Locking Down CF Servers

Pete Freitag, Foundeo Inc.

foundeo.com | hackmycf.com | fuseguard.com

About Pete Freitag

- Owner of Foundeo Inc.
    - HackMyCF - Remote ColdFusion Security Scanner
    - FuseGuard - Web App Firewall for CFML
    - Consulting - Install, Configure, Review, CFML Dev
- 17+ Years working with CF
- Author of CF9-11 Lockdown Guides, CFMX Cookbook (SAMs)
- blog: 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:

- Adobe ColdFusion 11 Lockdown Guide: http://bit.ly/cf11lockdown
- Adobe ColdFusion 10 Lockdown Guide: http://bit.ly/cf10lockdown
- Adobe ColdFusion 9 Lockdown Guide: http://bit.ly/cf9lockdown
- This talk assumes CF11, but is mostly the same for CF10 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?

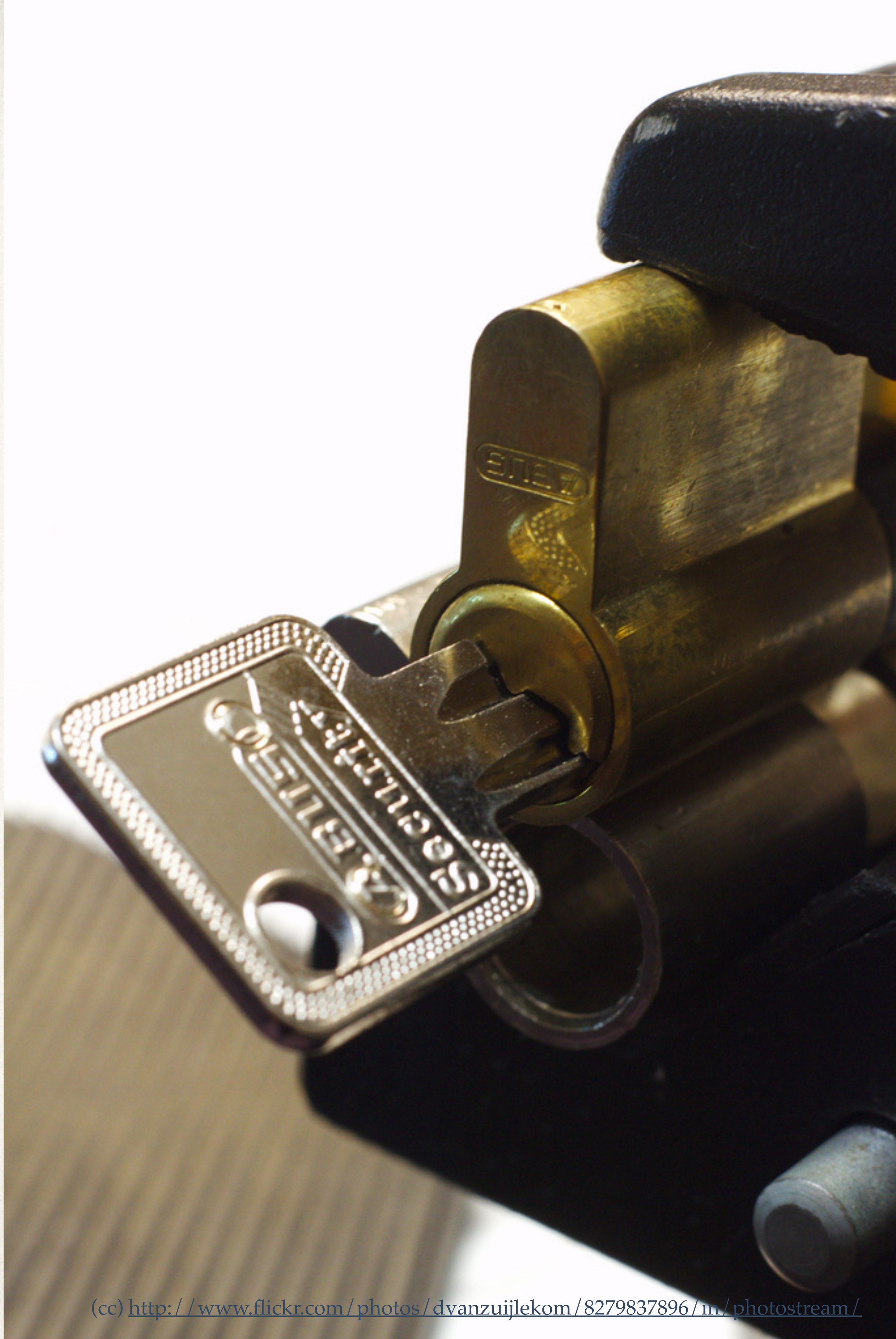
What is secure?

What tradeoffs are acceptable?

(cc) http://www.flickr.com/photos/toddler/4169974226/

Principal of Least Privilege

Grant only the minimum permission required to accomplish a task.



(cc) http://www.flickr.com/photos/dvanzuijlekom/8279837896/in/photostream/

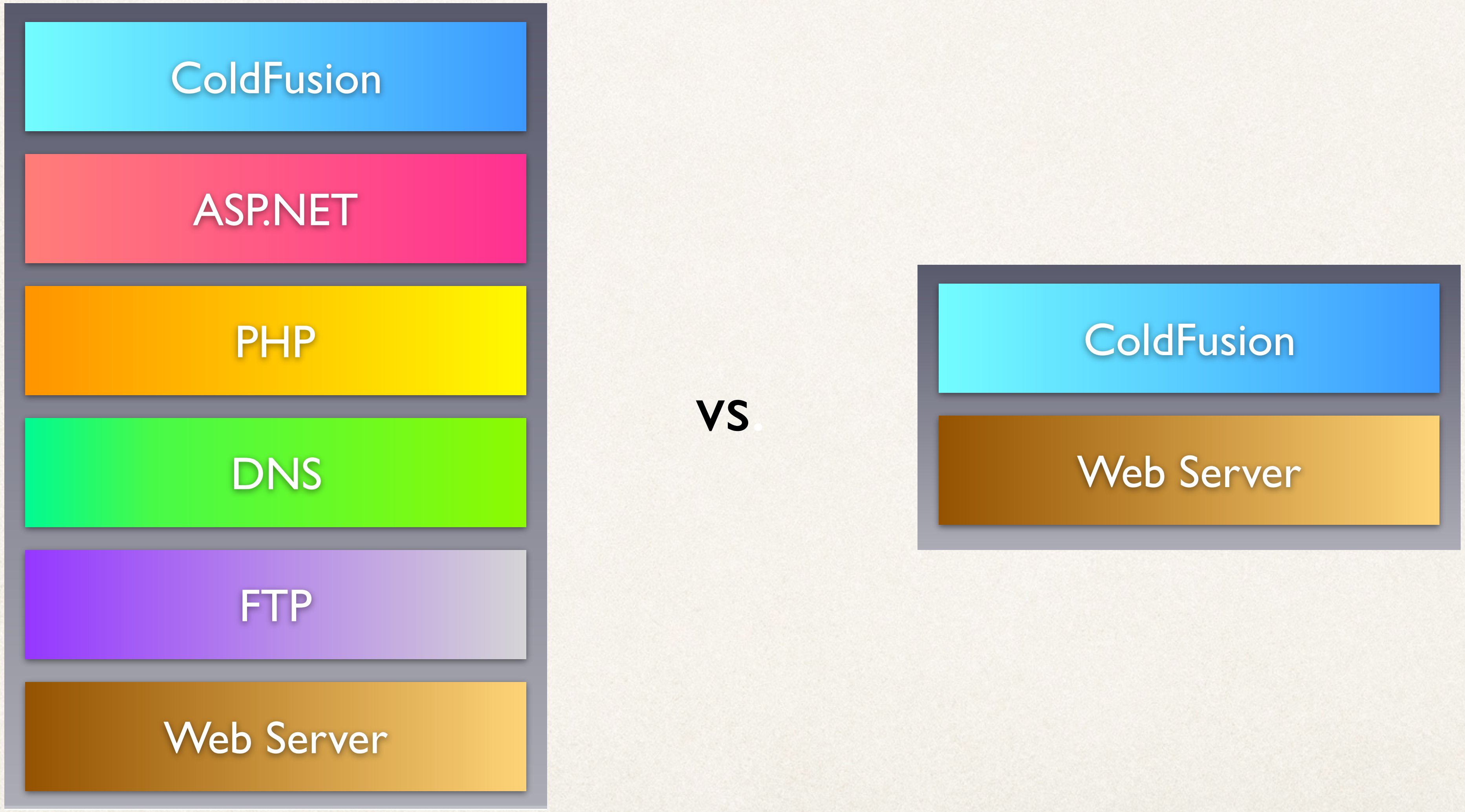
Defense in Depth

Multiple Layers of Redundant Security.

(cc) http://www.flickr.com/photos/flygraphix/4791988161/

Reduce Attack Surface

Reduce Attack Surface



ColdFusion

ASP.NET

PHP

DNS

FTP

Web Server

vs.

ColdFusion

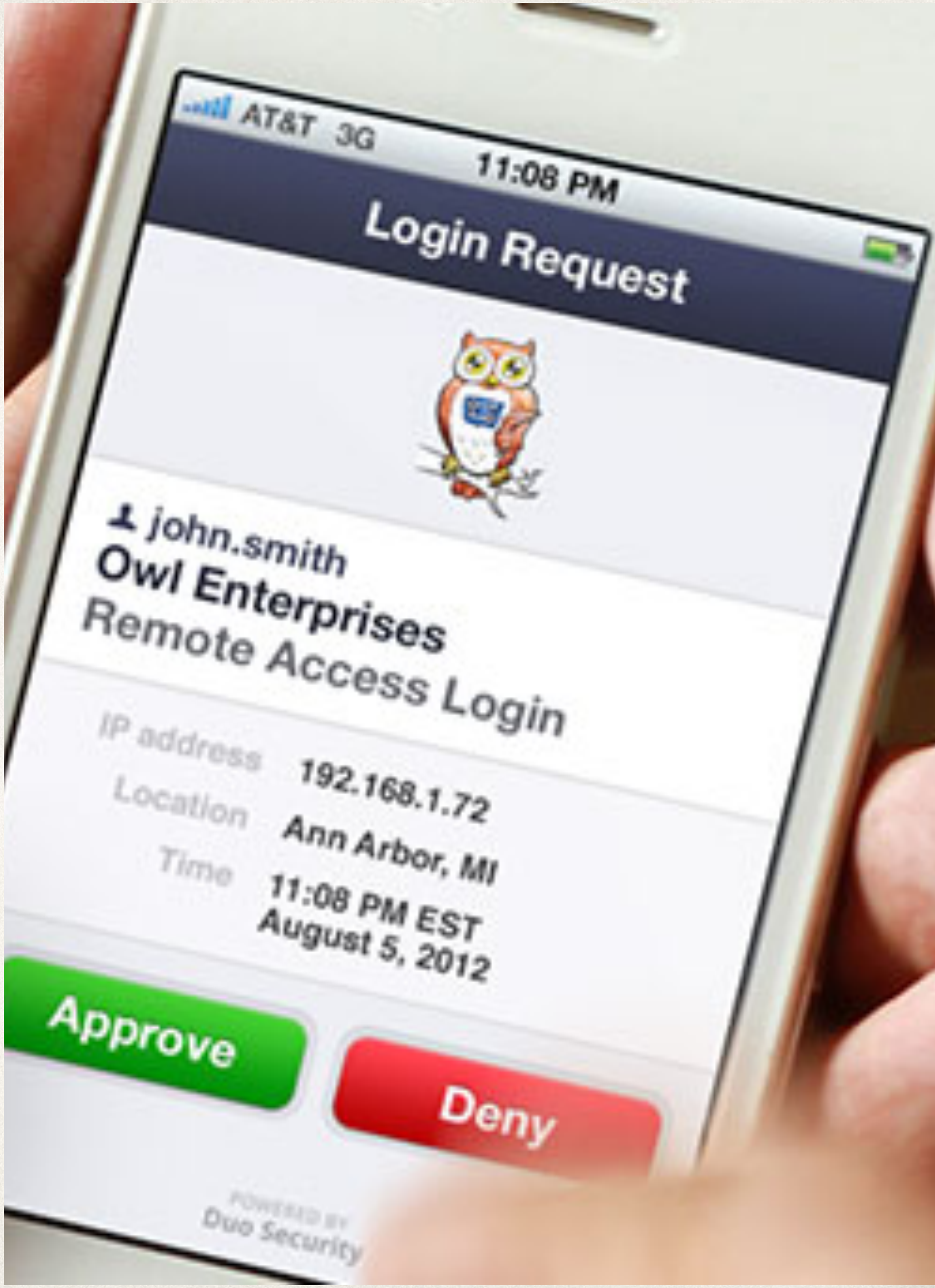
Web Server

Avoid Defaults

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

Services I Like:

- Duo Security: Two Factor Authentication
  - (RDP, SSH)
- Dome9: Cloud Firewall
  - Easily grant temporary access to administrative ports.



Login Request

john.smith
Owl Enterprises
Remote Access Login

IP address	192.168.1.72
Location	Ann Arbor, MI
Time	11:08 PM EST August 5, 2012

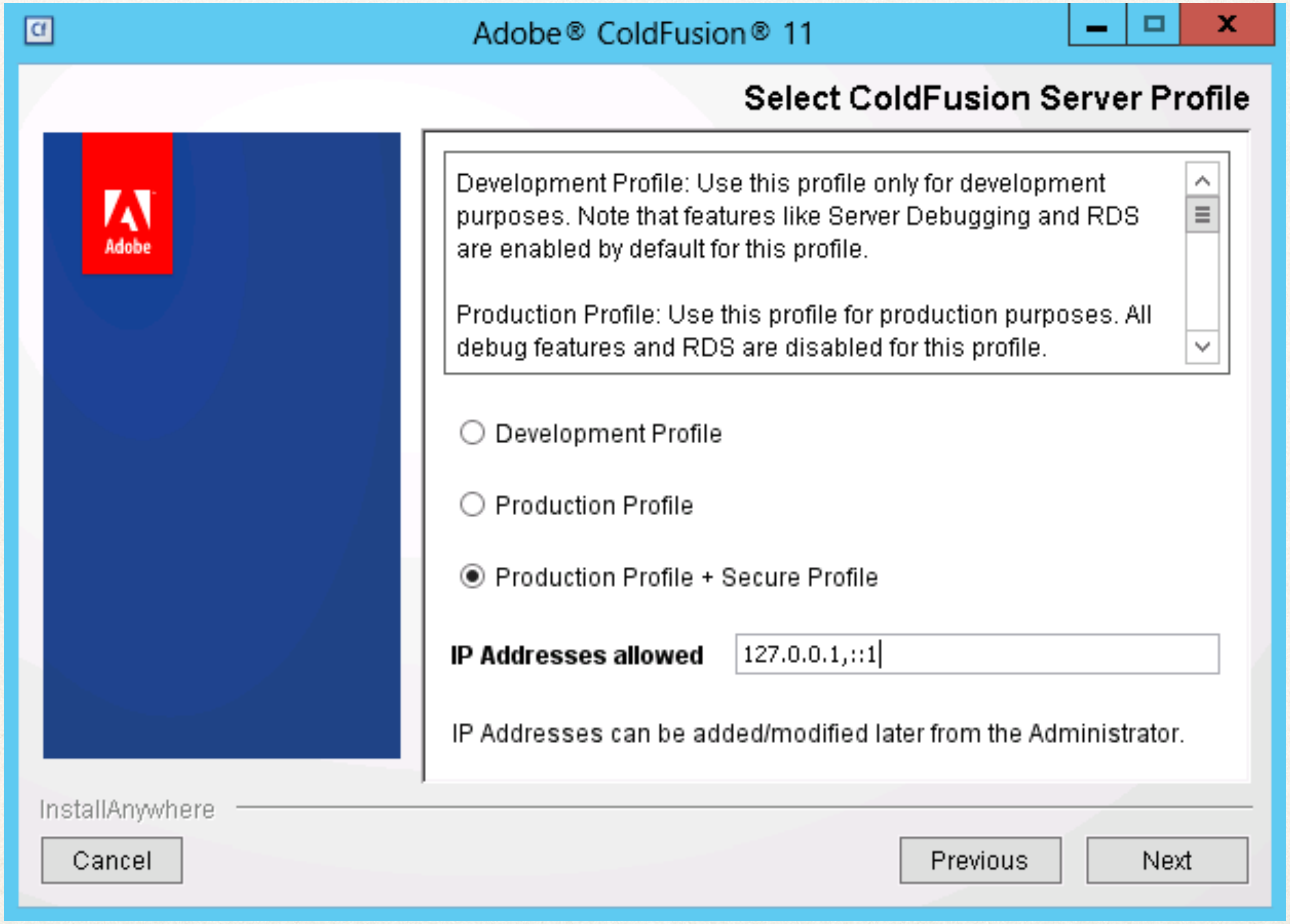
Pre-Installation

- 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/
    - 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.

Installation



Select ColdFusion Server Profile

Development Profile: Use this profile only for development purposes. Note that features like Server Debugging and RDS are enabled by default for this profile.

Production Profile: Use this profile for production purposes. All debug features and RDS are disabled for this profile.

○ Development Profile

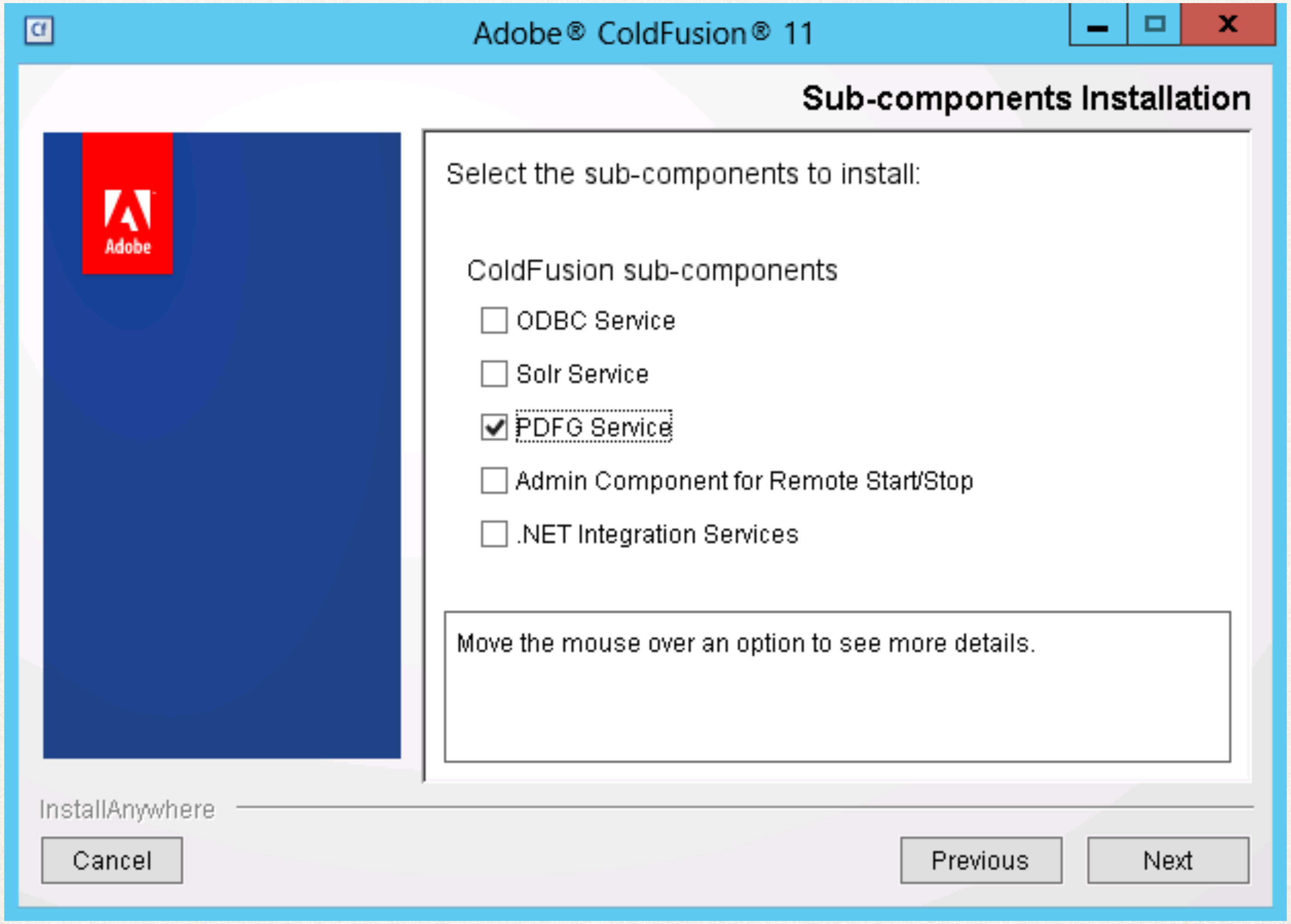
○ Production Profile

● Production Profile + Secure Profile

IP Addresses allowed 127.0.0.1,::1

IP Addresses can be added/modified later from the Administrator.

Installation



Adobe® ColdFusion® 11

Sub-components Installation

Select the sub-components to install:

ColdFusion sub-components

☐ ODBC Service

☐ Solr Service

☑ PDFG Service

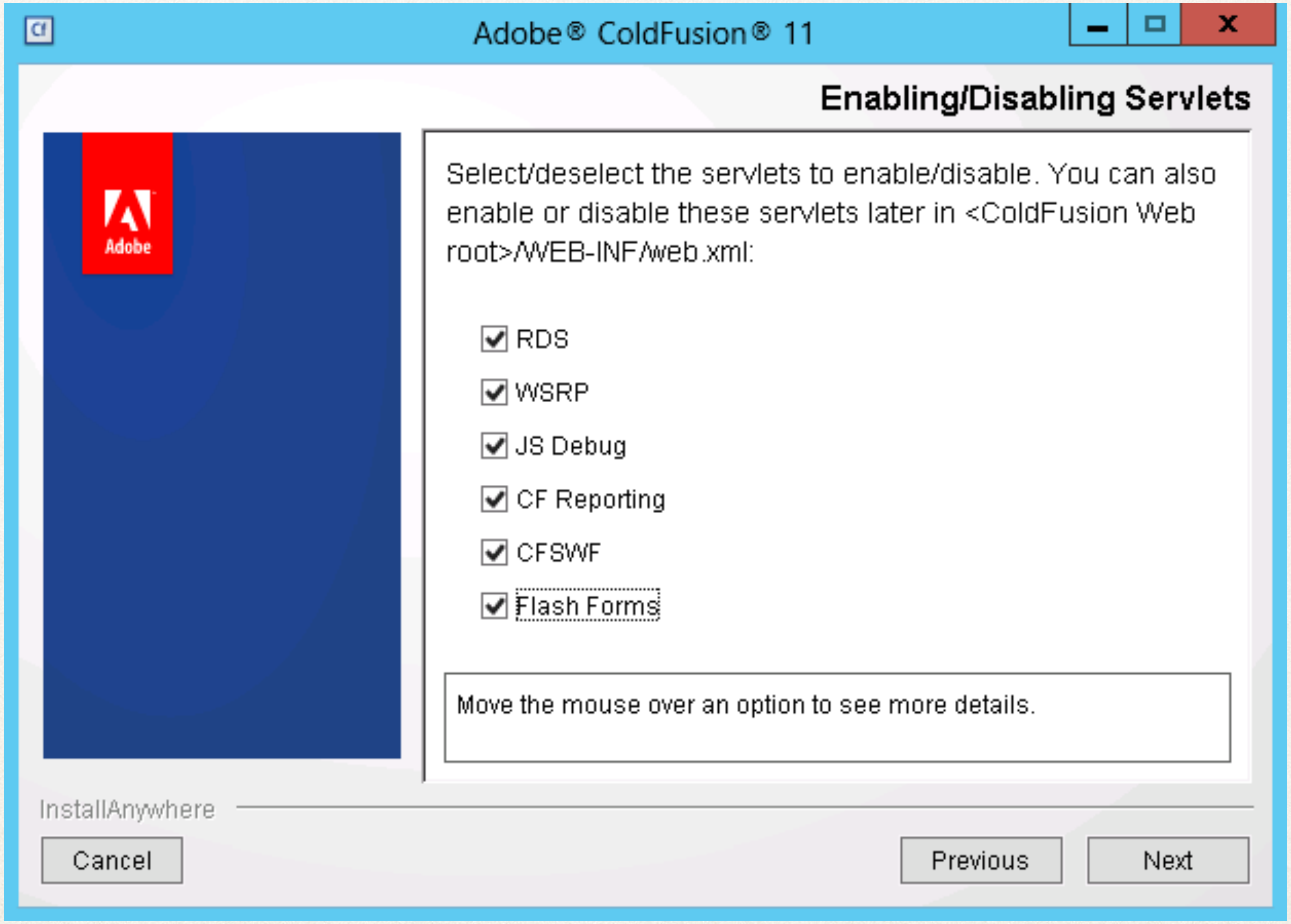
☐ Admin Component for Remote Start/Stop

☐ .NET Integration Services

Move the mouse over an option to see more details.

Install only necessary subcomponents

Installation



Enabling/Disabling Servlets

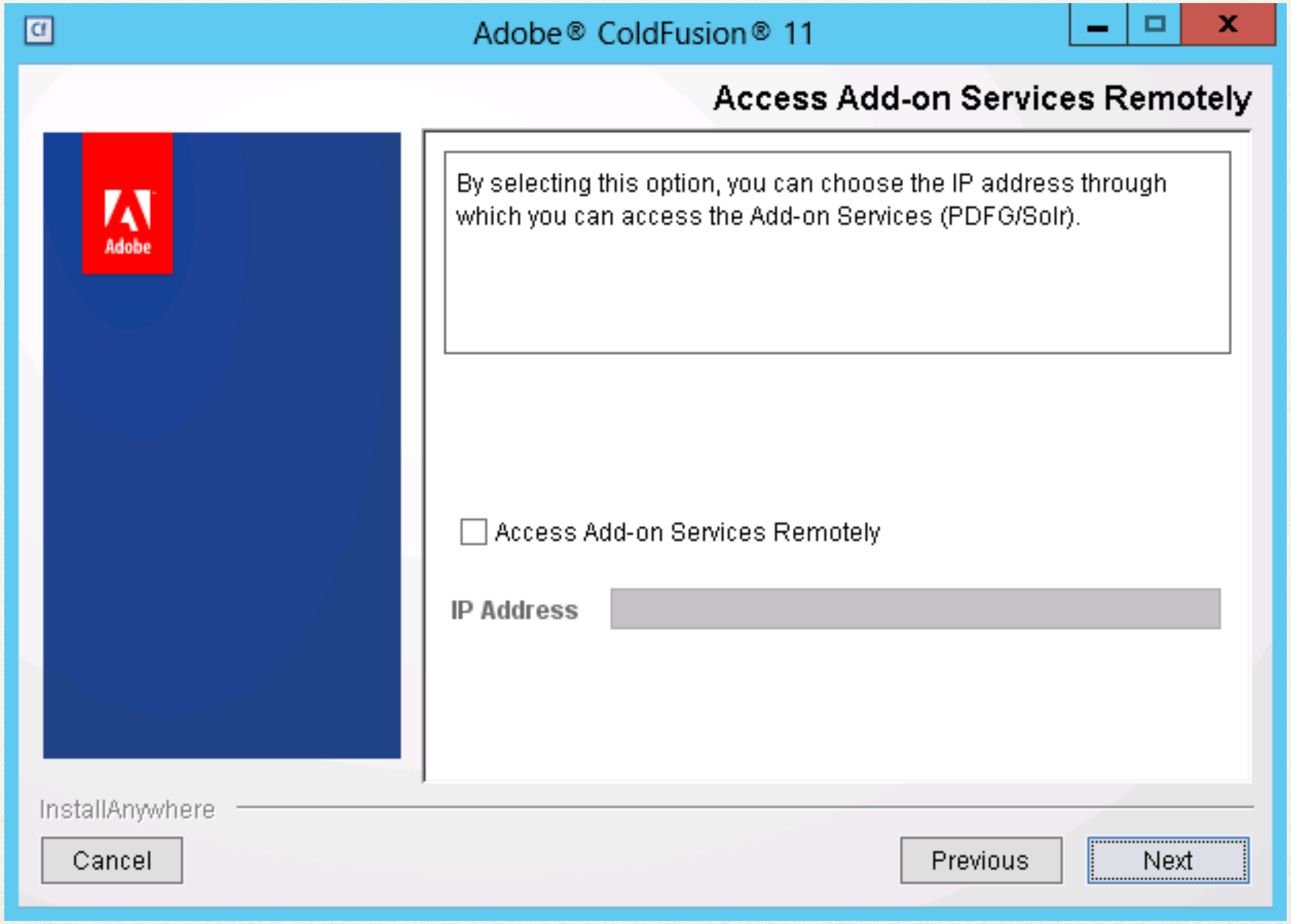
Select/deselect the servlets to enable/disable. You can also enable or disable these servlets later in <ColdFusion Web root>/WEB-INF/web.xml:

- ☑ RDS
- ☑ WSRP
- ☑ JS Debug
- ☑ CF Reporting
- ☑ CFSWF
- ☑ Flash Forms

Move the mouse over an option to see more details.

Disable unneeded Servlets

Installation



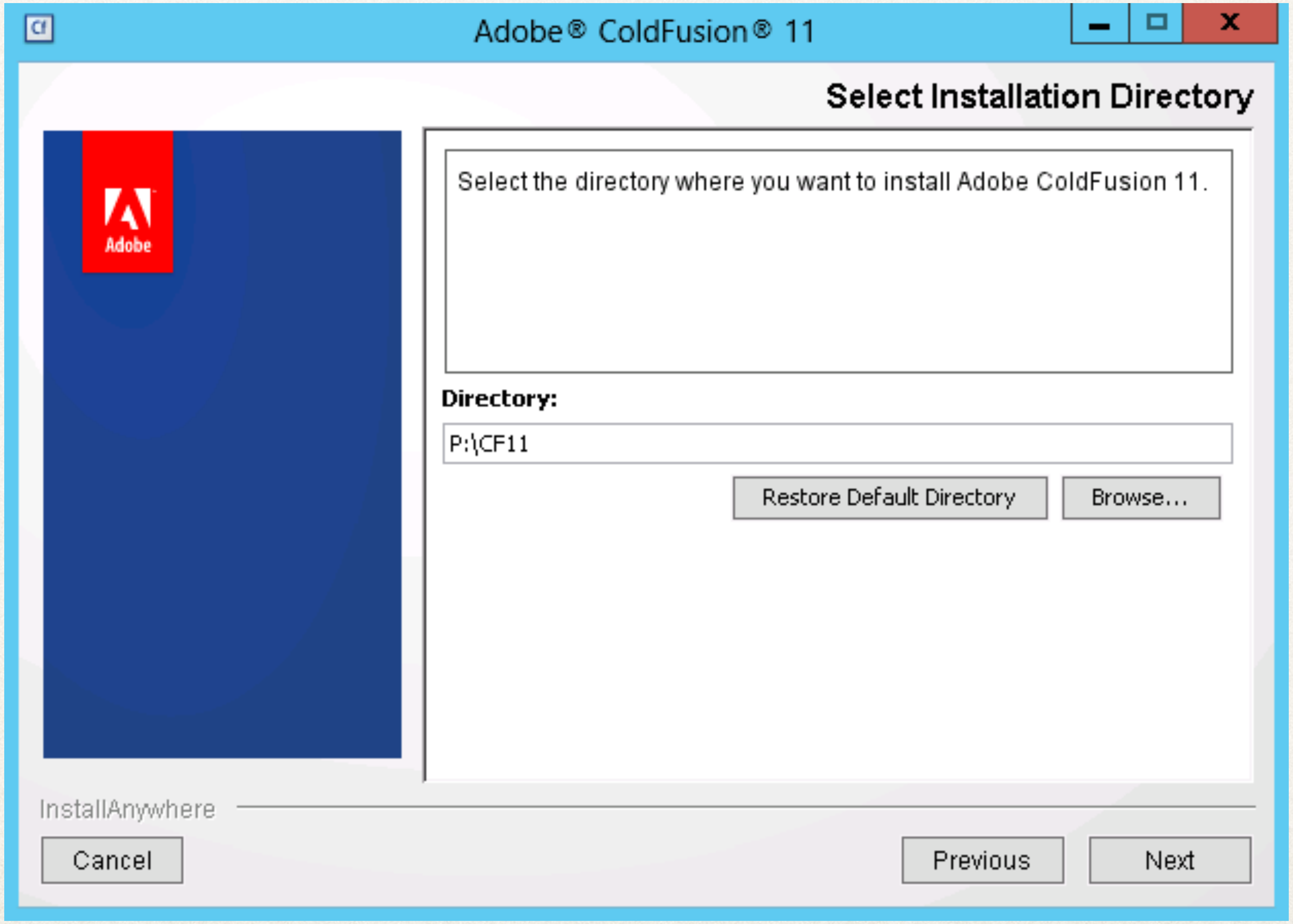
Access Add-on Services Remotely

By selecting this option, you can choose the IP address through which you can access the Add-on Services (PDFG/Solr).

□ Access Add-on Services Remotely

IP Address

Installation

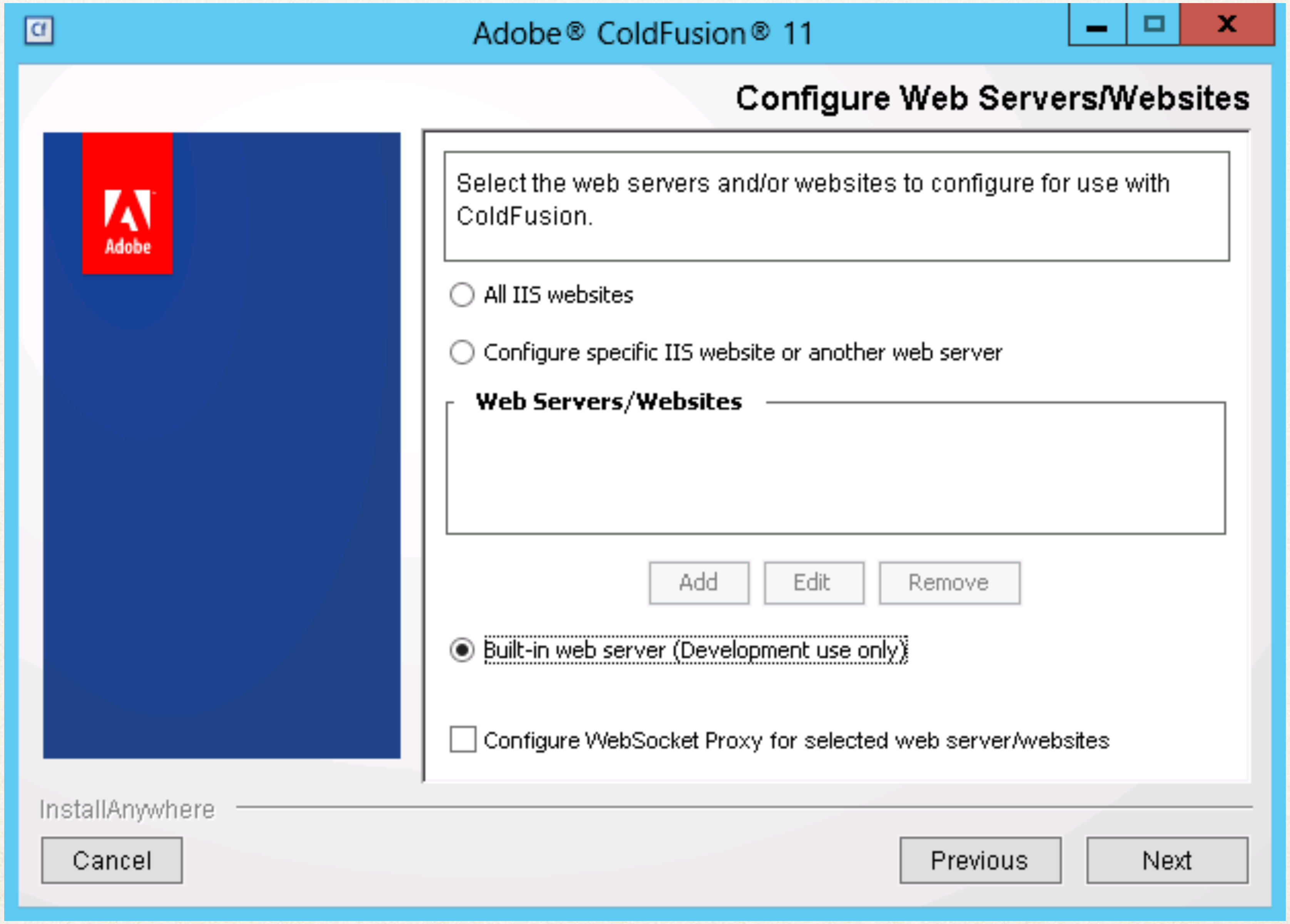


Select Installation Directory

Select the directory where you want to install Adobe ColdFusion 11.

Directory: P:\CF11

Installation



Adobe® ColdFusion® 11

Configure Web Servers/Websites

Select the web servers and/or websites to configure for use with ColdFusion.

○ All IIS websites

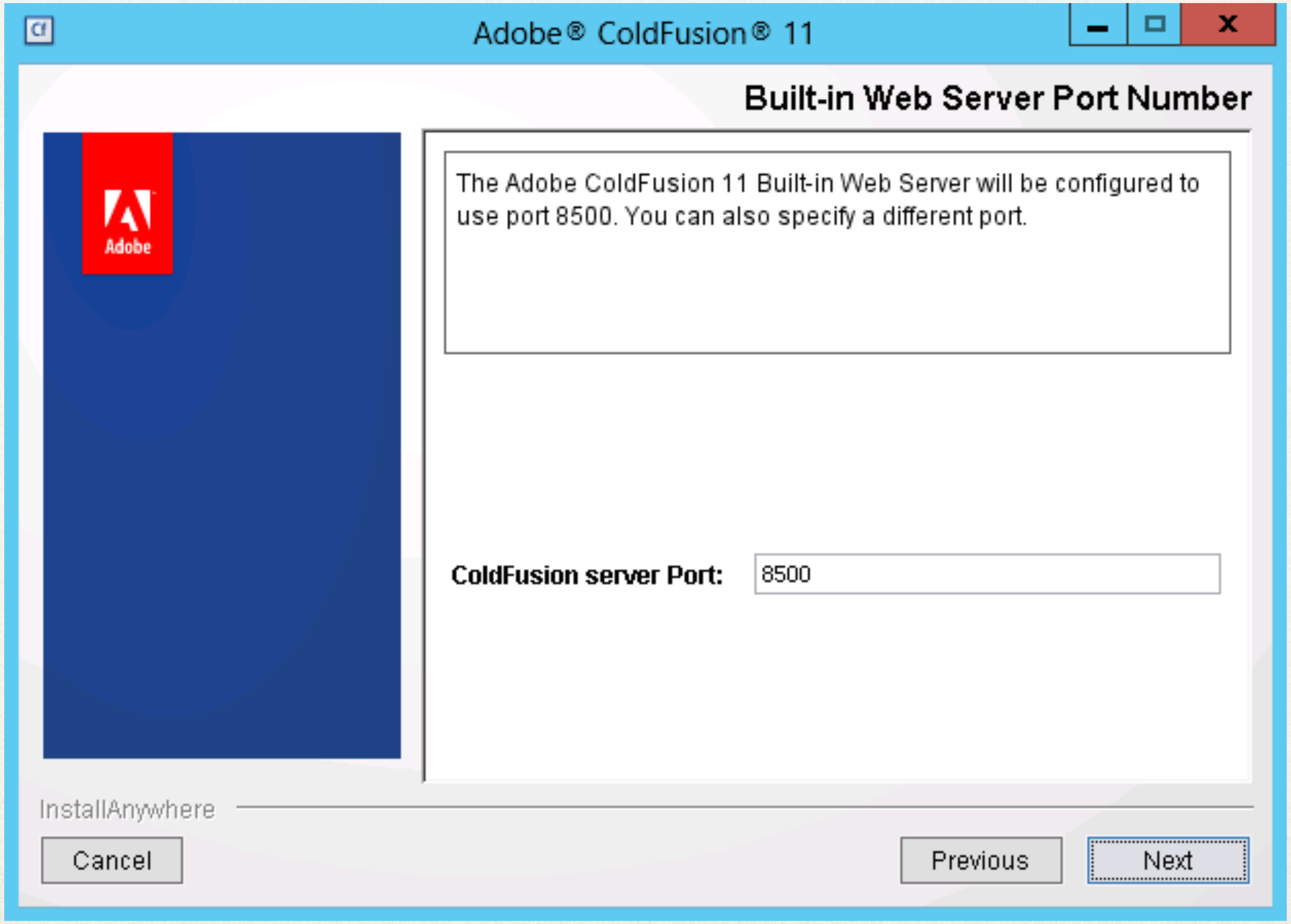
○ Configure specific IIS website or another web server

Web Servers/Websites

● Built-in web server (Development use only)

□ Configure WebSocket Proxy for selected web server/websites

Installation

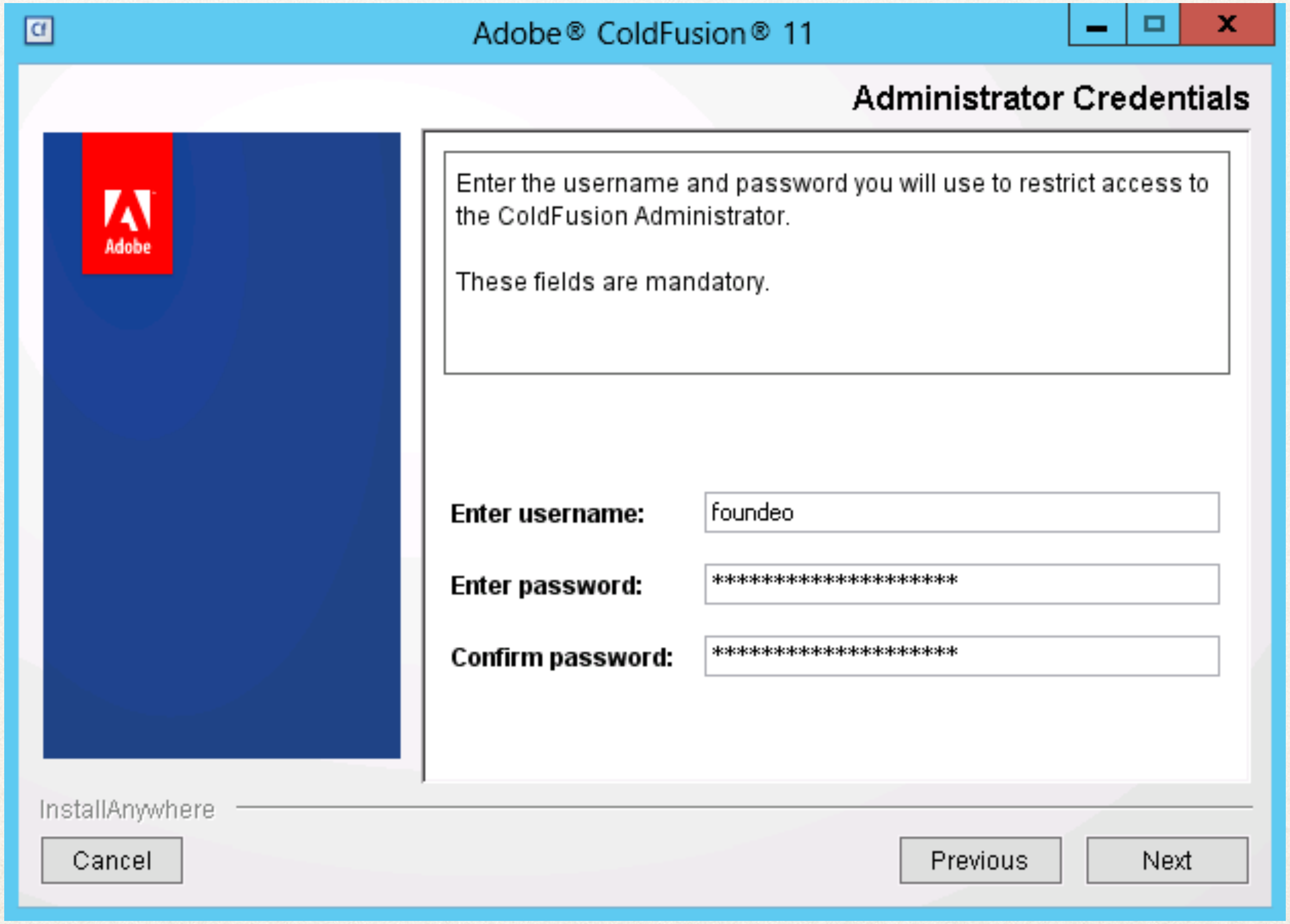


Built-in Web Server Port Number

The Adobe ColdFusion 11 Built-in Web Server will be configured to use port 8500. You can also specify a different port.

ColdFusion server Port: 8500

Installation



Administrator Credentials

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

These fields are mandatory.

Enter username: foundeo

Enter password: *******************

Confirm password: *******************

Post-Install

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

Accessing CF Administrator

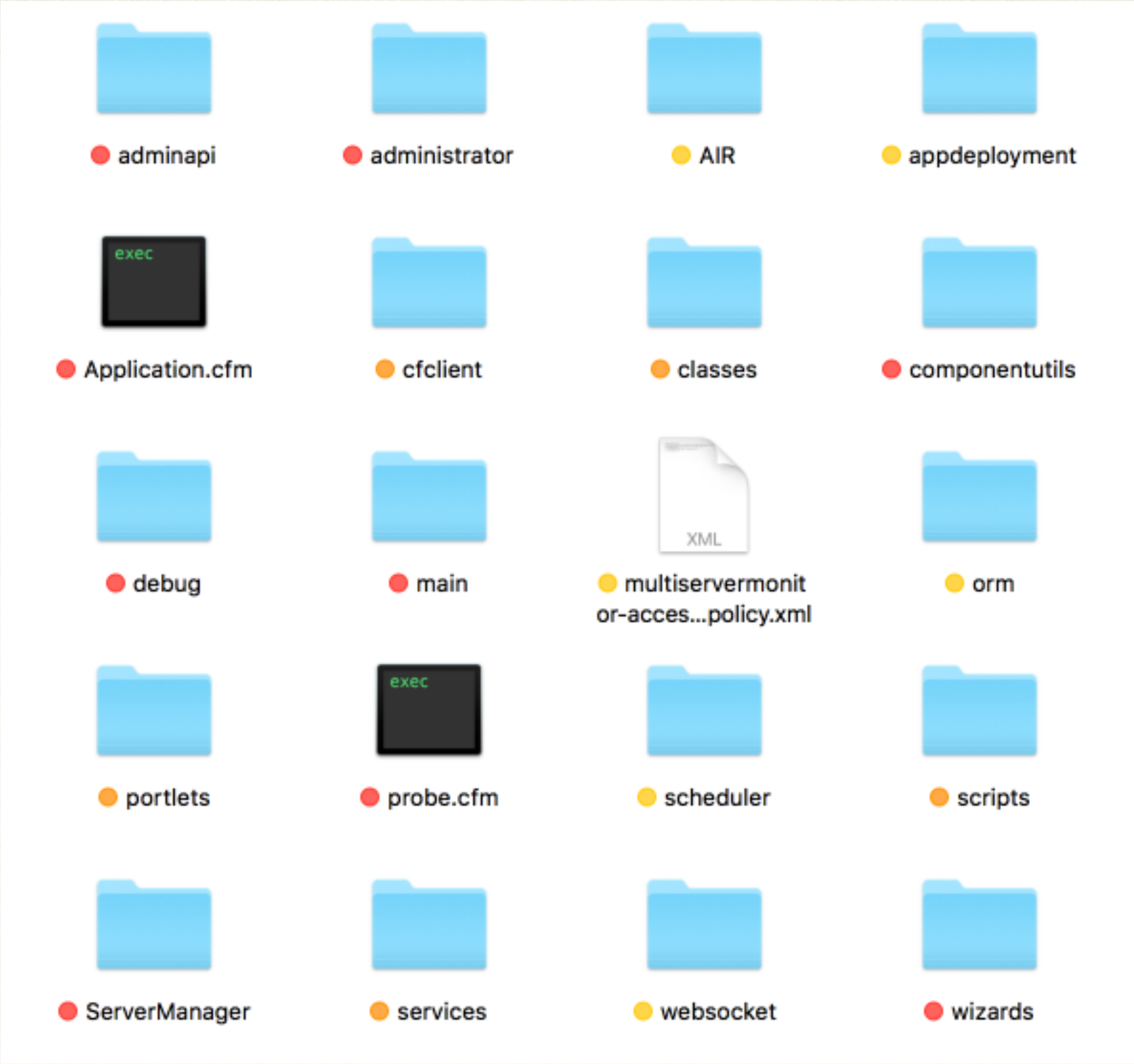
- Setup webserver (IIS / Apache)
    - IP Restrictions, SSL, Additional User Auth
- or Use Builtin Web Server

Using Builtin Web Server

- Pro: Easy /CFIDE block
- Con: Harder to configure SSL, Virtual Directories, IP Restrictions
- Works well if using RDP to access from localhost, or setting up ssh tunneling on unix
- If you need to access from public network, create a dedicated site, use SSL, IP restrictions, etc.

Block /CFIDE

- If possible block all CFIDE
    - If partially required block everything else.
    - Block server wide, not by virtual host
    - Always Restrict:
        - /CFIDE/administrator
        - /CFIDE/adminapi
    - CF11 no longer has /CFIDE/GraphData.cfm



Red = Should be blocked

Orange = Block if possible

Yellow = Low risk but can be blocked

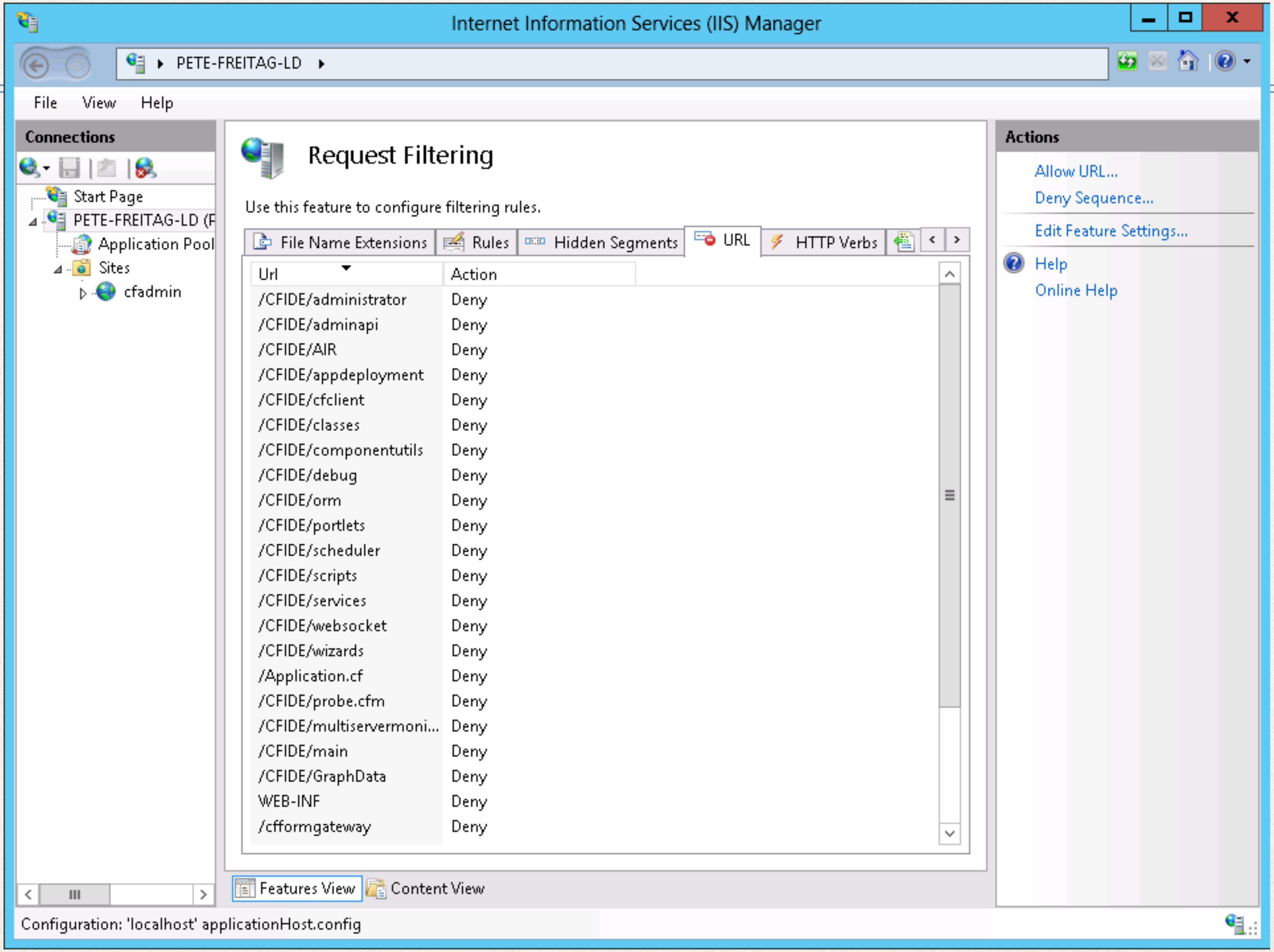
Apache

- RedirectMatch 404 (?i).*/CFIDE.*
- <LocationMatch "(?i).*/CFIDE">

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



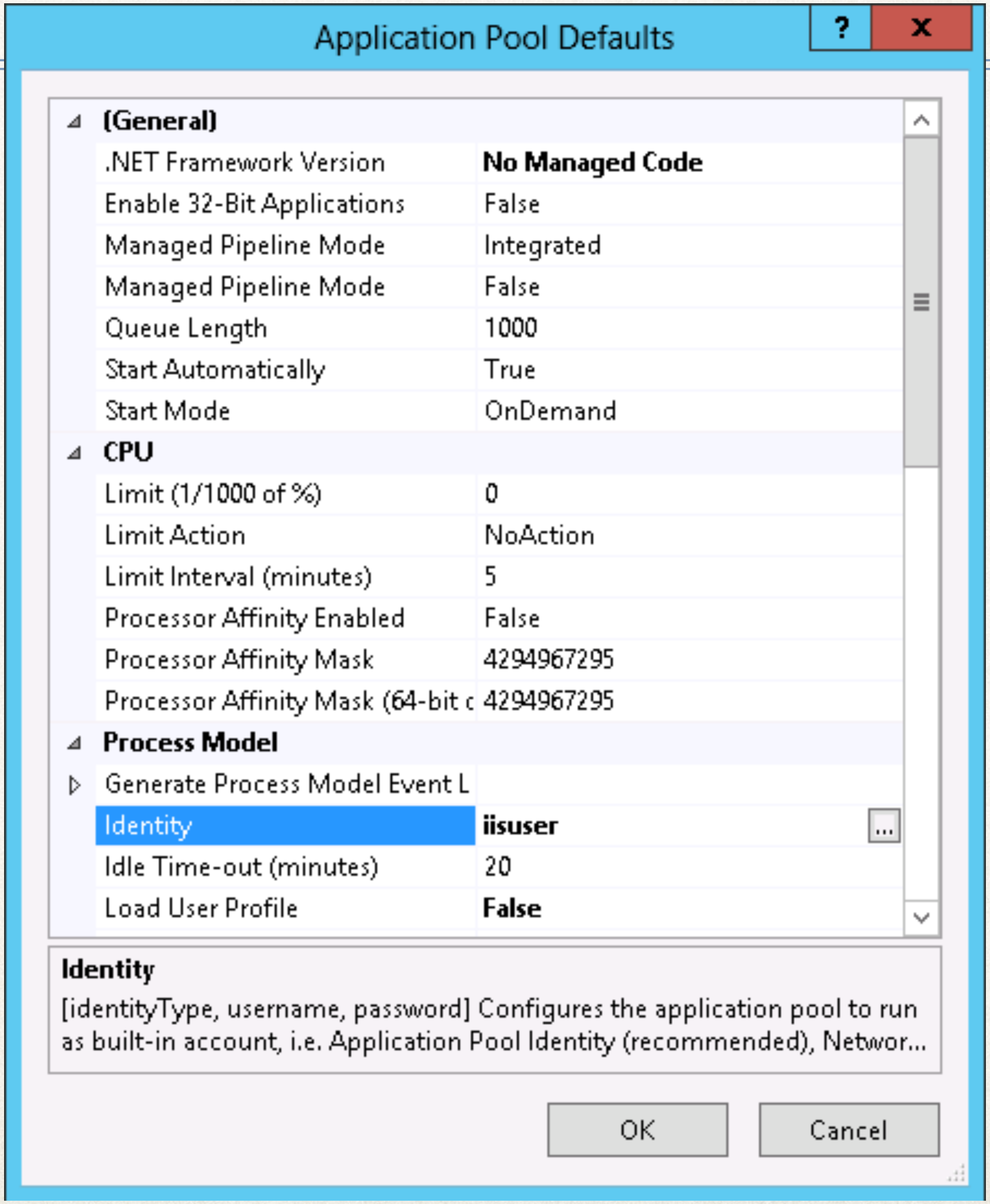
Request Filtering

Use this feature to configure filtering rules.

Url	Action
/CFIDE/administrator	Deny
/CFIDE/adminapi	Deny
/CFIDE/AIR	Deny
/CFIDE/appdeployment	Deny
/CFIDE/cfclient	Deny
/CFIDE/classes	Deny
/CFIDE/componentutils	Deny
/CFIDE/debug	Deny
/CFIDE/orm	Deny
/CFIDE/portlets	Deny
/CFIDE/scheduler	Deny
/CFIDE/scripts	Deny
/CFIDE/services	Deny
/CFIDE/websocket	Deny
/CFIDE/wizards	Deny
/Application.cf	Deny
/CFIDE/probe.cfm	Deny
/CFIDE/multiservermoni...	Deny
/CFIDE/main	Deny
/CFIDE/GraphData	Deny
WEB-INF	Deny
/cfformgateway	Deny

Configuration: 'localhost' applicationHost.config

Application Pool Defaults



(General)	
.NET Framework Version	**No Managed Code**
Enable 32-Bit Applications	False
Managed Pipeline Mode	Integrated
Managed Pipeline Mode	False
Queue Length	1000
Start Automatically	True
Start Mode	OnDemand
CPU	
Limit (1/1000 of %)	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	**iisuser**
Idle Time-out (minutes)	20
Load User Profile	**False**

Identity

[identityType, username, password] Configures the application pool to run as built-in account, i.e. Application Pool Identity (recommended), Networ...

Block unused servlet mappings

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

Restrict File Extensions

- By Folder (user upload directories):
  - Eg: Restrict folder to serve only jpg, png, gif files.
- Can be done globally or on site specific as well
  - The /jakarta virtual directory needs dll extension

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 User Permissions
Web Root	Read Only Additional as needed	Read Only
CF Root	Full Can be restricted further	/CFIDE
CF Connector	Read	Read Write (Logs)

File System Permissions

- /CFIDE and other directories under CF root can be restricted read only permission by the cf user to prevent runtime change.
- Run CF10/CF11 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 CF10-11)
  - 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.

Sandbox Security

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

Session Mechanism

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

CF10-11 / tomcat

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 `/CFIDE/scripts/` -> `/some-folder/`
  - Allows you to block `/CFIDE`
  - 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 | hackmycf.com | fuseguard.com