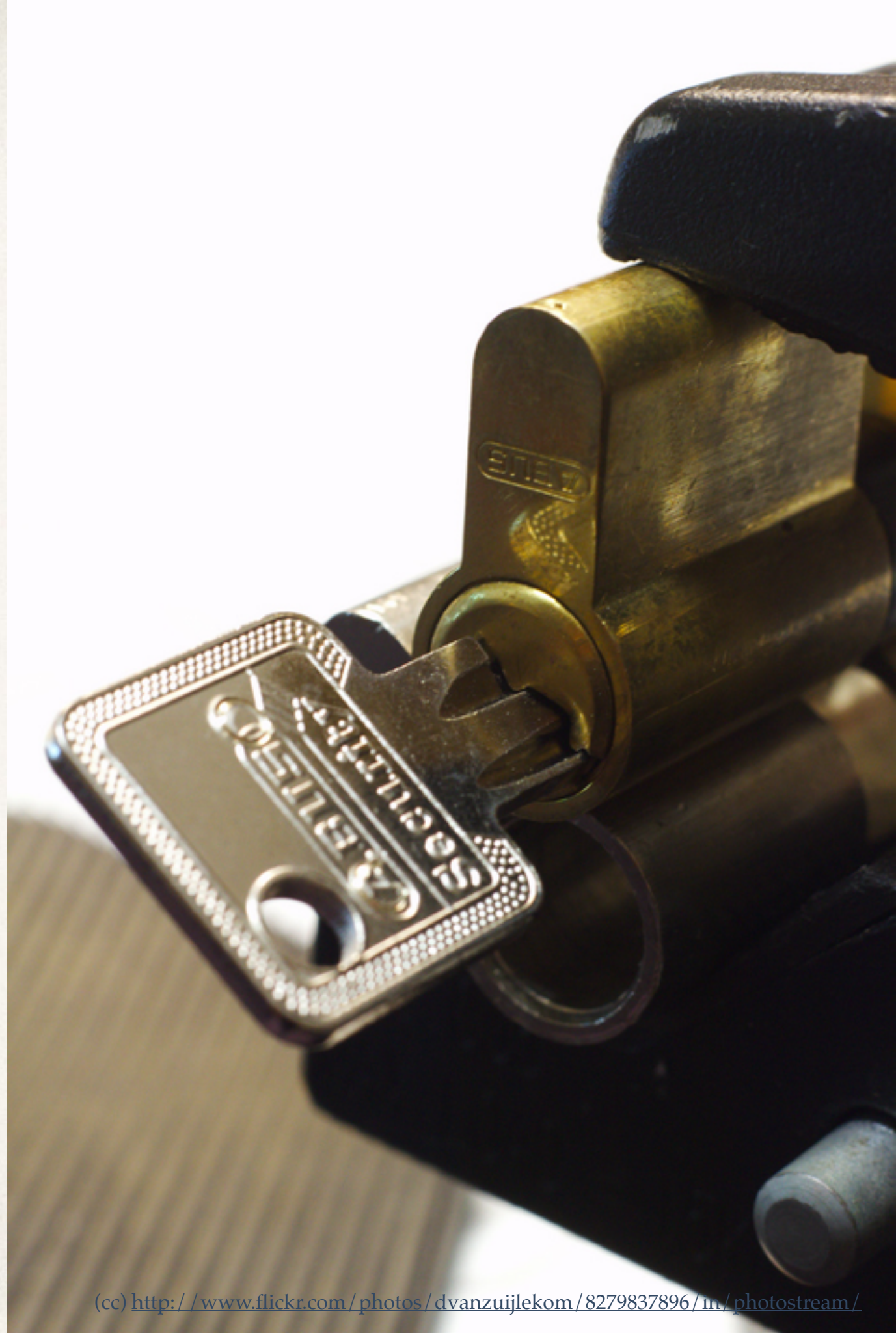




# Principal of Least Privilege

---

Grant only the minimum permission  
required to accomplish a task.





# Defense in Depth

---

Multiple Layers of Redundant Security.







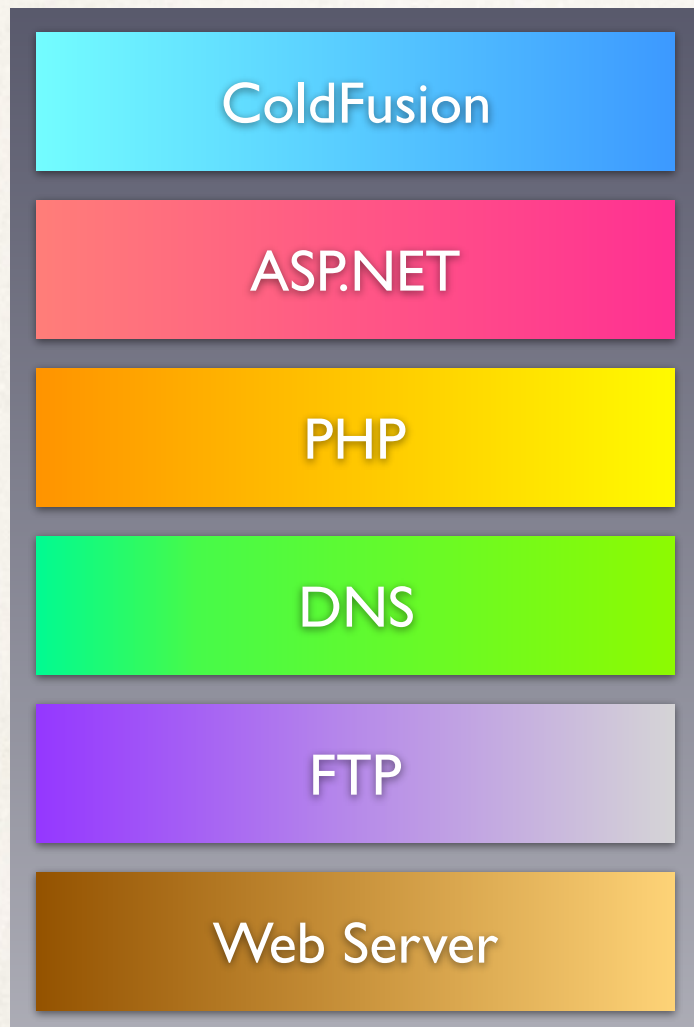
# Reduce Attack Surface

---

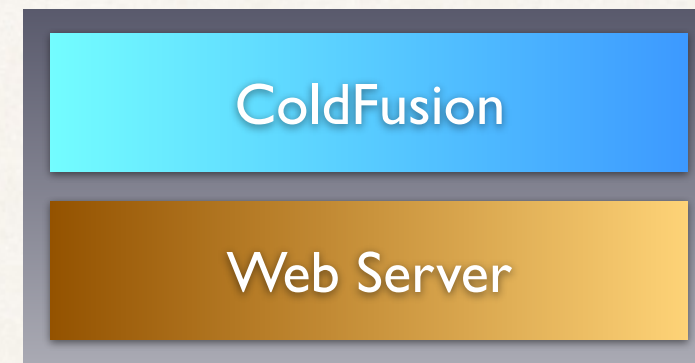


# Reduce Attack Surface

---



**VS**





# Avoid Defaults

---

Avoid using defaults for configurable options such as paths, usernames, etc.





# Security Tradeoffs

---

- ❖ **Security vs Usability**

- ❖ 5 second session timeout?
- ❖ Force password change too frequently.

- ❖ **Security vs Performance**

- ❖ Is HTTP vs HTTPS still a performance tradeoff? See: [www.httpvshttps.com](http://www.httpvshttps.com)

- ❖ **Security vs Time / Money**

- ❖ There is often no visible difference to stakeholders between secure and insecure.
- ❖ Security often not viewed as worthy investment until it is too late.



# Lockdown Guide Tips

---

- ❖ **Time** - Be prepared to spend some time performing the steps (2-4 hours, or more)
- ❖ **Test often** - most steps that will break something if performed incorrectly will tell you to test.
- ❖ **Decide** - the lockdown guide gives you guidance and instructions but it does not dictate that every step must be performed. Access the tradeoffs and implications as you go.



# What's New in CF2016 Lockdown

---

- ❖ `/CFIDE` is blocked by web server connectors by default
- ❖ `/CFIDE/scripts` moved to `/cf_scripts/scripts`
- ❖ Ships with Tomcat 8 instead of Tomcat 7
- ❖ Rearranged Lockdown Guide to *hopefully* improve workflow.



# Pre-Installation

---

- ❖ Lockdown and Patch OS
  - ❖ OS Vendors have Lockdown Guides as well.
    - ❖ [https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/6/html/Security\\_Guide/](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/)
    - ❖ Windows Security Compliance Toolkit: <http://technet.microsoft.com/en-us/library/cc677002.aspx>
- ❖ Ensure network firewall in place.
  - ❖ Remove all unnecessary software.



# Pre-Installation

---

- ❖ Windows: Create multiple partitions OS, CF, Web Root.
  - ❖ Limits impact of a path traversal vulnerability.
- ❖ Create a user account for CF to run as.



# Install Web Server

---

- ❖ IIS - Install Minimal Role Services:
  - ❖ Common HTTP Features: Default Document
  - ❖ Common HTTP Features: HTTP Errors
  - ❖ Common HTTP Features: Static Content
  - ❖ Health and Diagnostics: HTTP Logging
  - ❖ Security: Request Filtering
  - ❖ Security: IP and Domain Restrictions
  - ❖ Application Development: .NET Extensibility 4.5 (or latest version)
  - ❖ Application Development: ASP.NET 4.5 (or latest version)
  - ❖ Application Development: CGI
  - ❖ Application Development: ISAPI Extensions
  - ❖ Application Development: ISAPI Filters
  - ❖ Management Tools: IIS Management Console



# Internet Information Services (IIS) Manager

FOUNDEO-PFLD

File View Help

## Connections



- Start Page
- FOUNDEO-PFLD (WIN-KIRDR)
- Application Pools
- Sites
  - example.com

Site Level

Global / Server Level



## FOUNDEO-PFLD Home

Filter:

Go

Show All

Group by: Area

### ASP.NET



.NET  
Authorizat...



.NET  
Compilation



.NET Error  
Pages



.NET  
Globalization



.NET Trust  
Levels



Application  
Settings



Connection  
Strings



Machine Key



Pages and  
Controls



Providers



Session State



SMTP E-mail

### IIS



Authentic...



CGI



Compression



Default  
Document



Directory  
Browsing



Error Pages



FastCGI  
Settings



Handler  
Mappings



HTTP Respon...



IP Address  
and Doma...



ISAPI and  
CGI Restri...



ISAPI Filters



Logging



MIME Types



Modules



Output  
Caching



Request  
Filtering



Server  
Certificates



Worker

## Actions

[Open Feature](#)

### Manage Server

[Restart](#)

[Start](#)

[Stop](#)

[View Application Pools](#)

[View Sites](#)

[Get New Web Platform Components](#)

[Help](#)

Features View

Content View

Ready



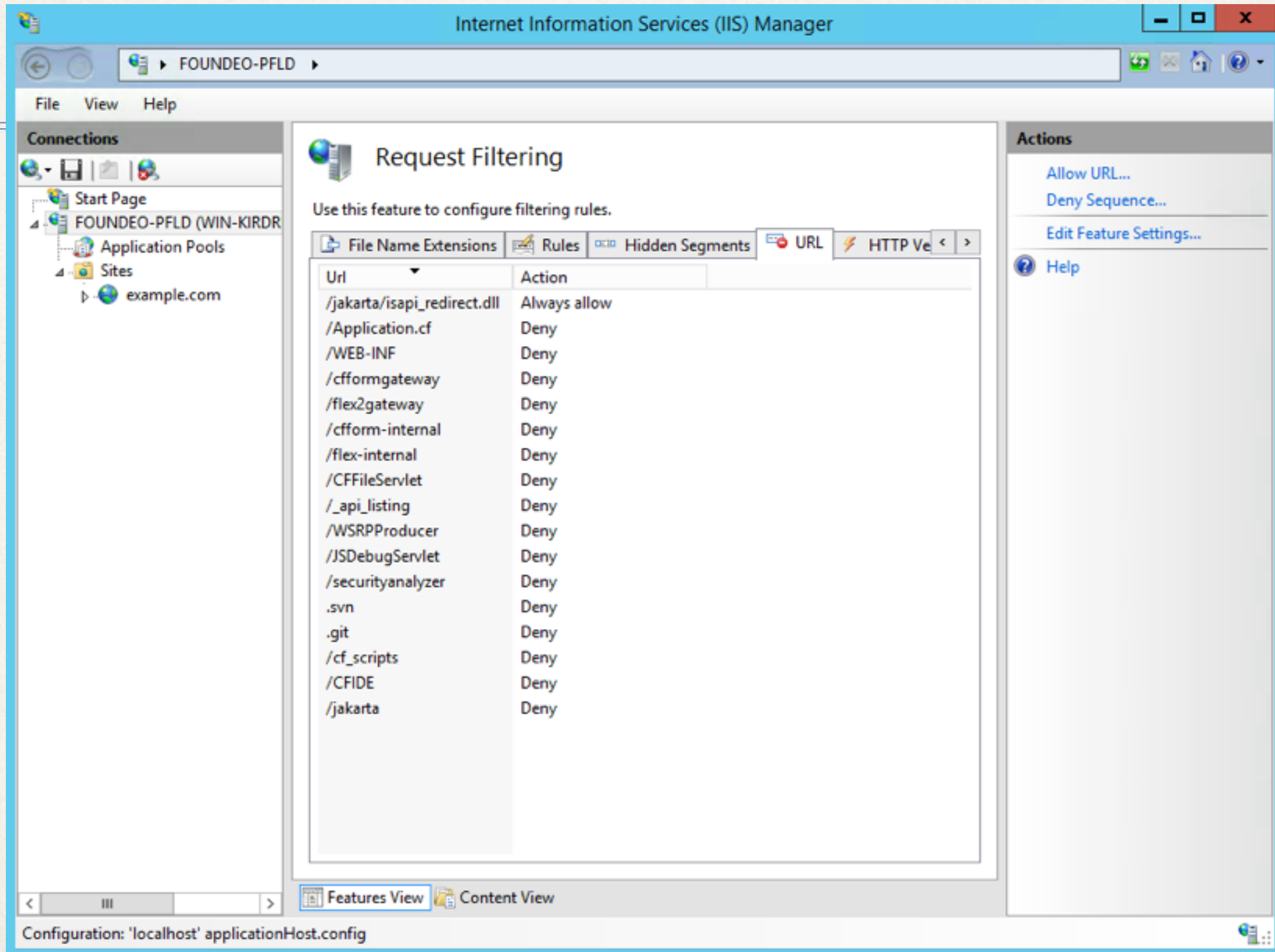
# IIS Request Filtering

---

- ❖ Block or whitelist URIs
- ❖ Block or whitelist by file extension
- ❖ Block or whitelist HTTP verbs
- ❖ Request Limits
  - ❖ Content Length
  - ❖ URL Length
  - ❖ Query String Length



# IIS Request Filtering





# Block servlet mapping URIs

---

- ❖ /cform-gateway
- ❖ /cform-internal
- ❖ /rest
- ❖ /CFIDE / main / rds.cfm
- ❖ /CFIDE / GraphData.cfm  
(cfchart on CF10)
- ❖ /WSRPProducer
- ❖ /CFFileServlet
- ❖ /CFFormGateway
- ❖ /flashservices / gateway
- ❖ /flex2gateway
- ❖ See web.xml



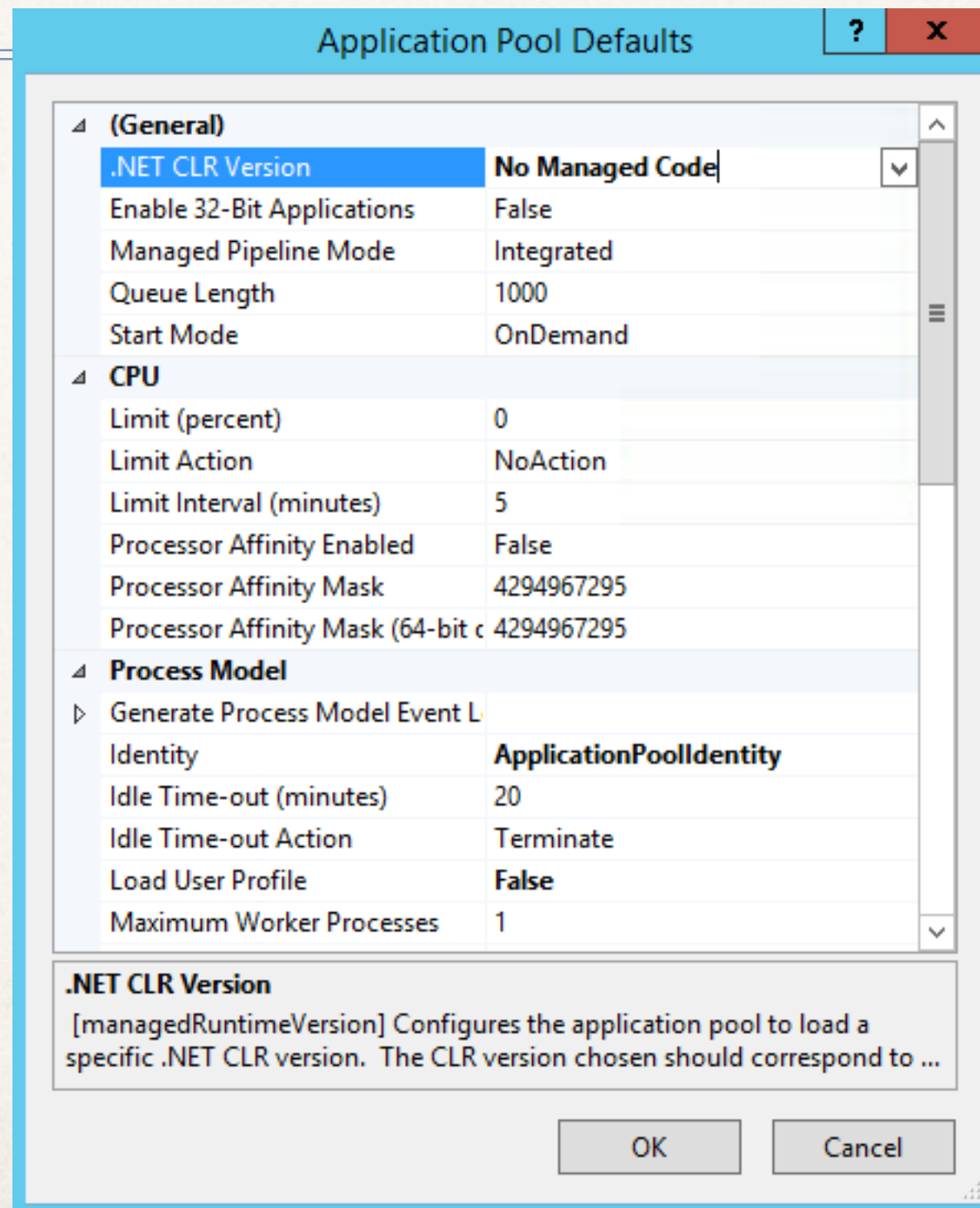
# Restrict File Extensions

---

- ❖ Can be setup per folder, site or globally for IIS
- ❖ Whitelist - only serve files in allowed list of extensions
  - ❖ eg: restrict /photos/ folder to only serve jpg, png, gif
  - ❖ eg: global whitelist: cfm, jpg, png, gif, js, css, pdf
    - ❖ Takes time to come up with list but worth it
    - ❖ The /jakarta virtual directory must allow dll extension
- ❖ Blacklist - do not serve files on blacklist / deny list.



# Application Pool Defaults



**Application Pool Defaults** [?] [X]

▲ **(General)**

.NET CLR Version	No Managed Code
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Queue Length	1000
Start Mode	OnDemand

▲ **CPU**

Limit (percent)	0
Limit Action	NoAction
Limit Interval (minutes)	5
Processor Affinity Enabled	False
Processor Affinity Mask	4294967295
Processor Affinity Mask (64-bit c	4294967295

▲ **Process Model**

▸ Generate Process Model Event L

Identity	ApplicationPoolIdentity
Idle Time-out (minutes)	20
Idle Time-out Action	Terminate
Load User Profile	False
Maximum Worker Processes	1

**.NET CLR Version**  
[managedRuntimeVersion] Configures the application pool to load a specific .NET CLR version. The CLR version chosen should correspond to ...

OK Cancel



# IIS Identities

---

- ❖ **Application Pool Identity** - user that the IIS process for your site is running as.
- ❖ **Anonymous Authentication Identity** - user that the app pool impersonates when handling an *unauthenticated* request for content.
  - ❖ All requests are *anonymous* unless you enable authentication.



# Application Pool Identity

---

- ❖ `ApplicationPoolIdentity` - default, low privilege, automatically isolates each application pool. Member of `IIS_IUSRS` group.
- ❖ *Custom User* - if using network shares with `ApplicationPoolIdentity` you have to grant entire machine access to share, so you may opt to create your own user in that case.



# Anonymous Authentication Identity

---

- ❖ IUSR
  - ❖ The default
  - ❖ No isolation between all sites
  - ❖ Implicit member of Users group.
- ❖ ApplicationPoolIdentity
  - ❖ Provides isolation between sites
  - ❖ Shares identity with Application Pool

# Additional IIS Lockdown

---

- ❖ Remove unused ASP.NET ISAPI Filters and Handler Mappings
  - ❖ Keep the StaticFile Handler (unless you do not serve js, css, images, etc)
  - ❖ Keep the ISAPI-dll handler - needed for CF connector.
- ❖ Remove Response headers such as X-Powered-By: ASP.NET

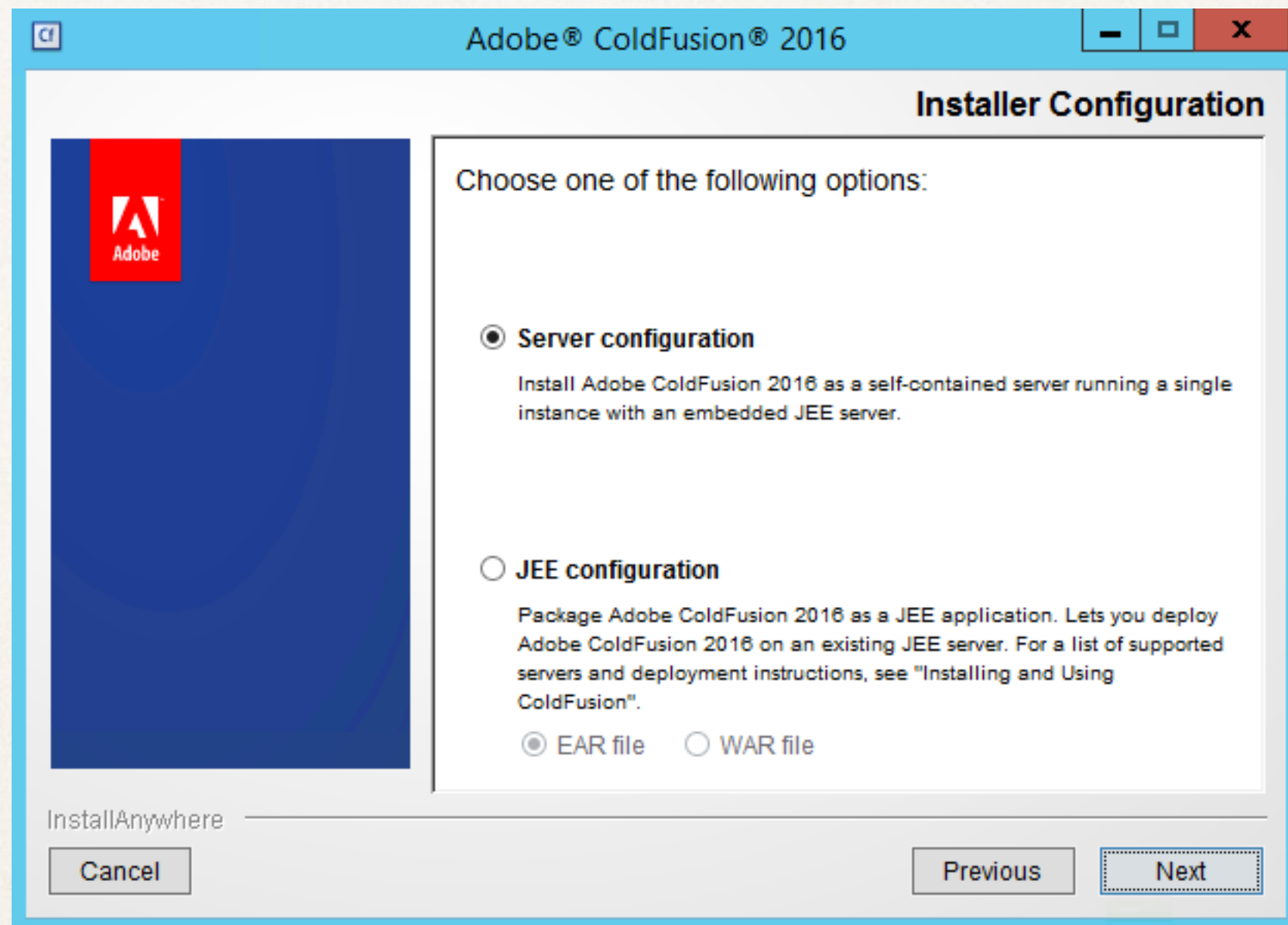


# Configure Apache

---

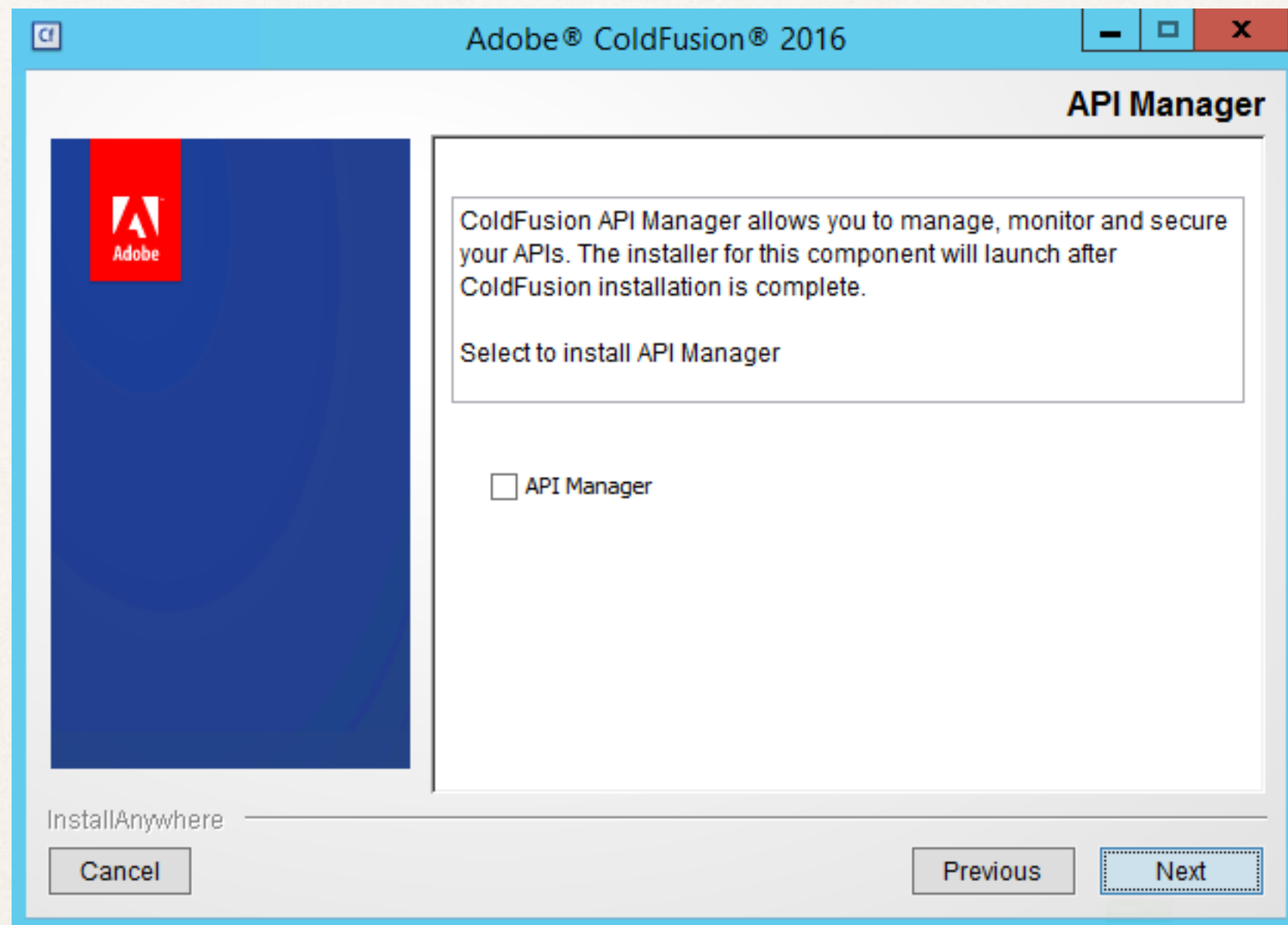
- ❖ Remove modules that you do not use (eg php)
  - ❖ `fgrep LoadModule *.conf`
- ❖ Block unused servlet mapping URI's
  - ❖ `RedirectMatch 404 (?i).*/flex2gateway.*`
- ❖ File Extension blacklist:
  - ❖ `RedirectMatch 404 (?i).*\.(jsp|php).*`
- ❖ Run SELinux enforcing mode if possible.

# Installation

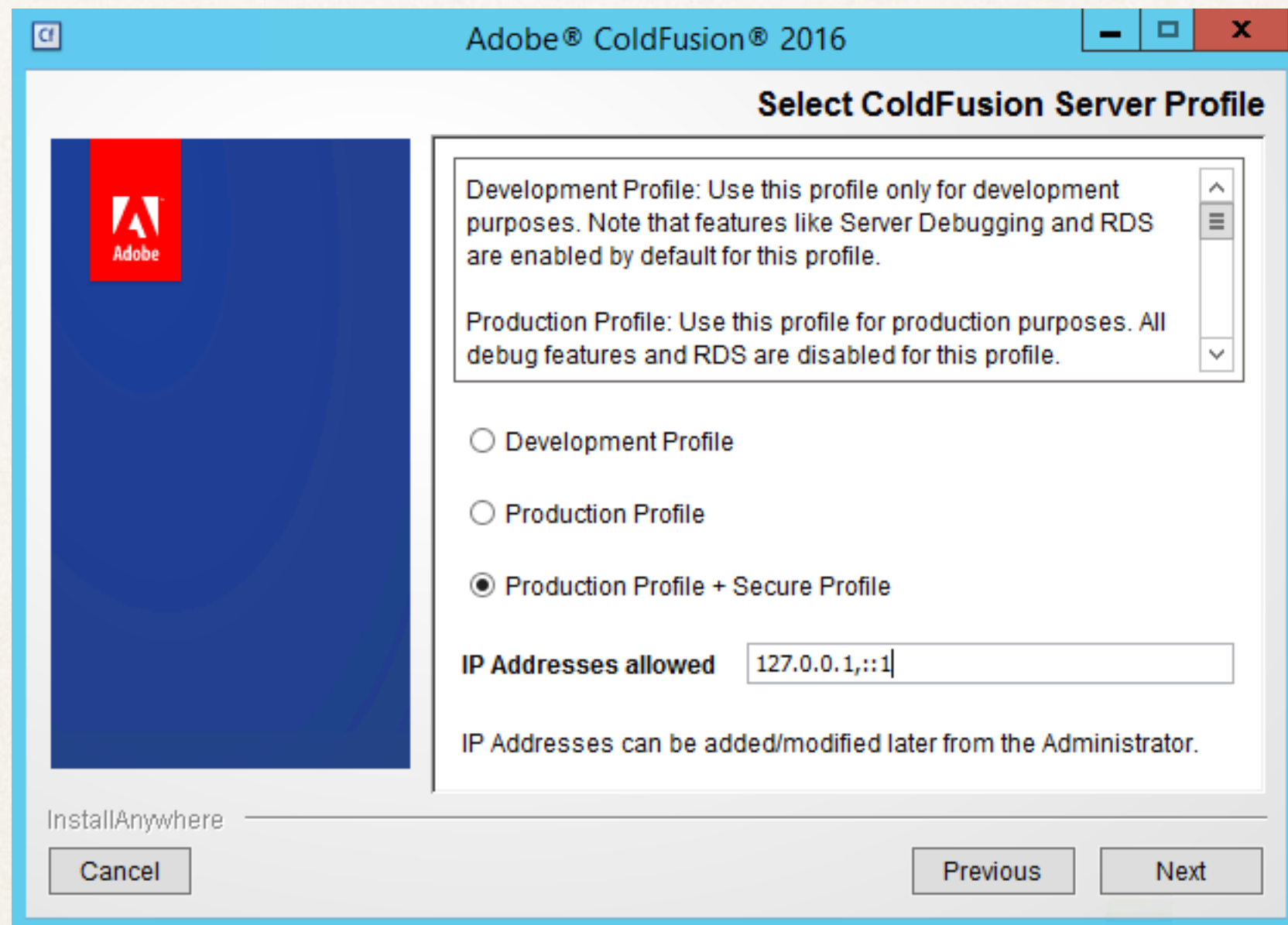




# Installation

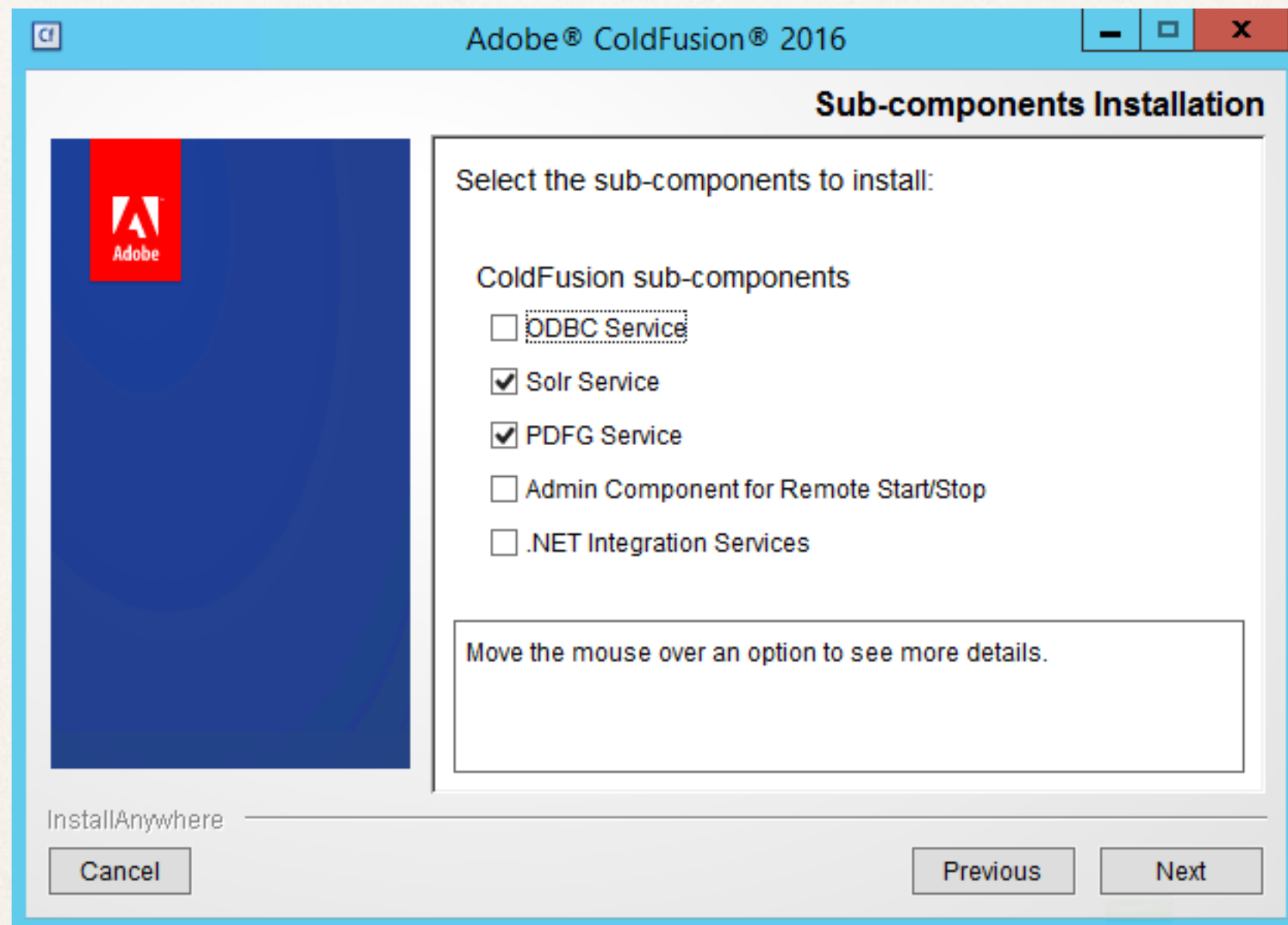


# Installation



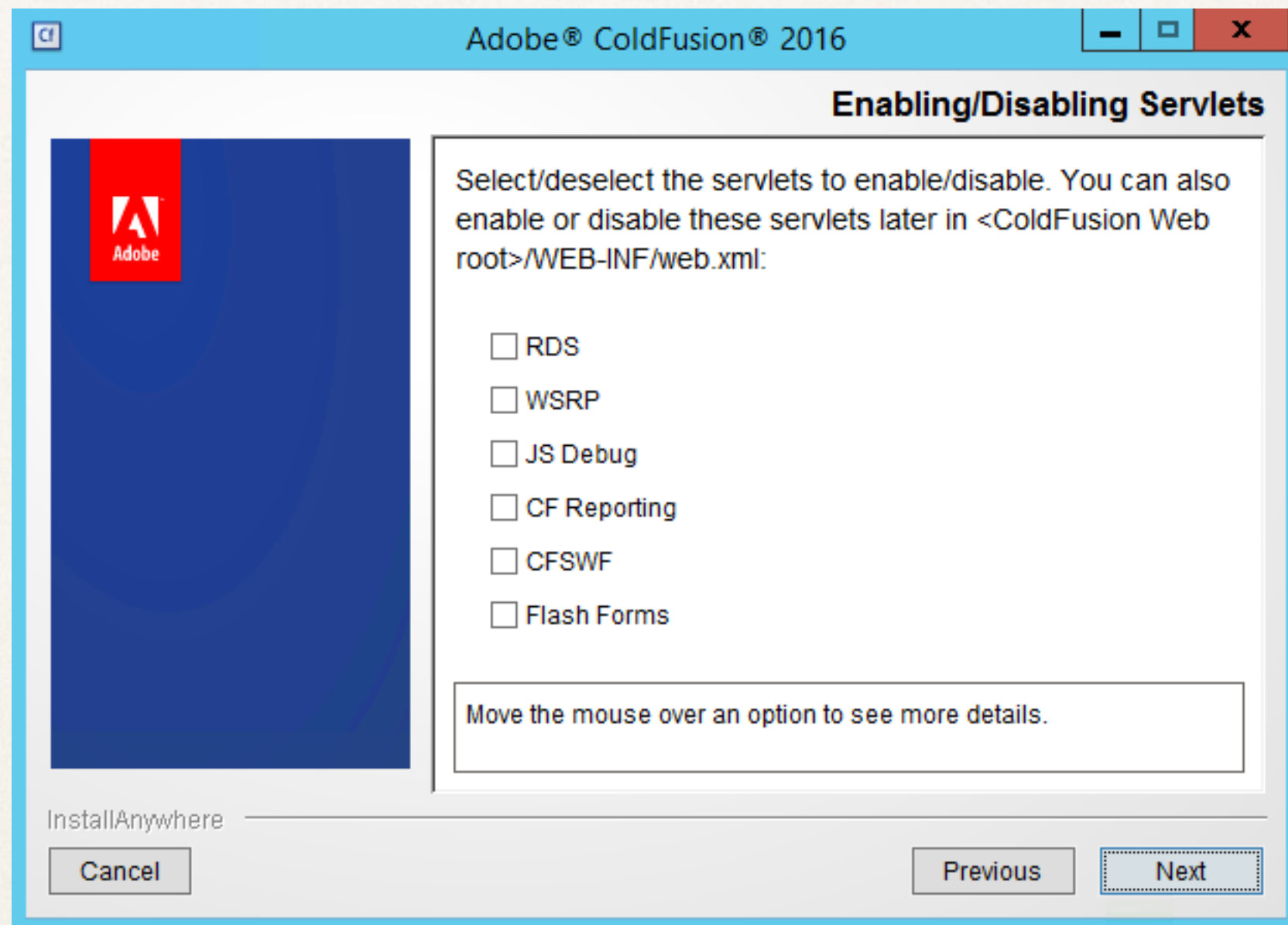


# Installation



Install only necessary subcomponents

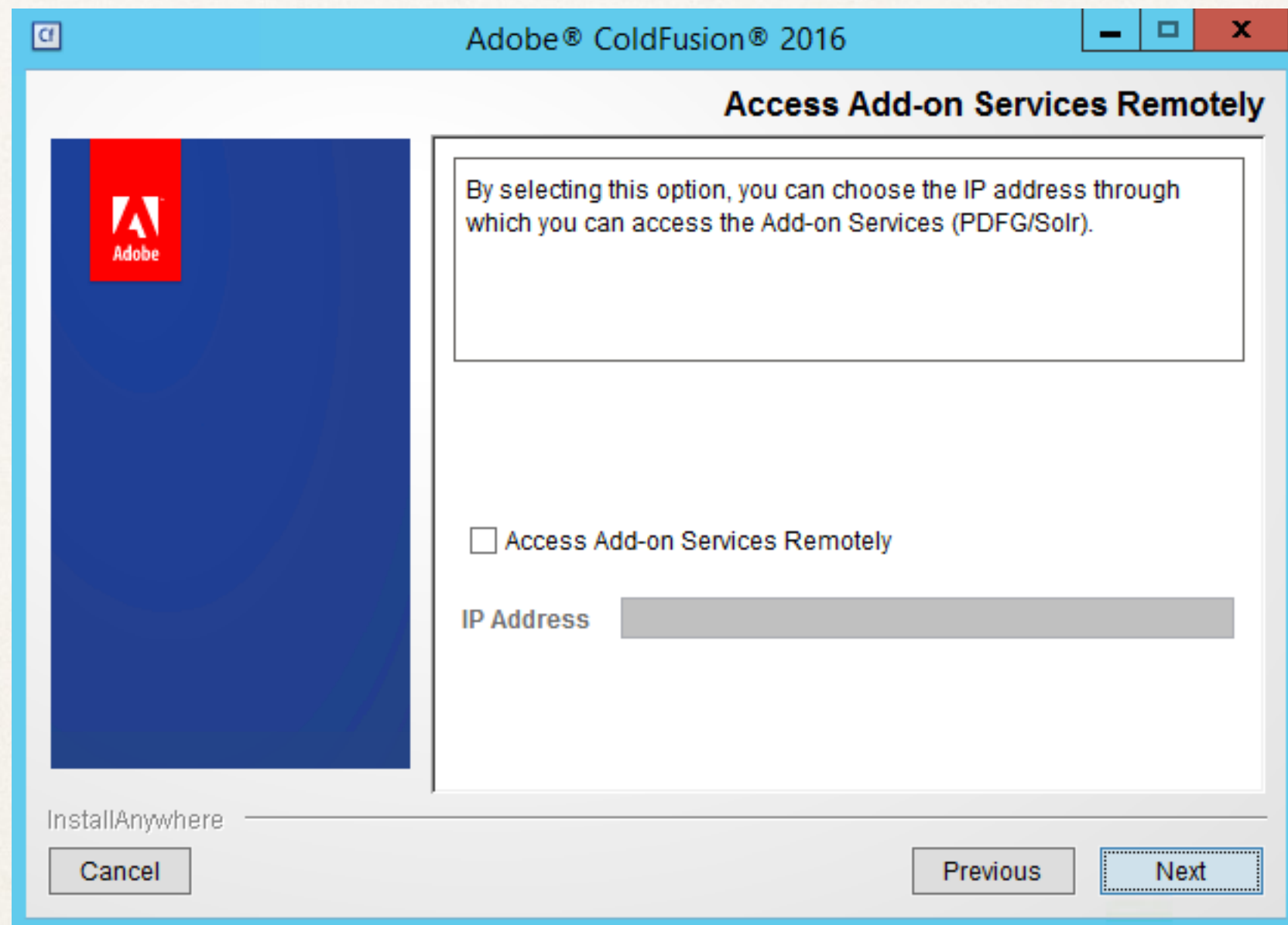
# Installation



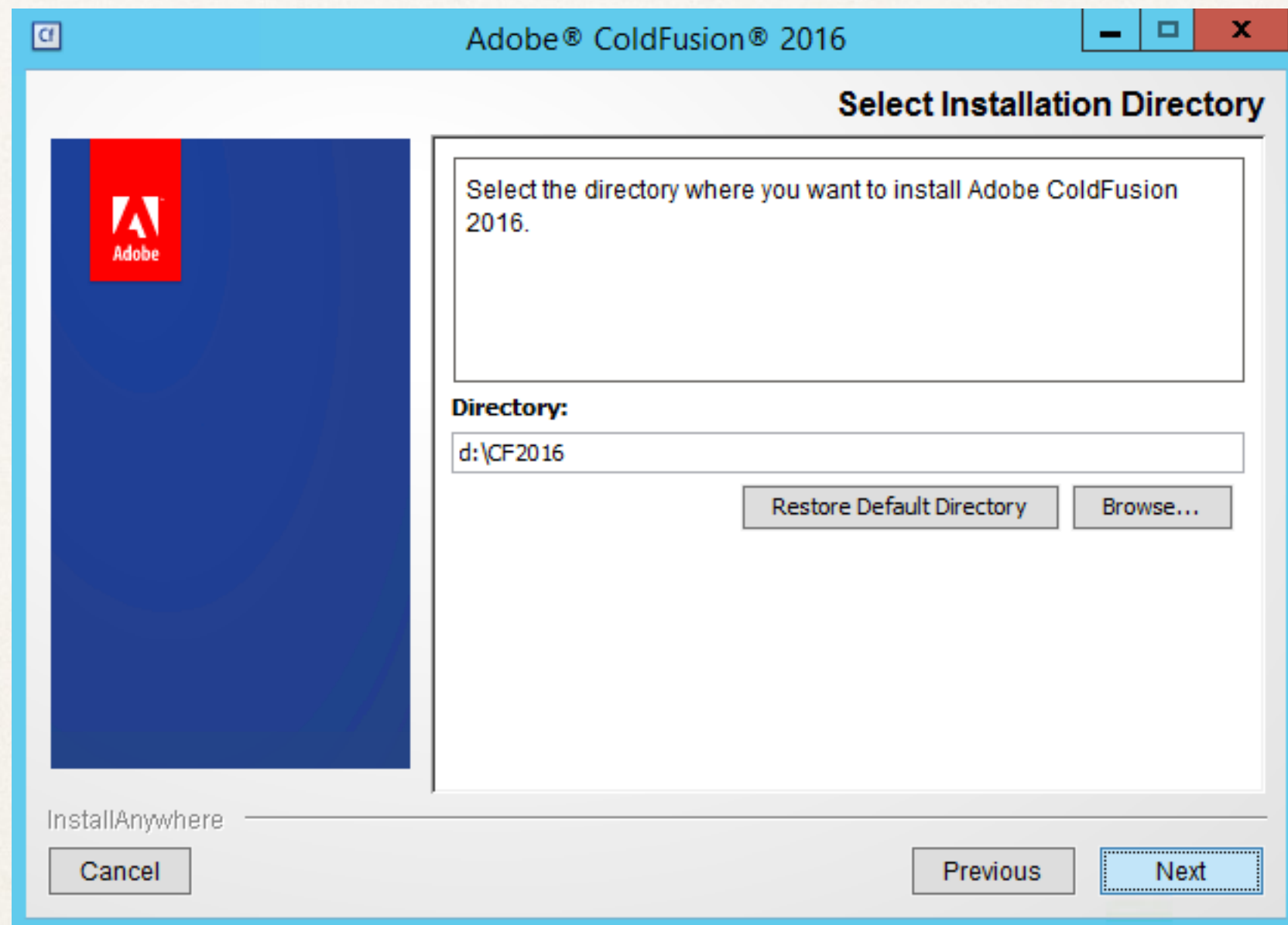
Disable unneeded Servlets



# Installation

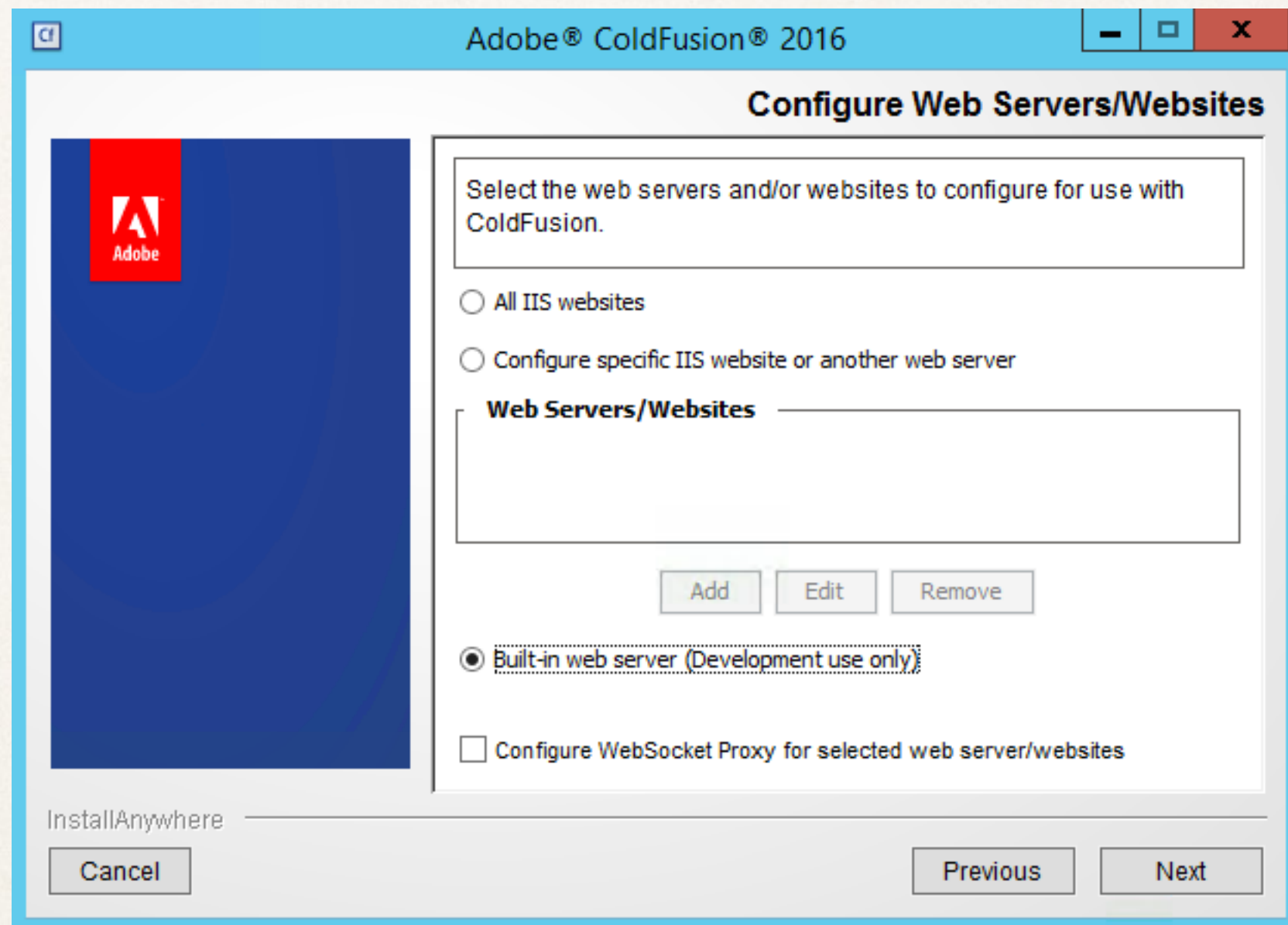


# Installation



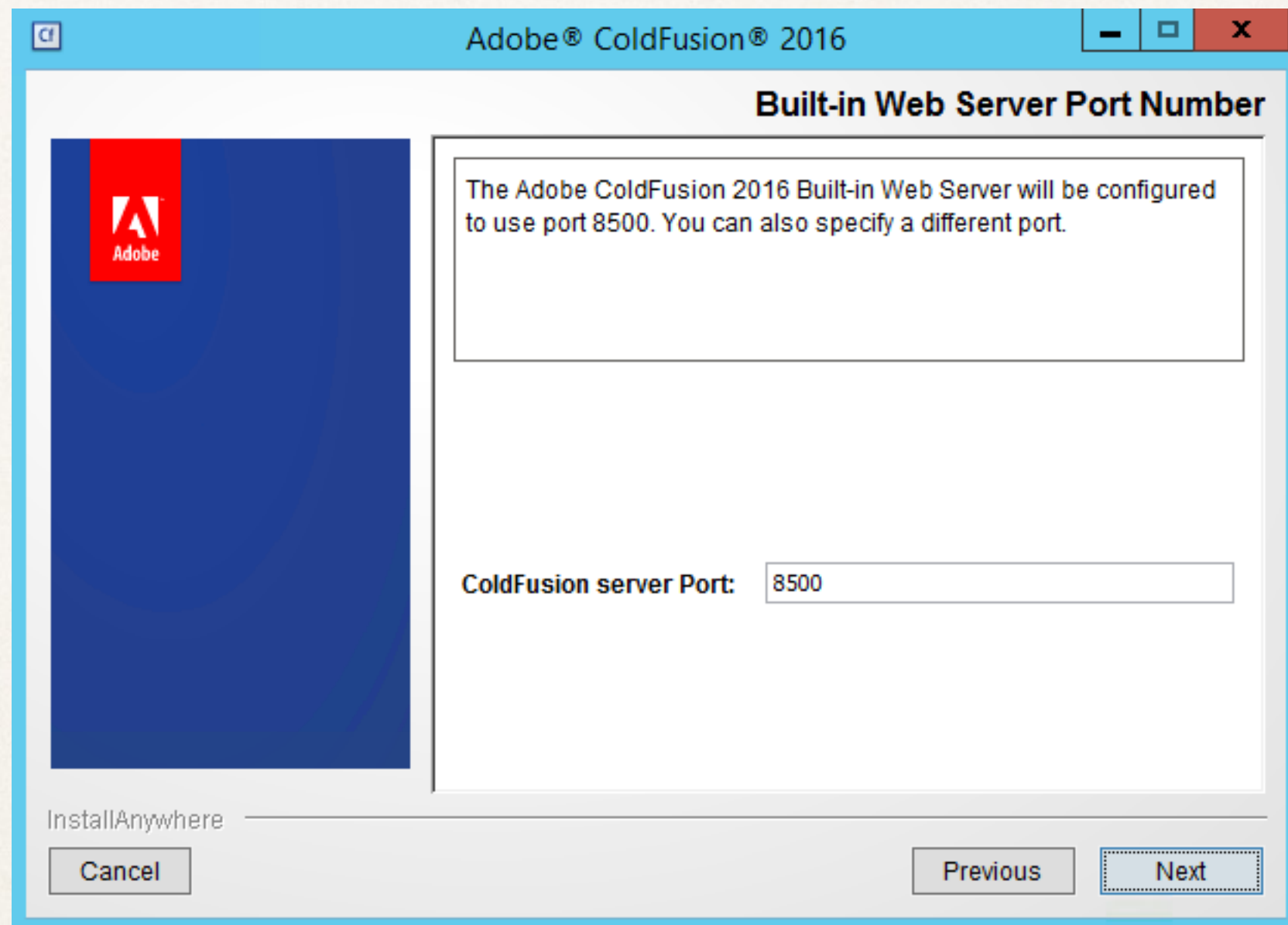


# Installation



Install CF Hotfixes before connecting web server

# Installation



Non default port



# Installation

Adobe® ColdFusion® 2016

## Administrator Credentials

Enter the username and password you will use to restrict access to the ColdFusion Administrator.

These fields are mandatory.

Enter username:

Enter password:

Confirm password:

InstallAnywhere

# Post-Install

---

- ❖ Install any / all CF security hotfixes and updates.
- ❖ Install / Update Web Server connectors
- ❖ Configure administrator settings.



# Accessing CF Administrator

---

- ❖ Use Builtin Web Server
  - ❖ Access locally over RDP
  - ❖ SSH Tunnel on Linux
  - ❖ If accessed outside of localhost add TLS / HTTPS
- ❖ Using webserver (IIS / Apache) - intentionally harder in CF2016
  - ❖ Use dedicated connector / edit `uriworkermapping.properties`
  - ❖ Setup IP Restrictions, SSL, Additional User Auth

# Dedicated User Account

---

- ❖ Windows: Change Service Log On identity. Otherwise CF runs with full permission to everything.
- ❖ Unix: The installer allows you to specify a user to run CF as.
  - ❖ The default *nobody* user is probably not the best choice as other services might share this account.



# File System Permissions

Path	CF User Permissions	Web Server Identity Permissions
Your Web Root	Read Only Additional as needed	Read Only
CF Install Dir	Full Can be restricted further	/cf_scripts Read Only
CF Connector	Read	Read Write (Logs)

# File System Permissions

---

- ❖ /cf\_scripts and other directories under CF root can be restricted read only permission by the cf user to prevent runtime change.
- ❖ Run CF10-2016 hotfix installer from command line as administrator.
  - ❖ `java -jar {coldfusion-home}\cfusion\hf-updates\hotfix_XXX.jar`



# Update JVM

---

- ✧ Update to latest supported JVM (1.8 currently for CF10-2016)
  - ✧ Java 1.6 & 1.7 (as of 4/15) no longer supported by Oracle!
  - ✧ Adobe recommends you run the latest supported JVM (eg 1.8. {highest number}) instead of specific version numbers.
- ✧ If using `cfsearch` or `cfhtmltopdf` the Add on Services Server has its own jvm configuration file: `jetty/jetty.lax`

# Sandbox Security

---

- ❖ Disable Unnecessary Risks, eg: cfexecute, cfregistry
- ❖ More flexible on Enterprise but still works on standard.
- ❖ Test before enabling.



# Session Mechanism

Feature	J2EE	CF
Configure in Application.cfc	No	Yes
Token size configurable	Yes	No
Configure in <u>web.xml</u>	Yes	No
Interoperates with J2EE applications	Yes	No
SessionRotate	No	Yes
SessionInvalidate	No	Yes

# web.xml Servlet Mappings

---



# Tomcat

---

- ❖ Shutdown port / password
  - ❖ Changing port on windows causes CF service stop to fail.
- ❖ Connector settings:
  - ❖ connector secret (have to redo when updating connector)
- ❖ Tomcat 7 Security Configuration Guide: <http://tomcat.apache.org/tomcat-7.0-doc/security-howto.html>

# ColdFusion Administrator

---



# ColdFusion Administrator

---

- ❖ Default ScriptSrc Directory

- ❖ Setup an alias so `/cf_scripts/scripts/` -> `/some-folder/`
- ❖ If you don't use `cfform`, `cfajaxproxy`, etc you can skip.
- ❖ If you use the builtin web server you need to configure an alias

# ColdFusion Administrator

---

- ❖ **Allowed file extensions for CFInclude tag**
  - ❖ Mitigates directory traversal / path injection that leads to code execution attack.
  - ❖ Comma separated list of file extensions that execute, typically can be set to just `cfm`



# ColdFusion Administrator

---

Additional Settings

# Additional Tools

---

- ❖ HackMyCF
- ❖ FuseGuard
- ❖ CF Unofficial Updater (CF9 and below)



# Questions?

---

[foundeo.com](https://foundeo.com) | [hackmycf.com](https://hackmycf.com) | [fuseguard.com](https://fuseguard.com)

Please fill in your evaluations