



# Managing

Version 2.13.10. Copyright (c) Codice Foundation

# Table of Contents

License .....	1
1. Securing .....	2
1.1. Security Hardening .....	2
1.1.1. Hardening Checklist .....	3
1.2. Auditing .....	3
1.2.1. Enabling Fallback Audit Logging .....	4
2. Installing .....	5
2.1. Installation Prerequisites .....	5
2.1.1. Hardware Requirements .....	6
2.1.2. Java Requirements .....	6
2.2. Installing With the DDF Distribution Zip .....	9
2.2.1. Configuring Operating Permissions and Allocations .....	11
2.2.1.1. Setting Directory Permissions .....	12
2.2.1.2. Configuring Memory Allocation for the DDF Java Virtual Machine .....	14
2.2.1.3. Enabling JMX .....	14
2.2.1.4. Configuring Memory for the Solr Server .....	15
2.2.2. Managing Keystores and Certificates .....	15
2.2.2.1. Managing Keystores .....	16
2.2.2.1.1. Adding an Existing Server Keystore .....	17
2.2.2.1.2. Adding an Existing Server Truststore .....	17
2.2.2.1.3. Creating a New Keystore/Truststore with an Existing Certificate and Private Key ..	17
2.2.2.1.4. Updating Key Store / Trust Store via the Admin Console .....	18
2.3. Initial Startup .....	20
2.3.1. Verifying Startup .....	20
2.3.2. DDF Directory Contents after Installation and Initial Startup .....	21
2.3.3. Completing Installation .....	22
2.3.3.1. Completing Installation from the Admin Console .....	22
2.3.3.2. Completing Installation from the Command Console .....	24
Configure Guest Claim Attributes .....	24
System Configuration Settings .....	25
2.3.3.3. Firewall Port Configuration .....	25
2.3.3.4. Internet Explorer 11 Enhanced Security Configuration .....	25
2.4. High Availability Initial Setup .....	26
2.4.1. High Availability Initial Setup Exceptions .....	26
2.4.1.1. Failover Proxy Integration .....	27
2.4.1.2. Identical Directory Structures .....	27

2.4.1.3. Highly Available Security Auditing .....	27
2.4.1.4. Shared Storage Provider .....	28
2.4.1.5. High Availability Certificates .....	28
2.4.1.6. High Availability Installation Profile .....	28
3. Configuring .....	29
3.1. Admin Console Tutorial .....	29
3.2. Console Command Reference .....	31
3.2.1. Feature Commands .....	31
3.2.1.1. Uninstalling Features from the Command Console .....	32
3.3. Configuration Files .....	32
3.3.1. Configuring Global Settings with custom.system.properties .....	33
3.3.2. Configuring with .config Files .....	42
3.4. Configuring User Access .....	43
3.4.1. Configuring Guest Access .....	43
3.4.1.1. Denying Guest User Access .....	44
3.4.1.2. Allowing Guest User Access .....	44
3.4.1.2.1. Configuring Guest Interceptor if Allowing Guest Users .....	44
3.4.1.2.2. Configuring Guest Claim Attributes .....	44
3.4.2. Configuring REST Services for Users .....	45
3.4.2.1. Configuring Included Identity Provider .....	45
3.4.2.1.1. Configuring Included STS .....	50
3.4.2.1.2. Connecting to External STS .....	52
3.4.2.2. Connecting to an External Identity Provider .....	53
3.4.2.3. Configuring Without an Identity Provider .....	53
3.4.2.3.1. Using STS without IdP .....	54
3.4.2.3.2. Connecting to External STS Without IdP .....	54
3.4.3. Configuring SOAP Services for Users .....	54
3.4.3.1. Connecting to Included STS with SOAP .....	54
3.4.3.2. Connecting to External STS with SOAP .....	55
3.4.4. Connecting to an LDAP Server .....	55
3.4.5. Configuring SSO Using a CAS Server .....	55
3.4.5.1. CAS Integration Using Standalone Servers .....	57
3.4.5.1.1. LDAP .....	57
3.4.5.1.2. CAS .....	58
3.4.5.1.3. STS .....	58
3.4.5.1.4. Configuring DDF .....	59
3.4.6. Updating System Users .....	60
3.4.7. Restricting Access to Admin Console .....	61

3.4.7.1. Restricting Feature, App, Service, and Configuration Access .....	62
3.4.8. Removing Default Users .....	63
3.4.9. Disallowing Login Without Certificates .....	64
3.4.10. Managing Certificate Revocation List (CRL) .....	64
3.4.10.1. Creating a Certificate Revocation List (CRL) .....	64
3.4.10.1.1. Revoke a Certificate and Create a New CRL that Contains the Revoked Certificate	65
3.4.10.1.2. Viewing a CRL .....	65
3.4.10.2. Enabling Certificate Revocation .....	65
3.4.10.2.1. Add Revocation to a Web Context .....	66
3.4.10.2.2. Adding Revocation to an Endpoint .....	66
3.4.10.2.3. Verifying Revocation .....	67
3.5. Configuring Data Management .....	68
3.5.1. Configuring Solr .....	68
3.5.1.1. Configuring Solr Catalog Provider Synonyms .....	68
3.5.1.1.1. Defining synonym rules in the Solr Provider .....	68
3.5.1.2. Hardening Solr .....	68
3.5.1.2.1. Hardening Solr Server Configuration .....	68
3.5.1.2.2. Solr Server Password Management .....	69
Do not Autogenerate a Solr Password .....	69
Change the Password to a Specific String .....	69
Restore the Default Password in Solr .....	70
Removing Basic Authentication from Solr .....	70
3.5.1.2.3. Configuring Solr Encryption .....	70
3.5.1.3. Accessing the Solr Admin UI .....	71
3.5.1.3.1. Configuring a Browser to Access Solr Admin UI .....	71
3.5.1.3.2. Using DDF Keystores .....	71
3.5.1.3.3. Solr Admin UI's URL .....	71
3.5.2. Changing Catalog Providers .....	71
3.5.3. Changing Hostname .....	72
3.5.4. Configuring Errors and Warnings .....	72
3.5.4.1. Enforcing Errors or Warnings .....	72
3.5.4.2. Hiding Errors or Warnings from Queries .....	72
3.5.4.3. Hiding Errors and Warnings from Users Based on Role .....	73
3.5.5. Content Directory Monitor .....	73
3.5.5.1. Installing the Content Directory Monitor .....	74
3.5.5.2. Configuring Permissions for the Content Directory Monitor .....	74
3.5.5.3. Configuring the Content Directory Monitor .....	74
3.5.5.4. Using the Content Directory Monitor .....	75

3.5.6. Configuring System Usage Message .....	77
3.5.7. Configuring Data Policy Plugins .....	78
3.5.7.1. Configuring the Metacard Attribute Security Policy Plugin .....	78
3.5.7.2. Configuring the Metacard Validation Marker Plugin .....	78
3.5.7.3. Configuring the Metacard Validity Filter Plugin .....	79
3.5.7.4. Configuring the XML Attribute Security Policy Plugin .....	79
3.5.8. Configuring Data Access Plugins .....	79
3.5.8.1. Configuring the Security Audit Plugin .....	79
3.6. Configuring Security Policies .....	80
3.6.1. Configuring the Web Context Policy Manager .....	80
3.6.1.1. Context Realms .....	80
3.6.1.2. Authentication Types .....	80
3.6.1.3. Required Attributes .....	81
3.6.1.4. White Listed Contexts .....	81
3.6.2. Configuring Catalog Filtering Policies .....	81
3.6.2.1. Setting Internal Policies .....	81
3.6.2.2. Setting XACML Policies .....	82
3.6.2.3. Catalog Filter Policy Plugins .....	82
3.7. Configuring User Interfaces .....	82
3.7.1. Configuring Intrigue .....	82
3.7.1.1. Configuring Default Layout for Intrigue .....	82
3.7.1.2. Configuring Map Layers for Intrigue .....	83
3.7.1.3. Map Configuration for Intrigue .....	84
3.7.1.4. Configuring User Access to Ingest and Metadata for Intrigue .....	85
3.7.1.5. Configuring the Intrigue Upload Editor .....	86
3.7.1.6. Configuring Search Options for Intrigue .....	86
3.7.1.7. Configuring Query Feedback for Intrigue .....	87
3.8. Configuring Federation .....	88
3.8.1. Enable SSL for Clients .....	88
3.8.2. Configuring HTTP(S) Ports .....	89
3.8.3. Configuring HTTP Proxy .....	90
3.8.4. Federation Strategy .....	90
3.8.4.1. Configuring Federation Strategy .....	90
3.8.4.1.1. Catalog Federation Strategy .....	91
3.8.5. Connecting to Sources .....	91
3.8.5.1. Federated Source for Atlassian Confluence(R) .....	93
3.8.5.2. CSW Specification Profile Federated Source .....	95
3.8.5.3. CSW Federation Profile Source .....	95

3.8.5.4. Content File System Storage Provider .....	96
3.8.5.5. GMD CSW Source .....	96
3.8.5.6. OpenSearch Source .....	97
3.8.5.7. Registry Store .....	99
3.8.5.8. Solr Catalog Provider .....	100
3.8.5.9. WFS 1.0 Source .....	102
3.8.5.10. WFS 1.1 Source .....	103
3.8.5.11. WFS 2.0 Source .....	105
3.8.6. Federating Through a Registry .....	107
3.8.6.1. Configuring Identity Node .....	107
3.8.6.1.1. Adding a Service Binding to a Node .....	110
3.8.6.2. Publishing to Other Nodes .....	110
3.8.6.3. Subscribing to Another Node .....	110
3.9. Environment Hardening .....	111
3.9.1. Known Issues with Environment Hardening .....	111
3.10. Configuring for Special Deployments .....	115
3.10.1. Multiple Installations .....	115
3.10.1.1. Reusing Configurations .....	115
3.10.1.2. Isolating Solr Cloud and Zookeeper .....	117
3.10.2. Configuring for a Fanout Proxy .....	118
3.10.3. Standalone Security Token Service (STS) Installation .....	118
3.10.4. Configuring for a Highly Available Cluster .....	118
3.11. Configuring UI Themes .....	119
3.11.1. Landing Page .....	119
3.11.1.1. Installing the Landing Page .....	119
3.11.1.2. Configuring the Landing Page .....	119
3.11.1.3. Customizing the Landing Page .....	119
3.11.2. Configuring Logout Page .....	120
3.11.3. Platform UI Themes .....	120
3.11.3.1. Navigating to UI Theme Configuration .....	120
3.11.3.2. Customizing the UI Theme .....	120
3.12. Miscellaneous Configurations .....	121
3.12.1. Configuring Thread Pools .....	121
3.12.2. Configuring Jetty ThreadPool Settings .....	121
3.12.3. Configuring Alerts .....	121
3.12.3.1. Configuring Decanter Service Level Agreement (SLA) Checker .....	121
3.12.3.2. Configuring Decanter Scheduler .....	122
4. Running .....	122

4.1. Starting .....	123
4.1.1. Run DDF as a Managed Service .....	123
4.1.1.1. Running as a Service with Automatic Start on System Boot .....	123
4.1.1.2. Karaf Documentation .....	125
4.2. Managed Services .....	125
4.2.1. Run Solr as Managed Service .....	126
4.2.1.1. Configure Solr as a Windows Service .....	126
4.2.1.2. Configure Solr as a Systemd Service .....	127
4.2.2. Starting from Startup Scripts .....	127
4.2.3. Starting as a Background Process .....	128
4.2.4. Stopping DDF .....	128
4.3. Maintaining .....	129
4.3.1. Console Commands .....	129
4.3.1.1. Console Command Help .....	129
4.3.1.2. CQL Syntax .....	130
4.3.1.3. Available Console Commands .....	130
4.3.1.3.1. Catalog Commands .....	131
4.3.1.3.2. Subscriptions Commands .....	134
4.3.1.3.3. Platform Commands .....	138
4.3.1.3.4. Persistence Store Commands .....	138
4.3.1.4. Command Scheduler .....	139
4.3.1.4.1. Schedule a Command .....	139
4.3.1.4.2. Updating a Scheduled Command .....	139
4.3.1.4.3. Output of Scheduled Commands .....	140
4.4. Monitoring .....	140
4.4.1. Metrics Reporting .....	140
4.4.2. Managing Logging .....	141
4.4.2.1. Configuring Logging .....	141
4.4.2.2. DDF log file .....	141
4.4.2.3. Controlling log level .....	141
4.4.2.4. Controlling the size of the log file .....	141
4.4.2.5. Number of backup log files to keep .....	141
4.4.2.6. Enabling logging of inbound and outbound SOAP messages for the DDF SOAP endpoint .....	141
4.4.2.7. Logging External Resources .....	142
4.4.2.8. Enabling HTTP Access Logging .....	142
4.4.2.9. Using the LogViewer .....	143
4.5. Troubleshooting .....	143
4.5.1. Deleted Records Are Being Displayed In The Search UI's Search Results .....	145

5. Data Management .....	146
5.1. Ingesting Data .....	146
5.1.1. Ingest Command .....	146
5.1.2. User Interface Ingest .....	147
5.1.3. Content Directory Monitor Ingest .....	147
5.1.4. External Methods of Ingesting Data .....	147
5.1.5. Other Methods of Ingesting Data .....	149
5.2. Backing Up the Catalog .....	149
5.3. Validating Data .....	149
5.3.1. Validator Plugins on Ingest .....	149
5.3.1.1. List of Validators run on ingest .....	150
5.3.2. Viewing Invalid Metacards .....	151
5.3.3. Manually Editing Attributes .....	151
5.3.4. Injecting Attributes .....	151
5.3.5. Overriding Attributes .....	152
5.4. Removing Expired Records from the Catalog .....	152
5.5. Migrating Data .....	152
5.6. Automatically Added Metacard Attributes .....	153
5.6.1. Attributes Added on Ingest .....	153
5.6.1.1. Attributes Added by Input Transformers .....	154
5.6.1.2. Attributes Added by Attribute Injection .....	154
5.6.1.3. Attributes Added by Default Attribute Types .....	154
5.6.1.4. Attributes Added by Attribute Overrides (Ingest) .....	155
5.6.1.5. Attributes Added by Pre-Authorization Plugins .....	155
5.6.1.6. Attributes Added by Pre-Ingest Plugins .....	155
5.6.2. Attributes Added on Query .....	155
5.6.2.1. Attributes Added by Attribute Overrides (Query) .....	155



# License

Copyright (c) Codice Foundation.

This work is licensed under a [Creative Commons Attribution 4.0 International License](#).

This document last updated: 2019-06-14 03:38:38:947.

Administrators will be installing, maintaining, and supporting existing applications. Use this section to prepare, install, configure, run, and monitor a DDF.

# 1. Securing

Security is an important consideration for DDF, so it is imperative to update configurations away from the defaults to unique, secure settings.

## IMPORTANT

### *Securing DDF Components*

DDF is enabled with an Insecure Defaults Service which will warn users/admins if the system is configured with insecure defaults.

A banner is displayed on the admin console notifying "The system is insecure because default configuration values are in use."

A detailed view is available of the properties to update.

Security concerns will be highlighted in the configuration sections to follow.

## 1.1. Security Hardening

### Security Hardening

To harden DDF, extra security precautions are required.

Where available, necessary mitigations to harden an installation of DDF are called out in the following configuration steps.

Refer to the [Hardening Checklist](#) for a compilation of these mitigations.

## NOTE

The security precautions are best performed as configuration is taking place, so hardening steps are integrated into configuration steps.

This is to avoid setting an insecure configuration and having to revisit during hardening. Most configurations have a security component to them, and important considerations for hardening are labeled as such during configuration as well as provided in a checklist format.

Some of the items on the checklist are performed during [installation](#) and others during [configuration](#). Steps required for hardening are marked as **Required for Hardening** and are collected here for convenience. Refer to the checklist during system setup.

### 1.1.1. Hardening Checklist

The following list enumerates the required mitigations needed for hardening:

- ☐ [Configure Auditing](#)
- ☐ [Set Directory Permissions](#)
- ☐ [Configure Keystore and Certificates](#)
- ☐ [Disallow Login Without Certificates](#)
- ☐ [Configure Certificate Revocation List](#)
  - ☐ [Deny Guest User Access](#) (if denying Guest users)
  - ☐ [Allow Guest User Access](#) (if allowing Guest users)
- ☐ [Configure Guest Claim Attributes](#) (if allowing Guest users)
- ☐ [Configure Guest User Authentication](#)
- ☐ [Create unique user role](#)
- ☐ [Limit Access to the STS](#)
- ☐ [Restricting Access to Admin Console](#)
- ☐ [Restrict Feature, App, Service, and Configuration Access](#)
- ☐ [Remove Default Users](#)
- ☐ [Harden Solr](#)
- ☐ [Environment Hardening](#)
- ☐ [Isolate Solr Cloud and Zookeeper](#). (If using)

## 1.2. Auditing

### • Required Step for Security Hardening

Audit logging captures security-specific system events for monitoring and review. DDF provides a [Audit Plugin](#) that logs all catalog transactions to the `security.log`. Information captured includes user identity, query information, and resources retrieved.

Follow all operational requirements for the retention of the log files. This may include using cryptographic mechanisms, such as encrypted file volumes or databases, to protect the integrity of audit information.

<b>NOTE</b>	The Audit Log default location is <code>&lt;DDF_HOME&gt;/data/log/security.log</code>
-------------	---

### *Audit Logging Best Practices*

For the most reliable audit trail, it is recommended to configure the operational environment of the DDF to generate alerts to notify administrators of:

#### **NOTE**

- auditing software/hardware errors
- failures in audit capturing mechanisms
- audit storage capacity (or desired percentage threshold) being reached or exceeded.

#### **WARNING**

The security audit logging function does not have any configuration for audit reduction or report generation. The logs themselves could be used to generate such reports outside the scope of DDF.

## **1.2.1. Enabling Fallback Audit Logging**

### **• Required Step for Security Hardening**

In the event the system is unable to write to the `security.log` file, DDF must be configured to fall back to report the error in the application log:

- edit `<DDF_HOME>/etc/org.ops4j.pax.logging.cfg`
  - uncomment the line (remove the `#` from the beginning of the line) for `log4j2` (`org.ops4j.pax.logging.log4j2.config.file = ${karaf.etc}/log4j2.config.xml`)
  - delete all subsequent lines

If you want to change the location of your systems security backup log from the default location: `<DDF_HOME>/data/log/securityBackup.log`, follow the next two steps:

- edit `<DDF_HOME>/security/configurations.policy`
  - find "Security-Hardening: Backup Log File Permissions"
  - below `grant codeBase "file:/pax-logging-log4j2"` add the path to the directory containing the new log file you will create in the next step.
- edit `<DDF_HOME>/etc/log4j2.config.xml`
  - find the entry for the `securityBackup` appender. (see example)
  - change value of `filename` and prefix of `filePattern` to the name/path of the desired failover security logs

### securityBackup Appender Before

```
<RollingFile name="securityBackup" append="true" ignoreExceptions="false"
             fileName="${sys:karaf.data}/log/securityBackup.log"
             filePattern="${sys:karaf.data}/log/securityBackup.log-%d{yyyy-MM-dd-
HH}-%i.log.gz">
```

### securityBackup Appender After

```
<RollingFile name="securityBackup" append="true" ignoreExceptions="false"
             fileName="<NEW_LOG_FILE>"
             filePattern="<NEW_LOG_FILE>-%d{yyyy-MM-dd-HH}-%i.log.gz">
```

#### WARNING

If the system is unable to write to the `security.log` file on system startup, fallback logging will be unavailable. Verify that the `security.log` file is properly configured and contains logs before configuring a fall back.

## 2. Installing

Set up a complete, secure instance of DDF. For simplified steps used for a testing, development, or demonstration installation, see the [DDF Quick Start](#).

#### IMPORTANT

Although DDF can be installed by any user, it is recommended for security reasons to have a non-`root` user execute the DDF installation.

#### NOTE

Hardening guidance assumes a Standard installation.

Adding other components does not have any security/hardening implications.

### 2.1. Installation Prerequisites

#### WARNING

For security reasons, DDF cannot be started from a user's home directory. If attempted, the system will automatically shut down.

These are the system/environment requirements to configure *prior* to an installation.

#### NOTE

The DDF process or user under which the DDF process runs must have permission to create and write files in the directories where the Solr cores are installed. If this permission is missing, DDF will not be able to create new Solr cores and the system will not function correctly.

### 2.1.1. Hardware Requirements

Table 1. Using the Standard installation of the DDF application:

Minimum and Recommended Requirements for DDF Systems		
Criteria	Minimum	Recommended
CPU	Dual Core 1.6 GHz	Quad Core 2.6 GHz
RAM	8 GB*	32 GB
Disk Space	40 GB	80 GB
Video Card	—	WebGL capable GPU
Additional Software	JRE 8 x64	JDK 8 x64

\*The amount of RAM can be increased to support memory-intensive applications. See [Memory Considerations](#)

#### Operating Systems



DDF has been tested on the following operating systems and with the following browsers. Other operating systems or browsers may be used but have not been officially tested.

Table 2. Tested Operating Systems and Browsers


Operating Systems	Browsers
Windows Server 2012 R2	Internet Explorer 11
Windows Server 2008 R2 Service Pack 1	Microsoft Edge
Windows 10	Firefox
Linux CentOS 7	Chrome
Debian 9	

### 2.1.2. Java Requirements

For a runtime system:

- [JRE 8 x64](#)  or [OpenJDK 8 JRE](#)  must be installed.
- The `JRE_HOME` environment variable must be set to the locations where the JRE is installed

For a development system:

- [JDK8](#) must be installed.
- The `JAVA_HOME` environment variable must be set to the location where the JDK is installed.
  1. Install/Upgrade to Java 8 x64 [J2SE 8 SDK](#) 
    - a. The recommended version is [8u60](#) or later.

- b. Java version must contain only number values.
2. Install/Upgrade to [JDK8](#) ↗.
3. Set the `JAVA_HOME` environment variable to the location where the JDK is installed.

**NOTE** Prior to installing DDF, ensure the system time is accurate to prevent federation issues.

*\*NIX Unset JAVA\_HOME if Previously Set*

**NOTE** Unset `JAVA_HOME` if it is already linked to a previous version of the JRE:

```
unset JAVA_HOME
```

If JDK was installed:

#### *Setting JAVA\_HOME variable*

Replace `<JAVA_VERSION>` with the version and build number installed.

1. Open a terminal window(\*NIX) or command prompt (Windows) with administrator privileges.
2. Determine Java Installation Directory (This varies between operating system versions).

#### *Find Java Path in \*NIX*

```
which java
```

#### *Find Java Path in Windows*

The path to the JDK can vary between versions of Windows, so manually verify the path under:

```
C:\Program Files\Java\jdk<M.m.p_build>
```

3. Copy path of Java installation to clipboard. (example: `/usr/java/<JAVA_VERSION>`)
4. Set `JAVA_HOME` by replacing `<PATH_TO_JAVA>` with the copied path in this command:

#### *Setting JAVA\_HOME on \*NIX*

```
JAVA_HOME=<PATH_TO_JAVA><JAVA_VERSION>  
export JAVA_HOME
```

#### *Setting JAVA\_HOME on Windows*

```
set JAVA_HOME=<PATH_TO_JAVA><JAVA_VERSION>  
setx JAVA_HOME "<PATH_TO_JAVA><JAVA_VERSION>"
```

### *Adding `JAVA_HOME` to `PATH` Environment Variable on Windows*

```
setx PATH "%PATH%;%JAVA_HOME%\bin"
```

5. Restart or open up a new Terminal (shell) or Command Prompt to verify `JAVA_HOME` was set correctly. It is not necessary to restart the system for the changes to take effect.

*\*NIX*

```
echo $JAVA_HOME
```

*Windows*

```
echo %JAVA_HOME%
```

If JRE was installed:

#### *Setting `JRE_HOME` variable*

Replace `<JAVA_VERSION>` with the version and build number installed.

1. Open a terminal window(\*NIX) or command prompt (Windows) with administrator privileges.
2. Determine Java Installation Directory (This varies between operating system versions).

*Find Java Path in \*NIX*

```
which java
```

*Find Java Path in Windows*

The path to the JRE can vary between versions of Windows, so manually verify the path under:

```
C:\Program Files\Java\jre<M.m.p_build>
```

3. Copy path of Java installation to clipboard. (example: `/usr/java/<JAVA_VERSION>`)
4. Set `JRE_HOME` by replacing `<PATH_TO_JAVA>` with the copied path in this command:

*Setting `JRE_HOME` on \*NIX*

```
JRE_HOME=<PATH_TO_JAVA><JAVA_VERSION>  
export JRE_HOME
```



### Setting `JRE_HOME` on Windows

```
set JRE_HOME=<PATH_TO_JAVA><JAVA_VERSION>
setx JRE_HOME "<PATH_TO_JAVA><JAVA_VERSION>"
```

### Adding `JRE_HOME` to `PATH` Environment Variable on Windows

```
setx PATH "%PATH%;%JRE_HOME%\bin"
```

5. Restart or open up a new Terminal (shell) or Command Prompt to verify `JRE_HOME` was set correctly. It is not necessary to restart the system for the changes to take effect.

### \*NIX

```
echo $JRE_HOME
```

### Windows

```
echo %JRE_HOME%
```

### File Descriptor Limit on Linux

- For Linux systems, increase the file descriptor limit by editing `/etc/sysctl.conf` to include:

```
fs.file-max = 6815744
```

### NOTE

- For the change to take effect, a restart is required.

### \*Nix Restart Command

```
init 6
```


## 2.2. Installing With the DDF Distribution Zip

### Check System Time

### WARNING

Prior to installing DDF, ensure the system time is accurate to prevent federation issues.

To install the DDF distribution zip, perform the following:

1. Download the DDF [zip file](#) .
2. After the [prerequisites](#) have been met, change the current directory to the desired install directory, creating a new directory if desired. This will be referred to as `<DDF_HOME>`.

**WARNING**

*Windows Pathname Warning*

Do not use spaces in directory or file names of the `<DDF_HOME>` path. For example, do not install in the default **Program Files** directory.

*Example: Create a Directory (Windows and \*NIX)*

```
mkdir new_installation
```

- a. Use a Non-**root** User on \*NIX. (Windows users skip this step)

It is recommended that the **root** user create a new install directory that can be owned by a non-**root** user (e.g., DDF\_USER). This can be a new or existing user. This DDF\_USER can now be used for the remaining installation instructions.

- b. Create a new group or use an existing group (e.g., DDF\_GROUP) (Windows users skip this step)

*Example: Add New Group on \*NIX*

```
groupadd DDF_GROUP
```

*Example: Switch User on \*NIX*

```
chown DDF_USER:DDF_GROUP new_installation  
  
su - DDF_USER
```

3. Change the current directory to the location of the zip file (ddf-2.13.10.zip).

*\*NIX (Example assumes DDF has been downloaded to a CD/DVD)*

```
cd /home/user/cdrom
```

*Windows (Example assumes DDF has been downloaded to the D drive)*

```
cd D:\
```

4. Copy ddf-2.13.10.zip to `<DDF_HOME>`.

*\*NIX*

```
cp ddf-2.13.10.zip <DDF_HOME>
```

*Windows*

```
copy ddf-2.13.10.zip <DDF_HOME>
```

5. Change the current directory to the desired install location.

*\*NIX or Windows*

```
cd <DDF_HOME>
```

6. The DDF zip is now located within the **<DDF\_HOME>**. Unzip ddf-2.13.10.zip.

*\*NIX*

```
unzip ddf-2.13.10.zip
```

#### *Windows Zip Utility Warning*

The Windows Zip implementation, which is invoked when a user double-clicks on a zip file in the Windows Explorer, creates a corrupted installation. This is a consequence of its inability to process long file paths. Instead, use the java jar command line utility to unzip the distribution (see example below) or use a third party utility such as 7-Zip.

#### **WARNING**

*Use Java to Unzip in Windows(Replace **<PATH\_TO\_JAVA>** with correct path and **<JAVA\_VERSION>** with current version.)*

```
"<PATH_TO_JAVA>\jdk<JAVA_VERSION>\bin\jar.exe" xf ddf-2.13.10.zip
```

The unzipping process may take time to complete. The command prompt will stop responding to input during this time.

### **2.2.1. Configuring Operating Permissions and Allocations**

Restrict access to sensitive files by ensuring that the only users with access privileges are administrators.

Within the **<DDF\_HOME>**, a directory is created named ddf-2.13.10. This directory will be referred to in the documentation as **<DDF\_HOME>**.

1. Do not assume the deployment is from a trusted source; verify its origination.
2. Check the available storage space on the system to ensure the deployment will not exceed the available space.
3. Set maximum storage space on the `<DDF_HOME>/deploy` and `<DDF_HOME>/system` directories to restrict the amount of space used by deployments.

#### 2.2.1.1. Setting Directory Permissions

- **Required Step for Security Hardening**

DDF relies on the Directory Permissions of the host platform to protect the integrity of the DDF during operation. System administrators **MUST** perform the following steps prior to deploying bundles added to the DDF.

##### **IMPORTANT**

The system administrator must restrict certain directories to ensure that the application (user) cannot access restricted directories on the system. For example the `DDF_USER` should have read-only access to `<DDF_HOME>`, except for the sub-directories `etc`, `data`, `solr` and `instances`.

## Setting Directory Permissions on Windows

Set directory permissions on the <DDF\_HOME>; all sub-directories except **etc**, **data**, and **instances**; and any directory intended to interact with the DDF to protect from unauthorized access.

1. Right-click on the <DDF\_HOME> directory.
2. Select **Properties -> Security -> Advanced**.
3. Under **Owner**, select **Change**.
4. Enter **Creator Owner** into the **Enter the Object Name...** field.
5. Select **Check Names**.
6. Select **Apply**.
  - a. If prompted **Do you wish to continue**, select **Yes**.
7. Remove all Permission Entries for any groups or users with access to <DDF\_HOME> other than **System, Administrators**, and **Creator Owner**.
  - a. Note: If prompted with a message such as: **You can't remove X because this object is inheriting permissions from its parent**. when removing entries from the Permission entries table:
    - i. Select **Disable Inheritance**.
    - ii. Select **Convert Inherited Permissions into explicit permissions on this object**.
    - iii. Try removing the entry again.
8. Select the option for **Replace all child object permission entries with inheritable permission entries from this object**.
9. Close the **Advanced Security Settings** window.

## Setting Directory Permissions on \*NIX

Set directory permissions to protect the DDF from unauthorized access.

- Change ownership of <DDF\_HOME>
  - `chown -R ddf-user <DDF_HOME>`
- Create instances sub-directory if does not exist
  - `mkdir -p <DDF_HOME>/instances`
- Change group ownership on sub-directories
  - `chgrp -R DDF_GROUP <DDF_HOME>/etc <DDF_HOME>/data <DDF_HOME>/instances <DDF_HOME>/solr`
- Change group permissions
  - `chmod -R g-w <DDF_HOME>/etc <DDF_HOME>/data <DDF_HOME>/instances <DDF_HOME>/solr`
- Remove permissions for other users
  - `chmod -R o-rwx <DDF_HOME>/etc <DDF_HOME>/data <DDF_HOME>/instances`

### 2.2.1.2. Configuring Memory Allocation for the DDF Java Virtual Machine

The amount of memory allocated to the Java Virtual Machine host DDF by the operating system can be increased by updating the `setenv` script:

*Setenv Scripts: \*NIX*

```
<DDF_HOME>/bin/setenv
Update the JAVA_OPTS -Xmx value
<DDF_HOME>/bin/setenv-wrapper.conf
Update the wrapper.java.additional -Xmx value
```

*Setenv Scripts: Windows*

```
<DDF_HOME>/bin/setenv.bat
Update the JAVA_OPTS -Xmx value
<DDF_HOME>/bin/setenv-windows-wrapper.conf
Update the wrapper.java.additional -Xmx value
```

### 2.2.1.3. Enabling JMX

By default, DDF prevents connections to JMX because the system is more secure when JMX is not enabled. However, many monitoring tools require a JMX connection to the Java Virtual Machine. To enable JMX, update the `setenv` script:

### *Setenv Scripts: \*NIX*

```
<DDF_HOME>/bin/setenv
Remove -XX:+DisableAttachMechanism from JAVA_OPTS
<DDF_HOME>/bin/setenv-wrapper.conf
Comment out the -XX:+DisableAttachMechanism line and re-number remainder lines
appropriately
```

### *Setenv Scripts: Windows*

```
<DDF_HOME>/bin/setenv.bat
Remove -XX:+DisableAttachMechanism from JAVA_OPTS
<DDF_HOME>/bin/setenv-windows-wrapper.conf
Comment out the -XX:+DisableAttachMechanism line and re-number remainder lines
appropriately
```

#### **2.2.1.4. Configuring Memory for the Solr Server**

##### **NOTE**

This section applies only to configurations that manage the lifecycle of the Solr server. It does not apply to Solr Cloud configurations.

The Solr server consumes large amount of memory when it ingests documents. If the Solr server runs out of memory, it terminates its process. To allocate more memory to the Solr server, increase the value of the `solr.mem` property.

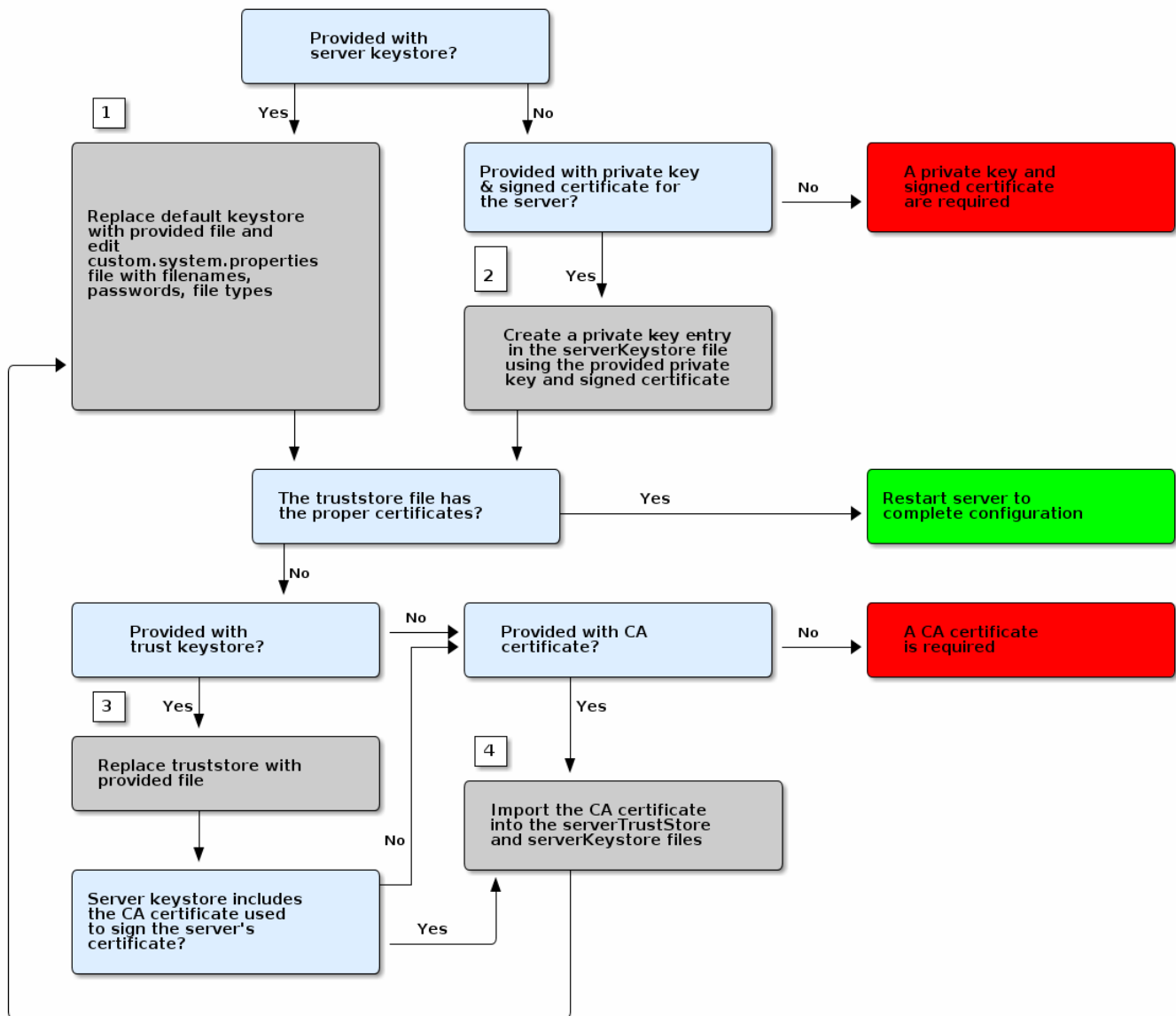
#### **2.2.2. Managing Keystores and Certificates**

- **Required Step for Security Hardening**

DDF uses certificates in two ways:

1. Ensuring the privacy and integrity of messages sent or received over a network.
2. Authenticating an incoming user request.

To ensure proper configuration of keystore, truststore, and certificates, follow the options below according to situation.



### Configuring Certificates Workflow

Jump to the steps referenced in the diagram:

#### Certificate Workflow Steps

1. [Adding an Existing Keystore](#)
2. [Creating a New Keystore/Truststore with an Existing Certificate and Private Key](#)
3. [Adding an Existing Truststore](#)
4. [Creating a Server Keystore](#)
  - a. [Creating a Server Truststore](#)

#### 2.2.2.1. Managing Keystores

Certificates, and sometimes their associated private keys, are stored in keystore files. DDF includes two



default keystore files, the server key store and the server trust store. The server keystore holds DDF's certificate and private key. It will also hold the certificates of other nodes whose signature DDF will accept. The truststore holds the certificates of nodes or other entities that DDF needs to trust.

**NOTE**

Individual certificates of other nodes should be added to the keystore instead of CA certificates. If a CA's certificate is added, DDF will automatically trust any certificate that is signed by that CA.

#### 2.2.2.1.1. Adding an Existing Server Keystore

If provided an existing keystore for use with DDF, follow these steps to replace the default keystore.

1. Remove the default keystore at `etc/keystore/serverKeystore.jks`.
2. Add the desired keystore file to the `etc/keystore` directory.
3. Edit `custom.system.properties` file to set filenames and passwords.
  - a. If using a type of keystore other than `jks` (such as `pcks12`), change the `javax.net.ssl.keyStoreType` property as well.
4. If the truststore has the correct certificates, restart server to complete configuration.
  - a. If provided with an existing server truststore, continue to [Adding an Existing Server Truststore](#).
  - b. Otherwise, [create a server truststore](#).

#### 2.2.2.1.2. Adding an Existing Server Truststore

1. Remove the default truststore at `etc/keystore/serverTruststore.jks`.
2. Add the desired truststore file to the `etc/keystore` directory.
3. Edit `custom.system.properties` file to set filenames and passwords.
  - a. If using a type of truststore other than `jks` (such as `pcks12`), change the `javax.net.ssl.trustStoreType` property as well.

If the provided server keystore does not include the CA certificate that was used to sign the server's certificate, [add the CA certificate into the serverKeystore file](#).

#### 2.2.2.1.3. Creating a New Keystore/Truststore with an Existing Certificate and Private Key

If provide an existing certificate create a new keystore and truststore with it.

**NOTE**

DDF requires that the keystore contains both the private key and the CA.

1. Using the private key, certificate, and CA certificate, create a new keystore containing the data from the new files.

```
cat client.crt >> client.key
openssl pkcs12 -export -in client.key -out client.p12
keytool -importkeystore -srckeystore client.p12 -destkeystore serverKeystore.jks
-srcstoretype pkcs12 -alias 1
keytool -changealias -alias 1 -destalias client -keystore serverKeystore.jks
keytool -importcert -file ca.crt -keystore serverKeystore.jks -alias "ca"
keytool -importcert -file ca-root.crt -keystore serverKeystore.jks -alias "ca-root"
```

2. Create the truststore using only the CA certificate. Based on the concept of CA signing, the CA should be the only entry needed in the truststore.

```
keytool -import -trustcacerts -alias "ca" -file ca.crt -keystore truststore.jks
keytool -import -trustcacerts -alias "ca-root" -file ca-root.crt -keystore
truststore.jks
```

3. Create a PEM file using the certificate, as some applications require that format.

```
openssl x509 -in client.crt -out client.der -outform DER
openssl x509 -in client.der -inform DER -out client.pem -outform PEM
```

**IMPORTANT**      The localhost certificate must be removed if using a system certificate.

#### 2.2.2.1.4. Updating Key Store / Trust Store via the Admin Console

Certificates (and certificates with keys) can be managed in the Admin Console.

1. Navigate to the Admin Console.
2. Select the **Security** application.
3. Select the **Certificates** tab.
4. Add and remove certificates and private keys as necessary.
5. Restart DDF.

**IMPORTANT**      The default trust store and key store files for DDF included in `etc/keystores` use self-signed certificates. Self-signed certificates should never be used outside of development/testing areas.

This view shows the alias (name) of every certificate in the trust store and the key store. It also displays if the entry includes a private key ("Is Key") and the encryption scheme (typically "RSA" or "EC").

This view allows administrators remove certificates from DDF's key and trust stores. It also allows administrators to import certificates and private keys into the keystores with the "+" button. The

import function has two options: import from a file or import over HTTPS. The file option accepts a Java Keystore file or a PKCS12 keystore file. Because keystores can hold many keys, the import dialog asks the administrator to provide the alias of the key to import. Private keys are typically encrypted and the import dialog prompts the administrator to enter the password for the private key. Additionally, keystore files themselves are typically encrypted and the dialog asks for the keystore ("Store") password.

The name and location of the DDF trust and key stores can be changed by editing the system properties files, `etc/custom.system.properties`. Additionally, the password that DDF uses to decrypt (unlock) the key and trust stores can be changed here.

#### IMPORTANT

DDF assumes that password used to unlock the keystore is the same password that unlocks private keys in the keystore.

The location, file name, passwords and type of the server and trust key stores can be set in the `custom.system.properties` file:

#### 1. Setting the Keystore and Truststore Java Properties

```
javax.net.ssl.keyStore=etc/keystores/serverKeystore.jks
javax.net.ssl.keyStorePassword=changeit
javax.net.ssl.trustStore=etc/keystores/serverTruststore.jks
javax.net.ssl.trustStorePassword=changeit
javax.net.ssl.keyStoreType=jks
javax.net.ssl.trustStoreType=jks
```

#### NOTE

If the server's fully qualified domain name is not recognized, the name may need to be added to the network's DNS server.

#### TIP

The DDF instance can be tested even if there is no entry for the FQDN in the DNS. First, test if the FQDN is already recognized. Execute this command:

```
ping <FQDN>
```

If the command responds with an error message such as unknown host, then modify the system's `hosts` file to point the server's FQDN to the loopback address. For example:

```
127.0.0.1 <FQDN>
```

### Changing Default Passwords

This step is not required for a hardened system.

#### NOTE

- The default password in `custom.system.properties` for `serverKeystore.jks` is `changeit`. This needs to be modified.
  - `ds-cfg-key-store-file: ../../keystores/serverKeystore.jks`
  - `ds-cfg-key-store-type: JKS`
  - `ds-cfg-key-store-pin: password`
  - `cn: JKS`
- The default password in `custom.system.properties` for `serverTruststore.jks` is `changeit`. This needs to be modified.
  - `ds-cfg-trust-store-file: ../../keystores/serverTruststore.jks`
  - `ds-cfg-trust-store-pin: password`
  - `cn: JKS`

## 2.3. Initial Startup

Run the DDF using the appropriate script.

*\*NIX*

```
<DDF_HOME>/bin/ddf
```

*Windows*

```
<DDF_HOME>/bin/ddf.bat
```

The distribution takes a few moments to load depending on the hardware configuration.

#### TIP

To run DDF as a service, see [Starting as a Service](#).

### 2.3.1. Verifying Startup

At this point, DDF should be configured and running with a Solr Catalog Provider. New features (endpoints, services, and sites) can be added as needed.

Verification is achieved by checking that all of the DDF bundles are in an **Active** state (excluding fragment bundles which remain in a **Resolved** state).

#### NOTE

It may take a few moments for all bundles to start so it may be necessary to wait a few minutes before verifying installation.

Execute the following command to display the status of all the DDF bundles:

View Status

```
ddf@local>list | grep -i ddf
```

**WARNING**

Entries in the **Resolved** state are expected, they are OSGi bundle fragments. Bundle fragments are distinguished from other bundles in the command line console list by a field named **Hosts**, followed by a bundle number. Bundle fragments remain in the **Resolved** state and can never move to the **Active** state.

Example: Bundle Fragment in the Command Line Console

```
96 | Resolved | 80 | 2.10.0.SNAPSHOT | DDF :: Platform :: PaxWeb :: Jetty Config, Hosts:
90
```

After successfully completing these steps, the DDF is ready to be configured.

**2.3.2. DDF Directory Contents after Installation and Initial Startup**

During DDF installation, the major directories and files shown in the table below are created, modified, or replaced in the destination directory.

Table 3. DDF Directory Contents

Directory Name	Description
bin	Scripts to start, stop, and connect to DDF.
data	The working directory of the system – installed bundles and their data
data/log/ddf.log	Log file for DDF, logging all errors, warnings, and (optionally) debug statements. This log rolls up to 10 times, frequency based on a configurable setting (default=1 MB)
data/log/ingest_error.log	Log file for any ingest errors that occur within DDF.
data/log/security.log	Log file that records user interactions with the system for auditing purposes.
deploy	Hot-deploy directory – KARs and bundles added to this directory will be hot-deployed (Empty upon DDF installation)
documentation	HTML and PDF copies of DDF documentation.
etc	Directory monitored for addition/modification/deletion of .config configuration files or third party .cfg configuration files.
etc/templates	Template .config files for use in configuring DDF sources, settings, etc., by copying to the etc directory.

Directory Name	Description
<code>lib</code>	The system's bootstrap libraries. Includes the <code>ddf-branding.jar</code> file which is used to brand the system console with the DDF logo.
<code>licenses</code>	Licensing information related to the system.
<code>solr</code>	Apache Solr server used when DDF manages Solr
<code>solr/server/logs/solr.log</code>	Log file for Solr.
<code>system</code>	Local bundle repository. Contains all of the JARs required by DDF, including third-party JARs.

### 2.3.3. Completing Installation

Upon startup, complete installation from either the Admin Console or the Command Console.

#### 2.3.3.1. Completing Installation from the Admin Console

Upon startup, the installation can be completed by navigating to the Admin Console at `https://{FQDN}:{PORT}/admin`.

#### WARNING

##### *Internet Explorer 10 TLS Warning*

Internet Explorer 10 users may need to enable TLS 1.2 to access the Admin Console in the browser.

##### *Enabling TLS1.2 in IE10*

1. Go to **Tools** -> Internet Options -> Advanced -> Settings -> Security.
2. Enable TLS1.2.

- Default user/password: `admin/admin`.

On the initial startup of the Admin Console, a series of prompts walks through essential configurations. These configurations can be changed later, if needed.

- Click **Start** to begin.

## Setup Types

DDF is pre-configured with several installation profiles.

- Standard Installation: **Recommended**. Includes these applications by default:
  - [Admin](#)
  - [Catalog](#)
  - [Platform](#)
  - [Security](#)
  - [Solr Catalog](#)
  - [Spatial](#)
  - [Intrigue](#)
- Minimum Installation: Includes these applications for a minimum install:
  - [Admin](#)
  - [Platform](#)
  - [Security](#)
- Development: Includes all demo, beta, and experimental applications.

## Configure Guest Claim Attributes Page

Setting the attributes on the **Configure Guest Claim Attributes** page determines the minimum claims attributes (and, therefore, permissions) available to a guest, or not signed-in, user.

To change this later, see [Configuring Guest Claim Attributes](#).

## System Configuration Settings

- System Settings: Set **hostname** and **ports** for this installation.
- Contact Info: Contact information for the point-of-contact or administrator for this installation.
- Certificates: Add PKI certificates for the Keystore and Truststore for this installation.
  - For a quick (test) installation, if the hostname/ports are not changed from the defaults, DDF includes self-signed certificates to use. Do not use in a working installation.
  - For more advanced testing, on initial startup of the **Admin Console** append the string **?dev=true** to the url (`https://{FQDN}:{PORT}/admin?dev=true`) to auto-generate self-signed certificates from a demo Certificate Authority(CA). This enables changing hostname and port settings during initial installation.
    - NOTE: **?dev=true** generates certificates on initial installation only. Do not use in a working installation.
  - For more information about importing certificate from a Certificate Authority, see [Managing Keystores and Certificates](#).

## Finished Page

Upon successful startup, the **Finish** page will redirect to the Admin Console to begin further configuration, ingest, or federation.

**NOTE** The redirect will only work if the certificates are configured in the browser. Otherwise the redirect link must be used.

### 2.3.3.2. Completing Installation from the Command Console

In order to install DDF from the Command Console, use the command **profile:install <profile-name>**. The **<profile-name>** should be the desired [Setup Type](#) in lowercase letters. To see the available profiles, use the command **profile:list**.

**NOTE** This only installs the desired Setup Type. There are other components that can be set up in the Admin Console Installer that cannot be setup on the Command Console. After installing the Setup Type, these other components can be set up as described below.

## Configure Guest Claim Attributes

The Guest Claim Attributes can be configured via the Admin Console after running the **profile:install** command. See [Configuring Guest Claim Attributes](#).



## System Configuration Settings

System Settings and Contact Info, as described in [System Configuration Settings](#), can be changed in `<DDF_HOME>/etc/custom.system.properties`. The certificates must be set up manually as described in [Managing Keystores and Certificates](#).

**NOTE** The system will need to be restarted after changing any of these settings.

### 2.3.3.3. Firewall Port Configuration

Below is a table listing all of the default ports that DDF uses and a description of what they are used for. Firewalls will need to be configured to open these ports in order for external systems to communicate with DDF.

*Table 4. Port List*

Port	Usage description
8993	https access to DDF admin and search web pages.
8101	For administering DDF instances gives ssh access to the administration console.
61616	DDF broker port for JMS messaging over the OpenWire protocol.
5672	DDF broker port for JMS messaging over multiple protocols: Artemis CORE, AMQP and OpenWire by default .
5671	DDF broker port for JMS messaging over: AMQP by default.
1099	RMI Registry Port
44444	RMI Server Port
8994	Solr Server Port. DDF does not listen on this port, but the Solr process does and it must be able to receive requests from DDF on this port.

**NOTE** These are the default ports used by DDF. DDF can be configured to use different ports.

### 2.3.3.4. Internet Explorer 11 Enhanced Security Configuration

Below are steps listing all of the changes that DDF requires to run on Internet Explorer 11 and several additional considerations to keep in mind.

1. In the IE11 **Settings > Compatibility View Settings** dialog, un-check **Display intranet sites in Compatibility View**.

2. In the **Settings > Internet Options > Security** tab, **Local intranet** zone:
  - a. Click the **Sites > Advanced** button, add the current host name to the list, e.g., <https://windows-host-name.domain.edu>, and close the dialog.
  - b. Make sure the security level for the **Local intranet** zone is set to **Medium-low** in **Custom level...**
    - i. **Enable Protected Mode** is checked by default, but it may need to be disabled if the above changes do not fully resolve access issues.
3. Restart the browser.

**NOTE**

During installation, make sure to use the host name and not localhost when setting up the DDF's hostname, port, etc.

## 2.4. High Availability Initial Setup

This section describes how to complete the initial setup of DDF in a [Highly Available Cluster](#).

### *Prerequisites*

- A failover proxy that can route HTTP traffic according to the pattern described in the Introduction to High Availability. It is recommended that a hardware failover proxy be used in a production environment.
- Solr Cloud: See the [Solr Cloud section](#) for installation and configuration guidance to connect DDF nodes to Solr Cloud.

Once the prerequisites have been met, the below steps can be followed.

**NOTE**

Unless listed in the [High Availability Initial Setup Exceptions](#) section, the normal steps can be followed for installing, configuring, and hardening.

1. Install the first DDF node. See the [Installation Section](#).
2. Configure the first DDF node. See the [Configuring Section](#).
3. Optional: If hardening the first DDF node (excluding setting directory permissions). See the [Hardening Section](#).
4. Export the first DDF node's configurations, install the second DDF node, and import the exported configurations on that node. See [Reusing Configurations](#).
5. If hardening, set directory permissions on both DDF nodes. See [Setting Directory Permissions](#).

### 2.4.1. High Availability Initial Setup Exceptions

These steps are handled differently for the initial setup of a Highly Available Cluster.

#### 2.4.1.1. Failover Proxy Integration

In order to integrate with a failover proxy, the DDF node's system properties (in `<DDF_HOME>/etc/custom.system.properties`) must be changed to publish the correct port to external systems and users. This must be done before installing the first DDF node. See [High Availability Initial Setup](#).

There are two internal port properties that must be changed to whatever ports the DDF will use on its system. Then there are two external port properties that must be changed to whatever ports the failover proxy is forwarding traffic through.

#### WARNING

Make sure that the failover proxy is already running and forwarding traffic on the chosen ports before starting the DDF. There may be unexpected behavior otherwise.

In the below example, the failover proxy with a hostname of `service.org` is forwarding https traffic via 8993 and http traffic via 8181. The DDF node will run on 1111 for https and 2222 for http (on the host that it's hosted on). The hostname of the DDF must match the hostname of the proxy.

```
org.codice.ddf.system.hostname=service.org
org.codice.ddf.system.httpsPort=1111
org.codice.ddf.system.httpPort=2222
org.codice.ddf.system.port=${org.codice.ddf.system.httpsPort}

org.codice.ddf.external.hostname=service.org
org.codice.ddf.external.httpsPort=8993
org.codice.ddf.external.httpPort=8181
org.codice.ddf.external.port=${org.codice.ddf.external.httpsPort}
```

#### 2.4.1.2. Identical Directory Structures

The two DDF nodes need to be under identical root directories on their corresponding systems. On Windows, this means they must be under the same drive.

#### 2.4.1.3. Highly Available Security Auditing

A third party tool will have to be used to persist the logs in a highly available manner.

- Edit the `<DDF_HOME>/etc/org.ops4j.pax.logging.cfg` file to enable log4j2, following the steps in [Enabling Fallback Audit Logging](#).
- Then put the appropriate log4j2 appender in `<DDF_HOME>/etc/log4j2.config.xml` to send logs to the chosen third party tool. See [Log4j Appenders](#) [↗](#).

#### 2.4.1.4. Shared Storage Provider

The storage provider must be in a location that is shared between the two DDF nodes and must be highly available. If hardening the Highly Available Cluster, this shared storage provider must be trusted/secured. One way to accomplish this is to use the default [Content File System Storage Provider](#) and configure it to point to a highly available shared directory.

#### 2.4.1.5. High Availability Certificates

Due to the nature of highly available environments, localhost is not suitable for use as a hostname to identify the DDF cluster. The default certificate that ships with the product uses localhost as the common name, so this certificate needs to be replaced. The following describes how to generate a certificate signed by the DDF Demo Certificate Authority that uses a proper hostname.

##### NOTE

This certificate, and any subsequent certificates signed by the Demo CA, are intended for testing purposes only, and should not be used in production.

Certificates need to have Subject Alternative Names (SANs) which will include the host for the failover proxy and for both DDF nodes. A certificate with SANs signed by the Demo CA can be obtained by navigating to `<DDF_HOME>/etc/certs/` and, assuming the proxy's hostname is `service.org`, running the following for UNIX operating systems:

```
./CertNew.sh -cn service.org -san "DNS:service.org"
```

or the following for Windows operating systems:

```
CertNew -cn service.org -san "DNS:service.org"
```

##### NOTE

Systems that use DDF version 2.11.4 or later will automatically get a DNS SAN entry matching the CN without the need to specify the `-san` argument to the `CertNew` command.

More customization for certs can be achieved by following the steps at [Creating New Server Keystore Entry with the CertNew Scripts](#).

#### 2.4.1.6. High Availability Installation Profile

Instead of having to manually turn features on and off, there is a High Availability installation profile. This profile will not show up in the UI Installer, but can be installed by executing `profile:install ha` on the command line **instead** of stepping through the UI Installer. This profile will install all of the High Availability supported features.

## 3. Configuring

DDF is highly configurable and many of the components of the system can be configured to use an included DDF implementation or replaced with an existing component of an integrating system.

### NOTE

#### *Configuration Requirements*

Because components can easily be installed and uninstalled, it's important to remember that for proper DDF functionality, at least the Catalog API, one Endpoint, and one Catalog Framework implementation must be active.

#### *Configuration Tools*

DDF provides several tools for configuring the system. The [Admin Console](#) is a useful interface for configuring applications, their features, and important settings. Alternatively, many configurations can be updated through [console commands](#) entered into the Command Console. Finally, configurations are stored in [configuration files](#) within the `<DDF_HOME>` directory.

#### *Configuration Outline*

While many configurations can be set or changed in any order, for ease of use of this documentation, similar subjects have been grouped together sequentially.

See [Keystores and certificates](#) to set up the certificates needed for messaging integrity and authentication. Set up [Users](#) with security attributes, then configure [data](#) attribute handling, and finally, define the [Security Policies](#) that map between users and data and make decisions about access.

Connecting DDF to other data sources, including other instances of DDF is covered in the [Configuring Federation](#) section.

Lastly, see the [Configuring for Special Deployments](#) section for guidance on common specialized installations, such as [fanout](#) or [multiple identical configurations](#).

### 3.1. Admin Console Tutorial

The Admin Console is the centralized location for administering the system. The Admin Console allows an administrator to configure and tailor system services and properties. The default address for the Admin Console is `https://{FQDN}:{PORT}/admin`.

#### *System Settings Tab*

The configuration and features installed can be viewed and edited from the **System** tab of the **Admin Console**.

#### *Managing Federation in the Admin Console*

It is recommended to use the **Catalog App** → **Sources** tab to configure and manage sites/sources.

#### *Viewing Currently Active Applications from Admin Console*

DDF displays all active applications in the Admin Console. This view can be configured according to preference. Either view has an > arrow icon to view more information about the application as currently configured.

Table 5. Admin Console Views

View	Description
Tile View	The first view presented is the Tile View, displaying all active applications as individual tiles.
List View	Optionally, active applications can be displayed in a list format by clicking the list view button.

#### Application Detailed View

Each individual application has a detailed view to modify configurations specific to that application. All applications have a standard set of tabs, although some apps may have additional ones with further information.

Table 6. Individual Application Views

Tab	Explanation
Configuration	The Configuration tab lists all bundles associated with the application as links to configure any configurable properties of that bundle.

#### Managing Features Using the Admin Console

DDF includes many components, packaged as *features*, that can be installed and/or uninstalled without restarting the system. Features are collections of OSGi bundles, configuration data, and/or other features.

NOTE	<i>Transitive Dependencies</i>
	Features may have dependencies on other features and will auto-install them as needed.

In the Admin Console, Features are found on the **Features** tab of the **System** tab.

1. Navigate to the **Admin Console**.
2. Select the **System** tab.
3. Select the **Features** tab.
4. Uninstalled features are shown with a **play** arrow under the **Actions** column.
  - a. Select the **play** arrow for the desired feature.
  - b. The **Status** will change from **Uninstalled** to **Installed**.
5. Installed features are shown with a **stop** icon under the **Actions** column.
  - a. Select the **stop** icon for the desired feature.

- b. The **Status** will change from **Installed** to **Uninstalled**.

## 3.2. Console Command Reference

DDF provides access to a powerful Command Console to use to manage and configure the system.

### 3.2.1. Feature Commands

Individual features can also be added via the Command Console.

1. Determine which feature to install by viewing the available features on DDF.

```
ddf@local>feature:list
```

2. The console outputs a list of all features available (installed and uninstalled). A snippet of the list output is shown below (the versions may differ):

State	Version	Name	Repository
Description			
[installed ]	[2.13.10 ]	security-handler-api	security-services-app-
2.13.10 API for authentication handlers for web applications.			
[installed ]	[2.13.10 ]	security-core	security-services-app-
2.13.10 DDF Security Core			
[uninstalled]	[2.13.10 ]	security-expansion	security-services-app-
2.13.10 DDF Security Expansion			
[uninstalled]	[2.13.10 ]	security-cas-client	security-services-app-
2.13.10 DDF Security CAS Client.			
[uninstalled]	[2.13.10 ]	security-cas-tokenvalidator	security-services-app-
2.13.10 DDF Security CAS Validator for the STS.			
[installed ]	[2.13.10 ]	security-pdp-authz	security-services-app-
2.13.10 DDF Security PDP.			
[uninstalled]	[2.13.10 ]	security-pep-serviceauthz	security-services-app-
2.13.10 DDF Security PEP Service AuthZ			
[uninstalled]	[2.13.10 ]	security-expansion-user-attributes	security-services-app-
2.13.10 DDF Security Expansion User Attributes Expansion			
[uninstalled]	[2.13.10 ]	security-expansion-metacard-attributes	security-services-app-
2.13.10 DDF Security Expansion Metacard Attributes Expansion			
[installed ]	[2.13.10 ]	security-sts-server	security-services-app-
2.13.10 DDF Security STS.			
[installed ]	[2.13.10 ]	security-sts-realm	security-services-app-
2.13.10 DDF Security STS Realm.			
[uninstalled]	[2.13.10 ]	security-sts-ldaplogin	security-services-app-
2.13.10 DDF Security STS JAAS LDAP Login.			
[uninstalled]	[2.13.10 ]	security-sts-ldapclaimshandler	security-services-app-
2.13.10 Retrieves claims attributes from an LDAP store.			

1. Check the bundle status to verify the service is started.

```
ddf@local>list
```

The console output should show an entry similar to the following:

```
[ 117] [Active      ] [          ] [Started] [ 75] DDF :: Catalog :: Source :: Dummy
(<version>)
```

### 3.2.1.1. Uninstalling Features from the Command Console

1. Check the feature list to verify the feature is installed properly.

```
ddf@local>feature:list
```

State	Version	Name	Repository
[installed ]	[2.13.10	] ddf-core	ddf-2.13.10
[uninstalled]	[2.13.10	] ddf-sts	ddf-2.13.10
[installed ]	[2.13.10	] ddf-security-common	ddf-2.13.10
[installed ]	[2.13.10	] ddf-resource-impl	ddf-2.13.10
[installed ]	[2.13.10	] ddf-source-dummy	ddf-2.13.10

1. Uninstall the feature.

```
ddf@local>feature:uninstall ddf-source-dummy
```

#### WARNING

Dependencies that were auto-installed by the feature are not automatically uninstalled.

1. Verify that the feature has uninstalled properly.

```
ddf@local>feature:list
```

State	Version	Name	Repository	Description
[installed ]	[2.13.10	] ddf-core	ddf-2.13.10	
[uninstalled]	[2.13.10	] ddf-sts	ddf-2.13.10	
[installed ]	[2.13.10	] ddf-security-common	ddf-2.13.10	
[installed ]	[2.13.10	] ddf-resource-impl	ddf-2.13.10	
[uninstalled]	[2.13.10	] ddf-source-dummy	ddf-2.13.10	

## 3.3. Configuration Files

Many important configuration settings are stored in the `<DDF_HOME>` directory.



**NOTE**

Depending on the environment, it may be easier for integrators and administrators to configure DDF using the Admin Console prior to disabling it for hardening purposes. The Admin Console can be re-enabled for additional configuration changes.

In an environment hardened for security purposes, access to the Admin Console or the Command Console might be denied and using the latter in such an environment may cause configuration errors. It is necessary to configure DDF (e.g., providers, Schematron rulesets, etc.) using `.config` files.

A template file is provided for some configurable DDF items so that they can be copied/renamed then modified with the appropriate settings.

**WARNING**

If the Admin Console is enabled again, all of the configuration done via `.config` files will be loaded and displayed. However, note that the name of the `.config` file is not used in the Admin Console. Rather, a universally unique identifier (UUID) is added when the DDF item was created and displays this UUID in the console (e.g., `OpenSearchSource.112f298e-26a5-4094-befc-79728f216b9b`)

### 3.3.1. Configuring Global Settings with `custom.system.properties`

Global configuration settings are configured via the properties file `custom.system.properties`. These properties can be manually set by editing this file or set via the initial configuration from the Admin Console.

**NOTE**

Any changes made to this file require a restart of the system to take effect.

**IMPORTANT**

The passwords configured in this section reflect the passwords used to decrypt JKS (Java KeyStore) files. Changing these values without also changing the passwords of the JKS causes undesirable behavior.

Table 7. Global Settings

Title	Property	Type	Description	Default Value	Required
<b>Keystore and Truststore Java Properties</b>					
Keystore	<code>javax.net.ssl.keyStore</code>	String	Path to server keystore	<code>etc/keystores/serverKeystore.jks</code>	Yes
Keystore Password	<code>javax.net.ssl.keyStorePassword</code>	String	Password for accessing keystore	<code>changeit</code>	Yes
Truststore	<code>javax.net.ssl.trustStore</code>	String	The trust store used for SSL/TLS connections. Path is relative to <code>&lt;DDF_HOME&gt;</code> .	<code>etc/keystores/serverTruststore.jks</code>	Yes

Title	Property	Type	Description	Default Value	Required
Truststore Password	<code>javax.net.ssl.trustStorePassword</code>	String	Password for server Truststore	<code>changeit</code>	Yes
Keystore Type	<code>javax.net.ssl.keyStoreType</code>	String	File extension to use with server keystore	<code>jks</code>	Yes
Truststore Type	<code>javax.net.ssl.trustStoreType</code>	String	File extension to use with server truststore	<code>jks</code>	Yes
<b>Headless mode</b>					
Headless Mode	<code>java.awt.headless</code>	Boolean	Force java to run in headless mode for when the server doesn't have a display device	<code>true</code>	No
<b>Global URL Properties</b>					
Internal Default Protocol	<code>org.codice.ddf.system.protocol</code>	String	Default protocol that should be used to connect to this machine.	<code>https://</code>	Yes
Internal Host	<code>org.codice.ddf.internal.hostname</code>	String	<p>The hostname or IP address this system runs on.</p> <p>If the hostname is changed during the install to something other than <code>localhost</code> a new keystore and truststore must be provided. See <a href="#">Managing Keystores and Certificates</a> for details.</p>	<code>localhost</code>	Yes
Internal HTTPS Port	<code>org.codice.ddf.system.httpsPort</code>	String	<p>The https port that the system uses.</p> <p>NOTE: This <b>DOES</b> change the port the system runs on.</p>	<code>8993</code>	Yes

Title	Property	Type	Description	Default Value	Required
Internal HTTP Port	<code>org.codice.ddf.system.HttpPort</code>	String	<p>The http port that the system uses.</p> <p>NOTE: This <b>DOES</b> change the port the system runs on.</p>	8181	Yes
Internal Default Port	<code>org.codice.ddf.system.port</code>	String	<p>The default port that the system uses. This should match either the above http or https port.</p> <p>NOTE: This <b>DOES</b> change the port the system runs on.</p>	8993	Yes
Internal Root Context	<code>org.codice.ddf.system.rootContext</code>	String	The base or root context that services will be made available under.	/services	Yes
External Default Protocol	<code>org.codice.ddf.external.protocol</code>	String	Default protocol that should be used to connect to this machine.	https://	Yes

Title	Property	Type	Description	Default Value	Required
External Host	<code>org.codice.ddf.external.hostname</code>	String	<p>The hostname or IP address used to advertise the system. Do not enter <code>localhost</code>. Possibilities include the address of a single node or that of a load balancer in a multi-node deployment.</p> <p>If the hostname is changed during the install to something other than <code>localhost</code> a new keystore and truststore must be provided. See <a href="#">Managing Keystores and Certificates</a> for details.</p> <p>NOTE: Does not change the address the system runs on.</p>	<code>localhost</code>	Yes
HTTPS Port	<code>org.codice.ddf.external.httpsPort</code>	String	<p>The https port used to advertise the system.</p> <p>NOTE: This does not change the port the system runs on.</p>	<code>8993</code>	Yes
External HTTP Port	<code>org.codice.ddf.external.httpPort</code>	String	<p>The http port used to advertise the system.</p> <p>NOTE: This does not change the port the system runs on.</p>	<code>8181</code>	Yes

Title	Property	Type	Description	Default Value	Required
External Default Port	<code>org.codice.ddf.external.port</code>	String	The default port used to advertise the system. This should match either the above http or https port.  NOTE: Does not change the port the system runs on.	8993	Yes
External Root Context	<code>org.codice.ddf.external.context</code>	String	The base or root context that services will be advertised under.	/services	Yes
<b>System Information Properties</b>					
Site Name	<code>org.codice.ddf.system.siteName</code>	String	The site name for DDF.	ddf.distribution	Yes
Site Contact	<code>org.codice.ddf.system.siteContact</code>	String	The email address of the site contact.		No
Version	<code>org.codice.ddf.system.version</code>	String	The version of DDF that is running.  This value should not be changed from the factory default.	2.13.10	Yes
Organization	<code>org.codice.ddf.system.organization</code>	String	The organization responsible for this installation of DDF.	Codice Foundation	Yes
Registry ID	<code>org.codice.ddf.system.registry-id</code>	String	The registry id for this installation of DDF.		No
<b>Thread Pool Settings</b>					
Thread Pool Size	<code>org.codice.ddf.system.threadPoolSize</code>	Integer	Size of thread pool used for handling UI queries, federating requests, and downloading resources. See <a href="#">Configuring Thread Pools</a>	128	Yes
<b>HTTPS Specific Settings</b>					

Title	Property	Type	Description	Default Value	Required
Cipher Suites	<code>https.cipherSuites</code>	String	Cipher suites to use with secure sockets. If using the JCE unlimited strength policy, use this list in place of the defaults:  .	<code>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,</code> <code>TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,</code> <code>TLS_DHE_RSA_WITH_AES_128_CBC_SHA,</code> <code>TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,</code> <code>TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</code>	No
Https Protocols	<code>https.protocols</code>	String	Protocols to allow for secure connections	<code>TLSv1.1,TLSv1.2</code>	No
Allow Basic Auth Over Http	<code>org.codice.allowBasicAuthOverHttp</code>	Boolean	Set to true to allow Basic Auth credentials to be sent over HTTP unsecurely. This should only be done in a test environment. These events will be audited.	<code>false</code>	Yes
Restrict the Security Token Service to allow connections only from DNSs matching these patterns	<code>ws-security.subject.cert.constraints</code>	String	Set to a comma separated list of regex patterns to define which hosts are allowed to connect to the STS	<code>.*</code>	Yes
<b>XML Settings</b>					
Parse XML documents into DOM object trees	<code>javax.xml.parsers.DocumentBuilderFactory</code>	String	Enables Xerces-J implementation of <code>DocumentBuilderFactory</code>	<code>org.apache.xerces.jaxp.DocumentBuilderFactoryImpl</code>	Yes
<b>Catalog Source Retry Interval</b>					

Title	Property	Type	Description	Default Value	Required
Initial Endpoint Contact Interval	<code>org.codice.ddf.platform.util.http.initialRetryInterval</code>	Integer	If a Catalog Source is unavailable, try to connect to it after the initial interval has elapsed. After every retry, the interval doubles, up to a given maximum interval. The interval is measured in seconds.	10	Yes
Maximum Endpoint Contact Interval	Maximum seconds between attempts to establish contact with unavailable Catalog Source.	Integer	Do not wait longer than the maximum interval to attempt to establish a connection with an unavailable Catalog Source. Smaller values result in more current information about the status of Catalog Sources, but cause more network traffic. The interval is measured in seconds.	300	Yes
File Upload Settings					

Title	Property	Type	Description	Default Value	Required
File extensions flagged as potentially dangerous to the host system or external clients	<code>bad.file.extensions</code>	String	Files uploaded with these bad file extensions will have their file names sanitized before being saved  E.g. sample_file.exe will be renamed to sample_file.bin upon ingest	<code>.exe, .jsp, .html, .js, .php, .phtml, .php3, .php4, .php5, .phps, .shtml, .jhtml, .pl, .py, .cgi, .msi, .com, .scr, .gadget, .application, .pif, .hta, .cpl, .msc, .jar, .kar, .bat, .cmd, .vb, .vbs, .vbe, .jse, .ws, .wsf, .wsc, .wsh, .ps1, .ps1xml, .ps2, .ps2xml, .psc1, .psc2, .msh, .msh1, .msh2, .mshxml, .msh1xml, .msh2xml, .scf, .lnk, .inf, .reg, .dll, .vxd, .cpl, .cfg, .config, .crt, .cert, .pem, .jks, .p12, .p7b, .key, .der, .csr, .jsb, .mhtml, .mht, .xhtml, .xht</code>	Yes
File names flagged as potentially dangerous to the host system or external clients	<code>bad.files</code>	String	Files uploaded with these bad file names will have their file names sanitized before being saved  E.g. crossdomain.xml will be renamed to file.bin upon ingest	<code>crossdomain.xml, clientaccesspolicy.xml, .htaccess, .htpasswd, hosts, passwd, group, resolv.conf, nfs.conf, ftpd.conf, ntp.conf, web.config, robots.txt</code>	Yes
Mime types flagged as potentially dangerous to external clients	<code>bad.mime.types</code>	String	Files uploaded with these mime types will be rejected from the upload	<code>text/html, text/javascript, text/x-javascript, application/x-shellscript, text/scriptlet, application/x-msdownload, application/x-msmetafile</code>	Yes
File names flagged as potentially dangerous to external clients	<code>ignore.files</code>	String	Files uploaded with these file names will be rejected from the upload	<code>.DS_Store, Thumbs.db</code>	Yes



Title	Property	Type	Description	Default Value	Required
<b>General Solr Catalog Properties</b>					
Solr Catalog Client	<code>solr.client</code>	String	Type of Solr configuration	<code>HttpSolrClient</code>	Yes
<b>Solr Cloud Properties</b>					
Zookeeper Nodes	<code>solr.cloud.zookeeper</code>	String	Zookeeper hostnames and port numbers	<code>zookeeperhost1:2181, zookeeperhost2:2181, zookeeperhost3:2181</code>	Yes
<b>Managed Solr Server Properties</b>					
Allow DDF to change the Solr server password if it detects the default password is in use	<code>solr.attemptAutoPasswordChange</code>	Boolean	If true, DDF attempts to change the default Solr server password to a randomly generated UUID. This property is only used if the <code>solr.client</code> property is <code>HttpSolrClient</code> and the <code>solrBasicAuth</code> property is <code>true</code> .	<code>true</code>	Yes
Solr Data Directory	<code>solr.data.dir</code>	String	Directory for Solr core files	<code>&lt;DDF_HOME&gt;/solr/server/solr</code>	Yes
Solr server HTTP port	<code>solr.http.port</code>	Integer	Solr server's port.	<code>8994</code>	Yes
Solr server URL	<code>solr.http.url</code>	String	URL for a HTTP Solr server (required for HTTP Solr)	-	Yes
Solr Heap Size	<code>solr.mem</code>	String	Memory allocated to the Solr Java process	<code>2g</code>	Yes
Encrypted Solr server password	<code>solr.password</code>	String	The password used for basic authentication to Solr. This property is only used if the <code>solr.client</code> property is <code>HttpSolrClient</code> and the <code>solrBasicAuth</code> property is <code>true</code> .	<code>admin</code>	Yes

Title	Property	Type	Description	Default Value	Required
Solr server username	<code>solr.username</code>	String	The username for basic authentication to Solr. This property is only used if the <code>solr.client</code> property is <code>HttpSolrClient</code> and the <code>solrBasicAuth</code> property is <code>true</code> .	<code>admin</code>	Yes
Use basic authentication for Solr server	<code>solr.useBasicAuth</code>	Boolean	If true, the HTTP Solr Client sends a username and password when sending requests to Solr server. This property is only used if the <code>solr.client</code> property is <code>HttpSolrClient</code> .	<code>true</code>	Yes
Start Solr server	<code>start.solr</code>	Boolean	If true, application manages Solr server lifecycle	<code>true</code>	Yes

These properties are available to be used as variable parameters in input url fields within the Admin Console. For example, the url for the local csw service (`https://{FQDN}:{PORT}/services/csw`) could be defined as:

```
${org.codice.ddf.system.protocol}${org.codice.ddf.system.hostname}:${org.codice.ddf.system.port}${org.codice.ddf.system.rootContext}/csw
```

This variable version is more verbose, but will not need to be changed if the system `host`, `port` or `root` context changes.

**WARNING** Only root can access ports < 1024 on Unix systems.

### 3.3.2. Configuring with .config Files

The DDF is configured using `.config` files. Like the Karaf `.cfg` files, these configuration files must be located in the `<DDF_HOME>/etc/` directory. Unlike the Karaf `.cfg` files, `.config` files must follow the naming convention that includes the *configuration persistence ID* (PID) that they represent. The filenames must be the pid with a `.config` extension. This type of configuration file also supports lists within configuration values (metatype `cardinality` attribute greater than 1) and String, Boolean,

Integer, Long, Float, and Double values.

#### IMPORTANT

This new configuration file format **must** be used for any configuration that makes use of lists. Examples include Web Context Policy Manager (`org.codice.ddf.security.policy.context.impl.PolicyManager.config`) and Security STS Guest Claims Handler (`ddf.security.sts.guestclaims.config`).

#### WARNING

Only one configuration file should exist for any given PID. The result of having both a `.cfg` and a `.config` file for the same PID is undefined and could cause the application to fail.

The main purpose of the configuration files is to allow administrators to pre-configure DDF without having to use the Admin Console. In order to do so, the configuration files need to be copied to the `<DDF_HOME>/etc` directory after DDF zip has been extracted.

Upon start up, all the `.config` files located in `<DDF_HOME>/etc` are automatically read and processed. DDF monitors the `<DDF_HOME>/etc` directory for any new `.config` file that gets added. As soon as a new file is detected, it is read and processed. Changes to these configurations from the Admin Console or otherwise are persisted in the original configuration file in the `<DDF_HOME>/etc` directory.

## 3.4. Configuring User Access

DDF does not define accounts or types of accounts to support access. DDF uses an *attribute based access control* (ABAC) model. For reference, ABAC systems control access by evaluating rules against the attributes of the entities (*subject* and *object*), actions, and the environment relevant to a request.

DDF can be configured to access many different types of user stores to manage and monitor user access.

### 3.4.1. Configuring Guest Access

Unauthenticated access to a secured DDF system is provided by the **Guest** user. By default, DDF allows guest access as part of the karaf security realm.

Because DDF does not know the identity of a Guest user, it cannot assign security attributes to the Guest. The administrator must configure the attributes and values (i.e. the "claims") to be assigned to Guests. The Guest Claims become the default minimum attributes for every user, both authenticated and unauthenticated. Even if a user claim is more restrictive, the guest claim will grant access, so ensure the guest claim is only as permissive as necessary.

The **Guest** user is uniquely identified with a Principal name of the format `Guest@UID`. The unique identifier is assigned to a Guest based on its source IP address and is cached so that subsequent Guest accesses from the same IP address within a 30-minute window will get the same unique identifier. To support administrators' need to track the source IP Address for a given Guest user, the IP Address and unique identifier mapping will be audited in the security log.

- Make sure that all the default logical names for locations of the security services are defined.

#### 3.4.1.1. Denying Guest User Access

To disable guest access for a context, use the [Web Context Policy Manager](#) configuration to remove **Guest** from the **Authentication Type** for that context. Only authorized users are then allowed to continue to the Search UI page.

##### NOTE

If using the included IdP for authentication, disable the **Allow Guest Access** option by [Configuring the IdP Server](#).

#### 3.4.1.2. Allowing Guest User Access

Guest authentication must be enabled and configured to allow guest users. Once the guest user is configured, redaction and filtering of metadata is done for the guest user the same way it is done for normal users.

To enable guest authentication for a context, use the [Web Context Policy Manager](#) configuration to change the **Authentication Type** for that context to **Guest**.

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Select the **Configuration** tab.
4. Select **Web Context Policy Manager**.
5. Select the desired context (`/`, `/search`, `/admin`, etc.).
6. Add **Guest** to the **Authentication Type** list.
  - a. Separate entries with a `|` symbol (eg. `/=SAML|Guest`).

##### 3.4.1.2.1. Configuring Guest Interceptor if Allowing Guest Users

- **Required Step for Security Hardening**

If a legacy client requires the use of the secured SOAP endpoints, the [guest interceptor](#) should be configured. Otherwise, the guest interceptor and **public** endpoints should be uninstalled for a hardened system.

##### 3.4.1.2.2. Configuring Guest Claim Attributes

A guest user's attributes define the most permissive set of claims for an unauthenticated user.

A guest user's claim attributes are stored in configuration, not in the LDAP as normal authenticated users' attributes are.

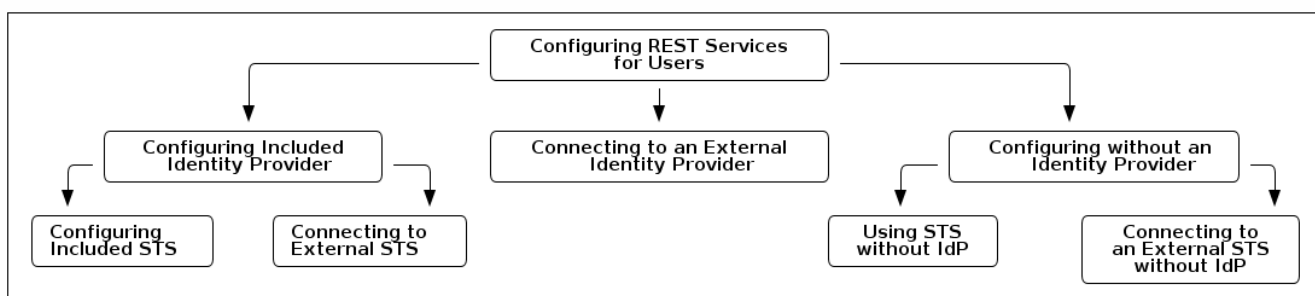
1. Navigate to the **Admin Console**.

2. Select the **Security** application.
3. Select the **Configuration** tab.
4. Select the **Security Guest Claims Handler**.
5. Add any additional attributes desired for the guest user.
6. Save changes.

### 3.4.2. Configuring REST Services for Users

If using REST services or connecting to REST sources, several configuration options are available.

DDF includes an [Identity Provider \(IdP\)](#), but can also be configured to support an [external IdP](#) or [no IdP](#) at all. The following diagram shows the configuration options.



#### *REST Services Configuration Options*

##### 3.4.2.1. Configuring Included Identity Provider

The included IdP is installed by default.

#### *Installing the IdP from the Admin Console*

1. Navigate to the **Admin Console**.
2. Select the **System** tab.
3. Select the **Features** tab.
4. Install **security-idp** feature.

#### *Installing the IdP from the Command Console*

Run the command **feature:install security-idp** from the Command Console.

#### *Configuring the IdP Server*

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Select the **Configuration** tab.
4. Select **IdP Server**.

## 5. Configure Authentication Request requirements

- Disable the **Require Signed AuthnRequests** option to allow processing of authentication requests without signatures.
- Disable the **Limit RelayStates to 80 Bytes** option to allow interoperability with Service Providers that are not compliant with the SAML Specifications and send RelayStates larger than 80 bytes.

## 6. Configure Guest Access:

- Disable the **Allow Guest Access** option to disallow a user to authenticate against the IdP with a guest account.

## 7. Configure the Service Providers (SP) Metadata:

- Select the **+** next to **SP Metadata** to add a new entry.
- Populate the new entry with:
  - an HTTPS URL (<https://>) such as <https://localhost:8993/services/saml/sso/metadata1>,
  - a file URL (file:), or
  - an XML block to refer to desired metadata.

### Service Provider Metadata Example

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID=
"https://localhost:8993/services/saml">
  <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>

MIIDEzCCAnygAwIBAgIJAIzc4FYrIp9mMA0GCSqGSIb3DQEBBQUAMHcx CzAJBgNVBAYTA1VTMQswCQYDVQQIDAjBw
jEMMAoGA1UECgwDRERGMQwwCgYDVQQLDANEZXYxGTAXBgNVBAMMEERERiBEZW1vIFJvb3QgQ0ExJDAiBgkqhkiG9w
0BCQEFWFRkZnJvb3RjYUBleGFtcGx1Lm9yZzAeFw0xNDEyMTAyMTU4MTAhaFw0xNTEyMTAyMTU4MTAhaMIGDMQswCQY
DVQQGEwJVUzELMAKGA1UECAwCQVoxETAPBgNVBACMCEDvb2R5ZWYyMQwwCgYDVQQKDANEREYxDDAKBgNVBAsMA0RL
djESMBAGA1UEAwwJbG9jYXVxb3N0MSQwIgyYJKoZIhvcNAQkBFhVsb2NhbgGhvc3RAZXhhbXBsZS5vcmcwZ8wDQYJK
oZIhvcNAQEBBQADgY0AMIGJAoGBAMECyNZbCTZphHQfB5g8FrgBq1RYzV7ikVw/pVGkz8gx3l3A99s8WtA4mRAeb6
n0vTR9yNB0ekW4nY0iEQq//YTi/frI1kz0QbEH1s2cI5nFButabD3PYGxUSuapbc+AS7+Pk1r0TDI4MRzPPkkTp4w
1ORQ/a6CfVsNr/mVg12CfAgMBAAAgZkgwZYwCQYDVROTBAlwADANBg1ghkgBhvhCAQ0EGhYYRk9SIFRFU1RJTkcg
UFVSUE9TRSBPTkxZMB0GA1UdDgQWBBSA95QIMyBAHRsd0R4s7C3BreFrSDAfBgNVHSMEGDAWgBThVMeX3wrCv6lfe
F47CyykSB9xjAgBgNVHREEGTAXgRVsb2NhbgGhvc3RAZXhhbXBsZS5vcmcwDQYJKoZIhvcNAQEFBQADgYEAtRUp7f
AxU/E6JD2Kj/+CTWqu8Elx13S0TxoIqv3gMoBW0ehyzEKjJi0bb1gUx07n1SmOESp5sE3jGTnh0GtYV0D219z/09n
90cd/imAEhknJllyyd0Sjpnal9JUd8uYxJexy8TJ2sMhsGAZ6EMTZCfT9m07XduxjsmDz0h1SGV0=

          </ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
```

```

<ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:X509Data>
    <ds:X509Certificate>

MIIDEzCCAnygAwIBAgIJAIzc4FYrIp9mMA0GCSqGSIb3DQEBBQUAMHcx CzAJBgNVBAYTA1VTMQswCQYDVQQIDAJBW
jEMMAoGA1UECgwDRERGMQwwCgYDVQQLDANEZXYxGTAXBgNVBAMMEERERiBEZW1vIFJvb3QgQ0ExJDAiBgkqhkiG9w
0BCQEFWRkZnJvb3RjYUBleGFtcGx1Lm9yZzAeFw0xNDEyMTAyMTU4MThaFw0xNTEyMTAyMTU4MThaMIGDMQswCQY
DVQQGEwJVUzELMAKGA1UECAwCQVoxETAPBgNVBACMCEdvb2R5ZWYyMQwwCgYDVQQKDANEREYxDDAKBgNVBASMA0RL
djESMBAGA1UEAwwJbG9jYWxob3N0MSQwIgYJKoZIhvcNAQkBFhVsb2NhbGhvc3RAZXhhbXBsZS5vcmcwgZ8wDQYJK
oZIhvcNAQEBBQADgY0AMIGJAoGBAMECyNZbCTZphHQfB5g8FrgBq1RYzV7ikVw/pVGkz8gx3L3A99s8WtA4mRAeb6
n0vTR9yNBOekW4nYOiEOq//YTi/frI1kz0QbEH1s2cI5nFButabD3PYGxUSuapbc+AS7+PkLr0TDI4MRzPPkTp4w
LORQ/a6CfVsNr/mVgL2CfAgMBAAAgjgZkwgZYwCQYDVROTBAlwADANBgIghkgBhvCAQ0EGhYYRk9SIFRFU1RJTkcq
UFVSUE9TRSBPTkxZMB0GA1UdDgQWBBSA95QIMyBAHRsd0R4s7C3BreFrSdAfBgNVHSMEGDAWgBThVMeX3wrCv6lfe
F47CvksBe9xjAgBgNVHREEGTAXgRVsb2NhbGhvc3RAZXhhbXBsZS5vcmcwDQYJKoZIhvcNAQEFBQADgYEAtRUp7f
AxU/E6JD2Kj/+CTWqu8Elx13S0TxoIqv3gMoBw0ehyzEKjJi0bb1gUx07n1Sm0ESp5sE3jGTnh0GtYV0D219z/09n
90cd/imAEhknJlarryd0Sjpnal9JUd8uYxJexy8TJ2sMhsGAZ6EMTZCft9m07XduxjsmDz0hlSGV0=

    </ds:X509Certificate>
  </ds:X509Data>
</ds:KeyInfo>
</md:KeyDescriptor>
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://localhost:8993/logout"/>
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://localhost:8993/logout"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
Redirect" Location="https://localhost:8993/services/saml/sso"/>
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://localhost:8993/services/saml/sso"/>
</md:SPSSODescriptor>
</md:EntityDescriptor>

```

### Configuring IdP as the Authentication Type

To use the IdP for authentication,

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Select the **Configuration** tab.
4. Select **Web Context Policy Manager**.
5. Under **Authentication Types**, set the IdP authentication type to context paths as necessary. Note that it should only be used on context paths that will be accessed by users via web browsers. For example:

- `/search=IdP`

Other authentication types can also be used in conjunction with the IdP type. For example, if you wanted to secure the entire system with the IdP, but still allow legacy clients that don't understand the



SAML ECP specification to connect, you could set `/=IdP|PKI`. With that configuration, any clients that failed to connect using either the SAML 2.0 Web SSO Profile or the SAML ECP specification would fall back to 2-way TLS for authentication.

#### NOTE

If you have configured `/search` to use IdP, ensure to select the "External Authentication" checkbox in Search UI standard settings.

#### Configuring the SP

To configure the IdP client (also known as the SP) that interacts with the specified IdP,

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Select the **Configuration** tab.
4. Select **IdP Client**.
5. Populate **IdP Metadata** field through one of the following:
  - a. an HTTPS URL (<https://>) e.g., <https://localhost:8993/services/idp/login/metadata>,
  - b. a file URL (file:), or
  - c. an XML block to refer to desired metadata.

#### IdP Client (SP) example.xml

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" entityID=
"https://localhost:8993/services/idp/login">
  <md:IDPSSODescriptor WantAuthnRequestsSigned="true" protocolSupportEnumeration=
"urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>
```

```
MIIDEzCCAnygAwIBAgIJAIzc4FYrIp9mMA0GCSqGSIb3DQEBBQUAMHcxCzAJBgNVBAYTA1VTMQswCQYDVQQIDAJB
wIEMMAoGA1UECgwDRERGMQwwCgYDVQQQLDANEZXYxGTAXBgNVBAMMEERERiBEZW1vIFJvb3QgQ0ExJDAiBgkqhkiG9w
0BCQEWFRkZnJvb3RjYUBleGFtcGxlLm9yZzAeFw0xNDEyMTAyMTU4MThaFw0xNTEyMTAyMTU4MThaMIGDMQswCQY
DVQQGEwJVUzELMAkGA1UECAwCQVoxETAPBgNVBACMCEdvb2R5ZWYyMQwwCgYDVQQKDANEREYxDDAKBgNVBAsMA0Rl
djESMBAGA1UEAwwJBG9jYXVob3N0MSQwIgYJKoZIhvcNAQkBFhVsb2NhbGhvc3RAZXhhbXBsZS5vcmcwZ8wDQYJK
oZIhvcNAQEBBQADgY0AMIGJAoGBAMECyNZbCTZphHQB5g8FrGq1RYzV7ikVw/pVGkz8gx3L3A99s8WtA4mRAeb6
n0vTR9yNB0ekW4nY0iE0q//YTi/frI1kz0QbEH1s2cI5nFButabD3PYGxUSuapbc+AS7+PkLr0TDI4MRzPPkkTp4w
LORQ/a6CfVsNr/mVgL2CfAgMBAAGjgZkwgZYwCQYDVVR0TBAIwADANBgUgBgUgBgUgBgUgBgUgBgUgBgUgBgUgBgUg
UFVSUE9TRSBPTkxZMB0GA1UdDgQWBBSA95QIMyBAHRsd0R4s7C3BreFrSDAfBgNVHSMEGDAWgBThVMeX3wrCv6lfe
F47CyykSB69xjAgBgNVHREEGTAGRVSb2NhbGhvc3RAZXhhbXBsZS5vcmcwDQYJKoZIhvcNAQEFBQADgYEAtRUp7f
AxU/E6JD2Kj/+CTWqu8Elx13S0TxoIqv3gMoBW0ehyzEKjJi0bb1gUx07n1SmOESp5sE3jGTnh0GtYV0D219z/09n
90cd/imAEhknJlAYyD0Sjpnal9JUd8uYxJexy8TJ2sMhsGAZ6EMTZCft9m07XduxjsmDz0hlSGV0=
      </ds:X509Certificate>
    </ds:X509Data>
```



```

    </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:KeyDescriptor use="encryption">
    <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
      <ds:X509Data>
        <ds:X509Certificate>

MIIDEzCCAnygAwIBAgIJAIzc4FYrIp9mMA0GCSqGSIb3DQEBBQUAMHcxCzAJBgNVBAYTA1VMTQswCQYDVQQIDAJBW
jEMMAoGA1UECgwDRERGMQwwCgYDVQQQLDANEZXYxGTAXBgNVBAMMEERERiBEZW1vIFJvb3QgQ0ExJDAiBgkqhkiG9w
0BCQEFWRkZnJvb3RjYUBleGFtcGxlM9yZzAeFw0xNDEyMTAyMTU4MTAhaFw0xNTEyMTAyMTU4MTAhaMIGDMQswCQY
DVQQGEwJVUzELMAkGA1UECAwCQVoxETAPBgNVBACMCEdvb2R5ZWYyMQwwCgYDVQQKDANEREYxDDAKBgNVBAsMA0Rl
djESMBAGA1UEAwwJbG9jYXxob3N0MSQwIgYJKoZIhvcNAQkBFhVs2NhbGhvc3RAZXhhbXBsZS5vcmcwZ8wDQYJK
oZIhvcNAQEBBQADgY0AMIGJAoGBAMECyNZbCTZphHQfB5g8FrgBq1RYzV7ikVw/pVGkz8gx3l3A99s8WtA4mRAeb6
n0vTR9yNB0ekW4nY0iEOq//YTt/frI1kz0QbEH1s2cI5nFButabD3PYGxUSuapbc+AS7+PkLr0TDI4MRzPPkkTp4w
LORQ/a6CfVsNr/mVgL2CfAgMBAAAgjgZkwgZYwCQYDVR0TBAlwADANBgIghkgBhvhCAQ0EGhYYRk9SIFRFU1RJTkcg
UFVSUE9TRSBPTkxZMB0GA1UdDgQWBBSA95QIMyBAHRsd0R4s7C3BreFrSDAfBgNVHSMEGDAWGBThVMeX3wrCv6lfe
F47CyvkSB69xjAgBgNVHREEGTAgRVsb2NhbGhvc3RAZXhhbXBsZS5vcmcwDQYJKoZIhvcNAQEFBQADgYEAtRUp7f
AxU/E6JD2Kj/+CTWqu8Elx13S0TxoIqv3gMoBW0ehyzEKjJi0bb1gUx07n1SmOESp5sE3jGTnh0GtYV0D219z/09n
90cd/imAEhknJlayyd0Sjpnal9JUd8uYxJexy8TJ2sMhsGAZ6EMTZCfT9m07XduxjsmDz0hlSGV0=

        </ds:X509Certificate>
      </ds:X509Data>
    </ds:KeyInfo>
  </md:KeyDescriptor>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://localhost:8993/logout"/>
  <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://localhost:8993/logout"/>
  <md:NameIDFormat>
    urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
  </md:NameIDFormat>
  <md:NameIDFormat>
    urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
  </md:NameIDFormat>
  <md:NameIDFormat>
    urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName
  </md:NameIDFormat>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://localhost:8993/services/idp/login"/>
  <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://localhost:8993/services/idp/login"/>
</md:IDPSSODescriptor>
</md:EntityDescriptor>

```

When using the included IdP, DDF can be configured to use the [included Security Token Service\(STS\)](#) or an [external STS](#).

#### 3.4.2.1.1. Configuring Included STS

An LDAP server can be used to maintain a list of DDF users and the attributes associated with them. The [Security Token Service \(STS\)](#) can use an LDAP server as an attribute store and convert those attributes to SAML claims.

DDF includes a demo [LDAP server](#), but an external LDAP is required for actual installation.

The STS is installed by default in DDF.

##### *Configuring STS*

1. Verify that the `serverKeystores.jks` file in `<DDF_HOME>/etc/keystores` trusts the hostnames used in your environment (the hostnames of LDAP, and any DDF users that make use of this STS server).
2. Navigate to the **Admin Console**.
3. Select the **System** tab.
4. Select the **Features** tab.
5. Start the `security-sts-ldaplogin` and `security-sts-ldapclaimshandler` features.
6. Select the **Configuration** tab.
7. Select the **Security STS LDAP Login** configuration.
8. Verify that the **LDAP URL**, **LDAP Bind User DN**, and **LDAP Bind User Password** fields match your LDAP server's information.
  - a. The default DDF LDAP settings will match up with the default settings of the OpenDJ embedded LDAP server. Change these values to map to the location and settings of the LDAP server being used.
9. Select the **Save changes** button if changes were made.
10. Open the **Security STS LDAP and Roles Claims Handler** configuration.
11. Populate the same URL, user, and password fields with your LDAP server information.
12. Select the **Save Changes** button.

##### *Configuring DDF Authentication Scheme*

Configure the DDF to use this authentication scheme.

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Open the **Web Context Policy Manager** configuration.
  - a. Under **Context Realms** add the contexts that should be protected under the ldap realm.
    - i. The default setting is `/=karaf`, the `karaf` realm refers to the `users.properties` user store file located in the `<DDF_HOME>/etc` directory. This can be changed to `/=ldap`, if it is desired that the entire container be protected under ldap. If the `/admin` context is changed to something other than the default (`karaf`), it will be required that you refresh the page in order to log in

again, or your changes may not be saved. This includes changing the root context to something other than **karaf**, without specifically setting **/admin** to a realm. The policies for all contexts will roll up, for example: the **/admin** context policy will roll up to the **karaf** realm with the default configuration because **/** is higher in the context heirarchy than **/admin** and no realm is specifically set for **/admin**.

- b. Under **Authentication Types**, make any desired authentication changes to contexts.
  - i. In order to use the SAML 2.0 Web SSO profile against a context, you must specify only the IdP authentication type.

#### *Security STS Client*

Configure the client connecting to the STS.

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Open the **Security STS Client** configuration.
4. Verify that the host/port information in the **STS Address** field points to your STS server. If you are using the default bundled STS, this information will already be correct.

See [Security STS Client](#) table for all configuration options.

The DDF should now use the SSO/STS/LDAP servers when it attempts to authenticate a user upon an attempted log in.

#### *STS Server*

Connect to the server hosting the STS.

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Select the **Security STS Server** configuration.
4. Verify the hostname and usernames are correct.

See [Security STS Server](#) table for all configuration options.

#### *SAML Name ID*

Set up alternatives to displaying the username of the logged in user.

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Select the **SAML NameID Policy** configuration.
4. Add any desired attributes to display instead of the username. (The first matching attribute will be used.)

### *Limiting Access to the STS*

Be sure to limit the hosts that are allowed to connect to the STS:

- **Required Step for Security Hardening**
  - Open the `<DDF_HOME>/etc/custom.system.properties` file.
  - Edit the line `ws-security.subject.cert.constraints = .*CN=<MY_HOST_CN>.*`.
    - By default this will only allow your hostname. To allow other desired hosts add their CNs to the regular expression within parentheses delimited by |:
      - `ws-security.subject.cert.constraints = .*CN=(<MY_HOST_CN>|<OTHER_HOST_CN>|<ANOTHER_HOST_CN>).*`
- 

#### **3.4.2.1.2. Connecting to External STS**

Configure DDF to connect to an external WSS STS.

##### *Security STS Address Provider*

Configure the STS address provider to use WSS.

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Select **Configuration**.
4. Select the **Security STS Address Provider**.
5. Enable the option **Use WSS STS**.

##### *Security STS WSS*

Configure the location and credentials for the STS.

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Select **Configuration**.
4. Select the **Security STS WSS** configuration.
5. Update the **Address**, **Endpoint Name**, and **Service Name** properties.

##### *Disable Security STS Client Configuration*

Disable the client configuration for the Security STS

1. Navigate to the **Admin Console**.
  2. Select the **System** tab.
  3. Select the **Features** tab.
-


4. Uninstall the **Security STS Client** feature.
- 

### 3.4.2.2. Connecting to an External Identity Provider

To connect to an external Identity Provider,

1. Provide the external IdP with DDF's Service Provider (SP) metadata. The SP metadata can be found at <https://<FQDN>:<PORT>/services/saml/sso/metadata>.
2. Replace the IdP metadata field in DDF.
  - a. Navigate to the **Admin Console**.
  - b. Select the **Security** application.
  - c. Select the **Configuration** tab.
  - d. Select **IdP Client**.
  - e. Populate the **IdP Metadata** field with the external IdP's metadata.

#### NOTE

DDF may not interoperate successfully with all IdPs. To identify the ones it can interoperate with, use the [The Security Assertion Markup Language \(SAML\) Conformance Test Kit \(CTK\)](#) 

#### *Service Provider Metadata*

It is not recommended to remove or replace the included Service Provider. To add an additional, external Service Provider, add the SP metadata to the **IdP Server** configuration. See [Configuring Security IdP Service Provider](#) for more detail.

---

### 3.4.2.3. Configuring Without an Identity Provider

To configure DDF to not use an Identity Provider (IdP),

1. Disable the IdP feature.
  - a. Navigate to the **Admin Console**.
  - b. Select the **System** tab.
  - c. Select the **Features** tab.
  - d. Uninstall the **security-idp** feature.
2. Change the Authentication Type if it is IdP.
  - a. Navigate to the **Admin Console**.
  - b. Select the **Security** application.
  - c. Select the **Configuration** tab.

d. Select **Web Context Policy Manager**

e. Under **Authentication Types**, remove the IdP authentication type from all context paths.

---

#### 3.4.2.3.1. Using STS without IdP

To configure DDF to use the included Security Token Service (STS) without an IdP, follow the same [Configuring STS](#) steps, with one additional configuration to make via the [Web Context Policy Manager](#).

*Configuring Authentication Types for STS*

1. Navigate to the **Admin Console**.
  2. Select the **Security** application.
  3. Select **Configuration**.
  4. Select the **Web Context Policy Manager**.
  5. Add any needed authentication types to the Authentication Types list, such as **PKI**, **Basic**, etc.
- 

#### 3.4.2.3.2. Connecting to External STS Without IdP

The process for [connecting to an external STS](#) is the same with or without an IdP.

---

### 3.4.3. Configuring SOAP Services for Users

If using SOAP services, DDF can be configured to use the included [Security Token Service \(STS\)](#), or [connected to an external STS](#).

#### 3.4.3.1. Connecting to Included STS with SOAP

DDF includes a STS implementation that can be used for user authentication over SOAP services.

*Configure the STS WSS*

Configure the STS WSS.

1. Navigate to the **Admin Console**.
  2. Select the **Security** application.
  3. Select **Configuration**.
  4. Select **Security STS WSS**.
  5. Update the **Claims** that should be requested by the STS.
-

### 3.4.3.2. Connecting to External STS with SOAP

See [connecting to an external STS](#) for initial STS setup.

### 3.4.4. Connecting to an LDAP Server

**WARNING**

The configurations for Security STS LDAP and Roles Claims Handler and Security STS LDAP Login contain plain text default passwords for the embedded LDAP, which is insecure to use in production.

Use the [Encryption Service](#), from the Command Console to set passwords for your LDAP server. Then change the LDAP Bind User Password in the [Security STS LDAP and Roles Claims Handler](#) configurations to use the encrypted password.

A claim is an additional piece of data about a principal that can be included in a token along with basic token data. A claims manager provides hooks for a developer to plug in claims handlers to ensure that the STS includes the specified claims in the issued token.

Claims handlers convert incoming user credentials into a set of attribute claims that will be populated in the SAML assertion. For example, the `LDAPClaimsHandler` takes in the user’s credentials and retrieves the user’s attributes from a backend LDAP server. These attributes are then mapped and added to the SAML assertion being created. Integrators and developers can add more claims handlers that can handle other types of external services that store user attributes.

See the [Security STS LDAP and Roles Claims Handler](#) for all possible configurations.

### 3.4.5. Configuring SSO Using a CAS Server

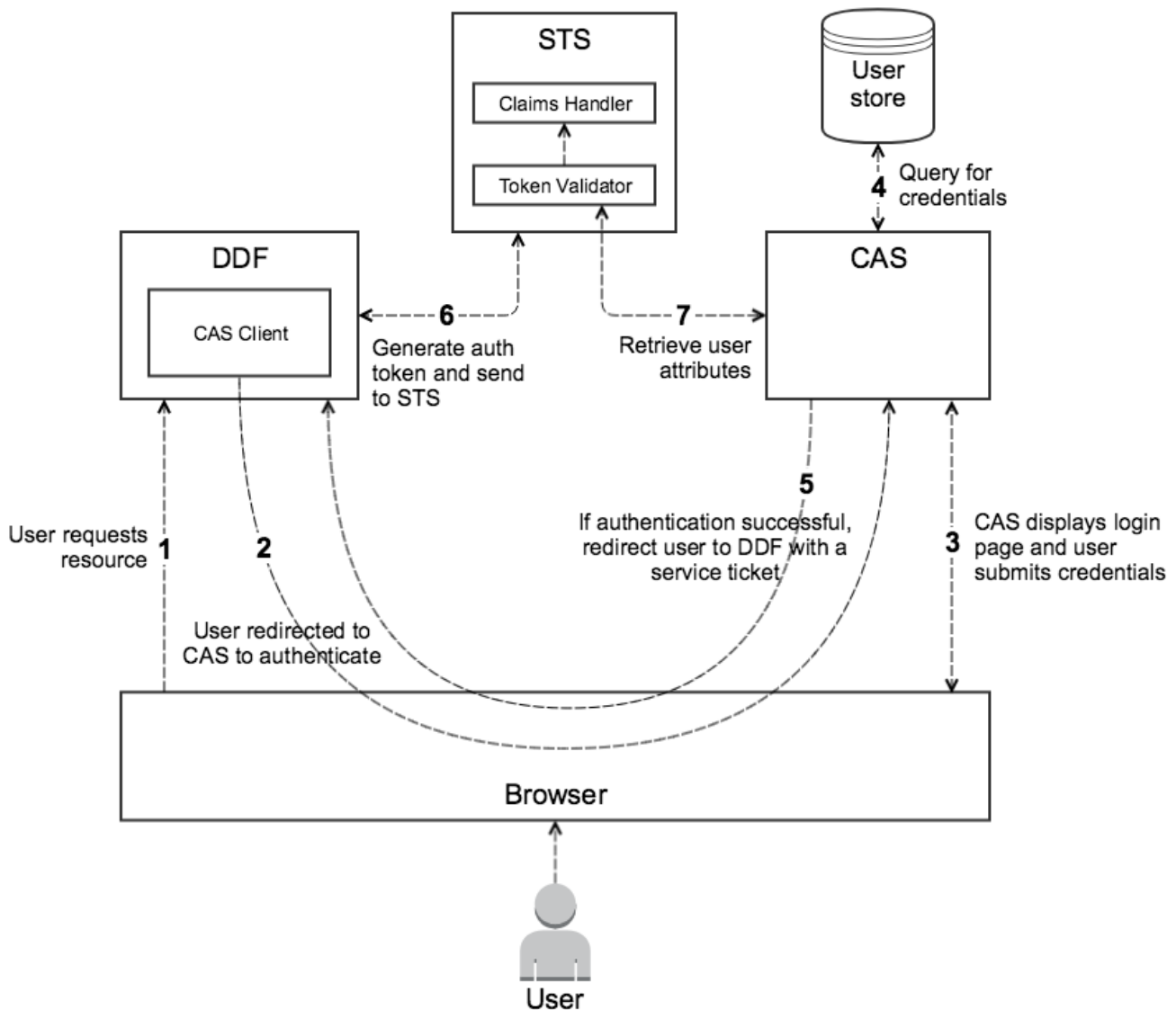
DDF contains a set of features which allow it to use CAS as its Single Sign-On (SSO) service. It communicates with a CAS server over the CAS Protocol v2 (see <https://apereo.github.io/cas/5.2.x/protocol/CAS-Protocol-V2-Specification.html>), and has been tested to work with version 3.6.0 of the CAS server. However, it should integrate with any 3.x server. The components which provide this support are listed below.

Table 8. Security CAS features

Feature Name	Description
<code>security-cas-client</code>	When a user makes a request to a context configured for CAS authentication, it is received by the CAS client. The client redirects unauthenticated users to CAS, and validates their service tickets after they authenticate.
<code>security-cas-tokenvalidator</code>	Once a user authenticates, DDF creates a CAS auth token which gets passed to the STS. This token contains a CAS proxy ticket which the STS can use to retrieve user attributes from the CAS server. The STS uses the CAS token validator to process these auth tokens and create a SAML assertion.

Feature Name	Description
security-sts-casclaimshandler	The CAS claims handler performs final processing on the user attributes returned by CAS. It takes a list of attributes and maps them to claims that DDF can use according to a user-defined mapping.

The diagram below gives an overview of the process of logging in for an unauthenticated user, showing where each of the features are used.



1. An unauthenticated user submits a request to a context in DDF which is configured to use CAS authentication.
2. The CAS client receives the request. It sees the user is unauthenticated and has no service ticket, and so redirects the user to CAS.
3. CAS displays the login page and the user submits their credentials.



4. CAS queries the user store for the given credentials. If the user does not exist, CAS will indicate that the credentials are invalid. Otherwise, the process will continue. Note that CAS supports many user management solutions, e.g. LDAP, Active Directory, X.509 certificates, etc.
5. CAS redirects the user back to DDF with a service ticket.
6. Again, the CAS client receives the request, but this time it finds the service ticket. The client sends a request to CAS to validate the ticket and also generate a proxy ticket. This proxy ticket allows a designated service (in this case the STS) to request user info from CAS. The client creates a CAS auth token containing the proxy ticket and sends it to the STS. Note: the ticket validation request is not shown.
7. The STS first passes the auth token to the CAS token validator. The validator extracts the proxy ticket and retrieves any user attributes that CAS is configured to release. The claims handler then maps these to standard DDF claims, and the STS returns an assertion containing these processed claims.
8. DDF then decides whether to display the requested resource.

#### 3.4.5.1. CAS Integration Using Standalone Servers

Integrating DDF with a local CAS server is as simple as installing and configuring the provided CAS features. However, things become a bit more complicated when the required components are installed on separate servers. This section provides step-by-step instructions for configuring each component in such a distributed setup. In particular, it will use LDAP as the user management solution.

##### TIP

It is important to keep track of the DNS hostnames used on each server for certificate authentication purposes.

It is possible to configure the STS to query LDAP directly to retrieve user attributes. However, it is recommended that the STS retrieve attributes through CAS instead. This simplifies integration, as only CAS must be able to query LDAP. It also allows CAS to use any user management solution without affecting DDF.

##### 3.4.5.1.1. LDAP

LDAP is used to maintain a list of trusted DDF users and the attributes associated with them. CAS queries it to determine if a user's credentials are valid, and to retrieve user attributes.

1. Obtain and unzip the DDF kernel: DDF-distribution-kernel-<VERSION>.zip.
2. Start the distribution
3. Deploy the Embedded LDAP application by copying the ldap-embedded-app-<VERSION>.kar into the <DDF\_HOME>/deploy directory. Verify that the LDAP server is installed by checking the DDF log or by performing an `la` command and verifying that the OpenDJ bundle is in the active state. Additionally, it should respond to LDAP requests on the default ports, which are 1389 and 1636.
4. Copy the assigned LDAP keystore and truststore files into the <DDF\_HOME>/etc/keystores folder, making sure they overwrite the existing serverKeystore.jks and serverTruststore.jks files.

5. Open the `<DDF_HOME>/etc/custom.system.properties` file and make sure the keystore passwords are set correctly.

**TIP**

The LDAP truststore file must contain the CAS server certificate. Otherwise, authentication will fail.

#### 3.4.5.1.2. CAS

CAS provides the authentication component for an SSO solution. Unlike LDAP and STS, version 3.x of the CAS server cannot be run inside DDF. Instead, it must be run using Tomcat. Deploying the CAS server is outside the scope of this guide, so follow the official CAS documentation to install and configure Tomcat/CAS. After installation

1. Open the `<TOMCAT>/webapps/cas/WEB-INF/cas.properties` file and modify the `cas.ldap.host`, `cas.ldap.port`, `cas.ldap.user.dn`, and `cas.ldap.password` fields to allow CAS to the embedded LDAP instance.
2. Configure CAS to provide user attributes when using the CAS protocol. CAS 3.x does not support this by default, but attribute release can be enabled with a few small changes. See <https://wiki.jasig.org/display/casum/attributes> for more information.

**TIP**

The CAS server truststore must contain the certificates for the embedded LDAP, STS server, and DDF.

#### 3.4.5.1.3. STS

The Security Token Service, unlike the LDAP, cannot currently be installed on a kernel distribution of DDF. To run an STS-only DDF installation, uninstall the catalog components that are not being used. This will increase performance. A list of unneeded components can be found on the STS page.

1. Copy the assigned STS keystore and truststore files into the `<DDF_HOME>/etc/keystores` folder, making sure they overwrite the existing `serverKeystore.jks` and `serverTruststore.jks` files.

**TIP**

The STS truststore must contain certificates for DDF and the CAS server.

2. Open the `<DDF_HOME>/etc/custom.system.properties` file and make sure the keystore passwords are set correctly.
3. Start the distribution
4. Enter the following commands to install the features used by the STS server:

```
feature:install security-cas-tokenvalidator
feature:install security-sts-casclaimshandler
```

5. Open the Admin Console and navigate to the System tab. The default admin credentials are:

username=admin, password=admin

6. Open the **Security STS CAS Token Validator** configuration.
7. Under **CAS Server URL**, type the URL for the CAS server, e.g. <https://cas:8443/cas>
8. Select the **Save** button
9. Open the **Security STS CAS Claims Handler** configuration.
10. Add attribute mappings to assign standard DDF claims from the appropriate CAS attribute. For example, suppose CAS is configured to return attributes **uid** and **email**:

```
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier=uid  
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress=email
```

All of the authentication components should be running and configured at this point. The final step is to configure a DDF instance to use CAS authentication.

#### 3.4.5.1.4. Configuring DDF

Once everything is configured and running, hooking up an existing DDF instance to the authentication scheme is performed by setting a few configuration properties.

1. Copy the assigned DDF keystore and truststore files into the **<DDF\_HOME>/etc/keystores** folder, making sure they overwrite the existing **serverKeystore.jks** and **serverTruststore.jks** files.

**TIP** The DDF truststore must contain certificates for the STS and CAS servers.

2. Open the **<DDF\_HOME>/etc/custom.system.properties** file and make sure the keystore passwords are set correctly.
3. Start the distribution.
4. Install the CAS client

```
feature:install security-cas-client
```

5. In the Admin Console navigate to the System tab and open the **Security CAS Client** configuration.
6. Set each configuration as appropriate for your environment. For example:

```
Server Name:      https://dib:8993/
CAS Server URL:   https://cas:8443/cas
CAS Login URL:    https://cas:8443/cas/login
CAS Logout URL:   https://cas:8443/cas/logout
Proxy Callback URL: https://localhost:8993/sso
Proxy Receptor URL: /sso
```

7. Open the **Security STS Client** configuration. Verify that the host/port information in the **STS WSDL Address** field points to the STS server.
8. Open the \*Web Context Policy Manager.
9. Under authentication types, assign CAS auth to the contexts which should be protected. In general, SAML auth should also be used. This avoids redirecting to CAS whenever hitting a new context in DDF, and so provides a noticeable performance benefit when first loading the UI. For example:

```
/search=SAML|CAS
```

The DDF should now use the CAS/STS servers when it attempts to authenticate a user upon an attempted login.

### 3.4.6. Updating System Users

By default, all system users are located in the `<DDF_HOME>/etc/users.properties` and `<DDF_HOME>/etc/users.attributes` files. The default users included in these two files are "admin" and "localhost". The `users.properties` file contains username, password, and role information; while the `users.attributes` file is used to mix in additional attributes. The `users.properties` file must also contain the user corresponding to the fully qualified domain name (FQDN) of the system where DDF is running. This FQDN user represents this host system internally when making decisions about what operations the system is capable of performing. For example, when performing a DDF Catalog Ingest, the system's attributes will be checked against any security attributes present on the metacard, prior to ingest, to determine whether or not the system should be allowed to ingest that metacard.

Additionally, the `users.attributes` file can contain user entries in a regex format. This allows an administrator to mix in attributes for external systems that match a particular regex pattern. The FQDN user within the `users.attributes` file should be filled out with attributes sufficient to allow the system to ingest the expected data. The `users.attributes` file uses a JSON format as shown below:

```

{
  "admin" : {
    "test" : "testValue",
    "test1" : [ "testing1", "testing2", "testing3" ]
  },
  "localhost" : {

  },
  ".*host.*" : {
    "reg" : "ex"
  }
}

```

For this example, the "admin" user will end up with two additional claims of "test" and "test1" with values of "testValue" and [ "testing1", "testing2", "testing3" ] respectively. Also, any host matching the regex ".**host**." would end up with the claim "reg" with the single value of "ex". The "localhost" user would have no additional attributes mixed in.

#### WARNING

It is possible for a regex in `users.attributes` to match users as well as a system, so verify that the regex pattern's scope will not be too great when using this feature.

#### WARNING

If your data will contain security markings, and these markings are being parsed out into the metacard security attributes via a PolicyPlugin, then the FQDN user **MUST** be updated with attributes that would grant the privileges to ingest that data. Failure to update the FQDN user with sufficient attributes will result in an error being returned for any ingest request.

#### WARNING

The following attribute values are not allowed:

- `null`
- `""`
- a non-String (e.g. `100`, `false`)
- an array including any of the above
- `[]`

Additionally, attribute names should not be repeated, and the order that the attributes are defined and the order of values within an array will be ignored.

### 3.4.7. Restricting Access to Admin Console

#### • Required Step for Security Hardening

If you have integrated DDF with your existing security infrastructure, then you may want to limit

access to parts of the DDF based on user roles/groups.

Limit access to the Admin Console to those users who need access. To set access restrictions on the Admin Console, consult the organization's security architecture to identify specific realms, authentication methods, and roles required.

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Select the **Configuration** tab.
4. Select the **Web Context Policy Manager**.
  - a. A dialogue will pop up that allows you to edit DDF access restrictions.
  - b. Once you have configured your [realms](#) in your security infrastructure, you can associate them with DDF contexts.
  - c. If your infrastructure supports multiple [authentication methods](#), they may be specified on a per-context basis.
  - d. Role requirements may be enforced by configuring the [required attributes](#) for a given context.
  - e. The [white listed contexts](#) allows child contexts to be excluded from the authentication constraints of their parents.

#### 3.4.7.1. Restricting Feature, App, Service, and Configuration Access

- **Required Step for Security Hardening**

Limit access to the individual applications, features, or services to those users who need access. Organizational requirements should dictate which applications are restricted and the extent to which they are restricted.

1. Navigate to the **Admin Console**.
2. Select the **Admin** application.
3. Select the **Configuration** tab.
4. Select the **Admin Configuration Policy**.
5. To add a feature or app permission:
  - a. Add a new field to "Feature and App Permissions" in the format of:

```
<feature name>/<app name> = "attribute name=attribute value","attribute name2=attribute value2", ...
```
  - b. For example, to restrict access of any user without an admin role to the catalog-app:

```
catalog-app = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/role=admin", ...
```
6. To add a configuration permission:

- a. Add a new field to "Configuration Permissions" in the format of:

```
configuration id = "attribute name=attribute value","attribute name2=attribute value2", ...
```

- b. For example, to restrict access of any user without an admin role to the Web Context Policy Manager:

```
org.codice.ddf.security.policy.context.impl.PolicyManager="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/role=admin"
```

If a permission is specified, any user without the required attributes will be unable to see or modify the feature, app, or configuration.

### 3.4.8. Removing Default Users

- **Required Step for Security Hardening**

The default security configuration uses a property file located at `<DDF_HOME>/etc/users.properties` to store users and passwords. A hardened system will remove this file and manage all users externally, via an LDAP server or by other means.

#### NOTE

*Default Users are an Insecure Default*

The Admin Console has an insecure default warning if the default users are not removed.

Once DDF is configured to use an external user (such as LDAP), remove the `users.properties` file from the `<DDF_HOME>/etc` directory. Use of a `users.properties` file should be limited to emergency recovery operations and replaced as soon as effectively possible.

The deletion of the default users in the `users.properties` file can be done automatically after 72 hours. This feature can be found at **Admin Console** → **Admin** → **Default Users Deletion Scheduler** → **Enable default users automatic deletion**.

#### WARNING

Once the default users are removed, the `<DDF_HOME>/bin/client` and `<DDF_HOME>/bin/client.bat` scripts will not work.

If SSH access to the Karaf shell is to be supported, edit the file `org.apache.karaf.shell.cfg` in the `<INSTALL_HOME>/etc` directory, changing the value of the `sshRealm` property from `karaf` to `ldap`.

#### *Emergency Use of `users.properties` file*

Typically, the DDF does not manage passwords. Authenticators are stored in an external identity management solution. However, administrators may temporarily use a `users.properties` file for emergencies.

#### **NOTE**

If a system recovery account is configured in `users.properties`, ensure:

- The use of this account should be for as short a time as possible.
- The default username/password of “admin/admin” should not be used.
- All organizational standards for password complexity should still apply.
- The password should be encrypted. For steps on how, see the section "Passwords Encryption" at <https://karaf.apache.org/manual/latest/security>.

#### *Compliance Reviews*

#### **NOTE**

It is recommended to perform yearly reviews of accounts for compliance with organizational account management requirements.

### **3.4.9. Disallowing Login Without Certificates**

DDF can be configured to prevent login without a valid PKI certificate.

- Navigate to **Admin Console**
- Under **Security**, select → **Web Context Policy Manager**
- Add a policy for each context requiring restriction
  - For example: `/search=SAML|PKI` will disallow login without certificates to the Search UI.
  - The format for the policy should be: `<CONTEXT>=SAML|PKI`
- Click **Save**

#### **NOTE**

Ensure certificates comply with organizational hardening policies.

### **3.4.10. Managing Certificate Revocation List (CRL)**

- **Required Step for Security Hardening**

For hardening purposes, it is recommended to implement a way to verify the CRL at least daily.

A Certificate Revocation List is a collection of formerly-valid certificates that should explicitly *not* be accepted.

#### **3.4.10.1. Creating a Certificate Revocation List (CRL)**

Create a CRL in which the token issuer’s certificate is valid. The example uses OpenSSL.



```
$> openssl ca -gencrl -out crl-tokenissuer-valid.pem
```

*Windows and OpenSSL*

**NOTE**

Windows does not include OpenSSL by default. For Windows platforms, a additional download of [OpenSSL](#) or an alternative is required.

#### 3.4.10.1.1. Revoke a Certificate and Create a New CRL that Contains the Revoked Certificate

```
$> openssl ca -revoke tokenissuer.crt  
  
$> openssl ca -gencrl -out crl-tokenissuer-revoked.pem
```

#### 3.4.10.1.2. Viewing a CRL

1. Use the following command to view the serial numbers of the revoked certificates: `$> openssl crl -inform PEM -text -noout -in crl-tokenissuer-revoked.pem`

#### 3.4.10.2. Enabling Certificate Revocation

**NOTE**

Enabling CRL revocation or modifying the CRL file will require a restart of DDF to apply updates.

1. Place the CRL in `<DDF_HOME>/etc/keystores`.
2. Add the line `org.apache.ws.security.crypto.merlin.x509crl.file=etc/keystores/<CRL_FILENAME>` to the following files (Replace `<CRL_FILENAME>` with the URL or file path of the CRL location):
  - a. `<DDF_HOME>/etc/ws-security/server/encryption.properties`
  - b. `<DDF_HOME>/etc/ws-security/issuer/encryption.properties`
  - c. `<DDF_HOME>/etc/ws-security/server/signature.properties`
  - d. `<DDF_HOME>/etc/ws-security/issuer/signature.properties`
3. (Replace `<CRL_FILENAME>` with the file path or URL of the CRL file used in previous step.)

Adding this property will also enable CRL revocation for any context policy implementing PKI authentication. For example, adding an authentication policy in the Web Context Policy Manager of `/search=SAML|PKI` will disable basic authentication, require a certificate for the search UI, and allow a SAML SSO session to be created. If a certificate is not in the CRL, it will be allowed through, otherwise it will get a 401 error. If no certificate is provided, the guest handler will grant guest access.

This also enables CRL revocation for the STS endpoint. The STS CRL Interceptor monitors the same `encryption.properties` file and operates in an identical manner to the PKI Authentication's CRL handler. Enabling the CRL via the `encryption.properties` file will also enable it for the STS, and also requires a restart.

If the CRL cannot be placed in `<DDF_HOME>/etc/keystores` but can be accessed via an **HTTPS** URL:

1. Navigate to the Admin Console.
2. Navigate to **System** → **Configuration** → **Certificate Revocation List (CRL)**
3. Add the **HTTPS** URL under **CRL URL address**
4. Check the **Enable CRL via URL** option

A local CRL file will be created and the `encryption.properties` and `signature.properties` files will be set as mentioned above.

#### 3.4.10.2.1. Add Revocation to a Web Context

The PKIHandler implements CRL revocation, so any web context that is configured to use PKI authentication will also use CRL revocation if revocation is enabled.

1. After enabling revocation (see above), open the **Web Context Policy Manager**.
2. Add or modify a Web Context to use PKI in authentication. For example, enabling CRL for the search ui endpoint would require adding an authorization policy of `/search=SAML|PKI`
3. If guest access is required, add `GUEST` to the policy. Ex, `/search=SAML|PKI|GUEST`.

With guest access, a user with a revoked certificate will be given a 401 error, but users without a certificate will be able to access the web context as the guest user.

The STS CRL interceptor does not need a web context specified. The CRL interceptor for the STS will become active after specifying the CRL file path, or the URL for the CRL, in the `encryption.properties` file and restarting DDF.

#### NOTE

Disabling or enabling CRL revocation or modifying the CRL file will require a restart of DDF to apply updates. If CRL checking is already enabled, adding a new context via the **Web Context Policy Manager** will not require a restart.

#### 3.4.10.2.2. Adding Revocation to an Endpoint

#### NOTE

This section explains how to add CXF's CRL revocation method to an endpoint and not the CRL revocation method in the `PKIHandler`.

This guide assumes that the endpoint being created uses CXF and is being started via Blueprint from inside the OSGi container. If other tools are being used the configuration may differ.

Add the following property to the `jasws` endpoint in the endpoint's `blueprint.xml`:

```
<entry key="ws-security.enableRevocation" value="true"/>
```

Example xml snippet for the `jaxws:endpoint` with the property:

```
<jaxws:endpoint id="Test" implementor="#testImpl"
                wsdlLocation="classpath:META-INF/wsdl/TestService.wsdl"
                address="/TestService">

    <jaxws:properties>
        <entry key="ws-security.enableRevocation" value="true"/>
    </jaxws:properties>
</jaxws:endpoint>
```

#### 3.4.10.2.3. Verifying Revocation

A **Warning** similar to the following will be displayed in the logs of the source and endpoint showing the exception encountered during certificate validation:

```
11:48:00,016 | WARN | tp2085517656-302 | WSS4JInInterceptor |
ecurity.wss4j.WSS4JInInterceptor 330 | 164 - org.apache.cxf.cxf-rt-ws-security - 2.7.3 |
org.apache.ws.security.WSSecurityException: General security error (Error during
certificate path validation: Certificate has been revoked, reason: unspecified)
    at
org.apache.ws.security.components.crypto.Merlin.verifyTrust(Merlin.java:838)[161:org.apac
he.ws.security.wss4j:1.6.9]
    at
org.apache.ws.security.validate.SignatureTrustValidator.verifyTrustInCert(SignatureTrustV
alidator.java:213)[161:org.apache.ws.security.wss4j:1.6.9]

[ ... section removed for space ]

Caused by: java.security.cert.CertPathValidatorException: Certificate has been revoked,
reason: unspecified
    at
sun.security.provider.certpath.PKIXMasterCertPathValidator.validate(PKIXMasterCertPathVal
idator.java:139)[:1.6.0_33]
    at
sun.security.provider.certpath.PKIXCertPathValidator.doValidate(PKIXCertPathValidator.jav
a:330)[:1.6.0_33]
    at
sun.security.provider.certpath.PKIXCertPathValidator.engineValidate(PKIXCertPathValidator
.java:178)[:1.6.0_33]
    at
java.security.cert.CertPathValidator.validate(CertPathValidator.java:250)[:1.6.0_33]
    at
org.apache.ws.security.components.crypto.Merlin.verifyTrust(Merlin.java:814)[161:org.apac
he.ws.security.wss4j:1.6.9]
    ... 45 more
```

## 3.5. Configuring Data Management

Data ingested into DDF has security attributes that can be mapped to users' permissions to ensure proper access. This section covers configurations that ensure only the appropriate data is contained in or exposed by DDF.

### 3.5.1. Configuring Solr

The default catalog provider for DDF is [Solr](#). If using another catalog provider, see [Changing Catalog Providers](#).

#### 3.5.1.1. Configuring Solr Catalog Provider Synonyms

When configured, text searches in Solr will utilize synonyms when attempting to match text within the catalog. Synonyms are used during keyword/anyText searches as well as when searching on specific text attributes when using the [like](#) / [contains](#) operator. Text searches using the [equality](#) / [exact match](#) operator will not utilize synonyms.

Solr utilizes a [synonyms.txt](#) file which exists for each Solr core. Synonym matching is most pertinent to metacards which are contained within 2 cores: [catalog](#) and [metacard\\_cache](#).

##### 3.5.1.1.1. Defining synonym rules in the Solr Provider

- Edit the [synonyms.txt](#) file under the [catalog](#) core. For each synonym group you want to define, add a line with the synonyms separated by a comma. For example:

```
United States, United States of America, the States, US, U.S., USA, U.S.A
```

- Save the file
- Repeat the above steps for the [metacard\\_cache](#) core.
- Restart the DDF.

**NOTE** Data does not have to be re-indexed for the synonyms to take effect.

#### 3.5.1.2. Hardening Solr

The following sections provide hardening guidance for Solr; however, they are provided only as reference and additional security requirements may be added.

##### 3.5.1.2.1. Hardening Solr Server Configuration

The Solr server configuration is configured to be secure by default. No additional hardening should be necessary. The default configuration starts Solr with TLS enabled and basic authentication required.

That means DDF must trust Solr's PKI certificate.

#### 3.5.1.2.2. Solr Server Password Management

By default, DDF is configured to use Solr server. To verify this, view the property `solr.client`. If the property is set to `HttpSolrClient`, DDF is configured to use Solr server.

To ensure the security of its communication with Solr server, DDF sends HTTP requests over TLS. Solr is configured to use basic authentication to further ensure the requests originated from DDF. There are several system properties that control basic authentication and password management.

- `solr.useBasicAuth` Send basic authentication header if property is `true`
- `solr.username` Username for basic authentication with Solr server.
- `solr.password` Password for basic authentication.
- `solr.attemptAutoPasswordChange` If this property is `true`, DDF attempts to change the default password to a randomly generated secure password if it detects the default password is in use. The new password is encrypted and then stored in the system properties.

The Solr distribution included with DDF comes already configured with a user. To see the username or default password, either inspect the file `<DDF_HOME>/etc/custom.system.properties` or refer to the properties [here](#).


A limitation of the current implementation is that the Solr password is not recoverable. Further, the migration command does not currently migrate the password. It may be necessary to reset the password:

- After a migration.
- If the administrator needs access to the Solr admin UI.
- If the administrator wants to use their own password.

#### Do not Autogenerate a Solr Password

1. To prevent DDF from attempting to change the password set the property `solr.attemptAutoPasswordChange` to `false` in the file `<DDF_HOME>/etc/custom.system.properties`

#### Change the Password to a Specific String

1. To change the Solr password to a specific string, send Solr an HTTP POST request. This is covered in the official [Solr documentation](#) . Here is an example that uses the command line utility `curl` to change the password from `admin` to `newpassword`:

```
curl -k -u "admin:admin" "https://{FQDN}:{PORT}/solr/admin/authentication" -H
'Content-type:application/json' -d '{"set-user': {'admin' : 'newpassword'}}"
```

2. Encrypt the password using the [Encryption Service](#). The encryption command enciphers the password. It is safe to save the persisted password in a file.
3. Update property `solr.password` in the file `<DDF_HOME>/etc/custom.system.properties` to be the output from the encryption command. Be sure to include `ENC(` and `)` characters produced by the encryption command. Note that the default password is not enclosed in `ENC()` because that is not necessary for cleartext. Cleartext is used by the system exactly as it appears. [follow these instructions](#).
4. Finally, restart DDF

## Restore the Default Password in Solr

1. Restore the `<DDF_HOME>/solr/server/solr/security.json` from a zip file of the DDF distribution.

## OR

1. Edit the `<DDF_HOME>/solr/server/solr/security.json` file. Solr stores a salted hash of the user passwords in this file.
2. Assuming the Solr username is `admin`, change the credentials section to match this string:

```
"credentials": {  
  "admin": "31u3dZLhFmlhsyYz1LxtUDoKR2j8oRnLwWcAH7Lbor4=  
F9eRJs+ZMI95YSQnBP/lGrLH8h60lKKizjMgC69J+WM="}
```

The quoted string following the username `admin` is the salted hash for the password `admin`.

3. Edit the file `<DDF_HOME>/etc/custom.system.properties` and change the value of `solr.password` to `admin`.
4. Optional: [Prevent DDF from automatically changing the Solr password](#).

## Removing Basic Authentication from Solr

To disable Solr's basic authentication mechanism, rename or remove the file `<DDF_HOME>/solr/server/solr/security.json` and restart Solr. The file `security.json` configures Solr to use basic authentication and defines Solr users. If the file is not present, Solr requires no login. This could be a security issue in many environments and it is recommended to never disable Solr authentication in an operational environment. If authentication is disabled, the system property `solr.useBasicAuth` may be set to `false`.

### 3.5.1.2.3. Configuring Solr Encryption

While it is possible to encrypt the Solr index, it decreases performance significantly. An encrypted Solr index also can only perform exact match queries, not relative or contextual queries. As this drastically reduces the usefulness of the index, this configuration is not recommended. The recommended approach is to encrypt the entire drive through the Operating System of the server on which the index

is located.

---

### 3.5.1.3. Accessing the Solr Admin UI

The Solr Admin UI for Solr server configurations is generally inaccessible through a web browser. A web browser can be configured to access the Solr Admin UI if required.

#### 3.5.1.3.1. Configuring a Browser to Access Solr Admin UI

The Solr server configuration is secure by default. Solr server requires a TLS connection with client authentication. Solr only allows access to clients that present a trusted certificate.

#### 3.5.1.3.2. Using DDF Keystores

Solr server uses the same keystores as DDF. A simple way to enable access to the Solr Admin UI is to install DDF's own private key/certificate entry into a browser. The method to export DDF's private key/certificate entry depend on the type of keystore being used. The method to import the private key/certificate entry into the browser depends on the operating system, and the browser itself. For more information consult the browser's documentation.

If the browser is not correctly configured with a certificate that Solr trusts, the browser displays an error message about client authentication failing, or a message that the client certificate is invalid.

#### 3.5.1.3.3. Solr Admin UI's URL

The Solr server's URL is configured in DDF's `custom.system.properties` file. See [solr.http.url](#) for more information. An *example* of a typical URL for the Solr Admin UI is `https://:hostname:8994`.

---

## 3.5.2. Changing Catalog Providers

This scenario describes how to reconfigure DDF to use a different catalog provider.

This scenario assumes DDF is already running.

*Uninstall Catalog Provider (if installed).*

1. Navigate to the **Admin Console**.
2. Select the **System** tab.
3. Select the **Features** tab.
4. Find and Stop the installed Catalog Provider

*Install the new Catalog Provider*

1. Navigate to the **Admin Console**.

2. Select the **System** tab.
3. Select the **Features** tab.
4. Find and Start the desired Catalog Provider.

### 3.5.3. Changing Hostname

By default, the STS server, STS client and the rest of the services use the system property `org.codice.ddf.system.hostname` which is defaulted to 'localhost' and not to the fully qualified domain name of the DDF instance. Assuming the DDF instance is providing these services, the configuration must be updated to use the **fully qualified domain name** as the service provider. If the DDF is being accessed from behind a proxy or load balancer, set the system property `org.codice.ddf.external.hostname` to the hostname users will be using to access the DDF.

This can be changed during [Initial Configuration](#) or later by editing the `<DDF_HOME>/etc/custom.system.properties` file.

### 3.5.4. Configuring Errors and Warnings

DDF performs several types of validation on metadata ingested into the catalog. Depending on need, configure DDF to act on the warnings or errors discovered.

#### 3.5.4.1. Enforcing Errors or Warnings

Prevent data with errors or warnings from being ingested at all.

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select **Configuration**.
4. Select **Metacard Validation Marker Plugin**.
5. Enter **ID** of validator(s) to enforce.
6. Select **Enforce errors** to prevent ingest for errors.
7. Select **Enforce warnings** to prevent ingest for warnings.

---

#### 3.5.4.2. Hiding Errors or Warnings from Queries

Prevent invalid metacards from being displayed in query results, unless specifically queried.

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select **Configuration**.



4. Select **Catalog Federation Strategy**.
  5. Deselect **Show Validations Errors** to hide metacards with errors.
  6. Deselect **Show Validations Warnings** to hide metacards with warnings.
- 

### 3.5.4.3. Hiding Errors and Warnings from Users Based on Role

- **Required Step for Security Hardening**

Prevent certain users from seeing data with certain types of errors or warnings. Typically, this is used for security markings. If the **Metacard Validation Filter Plugin** is configured to **Filter errors** and/or **Filter warnings**, metacards with errors/warnings will be hidden from users without the specified user attributes.

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select **Configuration**.
4. Select **Metacard Validation Filter Plugin**.
5. For **Attribute map**, enter both the metacard **SECURITY** attribute to filter and the user attribute to filter.
  - a. The default attribute for viewing invalid metacards is **invalid-state**
    - i. **invalid-state=<USER ROLE>**.
    - ii. Replace **<USER ROLE>** with the roles that should be allowed to view invalid metacards.

**NOTE**

To harden the system and prevent other DDF systems from querying invalid data in the local catalog, it is recommended to create and set user roles that are unique to the local system (ie. a user role that includes a UUID).

6. Select **Filter errors** to filter errors. Users without the **invalid-state** attribute will not see metacards with errors.
  7. Select **Filter warnings** to filter warnings. Users without the **invalid-state** attribute will not see metacards with warnings.
- 

### 3.5.5. Content Directory Monitor

The Content Directory Monitor (CDM) provides the capability to easily add content and metacards into the Catalog by placing a file in a directory.

### 3.5.5.1. Installing the Content Directory Monitor

The Content Directory Monitor is installed by default with a standard installation of the Catalog application.

### 3.5.5.2. Configuring Permissions for the Content Directory Monitor

#### TIP

If monitoring a WebDav server, then adding these permissions is not required and this section can be skipped.

Configuring a Content Directory Monitor requires adding permissions to the Security Manager before CDM configuration.

Configuring a CDM requires adding read and write permissions to the directory being monitored. The following permissions, replacing `<DIRECTORY_PATH>` with the path of the directory being monitored, are required for each configured CDM and should be placed in the CDM section inside `<DDF_HOME>/security/configurations.policy`.

#### WARNING

##### *Adding New Permissions*

After adding permissions, a system restart is required for them to take effect.

1. `permission java.io.FilePermission "<DIRECTORY_PATH>", "read";`
2. `permission java.io.FilePermission "<DIRECTORY_PATH>${/}-", "read, write";`

Trailing slashes after `<DIRECTORY_PATH>` have no effect on the permissions granted. For example, adding a permission for `"${/}test${/}path"` and `"${/}test${/}path${/}"` are equivalent. The recursive forms `"${/}test${/}path${/}-"`, and `"${/}test${/}path${/}${/}-"` are also equivalent.

Line 1 gives the CDM the permissions to read from the monitored directory path. Line 2 gives the CDM the permissions to recursively read and write from the monitored directory path, specified by the directory path's suffix `"${/}-"`.

If a CDM configuration is deleted, then the corresponding permissions that were added should be deleted to avoid granting unnecessary permissions to parts of the system.

### 3.5.5.3. Configuring the Content Directory Monitor

#### IMPORTANT

##### *Content Directory Monitor Permissions*

When configuring a Content Directory Monitor, make sure to set permissions on the new directory to allow DDF to access it. Setting permissions should be done **before** configuring a CDM. Also, don't forget to add permissions for products outside of the monitored directory. See [Configuring Permissions for the Content Directory Monitor](#) for in-depth instructions on configuring permissions.

**NOTE**

If there's a metacard that points to a resource outside of the CDM, then you must configure the [URL Resource Reader](#) to be able to download it.

**WARNING***Monitoring Directories In Place*

If monitoring a directory in place, then the [URL Resource Reader](#) must be configured prior to configuring the CDM to allow reading from the configured directory. This allows the Catalog to download the products.

Configure the CDM from the Admin Console:

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select the **Configuration** tab.
4. Select **Catalog Content Directory Monitor**.

See [Content Directory Monitor configurations](#) for all possible configurations.

#### 3.5.5.4. Using the Content Directory Monitor

The CDM processes files in a directory, and all of its sub-directories. The CDM offers three options:

- Delete
- Move
- Monitor in place

Regardless of the option, the DDF takes each file in a monitored directory structure and creates a metacard for it. The metacard is linked to the file. The behavior of each option is given below.

*Delete*

- Copies the file into the Content Repository.
- Creates a metacard in the Catalog from the file.
- **Erases** the original file from the monitored directory.

*Move*

- Copies the file into the directory **.\ingested (this will double the disk space used)**
- Copies the file into the Content Repository.
- Creates a metacard in the Catalog from the file.
- **Erases** the original file from the monitored directory.

*Monitor in place*

- Creates a metacard in the Catalog from the file.

- Creates a reference from the metacard to the original file in the monitored directory.
- If the original file is deleted, the metacard is removed from the Catalog.
- If the original file is modified, the metacard is updated to reflect the new content.
- If the original file is renamed, the old metacard is deleted and a new metacard is created.

### *Parallel Processing*

The CDM supports parallel processing of files (up to 8 files processed concurrently). This is configured by setting the number of **Maximum Concurrent Files** in the configuration. A maximum of 8 is imposed to protect system resources.

### *Read Lock*

When the CDM is set up, the directory specified is continuously scanned, and files are locked for processing based on the **ReadLock Time Interval**. This does not apply to the **Monitor in place** processing directive. Files will not be ingested without having a ReadLock that has observed no change in the file size. This is done so that files that are in transit will not be ingested prematurely. The interval should be dependent on the speed of the copy to the directory monitor (ex. network drive vs local disk). For local files, the default value of 500 milliseconds is recommended. The recommended interval for network drives is 1000 - 2000 milliseconds. If the value provided is less than 100, 100 milliseconds will be used. It is also recommended that the **ReadLock Time Interval** be set to a lower amount of time when the **Maximum Concurrent Files** is set above 1 so that files are locked in a timely manner and processed as soon as possible. When a higher **ReadLock Time Interval** is set, the time it takes for files to be processed is increased.

### *Attribute Overrides*

The CDM supports setting metacard attributes directly when DDF ingests a file. Custom overrides are entered in the form:

**attribute-name=attribute-value**

For example, to set the contact email for all metacards, add the attribute override:

**contact.point-of-contact-email=doctor@clinic.com**

Each override sets the value of a single metacard attribute. To set the value of an additional attribute, select the "plus" icon in the UI. This creates an empty line for the entry.

To set multi-valued attributes, use a separate override for each value. For example, to add the keywords *PPI* and *radiology* to each metacard, add the custom attribute overrides:

**topic.keyword=PPI**

**topic.keyword=radiology**

Attributes will only be overridden if they are part of the [metacard type](#) or are [injected](#).

All attributes in the [catalog taxonomy tables](#) are injected into all metacards by default and can be overridden.

## IMPORTANT

If an overridden attribute is not part of the [metacard type](#) or [injected](#) the attribute will not be added to the metacard.

For example, if the metacard type contains contact email,

**contact.point-of-contact-email**

but the value is not currently set, adding an attribute override will set the attribute value. To override attributes that are not part of the metacard type, [attribute injection](#) can be used.

### *Blacklist*

The CDM blacklist uses the "bad.files" and "bad.file.extensions" properties from the custom.system.properties file in "etc/" in order to prevent malicious or unwanted data from being ingested into DDF. While the CDM automatically omits hidden files, this is particularly useful when an operating system automatically generates files that should not be ingested. One such example of this is "thumbs.db" in Windows. This file type and any temporary files are included in the blacklist.

### *Errors*

If the CDM fails to read the file, an error will be logged in the ingest log. If the directory monitor is configured to **Delete** or **Move**, the original file is also moved to the **\.errors** directory.

### *Other*

- Multiple directories can be monitored. Each directory has an independent configuration.
- To support the monitoring in place behavior, DDF indexes the files to track their names and modification timestamps. This enables the Content Directory Monitor to take appropriate action when files are changed or deleted.
- The Content Directory Monitor recursively processes all subdirectories.

## 3.5.6. Configuring System Usage Message

The Platform UI configuration contains the settings for displaying messages to users at login or in banners in the headers and footers of all pages. For, example this configuration can provide warnings that system usage is monitored or controlled.

### *Configuring System Usage Message*

1. Navigate to the **Admin Console**.
2. Select the **Platform** application.
3. Select **Configuration**.
4. Select **Platform UI Configuration**.
5. Select **Enable System Usage Message**.
6. Enter text in the remaining fields and save.

See the [Platform UI](#) for all possible configurations.

### 3.5.7. Configuring Data Policy Plugins

Configure the data-related policy plugins to determine the accessibility of data held by DDF.

#### 3.5.7.1. Configuring the Metacard Attribute Security Policy Plugin

The Metacard Attribute Security Policy Plugin combines existing metacard attributes to make new attributes and adds them to the metacard.

- 1. Navigate to the **Admin Console**.
- 2. Select the **Catalog** application tile
- 3. Select the **Configuration** tab
- 4. Select the **Metacard Attribute Security Policy Plugin**.

Sample configuration of the [Metacard Attribute Security Policy Plugin](#).

To configure the plugin to combine the attributes `sourceattribute1` and `sourceattribute2` into a new attribute `destinationattribute1` using the union, enter these two lines under the title **Metacard Union Attributes**

Metacard Union Attributes
<code>sourceattribute1=destinationattribute1</code>
<code>sourceattribute2=destinationattribute1</code>

See [Metacard Attribute Security Policy Plugin configurations](#) for all possible configurations.

#### 3.5.7.2. Configuring the Metacard Validation Marker Plugin

By default, the Metacard Validation Marker Plugin will mark metacards with validation errors and warnings as they are reported by each metacard validator and then allow the ingest. To prevent the ingest of certain invalid metacards, the **Metacard Validity Marker** plugin can be configured to "enforce" one or more validators. Metacards that are invalid according to an "enforced" validator will not be ingested.

- 1. Navigate to the **Admin Console**.
- 2. Select the **Catalog** application.
- 3. Select the **Configuration** tab.
- 4. Select the **Metacard Validity Marker Plugin**.
  - a. If desired, enter the ID of any metacard validator to enforce. This will prevent ingest of metacards that fail validation.
  - b. If desired, check **Enforce Errors** or **Enforce Warnings**, or both.

See [Metacard Validity Marker Plugin configurations](#) for all possible configurations.

### 3.5.7.3. Configuring the Metacard Validity Filter Plugin

The [Metacard Validity Filter Plugin](#) determines whether metacards with validation errors or warnings are filtered from query results.

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select the **Configuration** tab.
4. Select the **Metacard Validity Filter Plugin**.
  - a. Check **Filter Errors** to hide metacards with errors from users.
  - b. Check **Filter Warnings** to hide metacards with warnings from users.

See [Metacard Validity Filter Plugin configurations](#) for all possible configurations.

### 3.5.7.4. Configuring the XML Attribute Security Policy Plugin

The XML Attribute Security Policy Plugin finds security attributes contained in a metacard's metadata.

1. Navigate to the Admin Console.
2. Select the **Catalog** application tile.
3. Select the **Configuration** tab.
4. Select the **XML Attribute Security Policy Plugin** configuration.

See [XML Attribute Security Policy Plugin configurations](#) for all possible configurations.

## 3.5.8. Configuring Data Access Plugins

Configure access plugins to act upon the rules and attributes configured by the policy plugins and user attributes.

### 3.5.8.1. Configuring the Security Audit Plugin

The [Security Audit Plugin](#) audits specific metacard attributes.

To configure the Security Audit Plugin:

1. Navigate to the **Admin Console**.
2. Select **Catalog** application.
3. Select **Configuration** tab.
4. Select **Security Audit Plugin**.

Add the desired metacard attributes that will be audited when modified.

See [Security Audit Plugin configurations](#) for all possible configurations.

## 3.6. Configuring Security Policies

User attributes and Data attributes are matched by security policies defined within DDF.

### 3.6.1. Configuring the Web Context Policy Manager

The Web Context Policy Manager defines all security policies for REST endpoints within DDF. It defines:

- the realms a context should authenticate against.
- the type of authentication that a context requires.
- any user attributes required for authorization.

See [Web Context Policy Manager Configurations](#) for detailed descriptions of all fields.

#### 3.6.1.1. Context Realms

The karaf realm is the only realm available by default and it authenticates against the `users.properties` file. As JAAS authentication realms are added to the STS, more realms become available to authenticate against.

For example, installing the `security-sts-ldaplogin` feature adds an ldap realm. Contexts can then be pointed to the ldap realm for authentication and STS will be instructed to authenticate them against ldap.

#### 3.6.1.2. Authentication Types

As you add REST endpoints, you may need to add different types of authentication through the Web Context Policy Manager.

Any web context that allows or requires specific authentication types should be added here with the following format:

```
/<CONTEXT>=<AUTH_TYPE>|<AUTH_TYPE|...
```

Table 9. Default Types of Authentication

Authentication Type	Description
saml	Activates single-sign on (SSO) across all REST endpoints that use SAML.
basic	Activates basic authentication.
PKI	Activates public key infrastructure authentication.



Authentication Type	Description
IdP	Activates SAML Web SSO authentication support. Additional configuration is necessary.
CAS	Enables SSO through a Central Authentication Server
guest	provides guest access

### 3.6.1.3. Required Attributes

The fields for required attributes allows configuring certain contexts to only be accessible to users with pre-defined attributes. For example, the default required attribute for the `/admin` context is `role=system-admin`, limiting access to the Admin Console to system administrators

### 3.6.1.4. White Listed Contexts

White listed contexts are trusted contexts which will bypass security. Any sub-contexts of a white listed context will be white listed as well, unless they are specifically assigned a policy.

## 3.6.2. Configuring Catalog Filtering Policies

Filtering is the process of evaluating security markings on data products, comparing them to the users permissions and protecting resources from inappropriate access.

There are two options for processing filtering policies: internally, or through the use of a policy formatted in eXtensible Access Control Markup Language (XACML). The procedure for setting up a policy differs depending on whether that policy is to be used internally or by the external XACML processing engine.

### 3.6.2.1. Setting Internal Policies

1. Navigate to the **Admin Console**.
2. Select the **Security** application.
3. Click the **Configuration** tab.
4. Click on the **Security AuthZ Realm** configuration.
5. Add any attribute mappings necessary to map between subject attributes and the attributes to be asserted.
  - a. For example, the above example would require two Match All mappings of `subjectAttribute1=assertedAttribute1` and `subjectAttribute2=assertedAttribute2`
  - b. Match One mappings would contain `subjectAttribute3=assertedAttribute3` and `subjectAttribute4=assertedAttribute4`.

With the `security-pdp-authz` feature configured in this way, the above Metacard would be displayed to the user. Note that this particular configuration would not require any XACML rules to be present. All

of the attributes can be matched internally and there is no reason to call out to the external XACML processing engine. For more complex decisions, it might be necessary to write a XACML policy to handle certain attributes.

---

### 3.6.2.2. Setting XACML Policies

To set up a XACML policy, place the desired XACML policy in the `<distribution root>/etc/pdp/policies` directory and update the included `access-policy.xml` to include the new policy. This is the directory in which the PDP will look for XACML policies every 60 seconds.

See [Developing XACML Policies](#) for more information about custom XACML policies.

---

### 3.6.2.3. Catalog Filter Policy Plugins

Several Policy Plugins for catalog filtering exist currently: [Metacard Attribute Security Policy Plugin](#) and [XML Attribute Security Policy Plugin](#). These Policy Plugin implementations allow an administrator to easily add filtering capabilities to some standard Metacard types for all Catalog operations. These plugins will place policy information on the Metacard itself that allows the [Filter Plugin](#) to restrict unauthorized users from viewing content they are not allowed to view.

---

## 3.7. Configuring User Interfaces

DDF has several user interfaces available for users.

### 3.7.1. Configuring Intrigue

Start here to configure Intrigue.

#### 3.7.1.1. Configuring Default Layout for Intrigue

Intrigue includes several options for users to display search results. By default, users start with a **3D map** and an **Inspector** to view details of results or groups of results. Add or remove additional **visualizations** to the default view through the **Default Layout UI**. Users can customize their individual views as well.

*Available Visualizations*

#### **3D Map** (Default)

Display a fully-interactive three-dimensional globe.

#### **2D Map**

Display a less resource-intensive two-dimensional map.

---

### Inspector (Default)

Display a view of detailed information about a search result.

### Histogram

Compare attributes of items in a search result set as a histogram.

### Table

Compare attributes of items in a search result set as a table.

#### Configuring Visualizations

1. Navigate to the **Admin Console**.
  2. Select the **Search UI** application.
  3. Select the **Default Layout** tab.
  4. **Add** or **Remove** visualizations as desired.
    - a. To add a visualization, select the **Add** icon.
    - b. To remove a visualization, select the **Delete** icon on the tab for that visualization.
  5. Select **Save** to complete.
- 

#### 3.7.1.2. Configuring Map Layers for Intrigue

Customize the look of the map displayed to users in Intrigue by adding or removing map layers through the **Map Layers UI**. Equivalent addition and deletion of a map layer can be found in [Map Configuration for Intrigue](#).

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select the **Map Layers** tab.
4. **Add**, **Configure** or **Remove** map layers as desired.

#### Adding a Map Layer (Imagery Provider)

Adding a Map Layer translates to adding an Imagery Provider

1. Enter a unique alphanumeric **Name** (no special characters).
  2. Enter the **Provider URL** for the server hosting the map layer instance.
  3. Select **Proxy** if security policies or the tile server does not allow Cross-Origin Resource Sharing (CORS).
  4. Select **Allow Credential Formatting** if map layer server prompts for credentials.
    - a. If selected, requests will fail if the server does not prompt for credentials.
-

5. Select from the list of available **Provider Types**.
6. Select a value for the **Alpha** to set the overall opacity of the *map layer*.
  - a. Setting **Alpha** to 0 will prevent the layer from loading.
7. Select **Show** to make the layer visible in Intrigue. (Deselect to hide.)
8. Select **Transparent** if *tile* images contain transparency.

#### *Deleting a Map Layer*

1. Delete an unneeded map layer with the **Delete Layer**(  ) icon associated with that layer.

To remove all map layers, select **RESET**.

#### *Reordering Map Layers*

1. Move layers **Up** and **Down** in loading order with the **Arrow Icons** associated with each layer.

#### *Map Layer Advanced Configuration*

Select **Advanced Configuration** to edit the JSON-formatted configuration directly. See [Catalog UI Search Configurations](#) for examples of map layer configurations.

External links to the specific API documentation of the map layer is also available from the **Advanced Configuration** menu.

---

### 3.7.1.3. Map Configuration for Intrigue

Customize the look of the map displayed to users in Intrigue through the **Catalog UI Search**. Equivalent addition and deletion of a map layer can be found in [Configuring Map Layers for Intrigue](#).

1. Navigate to the **Admin Console**.
2. Select the **Search UI** application.
3. Select the **Configuration** tab.
4. Select the **Catalog UI Search** configuration.

#### *Edit a Map Layer (Imagery Provider)*

1. Enter the properties of the map layer into the **Imagery Provider** in the proper syntax.
  - a. Example Imagery Provider Syntax: `{"type": "OSM", "url" "http://a.tile.openstreetmaps.org" "layers" ["layer1" "layer2"] "parameters" {"FORMAT" "image/png" "VERSION" "1.1.1"} "alpha" 0.5}`.
    - i. "type": format of imagery provider.
    - ii. "url": location of server hosting the imagery provider.
    - iii. "layers": names of individual layers. (enclose list in square brackets `[ ]`).
    - iv. "parameters": (enclose in braces `{ }`)

- A. "FORMAT": image type used by imagery provider.
- B. "VERSION": version of imagery provider to use.
- C. "alpha": opacity of imagery provider layer.

#### *Delete a Map Layer (Imagery Provider)*

1. Delete the properties in **Imagery Provider** text box.

#### *Edit a Terrain Provider*

1. Enter the properties into the **Terrain Provider** in the proper syntax.
  - a. A default Terrain Provider is provided: `{ "type": "CT", "url": "http://assets.agi.com/stk-terrain/tilesets/world/tiles" }`.
    - i. "type": format of terrain provider.
    - ii. "url": location of server hosting the terrain provider.

#### *Edit Gazetteer Configuration*

1. Check/Uncheck **Show Gazetteer** to control searching place names functionality.
2. Check/Uncheck **Use Online Gazetteer** to control Intrigue search gazetteer.
  - a. Unchecked: use local gazetteer service.

---

### **3.7.1.4. Configuring User Access to Ingest and Metadata for Intrigue**

Intrigue lets the administrator control user access to ingest and metadata. The administrator can show or hide the uploader, letting them control whether users can ingest products. They can also choose whether or not users can edit existing metadata. By default, the uploader is available to users and editing is allowed.

#### *Configuring The Uploader*

Choose to hide or show the uploader. Note that hiding the uploader will remove the users' ability to ingest.

1. Navigate to the **Admin Console**.
2. Select the **Search UI** application.
3. Select the **Configuration** tab.
4. Select **Catalog UI Search**.
5. Select "Show Uploader".
6. Select **Save** to complete.

#### *Configuring Editing of Metadata*

Allow or restrict the editing of metadata.

1. Navigate to the **Admin Console**.
  2. Select the **Search UI** application.
  3. Select the **Configuration** tab.
  4. Select **Catalog UI Search**.
  5. Select "Allow Editing".
  6. Select **Save** to complete.
- 

#### 3.7.1.5. Configuring the Intrigue Upload Editor

The upload editor in Intrigue allows users to specify attribute overrides which should be applied on ingest. Administrators control the list of attributes that users may edit and can mark certain attributes as required. They may also disable the editor if desired.

##### *Configure attribute list*

1. Navigate to the **Admin Console**.
2. Select the **Search UI** application.
3. Select the **Configuration** tab.
4. Select **Catalog UI Search**.
5. Use the "Upload Editor: Attribute Configuration" field to configure the attributes shown in the editor.
6. Use the "Upload Editor: Required Attributes" field to mark attributes as required.
7. Select **Save** to complete.

See [Intrigue Configurations](#) for more information regarding these configurations.

##### *Disabling*

The editor only appears if it has attributes to show. If the upload editing capability is not desired, simply remove all entries from the attribute configuration and the editor will be hidden.

---

#### 3.7.1.6. Configuring Search Options for Intrigue

Intrigue provides a few options to control what metacards may be searched. By default, the user can perform searches that produce historical metacards, archived metacards, and metacards from the local catalog. However, administrators can disable searching for any of these types of metacards.

##### *Configuring Search Options*

1. Navigate to the **Admin Console**.
  2. Select the **Search UI** application.
-

3. Select the **Configuration** tab.
4. Select Catalog UI Search.
5. Scroll down to the "Disable Local Catalog" option with the other options below it.
6. To disable searching for a metacard type, check the corresponding box.
7. Select **Save** to complete.

### 3.7.1.7. Configuring Query Feedback for Intrigue

Intrigue provides an option to allow users to submit Query Feedback.

#### *Configuring Query Feedback*

1. First, configure the **Email Service** to point to a mail server. See [Email Service Configurations](#).
2. Navigate to the **Admin Console**.
3. Select the **Search UI** application.
4. Select the **Configuration** tab.
5. Select **Catalog UI Search**.
6. Select the **Enable Query Feedback** option to enable the query comments option for users in Intrigue.
7. Add a **Query Feedback Email Subject Template**.
8. Add a **Query Feedback Email Body Template**. The template may include HTML formatting.
9. Add the **Query Feedback Email Destination**.
10. Select the **Save** button.

#### *Query Feedback Template Replacements*

The following keywords in the templates will be replaced with submission-specific values, or "Unknown" if unknown.

Template keyword	Replacement value
{{auth_username}}	Username of the security subsystem (see <a href="#">Security Framework</a> )
{{username}}	Username of the user who submitted the Query Feedback
{{email}}	Email of the user who submitted the Query Feedback
{{workspace_id}}	Workspace ID of the query
{{workspace_name}}	Workspace Name of the query
{{query}}	Query

Template keyword	Replacement value
{{query_initiated_time}}	Time of the query
{{query_status}}	Status of the query
{{query_results}}	Results of the query
{{comments}}	Comments provided by the user about the query

#### *Submitting Query Feedback from Intrigue*

1. Perform a search on any workspace.
2. Select the 3 dots on the results tab.
3. Choose the **Submit Feedback** option.
4. Add comments in the input box.
5. Select the **Send** button.

See [Catalog UI Search Configurations](#) for default Query Feedback configurations.

## 3.8. Configuring Federation

DDF is able to [federate](#) to other data sources, including other instances of DDF, with some simple configuration.

### 3.8.1. Enable SSL for Clients

In order for outbound secure connections (HTTPS) to be made from components like Federated Sources and Resource Readers configuration may need to be updated with keystores and security properties. These values are configured in the `<DDF_HOME>/etc/custom.system.properties` file. The following values can be set:

Property	Sample Value	Description
<code>javax.net.ssl.trustStore</code>	<code>etc/keystores/serverTruststore.jks</code>	The java keystore that contains the trusted public certificates for Certificate Authorities (CA's) that can be used to validate SSL Connections for outbound TLS/SSL connections (e.g. HTTPS). When making outbound secure connections a handshake will be done with the remote secure server and the CA that is in the signing chain for the remote server's certificate must be present in the trust store for the secure connection to be successful.
<code>javax.net.ssl.trustStorePassword</code>	<code>changeit</code>	This is the password for the truststore listed in the above property
<code>javax.net.ssl.keyStore</code>	<code>etc/keystores/serverKeystore.jks</code>	The keystore that contains the private key for the local server that can be used for signing, encryption, and SSL/TLS.



Property	Sample Value	Description
<code>javax.net.ssl.keyStorePassword</code>	<code>changeit</code>	The password for the keystore listed above
<code>javax.net.ssl.keyStoreType</code>	<code>jks</code>	The type of keystore
<code>https.cipherSuites</code>	<code>TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256</code>	The cipher suites that are supported when making outbound HTTPS connections
<code>https.protocols</code>	<code>TLSv1.1,TLSv1.2</code>	The protocols that are supported when making outbound HTTPS connections
<code>jdk.tls.client.protocols</code>	<code>TLSv1.1,TLSv1.2</code>	The protocols that are supported when making inbound HTTPS connections
<code>jdk.tls.ephemeralDHKeySize</code>	<code>'matched'</code>	For X.509 certificate based authentication (of non-exportable cipher suites), the DH key size matching the corresponding authentication key is used, except that the size must be between 1024 bits and 2048 bits. For example, if the public key size of an authentication certificate is 2048 bits, then the ephemeral DH key size should be 2048 bits unless the cipher suite is exportable. This key sizing scheme keeps the cryptographic strength consistent between authentication keys and key-exchange keys.

#### NOTE

<DDF\_HOME> Directory

DDF is installed in the <DDF\_HOME> directory.

### 3.8.2. Configuring HTTP(S) Ports

To change HTTP or HTTPS ports from the default values, edit the `custom.system.properties` file.

1. Open the file at <DDF\_HOME>/etc/custom.system.properties
2. Change the value after the = to the desired port number(s):
  - a. `org.codice.ddf.system.httpsPort=8993` to `org.codice.ddf.system.httpsPort=<PORT>`
  - b. `org.codice.ddf.system.httpPort=8181` to `org.codice.ddf.system.httpPort=<PORT>`
3. Restart DDF for changes to take effect.

## IMPORTANT

Do not use the Admin Console to change the HTTP port. While the Admin Console's Pax Web Runtime offers this configuration option, it has proven to be unreliable and may crash the system.

### 3.8.3. Configuring HTTP Proxy

The `platform-http-proxy` feature proxies https to http for clients that cannot use HTTPS and should not have HTTP enabled for the entire container via the `etc/org.ops4j.pax.web.cfg` file.

*Enabling the HTTP Proxy from the Admin Console*

1. Navigate to the **Admin Console**.
2. Select the **System** tab.
3. Select the **Features** tab.
4. Select `platform-http-proxy`.
5. Select the **Play** button to the right of the word "Uninstalled"

*Enabling the HTTP Proxy from the Command Console*

- Type the command `feature:install platform-http-proxy`

*Configuring HTTP Proxy Hostname*

1. Select **Configuration** tab.
2. Select **HTTP to HTTPS Proxy Settings**
  - a. Enter the Hostname to use for HTTPS connection in the proxy.
3. Click **Save changes**.

## NOTE

*HTTP Proxy and Hostname*

The hostname should be set by default. Only configure the proxy if this is not working.

### 3.8.4. Federation Strategy

A federation strategy federates a query to all of the Remote Sources in the query's list, processes the results in a unique way, and then returns the results to the client. For example, implementations can choose to halt processing until all results return and then perform a mass sort or return the results back to the client as soon as they are received back from a Federated Source.

An endpoint can optionally specify the federation strategy to use when it invokes the query operation. Otherwise, the Catalog provides a default federation strategy that will be used: the Catalog Federation Strategy.

#### 3.8.4.1. Configuring Federation Strategy

The Catalog Federation Strategy configuration can be found in the Admin Console.

1. Navigate to Admin Console.
2. Select **Catalog**
3. Select **Configuration**
4. Select **Catalog Federation Strategy**.

See [Federation Strategy configurations](#) for all possible configurations.

#### 3.8.4.1.1. Catalog Federation Strategy

The Catalog Federation Strategy is the default federation strategy and is based on sorting metacards by the sorting parameter specified in the federated query.

The possible sorting values are:

- metacard's effective date/time
- temporal data in the query result
- distance data in the query result
- relevance of the query result

The supported sorting orders are ascending and descending.

The default sorting value/order automatically used is relevance descending.

#### WARNING

The Catalog Federation Strategy expects the results returned from the Source to be sorted based on whatever sorting criteria were specified. If a metadata record in the query results contains null values for the sorting criteria elements, the Catalog Federation Strategy expects that result to come at the end of the result list.

### 3.8.5. Connecting to Sources

A **source** is a system consisting of a catalog containing Metacards.

Catalog sources are used to connect Catalog components to data sources, local and remote. Sources act as proxies to the actual external data sources, e.g., a RDBMS database or a NoSQL database.

#### *Types of Sources*

##### **Remote Source**

Read-only data sources that support query operations but cannot be used to create, update, or delete metacards.

##### **Federated Sources**

A federated source is a remote source that can be included in federated queries by request or as part of an enterprise query. Federated sources support query and site information operations only. Catalog modification operations, such as create, update, and delete, are not allowed. Federated

sources also expose an event service, which allows the Catalog Framework to subscribe to event notifications when metacards are created, updated, and deleted.

Catalog instances can also be federated to each other. Therefore, a Catalog can also act as a federated source to another Catalog.

## **Connected Sources**

A Connected Source is a local or remote source that is always included in every local and enterprise query, but is hidden from being queried individually. A connected source's identifier is removed in all query results by replacing it with DDF's source identifier. The Catalog Framework does not reveal a connected source as a separate source when returning source information responses.

## **Catalog Providers**

A Catalog Provider is used to interact with data providers, such as files systems or databases, to query, create, update, or delete data. The provider also translates between DDF objects and native data formats.

All sources, including federated source and connected source, support queries, but a Catalog provider also allows metacards to be created, updated, and deleted. A Catalog provider typically connects to an external application or a storage system (e.g., a database), acting as a proxy for all catalog operations.

## **Catalog Stores**

A Catalog Store is an editable store that is either local or remote.

### *Available Federated Sources*

The following Federated Sources are available in a standard installation of DDF:

### **Federated Source for Atlassian Confluence®**

Retrieve pages, comments, and attachments from an Atlassian Confluence® REST API.

### **CSW Specification Profile Federated Source**

Queries a CSW version 2.0.2 compliant service.

### **CSW Federation Profile Source**

Queries a CSW version 2.0.2 compliant service.

### **GMD CSW Source**

Queries a GMD CSW APISO compliant service.

### **OpenSearch Source**

Performs OpenSearch queries for metadata.

### **WFS 1.0 Source**

Allows for requests for geographical features across the web.

### WFS 1.1 Source

Allows for requests for geographical features across the web.

### WFS 2.0 Source

Allows for requests for geographical features across the web.

#### *Available Connected Sources*

The following Connected Sources are available in a standard installation of DDF:

### WFS 1.0 Source

Allows for requests for geographical features across the web.

### WFS 1.1 Source

Allows for requests for geographical features across the web.

### WFS 2.0 Source

Allows for requests for geographical features across the web.

#### *Available Catalog Stores*

The following Catalog Stores are available in a standard installation of DDF:

### Registry Store

Allows CSW messages to be turned into usable Registry metacards and for those metacards to be turned back into CSW messages.

#### *Available Catalog Providers*

The following Catalog Providers are available in a standard installation of DDF:

### Solr Catalog Provider

Uses Solr as a catalog.

#### *Available Storage Providers*

The following Storage Providers are available in a standard installation of DDF:

### Content File System Storage Provider

.Sources Details Availability and configuration details of available sources.

#### **3.8.5.1. Federated Source for Atlassian Confluence(R)**

The Confluence source provides a Federated Source to retrieve pages, comments, and attachments from an Atlassian Confluence® REST API and turns the results into Metacards the system can use. The Confluence source does provide a Connected Source interface but its functionality has not been verified.

Confluence Source has been tested against the following versions of Confluence with REST API v2

- Confluence 1000.444.5 (Cloud)
- Confluence 5.10.6 (Server)
- Confluence 5.10.7 (Server)

### *Installing the Confluence Federated Source*

The Confluence Federated Source is installed by default with a standard installation in the Catalog application.

Add a New Confluence Federated Source through the Admin Console:

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select the **Sources** tab.
4. Add a New source.
5. Name the New source.
6. Select **Confluence Federated Source** from **Binding Configurations**.

### *Configuring the Confluence Federated Source*

Configure an Existing Confluence Federated Source through the Admin Console:

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select the **Sources** tab.
4. Select the name of the source to edit.

See [Confluence Federated Source configurations](#) for all possible configurations.

#### **IMPORTANT**

If an additional attribute is not part of the Confluence metacard type or [injected](#), the attribute will not be added to the metacard.

### *Usage Limitations of the Confluence Federated Source*

Most of the fields that can be queried on Confluence have some sort of restriction on them. Most of the fields do not support the **like** aka **~** operation so the source will convert **like** queries to **equal** queries for attributes that don't support **like**. If the source receives a query with attributes it doesn't understand, it will just ignore them. If the query doesn't contain any attributes that map to Confluence search attributes, an empty result set will be returned.

Depending on your version of Confluence, when downloading attachments you might get redirected to a different download URL. The default URLResourceReader configuration allows redirects, but if the option was disabled in the past, the download will fail. This can be fixed by re-enabling redirects in the [URLResourceReader configuration](#).

---

### 3.8.5.2. CSW Specification Profile Federated Source

The CSW Specification Profile Federated Source should be used when federating to an *external* (non-DDF-based) CSW (version 2.0.2) compliant service.

#### *Installing the CSW Specification Profile Federated Source*

Add a New CSW Specification Profile Federated Source through the Admin Console:

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select the **Sources** tab.
4. Add a New source.
5. Name the New source.
6. Select **CSW Specification Profile Federated Source** from **Source Type**.

#### *Configuring the CSW Specification Profile Federated Source*

Configure an Existing CSW Specification Profile Federated Source through the Admin Console:

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select the **Sources** tab.
4. Select the name of the source to edit.

See [CSW Specification Profile Federated Source configurations](#) for all possible configurations.

#### *Usage Limitations of the CSW Specification Profile Federated Source*

- Nearest neighbor spatial searches are not supported.

---

### 3.8.5.3. CSW Federation Profile Source

The CSW Federation Profile Source is DDF's CSW Federation Profile which supports the ability to search collections of descriptive information (metadata) for data, services, and related information objects.

Use the CSW Federation Profile Source when federating to a DDF-based system.

#### *Installing the CSW Federation Profile Source*

Configure the CSW Federation Profile Source through the Admin Console:

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.

3. Add a New source.
4. Name the New source.
5. Select **CSW Specification Profile Federated Source** from **Source Type**.

#### *Configuring the CSW Federation Profile Source*

Configure an Existing CSW Federated Source through the Admin Console:

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select the **Sources** tab.
4. Select the name of the source to edit.

See [CSW Federation Profile Source configurations](#) for all possible configurations.

#### *Usage Limitations of the CSW Federation Profile Source*

- Nearest neighbor spatial searches are not supported.
- 

### **3.8.5.4. Content File System Storage Provider**

The Content File System Storage Provider is the default Storage Provider included with DDF

#### *Installing the Content File System Storage Provider*

The Content File System Storage Provider is installed by default with the Catalog application.

#### *Configuring Content File System Storage Provider*


To configure the Content File System Storage Provider:

1. Navigate to the **Admin Console**.
2. Select **Catalog**.
3. Select **Configuration**.
4. Select **Content File System Storage Provider**.

See [Content File System Storage Provider configurations](#) for all possible configurations.

---

### **3.8.5.5. GMD CSW Source**

The Geographic MetaData extensible markup language (GMD) CSW source supports the ability to search collections of descriptive information (metadata) for data, services, and related information objects, based on the [Application Profile ISO 19115/ISO19119](#) .



Use the GMD CSW source if querying a GMD CSW APISO compliant service.

#### *Installing the GMD CSW APISO v2.0.2 Source*

The GMD CSW source is installed by default with a standard installation in the Spatial application.

Configure a new GMD CSW APISO v2.0.2 Source through the Admin Console:

- Navigate to the **Admin Console**.
- Select the **Catalog** application.
- Select the **Sources** tab.
- Add a New source.
- Name the New source.
- Select **GMD CSW ISO Federated Source** from **Binding Configurations**.

#### *Configuring the GMD CSW APISO v2.0.2 Source*

Configure an existing GMD CSW APISO v2.0.2 Source through the Admin Console:

- Navigate to the **Admin Console**.
- Select the **Catalog** application.
- Select the **Sources** tab.
- Select the name of the source to edit.

See [GMD CSW APISO v2.0.2 Source configurations](#) for all possible configurations.

---

### **3.8.5.6. OpenSearch Source**

The OpenSearch source provides a [Federated Source](#) that has the capability to do [OpenSearch](#) queries for metadata from Content Discovery and Retrieval (CDR) Search V1.1 compliant sources. The OpenSearch source does not provide a [Connected Source](#) interface.

#### *Installing an OpenSearch Source*

The OpenSearch Source is installed by default with a standard installation in the Catalog application.

Configure a new OpenSearch Source through the Admin Console:

- Navigate to the **Admin Console**.
  - Select the **Catalog** application.
  - Select the **Sources** tab.
  - Add a New source.
  - Name the New source.
-

- Select **OpenSearch Source** from **Binding Configurations**.

### *Configuring an OpenSearch Source*

Configure an existing OpenSearch Source through the Admin Console:

- Navigate to the **Admin Console**.
- Select the **Catalog** application.
- Select the **Sources** tab.
- Select the name of the source to edit.

See [OpenSearch Source configurations](#) for all possible configurations.

### *Using OpenSearch Source*

Use the OpenSearch source if querying a CDR-compliant search service is desired.

*Table 10. Query to OpenSearch Parameter Mapping*

Element	OpenSearch HTTP Parameter	DDF Data Location
searchTerms	<b>q</b>	Pulled from the query and encoded in UTF-8.
routeTo	<b>src</b>	Pulled from the query.
maxResults	<b>mr</b>	Pulled from the query.
count	<b>count</b>	Pulled from the query.
startIndex	<b>start</b>	Pulled from the query.
maxTimeout	<b>mt</b>	Pulled from the query.
userDN	<b>dn</b>	DDF subject
lat	<b>lat</b>	Pulled from the query if it is a point-radius query and the radius is > 0. If multiple point radius searches are encountered, each point radius is converted to an approximate polygon as geometry criteria.
lon	<b>lon</b>	
radius	<b>radius</b>	

Element	OpenSearch HTTP Parameter	DDF Data Location
box	<b>bbox</b>	<p>Pulled from the query if it is a bounding-box query.</p> <p>Or else, calculated from the query if it is a single geometry or polygon query and the <b>shouldConvertToBBBox</b> configuration option is <b>true</b>. NOTE: Converting a polygon that crosses the antimeridian to a bounding box will produce an incorrect bounding box.</p> <p>Or else, calculated from the query if it is a geometry collection and the <b>shouldConvertToBBBox</b> configuration option is <b>true</b>. Note: An approximate bounding box is used to represent the geometry collection encompassing all of the geometries within it Area between the geometries are also included in the bounding box. Hence widen the search area.</p>
geometry	<b>geometry</b>	Pulled from the DDF query and combined as a geometry collection if multiple spatial query exist.
polygon	<b>polygon</b>	According to the OpenSearch Geo Specification this is deprecated. Use the geometry parameter instead.
start	<b>dtstart</b>	Pulled from the query if the query has temporal criteria for <b>modified</b> .
end	<b>dtend</b>	
filter	<b>filter</b>	Pulled from the query.
sort	<b>sort</b>	Calculated from the query. Format: <b>relevance</b> or <b>date</b> . Supports <b>asc</b> and <b>desc</b> using <b>:</b> as delimiter.

#### *Usage Limitations of the OpenSearch Source*

The OpenSearch source does not provide a [Connected Source](#) interface.

#### **3.8.5.7. Registry Store**

The Registry Store is the interface that allows CSW messages to be turned into usable Registry metacards and for those metacards to be turned back into CSW messages.

##### *Installing Registry Store*

The Registry Store is installed by default with the Registry application.

##### *Configuring Registry Store*

To configure the Registry store:

1. Navigate to the **Admin Console**.
  2. Select **Registry**.
  3. Select the **Remote Registries** Tab and click the **Add** button.
    - a. ALTERNATIVELY: Select the **Configuration** Tab and select **Registry Store**.
- 

### 3.8.5.8. Solr Catalog Provider

The Solr Catalog Provider is included with a standard installation of DDF. There are two configurations available:

*Solr Server (default)::*

DDF is bundled with a distribution of Apache Solr. This distribution includes special JAR libraries used by DDF. This DDF scripts manage the starting and stopping of the Solr server. Considerations include:

- No configuration necessary. Simply start DDF and DDF manages starting and stopping the Solr server.
- Backup can be performed using DDF console's **backup** command.
- This configuration cannot be scaled larger than the single Solr server.
- All data is located inside the {\$branding} home directory. If the Solr index grows large, the storage volume may run low on space.

*Installing Solr Server*

No installation is required because DDF includes a distribution of Apache Solr.

*Configuring Solr Server*

No configuration.

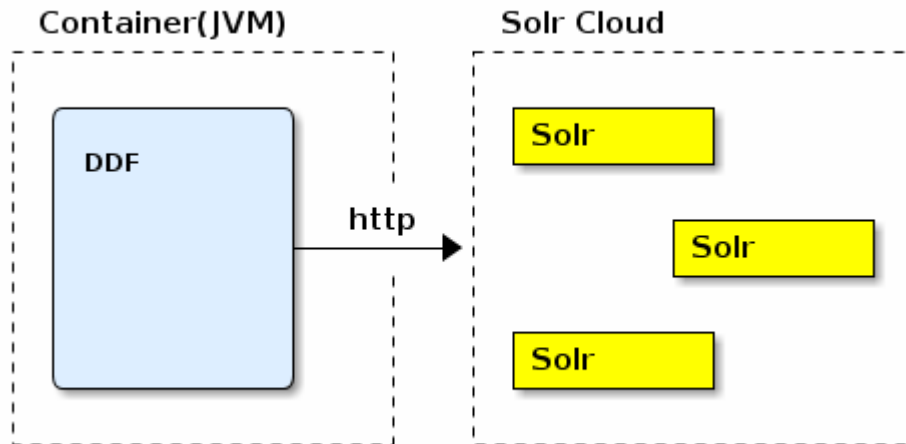
*Solr Cloud*

Solr Cloud is a cluster of distributed Solr servers used for high availability and scalability. If the DDF needs to be available with little or no downtime, then the Solr Cloud configuration should be used. The general considerations for selecting this configuration are:

- SolrCloud can scale to support over 2 billion indexed documents.
- Has network overhead and requires additional protection to be secure.
- Installation is more involved (requires Zookeeper)
- Configuration and administration is more complex due to replication, sharding, etc.
- No way to backup currently, but will automatically recover from system failure.

Configuration shared between Solr Server instances is managed by Zookeeper. Zookeeper helps

manage the overall structure.



### *Solr Cloud Deployment*

#### **NOTE**

The instructions on setting up Solr Cloud for DDF only include setup in a \*NIX environment.

### *Solr Cloud Prerequisites*

Before Solr Cloud can be installed:

- ZooKeeper 3.4.5 (Refer to [https://zookeeper.apache.org/doc/r3.1.2/zookeeperStarted.html#sc\\_Download](https://zookeeper.apache.org/doc/r3.1.2/zookeeperStarted.html#sc_Download) for installation instructions.)
- \*NIX environment
- JDK 8 or greater

#### **NOTE**

A minimum of three Zookeeper nodes required. Three Zookeeper nodes are needed to form a quorum. A three Zookeeper ensemble allows for a single server to fail and the service will still be available. More Zookeeper nodes can be added to achieve greater fault tolerance. The total number of nodes must always be an odd number. See [Setting Up an External Zoo Keeper Ensemble](#) for more information.

### *Installing Solr Cloud*

Before starting the install procedure, download the extension jars. The jars are needed to support geospatial and xpath queries and need to be installed on every Solr server instance after the Solr Cloud installation instructions have been followed.

The JARs can be found here:

- [http://artifacts.codice.org/service/local/repositories/releases/content/org/codice/thirdparty/jts/1.14.0\\_1/jts-1.14.0\\_1.jar](http://artifacts.codice.org/service/local/repositories/releases/content/org/codice/thirdparty/jts/1.14.0_1/jts-1.14.0_1.jar)

- b. <http://artifacts.codice.org/service/local/artifact/maven/content?r=public&g=ddf.platform.solr&a=solr-xpath&v=2.13.10>

Repeat the following procedure for each Solr server instance that will be part of the Solr Cloud cluster:

1. Refer to <https://cwiki.apache.org/confluence/display/solr/Apache+Solr+Reference+Guide> for installation instructions.
2. Copy downloaded jar files to: `<SOLR_INSTALL_DIR>/server/solr-webapp/webapp/WEB-INF/lib/`

#### NOTE

A minimum of two Solr server instances is required. Each Solr server instance must have a minimum of two shards. Having two Solr server instances guarantees that at least one Solr server is available if one fails. The two shards enables the document mapping to be restored if one shard becomes unavailable.

#### Configuring Solr Cloud

1. On the DDF server, edit `<DDF_HOME>/etc/custom.system.properties`:
  - a. Comment out the Solr Client Configuration for **Http Solr Client** section.
  - b. Uncomment the section for the **Cloud Solr Client**:
  - c. Set `solr.cloud.zookeeper` to `<ZOOKEEPER_1_HOSTNAME>:<PORT_NUMBER>, <ZOOKEEPER_2_HOSTNAME>:<PORT_NUMBER>, <ZOOKEEPER_n_HOSTNAME>:<PORT_NUMBER>`
  - d. Set `solr.data.dir` to the desired data directory.

#### Solr Cloud System Properties

```
solr.client = CloudSolrClient
solr.data.dir = ${karaf.home}/data/solr
solr.cloud.zookeeper = zk1:2181,zk2:2181,zk3:2181
```

#### 3.8.5.9. WFS 1.0 Source

The WFS Source allows for requests for geographical features across the web using platform-independent calls.

A Web Feature Service (WFS) source is an implementation of the `FederatedSource` interface provided by the DDF Framework.

Use the WFS Source if querying a WFS version 1.0.0 compliant service.

#### Installing the WFS v1.0.0 Source

The WFS v1.0.0 Source is installed by default with a standard installation in the Spatial application.

Configure a new WFS v1.0.0 Source through the Admin Console:

- Navigate to the **Admin Console**.
- Select the **Catalog** application.
- Select the **Sources** tab.
- Add a New source.
- Name the New source.
- Select **WFS v1.0.0 Source** from **Binding Configurations**.

#### *Configuring the WFS v1.0.0 Source*

Configure an existing WFS v1.0.0 Source through the Admin Console:

- Navigate to the **Admin Console**.
- Select the **Catalog** application.
- Select the **Sources** tab.
- Select the name of the source to edit.

See [WFS v1.0 Federated Source configurations](#) or [WFS v1.0 Connected Source configurations](#) for all possible configurations.

#### *WFS URL*

The WFS URL must match the endpoint for the service being used. The type of service and version are added automatically, so they do not need to be included. Some servers will throw an exception if they are included twice, so do not include those.

The syntax depends on the server. However, in most cases, the syntax will be everything before the **?** character in the URL that corresponds to the **GetCapabilities** query.

#### *Example GeoServer 2.5 Syntax*

```
http://www.example.org:8080/geoserver/ows?service=wfs&version=1.0.0&request=GetCapabilities
```

In this case, the WFS URL would be: <http://www.example.org:8080/geoserver/ows>

### **3.8.5.10. WFS 1.1 Source**

The WFS Source allows for requests for geographical features across the web using platform-independent calls.

A Web Feature Service (WFS) source is an implementation of the **FederatedSource** interface provided by the DDF Framework.

Use the WFS Source if querying a WFS version 1.1.0 compliant service.

#### *Installing the WFS v1.1.0 Source*

The WFS v1.1.0 Source is installed by default with a standard installation in the Spatial application.

Configure a new WFS v1.1.0 Source through the Admin Console:

- Navigate to the **Admin Console**.
- Select the **Catalog** application.
- Select the **Sources** tab.
- Add a New source.
- Name the New source.
- Select **WFS v1.1.0 Source** from **Binding Configurations**.

#### *Configuring the WFS v1.1.0 Source*

Configure an existing WFS v1.1.0 Source through the Admin Console:

- Navigate to the **Admin Console**.
- Select the **Catalog** application.
- Select the **Sources** tab.
- Select the name of the source to edit.

See [WFS v1.1 Federated Source configurations](#) for all possible configurations.

#### *WFS URL*

The WFS URL must match the endpoint for the service being used. The type of service and version are added automatically, so they do not need to be included. Some servers will throw an exception if they are included twice, so do not include those.

The syntax depends on the server. However, in most cases, the syntax will be everything before the **?** character in the URL that corresponds to the **GetCapabilities** query.

#### *Example GeoServer 2.12.1 Syntax*

```
http://www.example.org:8080/geoserver/wfs?service=wfs&version=1.1.0&request=GetCapabilities
```

In this case, the WFS URL would be: <http://www.example.org:8080/geoserver/wfs>



### 3.8.5.11. WFS 2.0 Source

The WFS 2.0 Source allows for requests for geographical features across the web using platform-independent calls.

Use the WFS Source if querying a WFS version 2.0.0 compliant service. Also see [Working with WFS Sources](#).

#### *Installing the WFS v2.0.0 Source*

The WFS v2.0.0 Source is installed by default with a standard installation in the Spatial application.

Configure a new WFS v2.0.0 Source through the Admin Console:

- Navigate to the **Admin Console**.
- Select the **Catalog** application.
- Select the **Sources** tab.
- Add a New source.
- Name the New source.
- Select **WFS v2.0.0 Source** from **Binding Configurations**.

#### *Configuring the WFS v2.0.0 Source*

Configure an existing WFS v2.0.0 Source through the Admin Console:

- Navigate to the **Admin Console**.
- Select the **Catalog** application.
- Select the **Sources** tab.
- Select the name of the source to edit.

See [WFS v2.0 Federated source configurations](#) or [WFS v2.0 Connected source configurations](#) for all possible configurations.

#### *WFS URL*

The WFS URL must match the endpoint for the service being used. The type of service and version is added automatically, so they do not need to be included. Some servers will throw an exception if they are included twice, so do not include those.

The syntax depends on the server. However, in most cases, the syntax will be everything before the **?** character in the URL that corresponds to the **GetCapabilities** query.

#### *Example GeoServer 2.5 Syntax*

```
http://www.example.org:8080/geoserver/ows?service=wfs&version=2.0.0&request=GetCapabilities
```

In this case, the WFS URL would be

```
http://www.example.org:8080/geoserver/ows
```

### *Mapping WFS Feature Properties to Metacard Attributes*

The WFS 2.0 Source allows for virtually any schema to be used to describe a feature. A feature is relatively equivalent to a metacard. The `MetacardMapper` was added to allow an administrator to configure which feature properties map to which metacard attributes.

### *Using the WFS `MetacardMapper`*

Use the WFS `MetacardMapper` to configure which feature properties map to which metacard attributes when querying a WFS version 2.0.0 compliant service. When feature collection responses are returned from WFS sources, a default mapping occurs which places the feature properties into metacard attributes, which are then presented to the user via DDF. There can be situations where this automatic mapping is not optimal for your solution. Custom mappings of feature property responses to metacard attributes can be achieved through the `MetacardMapper`. The `MetacardMapper` is set by creating a feature file configuration which specifies the appropriate mapping. The mappings are specific to a given feature type.

### *Installing the WFS `MetacardMapper`*

The WFS `MetacardMapper` is not installed by default with a standard application in the Spatial application.

### *Configuring the WFS `MetacardMapper`*

There are two ways to configure the `MetacardMapper`, one is to use the Configuration Admin available via the Admin Console. Additionally, a `feature.xml` file can be created and copied into the "deploy" directory.

### *Example WFS `MetacardMapper` Configuration*

The following shows how to configure the `MetacardMapper` to be used with the sample data provided with GeoServer. This configuration shows a custom mapping for the feature type 'states'. For the given type, we are taking the feature property 'states.STATE\_NAME' and mapping it to the metacard attribute 'title'. In this particular case, since we mapped the state name to title in the metacard, it will now be fully searchable. More mappings can be added to the `featurePropToMetacardAttrMap` line through the use of comma as a delimiter.

Example **MetacardMapper** Configuration Within a **feature.xml** file:

```
<feature name="geoserver-states" version="2.13.10"
  description="WFS Feature to Metacard mappings for GeoServer Example
{http://www.openplans.org/topp}states">
  <config name="org.codice.ddf.spatial.ogc.wfs.catalog.mapper.MetacardMapper-
geoserver.http://www.openplans.org/topp.states">
    featureType = {http://www.openplans.org/topp}states
    featurePropToMetacardAttrMap = states.STATE_NAME=title
  </config>
</feature>
```

### 3.8.6. Federating Through a Registry

Another approach to configuring federation is to use the **Registry** application to locate sources in a network/enterprise. See [Registry Application Reference](#) for details on installing the Registry application. Use the registry to subscribe to and federate with other instances of DDF.

#### NOTE

The **Node Information** and **Remote Registries** tabs appear in both the Registry application and the Catalog application.

#### NOTE

For direct federation configuration, sources and registries can be configured at <https://{FQDN}:{PORT}/admin/federation>.

#### 3.8.6.1. Configuring Identity Node

The "Identity Node" is the local DDF instance. Configure the information to share with other registries/nodes.

1. Navigate to **Registry** (or **Catalog**) application.
2. Navigate to **Node Information** tab.
3. Click the name of the identity node.
4. Complete all *required* and any desired *optional* fields.
  - a. Add any desired [service bindings](#) under the [Services](#) tab.
5. Click **Save**.

Table 11. General Information Tab

Field	Description	Type	Required
Node Name	This node's name as it should appear to external systems	string	yes

Field	Description	Type	Required
Node Description	Short description for this node	string	yes
Node Version	This node's Version	string	yes
Security Attributes	Security attributes associated with this node.	String	
Last Updated	Date this entry's data was last updated	Date	
Live Date	Date indicating when this node went live or operational	Date	
Custom Fields	click <b>Add</b> button to add custom fields	Configurable	no
Associations	click <b>Add</b> button to add associations	Configurable	no

Table 12. Services

Field	Description	Type	Required
Service Name	This service name	string	
Service Description	Short description for this service	string	
Service Version	This service version	string	
Service Type	Identifies the type of service this is by a URN.	string	
Bindings (Click <b>Add</b> to add a service binding)			
Binding Name	This binding name	String	yes
Binding Description	Short description for this binding	String	
Binding Version	This binding version		
Access URL	The URL used to access this binding		
Service Binding Type	The binding type for the service		
URL Property Key	Property that the accessURL value should be put into for source creation		
Custom Fields	click <b>Add</b> button to add custom fields	Configurable	no
Associations	click <b>Add</b> button to add associations	Configurable	no

Table 13. Organizations Tab (click **Add** to add an organization)

Field	Description	Type	Required
Organization Name	This organization's name	string	yes
Address	This organization's primary address	Expand to enter address information	yes
Telephone Number	Primary contact number for this organization		no
Email	Primary contact email for this organization		no
Custom Fields	click <b>Add</b> button to add custom fields	Configurable	no
Associations	click <b>Add</b> button to add associations	Configurable	no

Table 14. Contacts (click **Add** button to add contact info)

Field	Description	Type	Required
Contact Title	Contact Title	String	yes
Contact First Name	Contact First Name	String	yes
Contact Last Name	Contact Last Name	String	yes
Address	Address for listed contact	String	minimum one
Phone number	Contact phone number		minimum one
Email	Contact email	String	minimum one
Custom Fields	click <b>Add</b> button to add custom fields	Configurable	no
Associations	click <b>Add</b> button to add associations	Configurable	no

Table 15. Collections (Click **Add** to add Content Collection(s))

Field	Description	Type	Required
Content Name	Name for this metadata content	string	yes
Content Description	Short description for this metadata content	string	no
Content Object Type	The kind of content object this will be. Default value should be used in most cases.	string	yes
Custom Fields	click <b>Add</b> button to add custom fields	Configurable	no
Associations	click <b>Add</b> button to add associations	Configurable	no

#### 3.8.6.1.1. Adding a Service Binding to a Node

Advertise the methods other nodes use to connect to the local DDF instance.

1. Navigate to Admin Console.
  2. Select Registry or Catalog.
    - a. (**Node Information** tab is editable from either application.)
  3. Click the name of the desired local node.
  4. Click the **Services** tab.
  5. Click **Add** to add a service.
  6. Expand new Service.
  7. Enter Service name and details.
  8. Click **Add** to add binding.
  9. Select Service Binding type.
    - a. Select one of the defaults or *empty* for a custom service binding.
    - b. If selecting *empty*, fill in all required fields.
  10. Click Save.
- 

#### 3.8.6.2. Publishing to Other Nodes

Send details about the local DDF instance to other nodes.

1. Navigate to the **Remote Registries** tab in either Registry or Catalog application.
  2. Click **Add** to add a remote registry.
  3. Enter Registry Service (CSW) URL.
  4. Confirm **Allow Push** is checked.
  5. Click **Add** to save the changes.
  6. Navigate to the **Sources** Tab in Catalog App
  7. Click desired node to be published.
  8. Under **Operations**, click the *\*Publish to ... \** link that corresponds to the desired registry.
- 

#### 3.8.6.3. Subscribing to Another Node

Receive details about another node.

1. Navigate to the **Remote Registries** tab in either Registry or Catalog application.
-

2. Click **Add** to add a remote registry.
3. Add the URL to access node.
4. Enter any needed credentials in the Username/password fields.
5. Click **Save/Add**.

#### *Editing a Subscription*

Update the configuration of an existing subscription.

1. Navigate to the **Remote Registries** tab in either Registry or Catalog application.
2. Click the name of the desired subscription.
3. Make changes.
4. Click **Save**.

#### *Deleting a Subscription*

Remove a subscription.

1. Click the **Delete** icon at the top of the **Remote Registries** tab.
2. Check the boxes of the Registry Nodes to be deleted.
3. Select the **Delete** button.

---

## 3.9. Environment Hardening

- **Required Step for Security Hardening**

### **IMPORTANT**

It is recommended to apply the following security mitigations to the DDF.

### 3.9.1. Known Issues with Environment Hardening

The session timeout should be configured longer than the UI polling time or you may get session timeout errors in the UI.

Protocol/ Type	Risk	Mitigation
JMX	tampering, information disclosure, and unauthorized access	<ul style="list-style-type: none"><li>• Stop the management feature using the command line console: <code>feature:stop management</code>.</li></ul>

File System Access	tampering, information disclosure, and denial of service	<p>Set OS File permissions under the &lt;DDF_HOME&gt; directory (e.g. /deploy, /etc) to ensure unauthorized viewing and writing is not allowed.</p> <div>If Caching is installed:</div> <ul style="list-style-type: none"> <li>• Set permissions for the installation directory /data/product-cache such that only the DDF process and users with the appropriate permissions can view any stored product.</li> <li>• Caching can be turned off as well to mitigate this risk. <ul style="list-style-type: none"> <li>◦ To disable caching, navigate to Admin Console.</li> <li>◦ Select the <b>Catalog</b> application.</li> <li>◦ Select <b>Resource Download Settings</b>.</li> <li>◦ Uncheck the <b>Enable Product Caching</b> box.</li> </ul> </li> <li>• Install Security to ensure only the appropriate users are accessing the products. <ul style="list-style-type: none"> <li>◦ Navigate to the Admin Console</li> <li>◦ Select <b>Manage</b>.</li> <li>◦ Install the Security application, if applicable.</li> </ul> </li> <li>• Cached files are written by the user running the DDF process/application.</li> </ul> <p>On system: ensure that not everyone can change ACLs on your object.</p>
--------------------	--	---



SSH	tampering, information disclosure, and denial of service	<p>By default, SSH access to DDF is only enabled to connections originating from the same host running DDF. For remote access to DDF, first establish an SSH session with the host running DDF. From within that session, initiate a new SSH connection (to <b>localhost</b>), and use the <b>sshPort</b> as configured in the file <code>&lt;DDF_HOME&gt;/etc/org.apache.karaf.shell.cfg</code>.</p> <p>To allow direct remote access to the DDF shell from any host, change the value of the <b>sshHost</b> property to <code>0.0.0.0</code> in the <code>&lt;DDF_HOME&gt;/etc/org.apache.karaf.shell.cfg</code> file.</p> <p>SSH can also be authenticated and authorized through an external Realm, such as LDAP. This can be accomplished by editing the <code>&lt;DDF_HOME&gt;/etc/org.apache.karaf.shell.cfg</code> file and setting the value for <b>sshRealm</b>, e.g. to <code>ldap</code>. No restart of DDF is necessary after this change.</p> <p>By definition, all connections over SSH will be authenticated and authorized and secure from eavesdropping.</p> <div data-bbox="711 1014 862 1045"> <p><b>WARNING</b></p> </div> <div data-bbox="922 915 1458 1157"> <p>Enabling SSH will expose your file system such that any user with access to your DDF shell will have read/write/execute access to all directories and files accessible to your installation user.</p> </div> <div data-bbox="922 1199 1458 1356"> <p><b>Because of this, SSH is not recommended in a secure environment and should be turned off in a fully hardened system.</b></p> </div> <p>Set <code>karaf.shutdown.port=-1</code> in <code>&lt;DDF_HOME&gt;/etc/custom.properties</code> or <code>&lt;DDF_HOME&gt;/etc/config.properties</code>.</p>
-----	--	--

SSL/TLS	man-in-the-middle, information disclosure	<p>Update the <code>&lt;DDF_HOME&gt;/etc/org.ops4j.pax.web.cfg</code> file to add the entry <code>org.ops4j.pax.web.ssl.clientauthneeded=true</code>.</p> <div> <p><b>WARNING</b></p> <p>Setting this configuration may break compatibility to legacy systems that do not support two-way SSL.</p> </div> <div> <p><b>WARNING</b></p> <p>Setting this configuration will require a certificate to be installed in the browser.</p> </div>
Session Inactivity Timeout	unauthorized access	<p>Update the Session configuration to have no greater than a 10 minute Session Timeout.</p> <ul style="list-style-type: none"> <li>• Navigate to the <b>Admin Console</b>.</li> <li>• Select the <b>Security</b> application.</li> <li>• Select the <b>Configuration</b> tab.</li> <li>• Select <b>Session</b>.</li> <li>• Set <b>Session Timeout (in minutes)</b> to <b>10</b> (or less).</li> </ul>

Shell Command Access	command injection	<p>By default, some shell commands are disabled in order to secure the system. DDF includes a whitelist of allowed shell commands in <code>&lt;DDF_HOME&gt;/etc/org.apache.karaf.command.acl.shell.cfg</code>.</p> <p>By default, this list includes commands that are whitelisted only to administrators:</p> <ul style="list-style-type: none"> <li>• <code>complete</code></li> <li>• <code>echo</code></li> <li>• <code>format</code></li> <li>• <code>grep</code></li> <li>• <code>if</code></li> <li>• <code>keymap</code></li> <li>• <code>less</code></li> <li>• <code>set</code></li> <li>• <code>setopt</code></li> <li>• <code>sleep</code></li> <li>• <code>tac</code></li> <li>• <code>wc</code></li> <li>• <code>while</code></li> <li>• <code>.invoke</code></li> <li>• <code>unsetopt</code></li> </ul>
----------------------------	-------------------	---

## 3.10. Configuring for Special Deployments

In addition to standard configurations, several specialized configurations are possible for specific uses of DDF.

### 3.10.1. Multiple Installations

One common specialized configuration is installing multiple instances of DDF.

#### 3.10.1.1. Reusing Configurations

The Migration Export/Import capability allows administrators to export the current DDF configuration and use it to restore the same state for either a brand new installation or a second node for a Highly Available Cluster.

To export the current configuration settings:

1. Run the command `migration:export` from the Command Console.

- Files named `ddf-2.13.10.dar`, `ddf-2.13.10.dar.key`, and `ddf-2.13.10.dar.sha256` will be created in the `exported` directory underneath `<DDF_HOME>`. The `.dar` file contains the encrypted information. The `.key` and `.sha256` files contain the encryption key and a validation checksum. Copy the `.dar` file to a secure location and copy the `.key` and `.sha256` to a different secure location. Keeping all 3 files together represents a security risk and should be avoided.

To import previously exported configuration settings:

- Install DDF by unzipping its distribution.
- Restore all external files, softlinks, and directories that would not have been exported and for which warnings would have been generated during export. This could include (but is not limited to) external certificates or monitored directories.
- Launch the newly installed DDF.
- Make sure to install and re-enable the DDF `service` on the new system if it was installed and enabled on the original system.
- Copy the previously exported files from your secure locations to the `exported` directory underneath `<DDF_HOME>`.
- Either:
  - Step through the installation process.
  - Run the command `migration:import` from the Command Console.
- Or if an administrator wishes to restore the original profile along with the configuration (experimental):
  - Run the command `migration:import` with the option `--profile` from the Command Console.
- DDF will automatically restart if the command is successful. Otherwise address any generated warnings before manually restarting DDF.
- Finish `hardening` the system (e.g. file and directory permissions).

It is possible to decrypt the previously exported configuration settings but doing so is insecure and appropriate measures should be taken to secure the resulting decrypted file. To decrypt the exported file:

- Copy all 3 exported files (i.e. `.dar`, `.key`, and `.sha256`) to the `exported` directory underneath `<DDF_HOME>`.
- Run the command `migration:decrypt` from the Command Console.
- A file named `ddf-2.13.10.zip` will be created in the `exported` directory underneath `<DDF_HOME>`. This file represents the decrypted version of the `.dar` file.

## IMPORTANT

- The following is currently not supported when importing configuration files:
  - importing from a different DDF version
  - importing from a system installed on a different OS
  - importing from a system installed in a different directory location
- To keep the export/import process simple and consistent, all system configuration files are required to be under the `<DDF_HOME>` directory and not be softlinks. Presence of external files or symbolic links during export will not fail the export; they will yield warnings. It will be up to the administrator to manually copy these files over to the new system before proceeding with the import. The import process will verify their presence and consistency and yield warnings if they don't match the original files.
- The import process will restore all configurations done on the original system as part of the [hardening process](#) including changes to starting scripts and certificates.
- The import process can also restore the profile from the original system by restoring all applications, features, and/or bundles to the same state (i.e., installed, uninstalled, started, stopped, ...) they were in originally. Doing so is currently experimental and was tested only with the standard and HA profiles.

---

### 3.10.1.2. Isolating Solr Cloud and Zookeeper

- **Required Step for Security Hardening** (if using Solr Cloud/Zookeeper)

Zookeeper cannot use secure (SSL/TLS) connection. The configuration information that Zookeeper sends and receives is vulnerable to network sniffing. Also, the connections between the local Solr Catalog service and the Solr Cloud is not necessarily secure. The connections between Solr Cloud nodes are not necessarily secure. Any unencrypted network traffic is vulnerable to sniffing attacks. To use Solr Cloud and Zookeeper securely, these processes must be isolated on the network, or their communications must be encrypted by other means. The DDF process must be visible on the network to allow authorized parties to interact with it.

*Examples of Isolation:*

- Create a private network for Solr Cloud and Zookeeper. Only DDF is allowed to contact devices inside the private network.
- Use IPsec to encrypt the connections between DDF, Solr Cloud nodes, and Zookeeper nodes.
- Put DDF, Solr Cloud and Zookeeper behind a firewall that only allows access to DDF.

### 3.10.2. Configuring for a Fanout Proxy

Optionally, configure DDF as a fanout proxy such that only queries and resource retrieval requests are processed and create/update/delete requests are rejected. All queries are enterprise queries and no catalog provider needs to be configured.

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select the **Configuration** tab.
4. Select **Catalog Standard Framework**.
5. Select **Enable Fanout Proxy**.
6. Save changes.

DDF is now operating as a fanout proxy. Only queries and resource retrieval requests will be allowed. All queries will be federated. Create, update, and delete requests will not be allowed, even if a Catalog Provider was configured prior to the reconfiguration as a fanout.

### 3.10.3. Standalone Security Token Service (STS) Installation

To run a STS-only DDF installation, uninstall the catalog components that are not being used. The following list displays the features that can be uninstalled to minimize the runtime size of DDF in an STS-only mode. This list is not a comprehensive list of every feature that can be uninstalled; it is a list of the larger components that can be uninstalled without impacting the STS functionality.

*Unnecessary Features for Standalone STS*

- `catalog-core-standardframework`
- `catalog-opensearch-endpoint`
- `catalog-opensearch-source`
- `catalog-rest-endpoint`

### 3.10.4. Configuring for a Highly Available Cluster

This section describes how to make configuration changes after the initial setup for a DDF in a [Highly Available Cluster](#).

In a Highly Available Cluster, configuration changes must be made on both DDF nodes. The changes can still be made in the standard ways via the [Admin Console](#), the [Command Line](#), or the [file system](#).

Changes made in the Admin Console must be made through the HTTP proxy. This means that the below steps should be followed to make a change in the Admin Console:

**NOTE**

- Make a configuration change on the currently active DDF node
- Shut down the active DDF node, making the failover proxy switch to the standby DDF node
- Make the same configuration change on the newly active DDF node
- Start the DDF node that was just shut down

## 3.11. Configuring UI Themes

The optional configurations in this section cover minor changes that can be made to optimize DDF appearance.

### 3.11.1. Landing Page

The Landing Page is the first page presented to users of DDF. It is customizable to allow adding organizationally-relevant content.

#### 3.11.1.1. Installing the Landing Page

The Landing Page is installed by default with a standard installation.

#### 3.11.1.2. Configuring the Landing Page

The DDF landing page offers a starting point and general information for a DDF node. It is accessible at `/(index|home|landing(.htm|html))`.

#### 3.11.1.3. Customizing the Landing Page

Configure the Landing Page from the Admin Console:

1. Navigate to the **Admin Console**.
2. Select **Platform** Application.
3. Select **Configuration** tab.
4. Select **Landing Page**.

Configure important landing page items such as branding logo, contact information, description, and additional links.

See [Landing Page configurations](#) for all possible configurations.

### 3.11.2. Configuring Logout Page

The logout page is presented to users through the navigation of DDF and has a changeable timeout value.

1. Navigate to the **Admin Console**.
2. Select **Security** Application.
3. Select **Configuration** tab.
4. Select **Logout Page**.

The customizable feature of the logout page is the **Logout Page Time Out**. This is the time limit the IDP client will wait for a user to click log out on the logout page. Any requests that take longer than this time for the user to submit will be rejected.

1. **Default value:** 3600000 (milliseconds)

See [Logout Configuration](#) for detailed information.

### 3.11.3. Platform UI Themes

The Platform UI Configuration allows for the customization of attributes of all pages within DDF. It contains settings to display messages to users at login or in banners in the headers and footers of all pages, along with changing the colors of text and backgrounds.

#### 3.11.3.1. Navigating to UI Theme Configuration

1. Navigate to the **Admin Console**.
2. Select the **Platform** application.
3. Select **Configuration**.
4. Select **Platform UI Configuration**.

#### 3.11.3.2. Customizing the UI Theme

The customization of the UI theme across DDF is available through the capabilities of Platform UI Configuration. The banner has four items to configure:

1. **Header** (text)
2. **Footer** (text)
3. **Text Color**
4. **Background Color**

See the [Platform UI](#) for all possible configurations of the Platform UI Configuration.



## 3.12. Miscellaneous Configurations

The optional configurations in this section cover minor changes that can be made to optimize DDF.

### 3.12.1. Configuring Thread Pools

The `org.codice.ddf.system.threadPoolSize` property can be used to specify the size of thread pools used by:

- Federating requests between DDF systems
- Downloading resources
- Handling asynchronous queries, such as queries from the UI

By default, this value is set to 128. It is not recommended to set this value extremely high. If unsure, leave this setting at its default value of 128.


### 3.12.2. Configuring Jetty ThreadPool Settings

To prevent resource shortages in the event of concurrent requests, DDF allows configuring Jetty ThreadPool settings to specify the minimum and maximum available threads.

1. The settings can be changed at `etc/org.ops4j.pax.web.cfg` under Jetty Server ThreadPool Settings.
2. Specify the maximum thread amount with `org.ops4j.pax.web.server.maxThreads`
3. Specify the minimum thread amount with `org.ops4j.pax.web.server.minThreads`
4. Specify the allotted time for a thread to complete with `org.ops4j.pax.web.server.idleTimeout`

DDF does not support changing ThreadPool settings from the Command Console or the Admin Console.

### 3.12.3. Configuring Alerts

By default, DDF uses two services provided by Karaf Decanter for alerts that can be configured by configuration file. Further information on Karaf Decanter services and configurations can be found [here](#) .

#### 3.12.3.1. Configuring Decanter Service Level Agreement (SLA) Checker

The Decanter SLA Checker provides a way to create alerts based on configurable conditions in events posted to `decanter/collect/*` and can be configured by editing the file `<DDF_HOME>/etc/org.apache.karaf.decanter.sla.checker.cfg`. By default there are only two checks that will produce alerts, and they are based on the `SystemNotice` event property of `priority`.

*Table 16. Decanter SLA Configuration*

Property	Alert Level	Expression	Description
priority	warn	equal:1,2,4	Produce a warn level alert if priority is important (3)
priority	error	equal:1,2,3	Produce an error level alert if priority is critical (4)

### 3.12.3.2. Configuring Decanter Scheduler

The Decanter Scheduler looks up services implementing the Runnable interface with the service-property `decanter.collector.name` and executes the Runnable periodically. The Scheduler can be configured by editing the file `<DDF_HOME>/etc/org.apache.karaf.decanter.scheduler.simple.cfg`.

Table 17. Decanter Scheduler Configuration

Property Name	Description	Default Value
period	Decanter simple scheduler period (milliseconds)	300000 (5 minutes)
threadIdleTimeout	The time to wait before stopping an idle thread (milliseconds)	60000 (1 minute)
threadInitCount	Initial number of threads created by the scheduler	5
threadMaxCount	Maximum number of threads created by the scheduler	200

## 4. Running

Find directions here for running an installation of DDF.

### Starting

Getting an instance of DDF up and running.

### Managing Services

Running DDF as a managed service.

### Maintaining

Keeping DDF running with useful tasks.

### Monitoring

Tracking system health and usage.

### Troubleshooting

Common tips for unexpected behavior.

## 4.1. Starting

### 4.1.1. Run DDF as a Managed Service

#### 4.1.1.1. Running as a Service with Automatic Start on System Boot

Because DDF is built on top of Apache Karaf, DDF can use the Karaf Wrapper to run DDF as a service and enable automatic startup and shutdown. When DDF is started using Karaf Wrapper, new `wrapper.log` and `wrapper.log.n` (where `n` goes from 1 to 5 by default) log files will be generated to include wrapper and console specific information.

<b>WARNING</b>	When installing as a service on *NIX, do not use spaces in the path for <code>&lt;DDF_HOME&gt;</code> as the service scripts that are generated by the wrapper cannot handle spaces.
<b>WARNING</b>	Ensure that <code>JAVA_HOME</code> is properly set before beginning this process. See <a href="#">Java Requirements</a>

1. Create the service wrapper.

DDF can create native scripts and executable files to run itself as an operating system service. This is an optional feature that is not installed by default. To install the service wrapper feature, go the DDF console and enter the command:

```
ddf@local> feature:install -r wrapper
```

2. Generate the script, configuration, and executable files:

*\*NIX*

```
ddf@local> wrapper:install -i setenv-wrapper.conf -n ddf -d ddf -D "DDF Service"
```

*Windows*

```
ddf@local> wrapper:install -i setenv-windows-wrapper.conf -n ddf -d ddf -D "DDF Service"
```

3. (Windows users skip this step) (All \*NIX) If DDF was installed to run as a non-root user (as-recommended,) edit `<DDF_HOME>/bin/ddf-service` and change the property `#RUN_AS_USER=` to:

`<DDF_HOME>/bin/ddf-service`

```
RUN_AS_USER=<ddf-user>
```

where <ddf-user> is the intended username:

4. (Windows users skip down) (All \*NIX) Edit <DDF\_HOME>/bin/ddf-service. Add LimitNOFILE to the [Service] section.

<DDF\_HOME>/bin/ddf.service

```
LimitNOFILE=6815744
```

5. (Windows users skip this step) (\*NIX with systemd) Install the wrapper startup/shutdown scripts.

Install the service and start it when the system boots, use systemctl From an OS console, execute:

```
root@localhost# systemctl enable <DDF_HOME>/bin/ddf.service
```

6. (Windows users skip this step) (\*NIX without systemd) Install the wrapper startup/shutdown scripts.

If the system does not use systemd, use the init.d system to install and configure the service. Execute these commands as root or superuser:

```
root@localhost# ln -s <DDF_HOME>/bin/ddf-service /etc/init.d/  
root@localhost# chkconfig ddf-service --add  
root@localhost# chkconfig ddf-service on
```

7. (Windows only, if the system's JAVA\_HOME variable has spaces in it) Edit <DDF\_HOME>/etc/ddf-wrapper.conf. Put quotes around wrapper.java.additional.n system properties for n from 1 to 13 like so:

<DDF\_HOME>/etc/ddf-wrapper.conf

```
wrapper.java.additional.1=-
Djava.endorsed.dirs="%JAVA_HOME%/jre/lib/endorsed;%JAVA_HOME%/lib/endorsed;%KARAF_HOME%/lib/endorsed"
wrapper.java.additional.2=-
Djava.ext.dirs="%JAVA_HOME%/jre/lib/ext;%JAVA_HOME%/lib/ext;%KARAF_HOME%/lib/ext"
wrapper.java.additional.3=-Dkaraf.instances="%KARAF_HOME%/instances"
wrapper.java.additional.4=-Dkaraf.home="%KARAF_HOME%"
wrapper.java.additional.5=-Dkaraf.base="%KARAF_BASE%"
wrapper.java.additional.6=-Dkaraf.data="%KARAF_DATA%"
wrapper.java.additional.7=-Dkaraf.etc="%KARAF_ETC%"
wrapper.java.additional.8=-Dkaraf.restart.jvm.supported=true
wrapper.java.additional.9=-Djava.io.tmpdir="%KARAF_DATA%/tmp"
wrapper.java.additional.10=-
Djava.util.logging.config.file="%KARAF_BASE%/etc/java.util.logging.properties"
wrapper.java.additional.11=-Dcom.sun.management.jmxremote
wrapper.java.additional.12=-Dkaraf.startLocalConsole=false
wrapper.java.additional.13=-Dkaraf.startRemoteShell=true
```


#### 8. (Windows only) Install the wrapper startup/shutdown scripts.

Run the following command in a console window. The command must be run with elevated permissions.

```
<DDF_HOME>\bin\ddf-service.bat install
```

Startup and shutdown settings can then be managed through **Services** → **MMC Start** → **Control Panel** → **Administrative Tools** → **Services**.

#### 4.1.1.2. Karaf Documentation

Because DDF is built on top of Apache Karaf, more information on operating DDF can be found in the [Karaf documentation](#) .

## 4.2. Managed Services

The lifecycle of DDF and Solr processes can be managed by the operating system. The DDF documentation provides instructions to install DDF as a managed services on supported unix platforms. However, the documentation cannot account for all possible configurations. Please consult the documentation for the operating system and its init manager if the instructions in this document are inadequate.

- [Configure Solr to run as a managed service](#)

- [Configure DDF to run as a managed service](#)

### 4.2.1. Run Solr as Managed Service

These instructions are for configuring Solr as a service managed by the operating system.

#### 4.2.1.1. Configure Solr as a Windows Service

Windows users can use the **Task Scheduler** to start Solr as a background process.

1. If DDF is running, stop it.
2. Edit `<DDF_HOME>/etc/custom.system.properties` and set `start.solr=false`. This prevents the DDF scripts from attempting to manage Solr's lifecycle.
3. Start the **Windows Task Scheduler** and open the **Task Scheduler Library**.
4. Under the Actions pane, select **Create Basic Task....**
5. Provide a useful name and description, then select **Next**.
6. Select **When the computer starts** as the Trigger and select **Next**.
7. Select **Start a program** as the Action and select **Next**.
8. Select the script to start Solr:

```
<DDF_HOME>\bin\ddfsolr.bat
```

9. Add the argument `start` in the window pane and select **Next**.
10. Review the settings and select **Finish**.

It may be necessary to update the **Security Options** under the task **Properties** to **Run with highest privileges** or setting user to "SYSTEM".

Additionally, the process can be set to restart if it fails. The option can be found in the the **Properties > Settings** tab.

Depending on the system it may also make sense to delay the process from starting for a few minutes until the machine has fully booted. Open the task's **Properties** settings and

- a. Select **Triggers**.
- b. Select **Edit**.
- c. Select **Advanced Settings**.
- d. Select **Delay Task**.

#### 4.2.1.2. Configure Solr as a Systemd Service

These instructions are for unix operating systems running the systemd init manager. If configuring a Windows system, see [Configure Solr as a Windows Service](#)

1. If DDF is running, stop it.
2. Edit `<DDF_HOME>/etc/custom.system.properties` and set `start.solr=false`.
3. Edit the file `<DDF_HOME>/solr/services/solr.service`
  - a. Edit the property `Environment=JAVA_HOME` and replace `<JAVA_HOME>` with the absolute path to the directory where the Java Runtime Environment is installed.
  - b. Edit the property `ExecStart` and replace `<DDF_HOME>` with the absolute path to the `ddfsolr` file.
  - c. Edit the property `ExecStop` and replace `<DDF_HOME>` with the absolute path to the `ddfsolr` file.
  - d. Edit the property `User` and replace `<USER>` with the user ID of the Solr process owner.
4. From the operating system command line, enable a Solr service using a provided configuration file. Use the full path to the file.

```
systemctl enable <DDF_HOME>/solr/service/solr.service
```

5. Start the service.

```
systemctl start solr
```

6. Check the status of Solr

```
systemctl status solr
```

Solr will start automatically each time the system is booted.

Follow the below steps to start and stop DDF.

#### 4.2.2. Starting from Startup Scripts

Run one of the start scripts from a command shell to start the distribution and open a local console:

*Start Script: \*NIX*

```
<DDF_HOME>/bin/ddf
```

*Start Script: Windows*

```
<DDF_HOME>/bin/ddf.bat
```

### 4.2.3. Starting as a Background Process

Alternatively, to run DDF as a background process, run the **start** script:

*\*NIX*

```
<DDF_HOME>/bin/start
```

*Windows*

```
<DDF_HOME>/bin/start.bat
```

If console access is needed while running as a service, run the **client** script on the host where the DDF is running:

*\*NIX*

```
<DDF_HOME>/bin/client
```

**NOTE**

*Windows*

```
<DDF_HOME>/bin/client.bat -h <FQDN>
```

Use the **-h** option followed by the name (**<FQDN>**) or IP of the host where DDF is running.  
U

### 4.2.4. Stopping DDF

There are two options to stop a running instance:

- Call shutdown from the console:

*Shut down with a prompt*

```
ddf@local>shutdown
```

*Force Shutdown without prompt*

```
ddf@local>shutdown -f
```



- Keyboard shortcut for shutdown
  - **Ctrl-D**
  - **Cmd-D**
- Or run the stop script:

*\*NIX*

```
<DDF_HOME>/bin/stop
```

*Windows*

```
<DDF_HOME>/bin/stop.bat
```

#### IMPORTANT

##### *Shut Down*

Do not shut down by closing the window (Windows, Unix) or using the **kill -9** **<pid>** command (Unix). This prevents a clean shutdown and can cause significant problems when DDF is restarted. Always use the shutdown command or the shortcut from the command line console.

## 4.3. Maintaining

### 4.3.1. Console Commands

Once the distribution has started, administrators will have access to a powerful command line console, the Command Console. This Command Console can be used to manage services, install new features, and manage the state of the system.

The Command Console is available to the user when the distribution is started manually or may also be accessed by using the **bin/client.bat** or **bin/client** scripts.

#### NOTE

The majority of functionality and information available on the Admin Console is also available on the Command Line Console.

#### 4.3.1.1. Console Command Help

For details on any command, type **help** then the command. For example, **help search** (see results of this command in the example below).

## Example Help

```
ddf@local>help search
DESCRIPTION
    catalog:search
    Searches records in the catalog provider.
SYNTAX
    catalog:search [options] SEARCH_PHRASE [NUMBER_OF_ITEMS]
ARGUMENTS
    SEARCH_PHRASE
        Phrase to query the catalog provider.
    NUMBER_OF_ITEMS
        Number of maximum records to display.
        (defaults to -1)
OPTIONS
    --help
        Display this help message
    case-sensitive, -c
        Makes the search case sensitive
    -p, -provider
        Interacts with the provider directly instead of the framework.
```

The **help** command provides a description of the provided command, along with the syntax in how to use it, arguments it accepts, and available options.

### 4.3.1.2. CQL Syntax

The CQL syntax used with console commands should follow the OGC CQL format. GeoServer provides a description of the grammar and examples in this [CQL Tutorial](#).

#### CQL Syntax Examples

```
Finding all notifications that were sent due to a download:
ddf@local>store:list --cql "application='Downloads'" --type notification

Deleting a specific notification:
ddf@local>store:delete --cql "id='fdc150b157754138a997fe7143a98cfa'" --type notification
```

### 4.3.1.3. Available Console Commands

Many console commands are available, including DFF commands and the core Karaf console commands. For more information about these core Karaf commands and using the console, see the Commands documentation for Karaf 4.2.1 at [Karaf documentation](#).

For a complete list of all available commands, from the Command Console, press **TAB** and confirm when prompted.

Console commands follow a format of `namespace:command`.

To get a list of commands, type in the namespace of the desired extension then press **TAB**.

For example, type `catalog`, then press **TAB**.

Table 18. DDF Console Command Namespaces

Namespace	Description
<code>catalog</code>	The Catalog Shell Commands are meant to be used with any <code>CatalogProvider</code> implementations. They provide general useful queries and functions against the Catalog API that can be used for debugging, printing, or scripting.
<code>subscription</code>	The DDF PubSub shell commands provide functions to list the registered subscriptions in DDF and to delete subscriptions.
<code>platform</code>	The DDF Platform Shell Commands provide generic platform management functions
<code>store</code>	The Persistence Shell Commands are meant to be used with any <code>PersistentStore</code> implementations. They provide the ability to query and delete entries from the persistence store.

#### 4.3.1.3.1. Catalog Commands

##### WARNING

Most commands can bypass the Catalog framework and interact directly with the Catalog provider if given the `--provider` option, if available. No pre/post plugins are executed and no message validation is performed if the `--provider` option is used.

Table 19. Catalog Command Descriptions

Command	Description
<code>catalog:describe</code>	Provides a basic description of the Catalog implementation.
<code>catalog:dump</code>	Exports metacards from the local Catalog. Does not remove them. See <a href="#">date filtering options</a> below.
<code>catalog:envlist</code>	<div><b>IMPORTANT</b>      Deprecated as of ddf-catalog 2.5.0. Please use <code>platform:envlist</code>.</div> <div>Provides a list of environment variables.</div>
<code>catalog:export</code>	Exports Metacards and history from the current Catalog.
<code>catalog:import</code>	Imports Metacards and history into the current Catalog.

Command	Description
<code>catalog:ingest</code>	Ingests data files into the Catalog. XML is the default transformer used. See <a href="#">Ingest Command</a> for detailed instructions on ingesting data and <a href="#">Input Transformers</a> for all available transformers.
<code>catalog:inspect</code>	Provides the various fields of a metacard for inspection.
<code>catalog:latest</code>	Retrieves the latest records from the Catalog based on the Core.METACARD_MODIFIED date.
<code>catalog:migrate</code>	Allows two <code>CatalogProvider</code> s to be configured and migrates the data from the primary to the secondary.
<code>catalog:range</code>	Searches by the given range arguments (exclusively).
<code>catalog:remove</code>	Deletes a record from the local Catalog.
<code>catalog:removeall</code>	Attempts to delete all records from the local Catalog.
<code>catalog:replicate</code>	Replicates data from a federated source into the local Catalog.
<code>catalog:search</code>	Searches records in the local Catalog.
<code>catalog:spatial</code>	Searches spatially the local Catalog.
<code>catalog:transformers</code>	Provides information on available transformers.
<code>catalog:validate</code>	Validates an XML file against all installed validators and prints out human readable errors and warnings.

### *catalog:dump Options*

The `catalog:dump` command provides selective export of metacards based on date ranges. The `--created-after` and `--created-before` options allow filtering on the date and time that the metacard was created, while `--modified-after` and `--modified-before` options allow filtering on the date and time that the metacard was last modified (which is the created date if no other modifications were made). These date ranges are exclusive (i.e., if the date and time match exactly, the metacard will not be included). The date filtering options (`--created-after`, `--created-before`, `--modified-after`, and `--modified-before`) can be used in any combination, with the export result including only metacards that match all of the provided conditions.

If no date filtering options are provided, created and modified dates are ignored, so that all metacards match.

### *Date Syntax*

Supported dates are taken from the common subset of ISO8601, matching the datetime from the following syntax:

```
datetime      = time | date-opt-time
time          = 'T' time-element [offset]
date-opt-time = date-element ['T' [time-element] [offset]]
date-element  = std-date-element | ord-date-element | week-date-element
std-date-element = yyyy ['- MM ['- dd]]
ord-date-element = yyyy ['- DDD]
week-date-element = xxxx '-W' ww ['- e]
time-element   = HH [minute-element] | [fraction]
minute-element = ':' mm [second-element] | [fraction]
second-element = ':' ss [fraction]
fraction       = ('.' | ',') digit+
offset         = 'Z' | (('+' | '-') HH [':' mm [':' ss [('.') | ',') SSS]]]
```

### *catalog:dump Examples*

```
ddf@local>// Given we've ingested a few metacards
ddf@local>catalog:latest
#      ID                                     Modified Date                Title
1      a6e9ae09c792438e92a3c9d7452a449f    2019-06-14 03:38:38:947
2      b4aced45103a400da42f3b319e58c3ed    2019-06-14 03:38:38:947
3      a63ab22361e14cee9970f5284e8eb4e0    2019-06-14 03:38:38:947 myTitle

ddf@local>// Filter out older files
ddf@local>catalog:dump --created-after 2019-06-14 03:38:38:947 /home/user/ddf-catalog-
dump
1 file(s) dumped in 0.015 seconds

ddf@local>// Filter out new file
ddf@local>catalog:dump --created-before 2019-06-14 03:38:38:947 /home/user/ddf-catalog-
dump
2 file(s) dumped in 0.023 seconds

ddf@local>// Choose middle file
ddf@local>catalog:dump --created-after 2019-06-14 03:38:38:947 /home/user/ddf-catalog-
dump
1 file(s) dumped in 0.020 seconds

ddf@local>// Modified dates work the same way
ddf@local>catalog:dump --modified-after 2019-06-14 03:38:38:947 /home/user/ddf-catalog-
```

```

dump
1 file(s) dumped in 0.015 seconds

ddf@local>// Can mix and match, most restrictive limits apply
ddf@local>catalog:dump --modified-after 2019-06-14 03:38:38:947 /home/user/ddf-catalog-
dump
1 file(s) dumped in 0.024 seconds

ddf@local>// Can use UTC instead of (or in combination with) explicit time zone offset
ddf@local>catalog:dump --modified-after 2019-06-14 03:38:38:947 /home/user/ddf-catalog-
dump
2 file(s) dumped in 0.020 seconds
ddf@local>catalog:dump --modified-after 2019-06-14 03:38:38:947 /home/user/ddf-catalog-
dump
1 file(s) dumped in 0.015 seconds

ddf@local>// Can leave off time zone, but default (local time on server) may not match
what you expect!
ddf@local>catalog:dump --modified-after 2019-06-14 03:38:38:947 /home/user/ddf-catalog-
dump
1 file(s) dumped in 0.018 seconds

ddf@local>// Can leave off trailing minutes / seconds
ddf@local>catalog:dump --modified-after 2019-06-14 03:38:38:947 /home/user/ddf-catalog-
dump
2 file(s) dumped in 0.024 seconds

ddf@local>// Can use year and day number
ddf@local>catalog:dump --modified-after 2019-06-14 03:38:38:947 /home/user/ddf-catalog-
dump
2 file(s) dumped in 0.027 seconds

```

#### 4.3.1.3.2. Subscriptions Commands

**NOTE** The subscriptions commands are installed when the Catalog application is installed.

Table 20. Subscription Command Descriptions

Command	Description
<code>subscriptions:delete</code>	Deletes the subscription(s) specified by the search phrase or LDAP filter.
<code>subscriptions:list</code>	List the subscription(s) specified by the search phrase or LDAP filter.

#### *subscriptions:list Command Usage Examples*

Note that no arguments are required for the `subscriptions:list` command. If no argument is provided, all subscriptions will be listed. A count of the subscriptions found matching the list command's search phrase (or LDAP filter) is displayed first followed by each subscription's ID.

### *List All Subscriptions*

```
ddf@local>subscriptions:list
```

Total subscriptions found: 3

Subscription ID

my.contextual.id.v20|http://172.18.14.169:8088/mockCatalogEventConsumerBinding?WSDL

my.contextual.id.v30|http://172.18.14.169:8088/mockEventConsumerBinding?WSDL

my.contextual.id.json|http://172.18.14.169:8088/services/json/local/event/notification

### *List a Specific Subscription by ID*

```
ddf@local>subscriptions:list
```

```
"my.contextual.id.v20|http://172.18.14.169:8088/mockCatalogEventConsumerBinding?WSDL"
```

Total subscriptions found: 1

Subscription ID

my.contextual.id.v20|http://172.18.14.169:8088/mockCatalogEventConsumerBinding?WSDL

#### **WARNING**

It is recommended to always quote the search phrase (or LDAP filter) argument to the command so that any special characters are properly processed.

### List Subscriptions Using Wildcards

```
ddf@local>subscriptions:list "my*"
```

```
Total subscriptions found: 3
```

```
Subscription ID
```

```
my.contextual.id.v20|http://172.18.14.169:8088/mockCatalogEventConsumerBinding?WSDL
```

```
my.contextual.id.v30|http://172.18.14.169:8088/mockEventConsumerBinding?WSDL
```

```
my.contextual.id.json|http://172.18.14.169:8088/services/json/local/event/notification
```

```
ddf@local>subscriptions:list "*json*"
```

```
Total subscriptions found: 1
```

```
Subscription ID
```

```
my.contextual.id.json|http://172.18.14.169:8088/services/json/local/event/notification
```

```
ddf@local>subscriptions:list "*WSDL"
```

```
Total subscriptions found: 2
```

```
Subscription ID
```

```
my.contextual.id.v20|http://172.18.14.169:8088/mockCatalogEventConsumerBinding?WSDL
```

```
my.contextual.id.v30|http://172.18.14.169:8088/mockEventConsumerBinding?WSDL
```

The example below illustrates searching for any subscription that has "json" or "v20" anywhere in its subscription ID.

### List Subscriptions Using an LDAP Filter

```
ddf@local>subscriptions:list -f "(|(subscription-id=*json*) (subscription-id=*v20*))"
```

```
Total subscriptions found: 2
```

```
Subscription ID
```

```
my.contextual.id.v20|http://172.18.14.169:8088/mockCatalogEventConsumerBinding?WSDL
```

```
my.contextual.id.json|http://172.18.14.169:8088/services/json/local/event/notification
```

The example below illustrates searching for any subscription that has **json** and **172.18.14.169** in its subscription ID. This could be a handy way of finding all subscriptions for a specific site.



```
ddf@local>subscriptions:list -f "(&(subscription-id=*json*) (subscription-id=*172.18.14.169*))"
```

Total subscriptions found: 1

Subscription ID

my.contextual.id.json|http://172.18.14.169:8088/services/json/local/event/notification

### *subscriptions:delete Command Usage*

The arguments for the **subscriptions:delete** command are the same as for the **list** command, except that a search phrase or LDAP filter must be specified. If one of these is not specified an error will be displayed. When the **delete** command is executed it will display each subscription ID it is deleting. If a subscription matches the search phrase but cannot be deleted, a message in red will be displayed with the ID. After all matching subscriptions are processed, a summary line is displayed indicating how many subscriptions were deleted out of how many matching subscriptions were found.

### *Delete a Specific Subscription Using Its Exact ID*

```
ddf@local>subscriptions:delete  
"my.contextual.id.json|http://172.18.14.169:8088/services/json/local/event/notification"
```

Deleted subscription for ID =

my.contextual.id.json|http://172.18.14.169:8088/services/json/local/event/notification

Deleted 1 subscriptions out of 1 subscriptions found.

### *Delete Subscriptions Using Wildcards*

```
ddf@local>subscriptions:delete "my*"
```

Deleted subscription for ID =

my.contextual.id.v20|http://172.18.14.169:8088/mockCatalogEventConsumerBinding?WSDL

Deleted subscription for ID =

my.contextual.id.v30|http://172.18.14.169:8088/mockEventConsumerBinding?WSDL

Deleted 2 subscriptions out of 2 subscriptions found.

```
ddf@local>subscriptions:delete "*json*"
```

Deleted subscription for ID =

my.contextual.id.json|http://172.18.14.169:8088/services/json/local/event/notification

Deleted 1 subscriptions out of 1 subscriptions found.

## Delete All Subscriptions

```
ddf@local>subscriptions:delete *
```

Deleted subscription for ID =  
my.contextual.id.v30|http://172.18.14.169:8088/mockEventConsumerBinding?WSDL  
Deleted subscription for ID =  
my.contextual.id.v20|http://172.18.14.169:8088/mockCatalogEventConsumerBinding?WSDL  
Deleted subscription for ID =  
my.contextual.id.json|http://172.18.14.169:8088/services/json/local/event/notification

Deleted 3 subscriptions out of 3 subscriptions found.

## Delete Subscriptions Using an LDAP Filter

```
ddf@local>subscriptions:delete -f "(&(subscription-id=*WSDL) (subscription-id=*172.18.14.169*))"
```

Deleted subscription for ID =  
my.contextual.id.v20|http://172.18.14.169:8088/mockCatalogEventConsumerBinding?WSDL  
Deleted subscription for ID =  
my.contextual.id.v30|http://172.18.14.169:8088/mockEventConsumerBinding?WSDL

Deleted 2 subscriptions out of 2 subscriptions found.

### 4.3.1.3.3. Platform Commands

Table 21. Platform Command Descriptions

Command	Description
<code>platform:describe</code>	Shows the current platform configuration.
<code>platform:envlist</code>	Provides a list of environment variables.

### 4.3.1.3.4. Persistence Store Commands

Table 22. Persistence Store Command Descriptions

Command	Description
<code>store:delete</code>	Delete entries from the persistence store that match a given CQL statement
<code>store:list</code>	Lists entries that are stored in the persistence store.

#### 4.3.1.4. Command Scheduler

The Command Scheduler allows administrators to schedule Command Line Commands to be run at specified intervals.

The Command Scheduler allows administrators to schedule Command Line Shell Commands to be run in a platform-independent way. For instance, if an administrator wanted to use the Catalog commands to export all records of a Catalog to a directory, the administrator could write a cron job or a scheduled task to remote into the container and execute the command. Writing these types of scripts are specific to the administrator's operating system and also requires extra logic for error handling if the container is up. The administrator can also create a Command Schedule, which currently requires only two fields. The Command Scheduler only runs when the container is running, so there is no need to verify if the container is up. In addition, when the container is restarted, the commands are rescheduled and executed again. A command will be repeatedly executed indefinitely according to the configured interval until the container is shutdown or the Scheduled Command is deleted.

##### NOTE

There will be further attempts to execute the command according to the configured interval even if an attempt fails. See the log for details about failures.

##### 4.3.1.4.1. Schedule a Command

Configure the Command Scheduler to execute a command at specific intervals.

1. Navigate to the **Admin Console** (<https://{FQDN}:{PORT}/admin>).
2. Select the **Platform** application.
3. Click on the **Configuration** tab.
4. Select **Platform Command Scheduler**.
5. Enter the command or commands to be executed in the **Command** text field. Commands can be separated by a semicolon and will execute in order from left to right.
6. Enter an interval in the **Interval** field. This can either be a Quartz Cron expression or a positive integer (seconds) (e.x. `0 0 0 1/1 * ? * or 12`).
7. Select the interval type in the **Interval Type** drop-down.
8. Click the **Save changes** button.

##### NOTE

Scheduling commands will be delayed by 1 minute to allow time for bundles to load when DDF is starting up.

##### 4.3.1.4.2. Updating a Scheduled Command

Change the timing, order, or execution of scheduled commands.

1. Navigate to the **Admin Console**.
2. Click on the **Platform** application.

3. Click on the **Configuration** tab.
4. Under the **Platform Command Scheduler** configuration are all of the scheduled commands. Scheduled commands have the following syntax: `ddf.platform.scheduler.Command.{GUID}` such as `ddf.platform.scheduler.Command.4d60c917-003a-42e8-9367-1da0f822ca6e`.
5. Find the desired configuration to modify, and update fields.
6. Click the **Save changes** button.

#### 4.3.1.4.3. Output of Scheduled Commands

Commands that normally write out to the console will write out to the log. For example, if an `echo "Hello World"` command is set to run every five seconds, the log contains the following:

*Sample Command Output in the Log*

```
16:01:32,582 | INFO | heduler_Worker-1 | ddf.platform.scheduler.CommandJob | 68 |
platform-scheduler | Executing command [echo Hello World]
16:01:32,583 | INFO | heduler_Worker-1 | ddf.platform.scheduler.CommandJob | 70 |
platform-scheduler | Execution Output: Hello World
16:01:37,581 | INFO | heduler_Worker-4 | ddf.platform.scheduler.CommandJob | 68 |
platform-scheduler | Executing command [echo Hello World]
16:01:37,582 | INFO | heduler_Worker-4 | ddf.platform.scheduler.CommandJob | 70 |
platform-scheduler | Execution Output: Hello World
```

In short, administrators can view the status of a run within the log as long as INFO was set as the status level.

## 4.4. Monitoring

The DDF contains many tools to monitor system functionality, usage, and overall system health.

### 4.4.1. Metrics Reporting

Metrics are available in several formats and levels of detail.

Complete the following procedure now that several queries have been executed.

1. Select **Platform**
2. Select **Metrics** tab
3. For individual metrics, choose the format desired from the desired timeframe column:
  - a. PNG
  - b. CSV
  - c. XLS

4. For a detailed report of all metrics, at the bottom of the page are selectors to choose time frame and summary level. A report is generated in *xls* format.

### 4.4.2. Managing Logging

The DDF supports a dynamic and customizable logging system including log level, log format, log output destinations, roll over, etc.

#### 4.4.2.1. Configuring Logging

Edit the configuration file `<DDF_HOME>/etc/org.ops4j.pax.logging.cfg`

#### 4.4.2.2. DDF log file

The name and location of the log file can be changed with the following setting:

```
log4j.appender.out.file=<KARAF.DATA>/log/ddf.log
```

#### 4.4.2.3. Controlling log level

A useful way to debug and detect issues is to change the log level:

```
log4j.rootLogger=DEBUG, out, osgi:VmLogAppender
```

#### 4.4.2.4. Controlling the size of the log file

Set the maximum size of the log file before it is rolled over by editing the value of this setting:

```
log4j.appender.out.maxFileSize=20MB
```

#### 4.4.2.5. Number of backup log files to keep

Adjust the number of backup files to keep by editing the value of this setting:

```
log4j.appender.out.maxBackupIndex=10
```

#### 4.4.2.6. Enabling logging of inbound and outbound SOAP messages for the DDF SOAP endpoints

By default, the DDF start scripts include a system property enabling logging of inbound and outbound SOAP messages.


```
-Dcom.sun.xml.ws.transport.http.HttpAdapter.dump=true
```

In order to see the messages in the log, one must set the logging level for `org.apache.cxf.services` to `INFO`. By default, the logging level for `org.apache.cxf` is set to `WARN`.

```
ddf@local>log:set INFO org.apache.cxf.services
```

#### 4.4.2.7. Logging External Resources

Other appenders can be selected and configured.

For more detail on configuring the log file and what is logged to the console see: [Karaf Documentation: Log](#) .

#### 4.4.2.8. Enabling HTTP Access Logging

To enable access logs for the current DDF, do the following:

- Update the `jetty.xml` file located in `etc/` adding the following xml:

```
<Get name="handler">
  <Call name="addHandler">
    <Arg>
      <New class="org.eclipse.jetty.server.handler.RequestLogHandler">
        <Set name="requestLog">
          <New id="RequestLogImpl" class="org.eclipse.jetty.server.NCSARequestLog">
            <Arg><SystemProperty name="jetty.logs" default="data/log/"
          />yyyy_mm_dd.request.log</Arg>
            <Set name="retainDays">90</Set>
            <Set name="append">true</Set>
            <Set name="extended">false</Set>
            <Set name="LogTimeZone">GMT</Set>
          </New>
        </Set>
      </New>
    </Arg>
  </Call>
</Get>
```

Change the location of the logs to the desired location. In the settings above, location will default to `data/log` (same place where the log is located).

The log is using *National Center for Supercomputing Association Applications (NCSA)* or Common format (hence the class 'NCSARequestLog'). This is the most popular format for access logs and can be parsed by many web server analytics tools. Here is a sample output:

```
127.0.0.1 - - [14/Jan/2013:16:21:24 +0000] "GET /favicon.ico HTTP/1.1" 200 0
127.0.0.1 - - [14/Jan/2013:16:21:33 +0000] "GET /services/ HTTP/1.1" 200 0
127.0.0.1 - - [14/Jan/2013:16:21:33 +0000] "GET /services/?stylesheet=1 HTTP/1.1" 200
0
127.0.0.1 - - [14/Jan/2013:16:21:33 +0000] "GET /favicon.ico HTTP/1.1" 200 0
```

4.4.2.9. Using the LogViewer

Monitor system logs with the **LogViewer**, a convenient "viewing portal" for incoming logs.

- Navigate to the LogViewer at `https://{FQDN}:{PORT}/admin/logviewer`
- or

- Navigate to the Admin Console
- Navigate to the **System** tab
- Select **Logs**

The LogViewer displays the most recent 500 log messages by default, but will grow to a maximum of 5000 messages. To view incoming logs, select the **PAUSED** button to toggle it to **LIVE** mode. Switching this back to **PAUSED** will prevent any new logs from being displayed in the LogViewer. Note that this only affects the logs displayed by the LogViewer and does not affect the underlying log.

Log events can be filtered by:


- Log level (**ERROR**, **WARNING**, etc).
  - The LogViewer will display at the currently configured log level for the Karaf logs.
    - See [Controlling Log Level](#) to change log level.
- Log message text.
- Bundle generating the message.

WARNING	<p>It is not recommended to use the LogViewer if the system logger is set to a low reporting level such as <b>TRACE</b>. The volume of messages logged will exceed the polling rate, and incoming logs may be missed.</p> <p>The actual logs being polled by the LogViewer can still be accessed at <code>&lt;DDF_HOME&gt;/data/log</code></p>
NOTE	<p>The LogViewer settings don't change any of the underlying logging settings, only which messages are displayed. It does not affect the logs generated or events captured by the system logger.</p>

4.5. Troubleshooting

If, after configuration, a DDF is not performing as expected, consult this table of common fixes and workarounds.

Table 23. General Troubleshooting

Issue	Solution
Unable to unzip distribution on Windows platform	The default Windows zip utility is not compatible with the DDF distribution zip file. Use Java or a third-party zip utility.
Unable to federate on Windows Platform	Windows default firewall is not compatible with DDF.
Ingesting more than 200,000 data files stored NFS shares may cause Java Heap Space error (Linux-only issue).	<p>This is an NFS bug where it creates duplicate entries for some files when doing a file list. Depending on the OS, some Linux machines can handle the bug better and able get a list of files but get an incorrect number of files. Others would have a Java Heap Space error because there are too many file to list.</p> <p>As a workaround, ingest files in batches smaller than 200,000.</p>
Ingesting serialized data file with scientific notation in WKT string causes RuntimeException.	WKT string with scientific notation such as POINT (-34.8932113039107 -4.77974239601E-5) won't ingest. This occurs with serialized data format only.
<p>Exception Starting DDF (Windows)</p> <p>An exception is sometimes thrown starting DDF on a Windows machine (x86).</p> <p>If using an unsupported terminal,  <code>java.lang.NoClassDefFoundError: Could not initialize class org.fusesource.jansi.internal.Kernel32</code> is thrown.</p>	<p>Install missing Windows libraries.</p> <p>Some Windows platforms are missing libraries that are required by DDF. These libraries are provided by the <a href="#">Microsoft Visual C++ 2008 Redistributable Package x64</a> .</p>
<p>CXF BusException</p> <p>The following exception is thrown:  <code>org.apache.cxf.BusException: No conduit initiator</code></p>	<p>Restart DDF. . Shut down DDF:  <code>ddf@local&gt;shutdown</code> . Start up DDF: <code>./ddf</code></p>



Issue	Solution
<p>Distribution Will Not Start</p> <p>DDF will not start when calling the start script defined during installation.</p>	<p>Complete the following procedure.</p> <ol style="list-style-type: none"> <li>1. Verify that Java is correctly installed. <code>java -version</code></li> <li>2. This should return something similar to: <code>java version "1.8.0_45" Java™ SE Runtime Environment (build 1.8.0_45-b14) Java HotSpot™ Server VM (build 25.45-b02, mixed mode)</code></li> <li>3. If running *nix, verify that bash is installed. <code>echo \$SHELL</code></li> <li>4. This should return: <code>/bin/bash</code></li> </ol>
<p>Multiple <code>java.exe</code> processes running, indicating more than one DDF instance is running.</p> <p>This can be caused when another DDF is not properly shut down.</p>	<p>Perform one or all of the following recommended solutions, as necessary.</p> <ul style="list-style-type: none"> <li>• Wait for proper shutdown of DDF prior to starting a new instance.</li> <li>• Verify running <code>java.exe</code> are not DDF (e.g., kill/close if necessary).</li> <li>• Utilize automated start/stop scripts to run DDF as a service.</li> </ul>

#### 4.5.1. Deleted Records Are Being Displayed In The Search UI's Search Results

When queries are issued by the Search UI, the query results that are returned are also cached in an internal Solr database for faster retrieval when the same query may be issued in the future. As records are deleted from the catalog provider, this Solr cache is kept in sync by also deleting the same records from the cache if they exist.

Sometimes the cache may get out of sync with the catalog provider such that records that should have been deleted are not. When this occurs, users of the Search UI may see stale results since these records that should have been deleted are being returned from the cache. Records in the cache can be manually deleted using the URL commands listed below from a browser. In these command URLs, `metacard_cache` is the name of the Solr query cache.

- To delete all of the records in the Solr cache:

### *Deletion of all records in Solr query cache*

```
https://{FQDN}:{PORT}/solr/metacard_cache/update?stream.body=<delete><query>*:*/query></delete>&commit=true
```

- To delete a specific record in the Solr cache by ID (specified by the `original_id_txt` field):

### *Deletion of record in Solr query cache by ID*

```
https://{FQDN}:{PORT}/solr/metacard_cache/update?stream.body=<delete><query>original_id_txt:50ffd32b21254c8a90c15fccfb98f139</query></delete>&commit=true
```

- To delete record(s) in the Solr cache using a query on a field in the record(s) - in this example, the `title_txt` field is being used with wildcards to search for any records with word remote in the title:

### *Deletion of records in Solr query cache using search criteria*

```
https://{FQDN}:{PORT}/solr/metacard_cache/update?stream.body=<delete><query>title_txt:*remote*</query></delete>&commit=true
```

## 5. Data Management

### 5.1. Ingesting Data

Ingesting is the process of getting metacard(s) into the Catalog Framework. Ingested files are "transformed" into a neutral format that can be searched against as well as migrated to other formats and systems. There are multiple methods available for ingesting files into the DDF.

#### NOTE

##### *Guest Claims Attributes and Ingest*

Ensure that appropriate [Guest Claims](#) are configured to allow guest users to ingest data and query the catalog.

#### 5.1.1. Ingest Command

The Command Console has a command-line option for ingesting data.

#### NOTE

Ingesting with the console ingest command creates a metacard in the catalog, but does not copy the resource to the content store. The Ingest Command requires read access to the directory being ingested from, see the [URL Resource Reader](#) for configuring read permissions on the directory.

The syntax for the ingest command is

```
ingest -t <transformer type> <file path>
```

Select the **<transformer type>** based on the type of file(s) ingested. Metadata will be extracted if it exists in a format compatible with the transformer. The default transformer is the [XML input transformer](#), which supports the metadata schema **catalog:metacard**. To see a list of all transformers currently installed, and the file types supported by each, run the **catalog:transformers** command.

For more information on the schemas and file types(mime-types) supported by each transformer see the [Input Transformers](#).

The **<file path>** is relative to the **<DDF\_HOME>** directory. This can be the path to a file or a directory containing the desired files.

#### NOTE

*Windows Users*

On Windows, put the file path in quotes: **"path/to/file"**.

Successful command line ingest operations are accompanied with messaging indicating how many files were ingested and how long the operations took. The ingest command also prints which files could not be ingested with additional details recorded in the ingest log. The default location of the log is **<DDF\_HOME>/data/log/ingest\_error.log**.

### 5.1.2. User Interface Ingest

Files can also be ingested directly from Intrigue.

#### WARNING

The Intrigue uploader is intended for the upload of products (such as images or documents), not metadata files (such as Metacard XML). A user will not be able to specify which input transformer is used to ingest the document.

See [Ingesting from Intrigue](#) for details.

### 5.1.3. Content Directory Monitor Ingest

The Catalog application contains a Content Directory Monitor feature that allows files placed in a single directory to be monitored and ingested automatically. For more information about configuring a directory to be monitored, see [Configuring the Content Directory Monitor](#).

Files placed in the monitored directory will be ingested automatically. If a file cannot be ingested, they will be moved to an automatically-created directory named **.errors**. More information about the ingest operations can be found in the ingest log. The default location of the log is **<DDF\_HOME>/data/log/ingest\_error.log**. Optionally, ingested files can be automatically moved to a directory called **.ingested**.

### 5.1.4. External Methods of Ingesting Data

Third-party tools, such as [cURL.exe](#)  and the [Chrome Advanced Rest Client](#) , can be used to send

files to DDF for ingest.

#### *Windows Example*

```
curl -H "Content-type: application/json;id=geojson" -i -X POST -d  
@"C:\path\to\geojson_valid.json" https://{FQDN}:{PORT}/services/catalog
```

#### *\*NIX Example*

```
curl -H "Content-type: application/json;id=geojson" -i -X POST -d @geojson_valid.json  
https://{FQDN}:{PORT}/services/catalog
```

Where:

- H** adds an HTTP header. In this case, Content-type header `application/json;id=geojson` is added to match the data being sent in the request.
- i** requests that HTTP headers are displayed in the response.
- X** specifies the type of HTTP operation. For this example, it is necessary to POST (ingest) data to the server.
- d** specifies the data sent in the POST request. The `@` character is necessary to specify that the data is a file.

The last parameter is the URL of the server that will receive the data.

This should return a response similar to the following (the actual catalog ID in the id and Location URL fields will be different):

#### *Sample Response*

```
HTTP/1.1 201 Created  
Content-Length: 0  
Date: Mon, 22 Apr 2015 22:02:22 GMT  
id: 44dc84da101c4f9d9f751e38d9c4d97b  
Location: https://{FQDN}:{PORT}/services/catalog/44dc84da101c4f9d9f751e38d9c4d97b  
Server: Jetty(7.5.4.v20111024)
```

1. Use a web browser to verify a file was successfully ingested. Enter the URL returned in the response's HTTP header in a web browser. For instance in our example, it was `/services/catalog/44dc84da101c4f9d9f751e38d9c4d97b`. The browser will display the catalog entry as XML in the browser.
2. Verify the catalog entry exists by executing a query via the OpenSearch endpoint.
3. Enter the following URL in a browser `/services/catalog/query?q=ddf`. A single result, in Atom format, should be returned.

A resource can also be ingested with metacard metadata associated with it using the multipart/mixed

content type.

#### *Example*

```
curl -k -X POST -i -H "Content-Type: multipart/mixed" -F  
parse.resource=@/path/to/resource -F parse.metadata=@/path/to/metacard  
https://{FQDN}:{PORT}/services/catalog
```

More information about the ingest operations can be found in the ingest log. The default location of the log is `<DDF_HOME>/data/log/ingest_error.log`.

### 5.1.5. Other Methods of Ingesting Data

The DDF provides endpoints for both REST and SOAP services, allowing integration with other data systems and the ability to further automate ingesting data into the catalog. See [Available Endpoints](#) for more information.

## 5.2. Backing Up the Catalog

To backup local catalog records, a Catalog Backup Plugin is available. It is not installed by default for performance reasons.

See [Catalog Backup Plugin](#) for installation and configuration instructions).

## 5.3. Validating Data

DDF enables administrators to isolate metacards with data validation issues and to edit the metacard to correct validation errors. Additional attributes can be added to metacards as needed.

### 5.3.1. Validator Plugins on Ingest

On ingest, some validator plugins are run to ensure the data being ingested will be valid depending on whether **Enforce errors** is selected within the admin console. Below is a list of the validators run against the data ingested.

**NOTE**

To navigate to turn on/off **Enforce errors**:

1. Navigate to the **Admin Console**.
2. Select the **System** tab.
3. Select the **Configuration** tab.
4. Select **Metacard Validation Marker Plugin**.
  - a. If **Enforce errors** is checked, these validators below will be run on ingest.
  - b. If **Enforce errors** is not checked, these validators below will **not** be run on ingest.

#### 5.3.1.1. List of Validators run on ingest

- TDF Schema Validation Service
  - This service validates a TDO against a TDF schema.
- Size Validator
  - Validates the size of an attribute's value(s).
- Range Validator
  - Validates an attribute's value(s) against an **inclusive** numeric range.
- Enumeration Validator
  - Validates an attribute's value(s) against a set of acceptable values.
- Future Date Validator
  - Validates an attribute's value(s) against the current date and time, validating that they are in the future.
- Past Date Validator
  - Validates an attribute's value(s) against the current date and time, validating that they are in the past.
- ISO3 Country Code Validator
  - Validates an attribute's value(s) against the ISO\_3166-1 Alpha3 country codes.
- Pattern Evaluator
  - Validates an attribute's value(s) against a regular expression.
- Required Attributes Metacard Validator
  - Validates that a metacard contains certain attributes.
- Duplication Validator
  - Validates metacard against the local catalog for duplicates based on configurable attributes.
- Relationship Validator

- Validates values that an attribute **must have, can only have**, and/or **can't have**.
- Metacard WKT Validator
  - Validates a location metacard attribute (WKT string) against valid geometric shapes.

### 5.3.2. Viewing Invalid Metacards

To view invalid metacards, query for them through Intrigue. Viewing will require DDF-administrator privileges, if [Catalog Federation Strategy](#) is configured to filter invalid metacards.

1. Navigate to **Intrigue** (<https://{FQDN}:{PORT}/search>).
2. Select **Advanced Search**.
3. Change the search property to **metacard-tags**.
4. Change the value of the property to **invalid**.
5. Select **Search**.

### 5.3.3. Manually Editing Attributes

For small numbers of metacards, or for metacards ingested without overrides, attributes can be edited directly.

#### WARNING

Metacards retrieved from connected sources or from a fanout proxy will appear to be editable but are not truly local so changes will not be saved.

1. Navigate to **Intrigue**.
2. Search for the metacard(s) to be updated.
3. Select the metacards to be updated from the results list.
4. Select **Summary** or **Details**.
5. Select **Actions** from the **Details** view.
6. Select **Add**.
7. Select attribute from the list of available attributes.
8. Add any values desired for the attribute.

### 5.3.4. Injecting Attributes

To create a new attribute, it must be injected into the metacard before it is available to edit or override.

Injects are defined in a JSON-formatted file See [Developing Attribute Injects](#) for details on creating an attribute injection file.

### 5.3.5. Overriding Attributes

Automatically change the value of an existing attribute on ingest by setting an attribute override.

#### NOTE

Attribute overrides are available for the following ingest methods:

- Content Directory Monitor.
- Confluence source.

1. Navigate to the **Admin Console**.
2. Select the **Catalog** application.
3. Select **Configuration**.
4. Select the configuration for the desired ingest method.
  - a. **Catalog Content Directory Monitor**.
  - b. **Confluence Connected Source**.
  - c. **Confluence Federated Source**.
5. Select **Attribute Overrides**.
6. Enter the key-value pair for the attribute to override and the value(s) to set.

## 5.4. Removing Expired Records from the Catalog

DDF has many ways to remove expired records from the underlying Catalog data store. Nevertheless, the benefits of data standardization is that an attempt can be made to remove records without the need to know any vendor-specific information. Whether the data store is a search server, a No-SQL database, or a relational database, expired records can be removed universally using the Catalog API and the Catalog Commands.

## 5.5. Migrating Data

Data migration is the process of moving metacards from one catalog provider to another. It is also the process of translating metadata from one format to another. Data migration is necessary when a user decides to use metadata from one catalog provider in another catalog provider.

The process for changing catalog providers involves first exporting the metadata from the original catalog provider and ingesting it into another.

From the Command Console, use these commands to export data from the existing catalog and then import into the new one.

**catalog:export**

Exports Metacards and history from the current Catalog to an auto-generated file inside <DDF\_HOME>.



Use the `catalog:export --help` command to see all available options.

`catalog:import <FILE_NAME>`

Imports Metacards and history into the current Catalog.

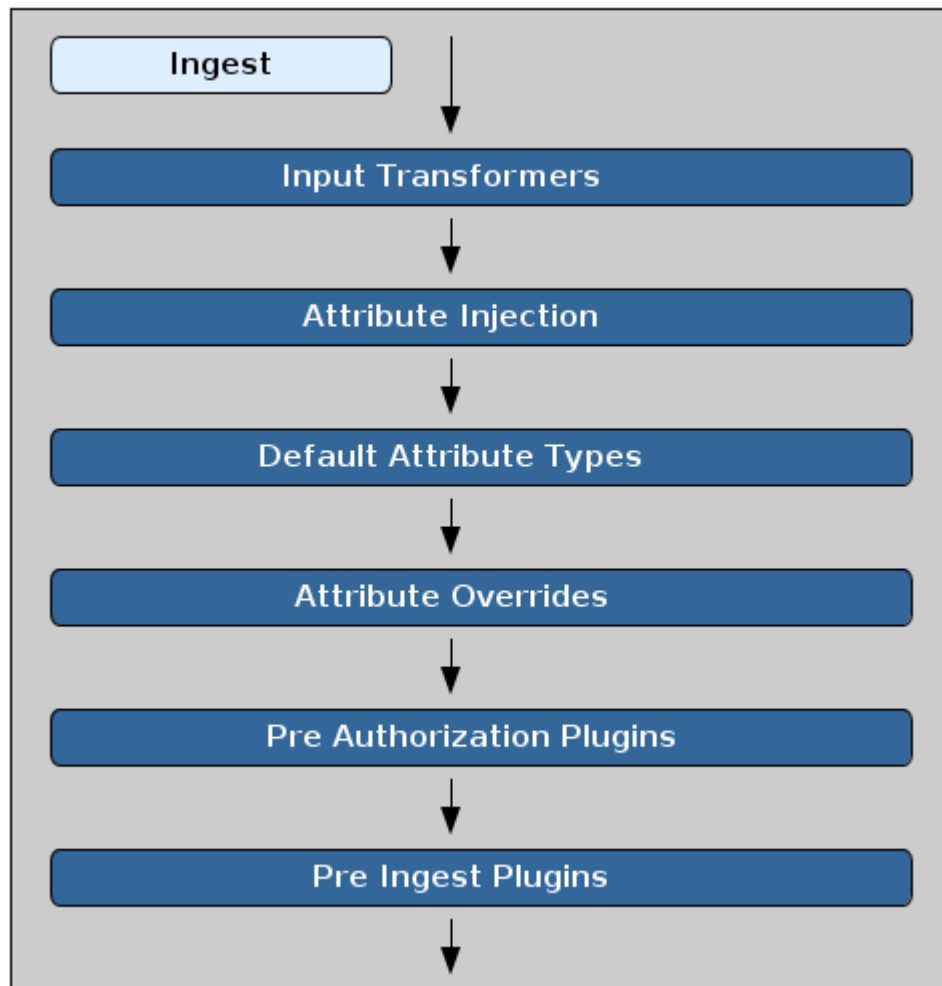
Use the `catalog:import --help` command to see all available options.

## 5.6. Automatically Added Metacard Attributes

This section describes how attributes are automatically added to metacards.

### 5.6.1. Attributes Added on Ingest

A metacard is first created and populated by parsing the ingested resource with an [Input Transformer](#). Then [Attributes Are Injected](#), [Default Attribute Types](#) are applied, and [Attribute are Overridden](#). Finally the metacard is passed through a series of [Pre-Authorization Plugins](#) and [Pre-Ingest Plugins](#).



*Ingest Attribute Flow*

#### 5.6.1.1. Attributes Added by Input Transformers

[Input Transformers](#) create and populate metacards by parsing a resource. See [File Format Specific Attributes](#) to see the attributes used for specific file formats.

DDF chooses which input transformer to use by:

1. Resolving the mimetype for the resource.
2. Gathering all of the input transformers associated with the resolved mimetype. See [Supported File Formats](#) for a list of supported mimetypes.
3. Iterating through the transformers until a successful transformation is performed.

The first transformer that can successfully create a metacard from the ingested resource is chosen. If no transformer can successfully transform the resource, the ingest process fails.

##### IMPORTANT

Each of the ingest methods have their own subtle differences when resolving the resource's mimetype/input transformer.  
For example: a resource ingested through Intrigue may not produce the same metacard attributes as the same resource ingested through the Content Directory Monitor.

#### 5.6.1.2. Attributes Added by Attribute Injection

[Attribute Injection](#) is the act of adding attributes to a metacard's [Metacard Type](#). A [Metacard Type](#) indicates the attributes available for a particular metacard, and is created at the same time as the metacard.

##### NOTE

Attribute values can only be set/modified if the attribute exists in the metacard's metacard type.  
Attributes are initially injected with blank values. However, if an attempt is made to inject an attribute that already exists, the attribute will retain the original value.

See [Catalog Taxonomy Definitions](#) for a list of attributes injected by default.

See [Developing Attribute Injections](#) to learn how to configure attribute injections.

#### 5.6.1.3. Attributes Added by Default Attribute Types

[Developing Default Attribute Types](#) is a configurable way to assign default values to a metacard's attributes.

Note that the attribute must be part of the metacard's [Metacard Type](#) before it can be assigned a default value.

See [Attributes Added By Attribute Injection](#) for more information about injecting attributes into the metacard type.

#### 5.6.1.4. Attributes Added by Attribute Overrides (Ingest)

[Attribute Overriding](#) is the act of replacing existing attribute values with a new value.

Attribute overrides can be configured for the [Content Directory Monitor](#).

Note that the attribute must be part of the metacard's [Metacard Type](#) before it can be overridden.

See [Attributes Added By Attribute Injection](#) for more information about injecting attributes into the metacard type.

#### 5.6.1.5. Attributes Added by Pre-Authorization Plugins

The [Pre-Authorization Plugins](#) provide an opportunity to take action before any security rules are applied.

- The [Metacard Ingest Network Plugin](#) is a configurable plugin that allows the conditional insertion of new attributes on metacards during ingest based on network information from the ingest request. See [Configuring the Metacard Ingest Network Plugin](#) for configuration details.

#### 5.6.1.6. Attributes Added by Pre-Ingest Plugins

The [Pre-Ingest Plugins](#) are responsible for setting attribute fields on metacards before they are stored in the catalog.

- The [Expiration Date Pre-Ingest Plugin](#) adds or updates expiration dates which can be used later for archiving old data.
- The [Geocoder Plugin](#) is responsible for populating the metacard's `Location.COUNTRY_CODE` attribute if the metacard has an associated location. If the metacard's country code is already populated, the plugin will not override it.
- The [Identification Plugin](#) assigns IDs to registry metacards and adds/updates IDs on create and update.
- The [Metacard Groomer](#) plugin adds/updates IDs and timestamps to the created metacard.

### 5.6.2. Attributes Added on Query

Metacards resulting from a query will undergo [Attribute Injection](#), then have their [Attributes Overridden](#).

#### 5.6.2.1. Attributes Added by Attribute Overrides (Query)

[Attribute Overriding](#) is the act of replacing existing attribute values with a new value.

Attribute overrides can be configured for query results from the following [Sources](#):

- [Federated Source For Atlassian Confluence](#).
- [CSW Specification Profile Federated Source](#).

- [GMD CSW Federated Source](#).

Note that the attribute must be part of the metacard's [Metacard Type](#) before it can be overridden. See [Attributes Added By Attribute Injection](#) for more information about injecting attributes into the metacard type.